

HP Systems Insight Manager 5.2 Technical Reference Guide

Printed in the US
HP Part Number: 356920-401
Published: February 2008
Edition: 5.2



Table of Contents

1	Legal notices.....	29
	Warranty.....	29
	Restricted rights legend.....	29
	Copyright notice.....	29
	Trademark notices.....	29
	Release history.....	29
2	Introduction.....	31
	Online help.....	31
	HP SIM help categories.....	31
3	Product overview.....	33
	Additional resources.....	33
	Features.....	33
	HP SIM management.....	33
	Security.....	34
	Installation.....	34
	Discovery.....	34
	Custom tools.....	34
	Reporting.....	34
	Partner applications.....	34
	What's new?.....	37
	Installation.....	37
	First Time Wizard.....	38
	Security.....	38
	Users and authorizations.....	38
	Discovery and identification.....	38
	Setting up managed systems.....	38
	Data Collection.....	38
	Automatic event handling.....	39
	License Manager.....	39
	Reporting.....	39
	Navigation.....	39
	Task Wizard.....	39
	Miscellaneous features.....	40
	Product architecture.....	40
	Central management server.....	40
	Managed systems.....	40
	System collections.....	40
	Web-browser clients.....	41
	Assistance.....	41
	Additional resources.....	41
	Technical support.....	41
	Technical FAQs.....	42
	Related topics.....	42
4	Getting started.....	43
	Product registration.....	43
	Signing in.....	44
	Signing in to the GUI.....	44
	Manually signing in to HP SIM.....	45
	Automatically signing in.....	45

Signing in using Secure Sockets Layer.....	46
Logging in to the CLI.....	47
Logging in to the CMS directly.....	47
Using an SSH client to log in remotely.....	47
Signing out	48
Signing out from the GUI	48
Logging out from the Command Line Interface.....	48
Using the First Time Wizard.....	48
Configuring the managed environment.....	49
Entering WBEM settings.....	50
Entering SNMP settings.....	51
Enabling automatic system discovery.....	52
Configuring managed systems.....	53
Configuring e-mail settings.....	54
First Time Wizard summary	54
Finishing the First Time Wizard	55
Operating-system-specific collections, reports, and tools	56
Operating-system-specific collections.....	56
Operating-system-specific reports.....	56
Operating-system-specific tools.....	57
Windows.....	57
Linux.....	57
HP-UX.....	57
Other.....	58
Setting up managed systems.....	58
Overview.....	58
Linux CMS.....	58
Setting up managed systems from a Linux CMS.....	58
Installing the ProLiant or Integrity Support Pack on a Linux system for the first time.....	58
Configuring the managed system software.....	59
Setting up Linux managed systems manually.....	59
Example: Setting up remote Linux systems from a Linux CMS.....	60
HP-UX CMS.....	61
Installing the required software on an HP-UX system.....	61
Configuring the managed system software.....	62
Setting up HP-UX managed systems manually.....	67
Example: Setting up remote HP-UX systems from an HP-UX CMS.....	69
Windows CMS.....	69
Setting up managed systems from a Windows CMS.....	69
Configuring the managed system software using the Configure or Repair Agents feature from the CMS.....	69
Example: Setting up Windows managed systems manually.....	76
Performing initial setup.....	76
Initial setup process.....	77
Navigating the Home page.....	78
Graphical user interface features.....	78
Customizing the Home page.....	79
Customizing the System Status panel.....	80
Enlarging the System Status panel.....	81
Utilizing RSS capabilities.....	82
Setting language locale.....	82
Setting the web browser language or locale.....	83
Configuring the language settings in Internet Explorer for Japanese.....	83
Configuring the language settings in Mozilla for Japanese.....	83
Configuring the language or locale settings in Windows.....	83
Configuring Windows XP language settings for Japanese.....	83
Configuring Windows 2000 locale settings for Japanese.....	84
Configuring HP-UX and Linux language settings.....	84
Configuring HP SIM.....	84

CMS locale.....	84
Target locale.....	84
Using command line interface commands.....	85
manpages.....	86
Commands.....	86
Entering commands.....	88
Permissions.....	88
Quotation marks.....	89
Resource library.....	89
5 Discovery and identification.....	93
Automatic discovery.....	93
Internet Protocol.....	93
Event-based automatic discovery.....	93
Discovery templates.....	94
First discovery.....	94
Subsequent discoveries.....	94
Manual discovery.....	95
Hosts files.....	95
Options for adding a single system.....	95
Configuring automatic discovery.....	97
Creating a new discovery task.....	98
Creating an automatic discovery task using the command line interface.....	99
Editing a discovery task.....	100
Disabling or enabling a discovery task.....	100
Deleting a discovery task.....	101
Running a discovery task.....	101
System types.....	102
System discovered by HP SIM.....	104
HP BladeSystem Integrated Manager systems discovered by HP SIM.....	104
Storage devices discovered by HP SIM.....	104
StorageWorks XP.....	104
StorageWorks VA.....	105
StorageWorks EVA.....	105
StorageWorks MSA.....	105
StorageWorks Tape Library.....	105
EMC Array.....	105
HDS Array.....	105
StorageWorks EVA.....	105
Network Appliance NAS.....	105
StorageWorks NAS.....	106
Fibre Channel.....	106
Obtaining, installing, and configuring providers and agents.....	106
Configuring management protocols.....	108
Sending test traps and indications.....	108
Configuring automatic discovery general settings.....	109
Discovery filters.....	111
Managing discovery templates.....	111
Creating a new discovery template file.....	112
Template file format.....	112
Editing a discovery template.....	113
Deleting a discovery template.....	113
Adding a system manually.....	114
Command line interface.....	116
Managing hosts files.....	116
Creating a new hosts file.....	117
Hosts file format.....	118
Editing a hosts file.....	118

Deleting a hosts file.....	119
Adding systems in a hosts file to the HP SIM database.....	119
Creating a task to import a hosts file for HP SIM integration.....	120
Importing the .dat file.....	120
Displaying the systems.....	120
Exporting Insight Manager (WIN32) files.....	120
Batch-adding systems using the CLI.....	121
Hosts file extensions.....	121
Default values.....	123
IP ranges.....	124
Identification.....	124
Initial identification.....	125
Identifying systems.....	126
Managing system types.....	126
Navigating the Manage System Types page.....	126
System type.....	127
Columns.....	127
Total.....	127
Available buttons.....	127
About System Type Manager.....	128
Why add or modify system identification?.....	128
Options for creating a System Type Manager rule.....	128
Creating STM rules.....	129
Command line interface.....	131
Editing STM rules.....	131
Deleting STM rules.....	132
Additional information for creating STM rules.....	132
Things you should know about DMI identification.....	132
Adding new DMI rules (from Windows CMS only).....	133
Adding new SNMP rules.....	133
6 Users and authorizations.....	135
Users authorization templates.....	136
Users and user groups.....	137
Creating new users.....	138
Command line interface.....	139
Creating new user groups.....	139
Command line interface.....	140
Editing user accounts and user groups.....	141
Command line interface.....	142
Deleting user accounts and user groups.....	142
Command line interface.....	143
User and user group reports.....	143
Command line interface.....	144
Default user templates.....	144
Toolboxes.....	145
Creating new toolboxes.....	145
Command line interface.....	146
Editing toolboxes.....	146
Command line interface.....	147
Deleting toolboxes.....	147
Command line interface.....	147
Toolbox report.....	148
Command line interface.....	148
Authorizations.....	148
Creating new authorizations.....	150
Command line interface.....	152
Updating authorizations.....	153

Command line interface.....	154
Deleting authorizations.....	154
Command line interface.....	154
Authorizations report.....	154
Command line interface.....	155
System groups.....	155
Managing system groups from the GUI.....	155
Managing system groups from the CLI using mxngroup.....	156
7 Directory Services.....	157
Configuring directory servers.....	157
Configuring directory groups.....	158
8 Networking and security.....	161
Secure Sockets Layer and certificates.....	161
Sign-in and accounts.....	161
Single Login, Replicate Agent Settings, and Install Software and Firmware.....	161
Certificates.....	162
About login.....	162
Single Login.....	162
Signing in.....	163
Sign in authentication on Linux and HP-UX.....	163
Configuring PAM on a Linux system.....	164
Configuring PAM on an HP-UX system.....	164
About secure task execution.....	164
Configuring the system link.....	165
Configuring sign-in events.....	166
Configuring browser timeout options.....	166
Changing the HP SIM default SSL port.....	167
Server certificates.....	167
Creating a server certificate.....	169
Editing a server certificate.....	170
Importing a server certificate.....	171
Exporting a server certificate.....	172
Creating a certificate signing request.....	173
Submitting a certificate signing request.....	173
Importing a CA-signed certificate.....	174
Synchronizing certificates.....	175
Replicating trusted certificates.....	175
Migrating trusted system certificates from the Source Central Management Server (CMS) to the target CMS.....	175
Migrating certificates when the source CMS has many trusted certificates.....	175
Migrating certificates when the source CMS has a lower number of trusted certificates.....	176
Using the Replicate Agent Settings feature.....	176
Possible certificate errors.....	177
Trusted certificates.....	177
Importing trusted certificates.....	178
Exporting trusted certificates.....	179
Exporting the system certificate from HP SIM.....	179
Exporting the system certificate from the browser (Microsoft Internet Explorer only).....	179
Deleting trusted certificates.....	180
Requiring trusted certificates.....	181
Setting up trust relationships.....	181
Configuration of the managed system.....	393
Importing the HP SIM certificate over the network.....	393
Importing the HP SIM certificate from a file.....	182
Setting up the managed server running Management HTTP Server.....	183
Importing the HP SIM certificate.....	183

Requesting the HP SIM certificate.....	183
Onboard Administrator configuration.....	183
HP StorageWorks Command View EVA configuration.....	183
HP SIM configuration.....	183
Suppressing browser warning messages.....	184

9 Monitoring systems, clusters, and events..... 187

About collections.....	187
Types of collections.....	187
Navigating the System and Event Collections panel.....	189
Tree controls and customization.....	190
Overviews.....	190
Systems.....	190
Events.....	190
Customizing system or cluster collections.....	191
Displaying collection type.....	191
Expanding or collapsing collections.....	192
Customize collections table.....	192
Available buttons.....	192
Creating system or cluster collections.....	192
Command line interface.....	194
Editing system or cluster collections.....	194
Command line interface.....	195
Saving collections.....	196
Moving system or cluster collections.....	197
Command line interface.....	197
Copying system or cluster collections.....	197
Command line interface.....	198
Deleting system or cluster collections.....	198
Command line interface.....	199
Setting properties for a system or cluster collection.....	199
Command line interface.....	199
Customizing event collections.....	200
Displaying collection type.....	200
Expanding or collapsing collections.....	200
Customize collections table.....	201
Available buttons.....	201
Command line interface.....	201
Creating event collections.....	202
Command line interface.....	203
Editing event collections.....	203
Command line interface.....	204
Moving event collections.....	205
Command line interface.....	205
Copying event collections.....	205
Command line interface.....	206
Deleting event collections.....	207
Command line interface.....	207
Setting properties for an event collection.....	207
Command line interface.....	207
System table view page.....	208
Navigating the system table view page.....	208
Tabs.....	209
Quick Launch.....	209
View as.....	210
System health status summary.....	210
Table information.....	210
System view columns.....	210

Selection.....	210
Health status.....	210
Management processor.....	211
Software status.....	211
HP Performance Management Pack.....	211
HP ProLiant Essentials Vulnerability and Patch Management Pack.....	211
HP ProLiant Essentials Virtual Machine Management Pack.....	212
Contract and Warranty status.....	212
Aggregate Event status.....	212
System Name.....	212
System Type.....	213
System Address.....	213
Product Name.....	213
Operating system name.....	213
System table view page buttons.....	214
Customizing the view.....	214
Navigating the tree view page.....	215
Tabs.....	215
View as.....	215
Quick Launch.....	215
Expanding the tree view.....	216
Tree view hierarchy.....	216
Selection in the tree view.....	216
Available drilldowns.....	216
Selection states for collections.....	217
Tree view buttons.....	217
Navigating the icon view page.....	218
Tabs.....	218
Quick Launch.....	218
View as.....	218
System health status summary.....	219
Icon view buttons.....	219
Navigating the picture view page.....	219
Rack view page.....	219
Enclosure view page.....	219
View as.....	220
Quick Launch.....	220
Creating and editing racks.....	220
Creating a rack.....	220
Editing a rack.....	222
About management processors.....	222
About racks and enclosures.....	223
Customizing the system table view page.....	224
Deleting systems from the HP SIM database.....	225
Printing a system collection view.....	225
System status types.....	226
WBEM operational status types.....	227
Software status types.....	228
Cluster table view page.....	229
Tabs.....	229
Navigating the Cluster Table View Page.....	229
Tabs.....	230
View as.....	230
Quick Launch.....	230
Cluster status summary.....	231
Cluster collection columns.....	231
Selection.....	231
CS.....	231
Cluster Name.....	231

Cluster Address.....	232
Cluster Type.....	232
Cluster Description.....	232
Buttons.....	232
Customizing the view.....	232
Customizing the cluster table view page.....	233
Deleting clusters from the database.....	233
Printing a cluster collection view.....	234
Event table view page.....	234
Navigating the event table view page.....	235
Tabs.....	236
Quick Launch.....	236
Filter criteria.....	236
Event status summary.....	237
Table information.....	237
Event collection columns.....	237
Selection.....	238
State.....	238
Severity.....	238
Event Type.....	238
System Name.....	238
Event Time.....	238
Assign To.....	238
Comments.....	238
System Type.....	239
Rack Name.....	239
Enclosure Name.....	239
Case Status.....	239
Case ID.....	239
Event management buttons.....	239
Customizing the view.....	240
Customizing the event table view page.....	240
Clearing events from the collection.....	241
Deleting events from the database.....	241
Assigning events to users.....	242
Entering comments on events.....	242
Printing an event collection view.....	243
Event severity types.....	243
Event details section.....	244
Event identification and details.....	244
Searching for systems and events.....	245
Tool search.....	246
Basic and advanced search.....	246
Basic search.....	246
Advanced search.....	247
Hierarchical displays.....	247
Save as.....	247
View.....	247
Performing a basic search.....	247
Performing an advanced search for systems.....	248
Printing system search results.....	249
Deleting system search results from a search view.....	250
Performing an advanced search for events.....	250
Printing event search results.....	251
Deleting event search results.....	251
Performing an advanced search for clusters.....	252
Printing cluster search results.....	253
Deleting cluster search results.....	253
Search criteria.....	253

Software and firmware criteria.....	256
Cleared state criterion.....	257
Server role criteria.....	257
Assignee criteria.....	257
Event type criteria.....	257
Memory range criteria.....	258
Reference.....	258
Default shared collections.....	258
Shared system collections.....	258
Shared event collections.....	262
Collection naming conventions.....	263
10 Storage integration.....	265
Storage integration using SMI-S.....	265
About storage systems.....	265
Introduction to SMI-S for HP Systems Insight Manager.....	265
About SMI-S.....	266
Key components.....	266
CIM.....	266
WBEM.....	266
SLP.....	266
Profiles.....	266
SMI-S implementation.....	266
Clients, servers, and providers.....	267
WBEM communication.....	267
Configuring HP SIM with storage systems.....	268
Configuring HP Systems Insight Manager with storage systems.....	268
Configure HP SIM to discover storage systems.....	268
Subscribe to WBEM indication events.....	268
Viewing storage systems.....	268
Viewing storage system collections.....	268
Viewing individual storage systems.....	269
Viewing storage system reports.....	269
Existing storage system reports.....	269
Custom reports.....	270
Viewing storage array capacity.....	270
Viewing storage capacity for all arrays.....	270
Viewing storage capacity for a single array.....	270
Changes to HP SIM storage functionality when HP Storage Essentials is installed.....	270
Storage integration using SNMP.....	272
Overview.....	272
Storage events.....	272
Storage inventory details.....	272
About storage discovery using SNMP.....	273
Discovery and identification.....	273
Discovering storage using SNMP.....	274
Using HP SIM with SNMP storage solutions.....	275
Viewing a storage event.....	275
Creating a storage by type group.....	275
Event collection and launch.....	275
11 Managing with tasks.....	277
About default system functions.....	277
Biweekly Data Collection.....	278
Daily Device Identification.....	278
Delete Events Older Than 90 Days.....	278
Hardware Status Polling for Non Servers.....	279
Hardware Status Polling for Servers.....	279

Hardware Status Polling for Systems No Longer Disabled.....	279
Initial Data Collection.....	279
Initial Hardware Status Polling.....	279
Software Version Status Polling.....	279
Software Version Status Polling for Systems no Longer Disabled.....	279
Bypassing target verification.....	279
Creating a task.....	280
Command line interface.....	282
Applying a time filter.....	283
Scheduling a task.....	283
Viewing all scheduled tasks.....	284
Running a scheduled task.....	284
Command-line interface.....	285
Editing a scheduled task.....	285
Deleting a scheduled task.....	286
Viewing task results.....	286
Viewing task instance results.....	286
Viewing target details.....	287
Related topics.....	287
Printing reports.....	287
Stopping a task.....	288
Deleting task results.....	288
Command line interface.....	289
Task status types.....	289
Task results list.....	289
Navigating the All Scheduled Tasks page.....	290
User privileges.....	291
Run now.....	291
Edit.....	291
Delete.....	291
Enable/Disable.....	291
View task results.....	291

12 Tools that extend management.....293

Quick Launch menu.....	295
Tool search.....	296
Searching for tools.....	297
Cluster Monitor.....	298
Configuring cluster resource settings.....	299
Configuring node resource settings.....	299
Cluster Monitor Cluster tab.....	300
Cluster Monitor Nodes tab.....	300
Cluster Monitor Network tab.....	300
Cluster Monitor Resources tab.....	301
MSCS status.....	302
Monitoring MSCS status.....	302
Cluster resources supported by HP SIM.....	302
Cluster Monitor states.....	302
Cluster Monitor resources and associated settings.....	303
Cluster Monitor polling rate.....	303
CPU polling rate.....	303
Disk polling rate.....	303
MSCS status polling rate.....	303
System status polling rate.....	304
Cluster Monitor resource thresholds.....	304
Disk capacity thresholds.....	304
CPU utilization thresholds.....	304
Command line tools.....	304

Command line interface.....	305
Configuring or repairing agents.....	305
Overview.....	305
Windows CMS.....	306
Configuring managed systems from a Windows Central Management Server.....	312
Related Topics.....	312
HP-UX and Linux CMS.....	312
Configuring managed systems from a HP-UX and Linux Central Management Server.....	312
Related Topics.....	317
Learn More - Installing the WBEM/WMI Provider for Windows.....	317
Learn More - Installing the SNMP Provider for Windows.....	318
Learn More - Installing OpenSSH from CRA.....	319
Learn More - Installing the Version Control Agent.....	319
HP Version Control Agent.....	320
HP Version Control Repository Manager.....	320
Learn More - Configuring WBEM/WMI.....	320
Learn More - Configuring a non-administrative account for HP SIM to access WMI data.....	321
Learn More - Configuring SNMP.....	321
Learn More - Configuring SSH.....	322
Learn More - Configuring VCA.....	322
Learn More - Setting the administrator password for Insight Management Agents.....	322
Custom tools.....	322
Menu placement.....	324
Creating a new remote tool.....	324
Creating a new CMS tool.....	326
Creating a new web page tool.....	328
Managing custom tools.....	329
New.....	330
Edit.....	330
View tool definition.....	330
Run Now/Schedule.....	330
Delete.....	330
Editing a remote tool.....	330
Editing a CMS tool.....	331
Editing a web page tool.....	332
Deleting a custom tool.....	333
Viewing tool definition files.....	334
Removing and restoring custom tools.....	334
Removing a tool.....	334
Restoring a tool.....	334
Environment variables for custom tools.....	334
Examples of using parameter strings in custom tools.....	336
Custom tools reference.....	337
Tool types.....	337
Parameterized strings.....	337
Parameterized strings substitution table.....	337
Tool filtering.....	339
Version numbers.....	341
Other requirements.....	341
Document type definition.....	342
Configuring DMI access.....	354
Configuring SNMP access.....	354
Device ping.....	355
Disk thresholds.....	355
Setting disk thresholds.....	355
Removing disk thresholds.....	355
Setting disk thresholds.....	356
Creating a task to delete disk thresholds on a monthly basis.....	356
Creating the task.....	356

License manager.....	357
About licenses.....	358
Collecting license information.....	359
Viewing licensed systems.....	361
Managing licenses.....	362
Adding licenses individually.....	364
Adding licenses from a file.....	365
Assigning and unassigning licenses.....	366
Assigning a license.....	367
Unassigning a license.....	367
System license information reporting.....	368
System license information reporting.....	368
Related procedures.....	369
Related topics.....	369
Licensing with ProLiant Essentials applications.....	369
Management processor tools.....	370
Controlling system power options through management processors.....	371
Controlling the system locator LED through management processors.....	371
Creating new users on management processors.....	372
Editing management processor users.....	372
Deleting management processor users.....	373
Configuring LAN access on management processors.....	374
Configuring LDAP settings on management processors.....	374
Executing internal control actions through management processors.....	375
Upgrading management processor firmware.....	375
Deploying SSH public keys to management processors.....	375
Cycling on the power on an HP ProLiant iLO.....	376
Powering on a system managed by an HP ProLiant iLO.....	376
Powering off a system managed by an HP ProLiant iLO.....	376
Turning on the UID for a system managed by an HP ProLiant iLO.....	377
Turning off the UID for a system managed by an HP ProLiant iLO.....	377
Managing Communications.....	377
.....	378
Communication status.....	378
Manage Communications table columns.....	378
Selection.....	378
System Name.....	378
Identification.....	379
Events.....	379
Run Tools.....	379
Version Control.....	379
System Type.....	379
OS Name.....	379
Manage Communications main page buttons.....	379
Advise and Repair.....	380
Quick Repair.....	380
Update.....	380
Print.....	380
Advising and repairing managed system settings.....	380
Identification tab.....	381
Events tab.....	381
Run Tools tab.....	382
Version Control tab.....	382
Repairing managed system settings.....	383
Updating communication statuses.....	385
Printing Manage Communications table.....	386
Firewall.....	386
Ports used by HP SIM which might need to be configured in a firewall.....	386
Configuring the firewall.....	387

Configuring the firewall on a Windows system.....	387
Configuring the firewall on an HP-UX system.....	387
Configuring the firewall on a Linux system.....	388
Installing and configuring protocols.....	389
Trusted certificates.....	391
Importing trusted certificates.....	392
.....	392
Setting trust relationships.....	393
Configuration of the managed system.....	393
Importing the HP SIM certificate over the network.....	393
Configuring WMI Mapper proxy.....	394
SNMP.....	394
Simple Network Management Protocol.....	394
Installing the SNMP agent.....	395
Configuring SNMP to send test traps.....	395
Web-Based Enterprise Management.....	397
Subscribing to WBEM indications.....	398
Subscribing to WBEM indications through the Configure or Repair Agents pages.....	398
Subscribing to WBEM indications through the Options menu.....	400
Secure Shell.....	401
WMI Mapper.....	401
Adding a WMI Mapper Proxy.....	401
Pinging managed systems.....	402
Installing the HP ProLiant Support Pack.....	402
System Type Manager rules.....	402
Installing and configuring version control.....	404
HP Version Control Agent.....	405
HP Version Control Repository Manager.....	405
Accessing VCRM from HP SIM	405
Accessing VCRM In-Place	405
Version control repository.....	405
Updating the repository:.....	406
Specifying a Version Control Repository in HP SIM.....	406
Managing MIBs.....	407
Viewing a MIB.....	407
Editing a MIB.....	408
Compiling a MIB.....	408
Registering a MIB.....	409
Registering a MIB in HP SIM.....	410
Updating a MIB.....	410
Service trap and service MIB information.....	410
Unregistering a MIB.....	411
Presentation of SNMP traps in HP SIM.....	411
Installing OpenSSH.....	412
Deploying OpenSSH to multiple systems using RDP.....	413
Installing OpenSSH Using RDP.....	413
Copying the public key from HP SIM to the target systems.....	413
Creating an OpenSSH task through the CLI.....	414
Creating an OpenSSH task.....	414
Creating an OpenSSH task from the command line with an XML file.....	415
Creating an OpenSSH task from the command line without an XML file.....	415
PMP tools.....	416
Replicate Agent Settings.....	417
Creating a Replicate Agent Settings task.....	418
Replicate Agent Settings - Reference.....	419
Determining a trust relationship.....	419
Changing a trust relationship.....	419
Wake on LAN feature.....	419
Replicate Agent Settings events.....	419

RPM Package Manager.....	419
Installing RPM.....	420
Uninstalling RPM.....	420
Querying RPM.....	420
Verifying RPM.....	421
Server Migration Pack.....	421
SMP Universal licensing.....	421
Accessing the Server Migration Pack.....	422
System Management Homepage.....	422
Accessing the System Management Homepage.....	422
System Page.....	423
System tab.....	423
System Status.....	424
More Information.....	425
Identification.....	425
Orphan systems.....	425
Firmware Revision.....	426
Product Description.....	426
HP Insight Power Manager.....	427
Contact Information.....	427
Entitlement Information.....	429
Asset Information.....	427
Management Processor.....	427
Host Server.....	427
Storage Server.....	428
Associations.....	428
System tab for management processors.....	428
System Status.....	428
Identification.....	429
Product Description.....	429
Entitlement Information.....	429
System tab for virtual machine hosts.....	430
System tab for virtual machine guests.....	432
Virtual machine controls - Launching the remote console.....	434
Virtual machine controls - Starting or resuming virtual machine guests.....	434
Virtual machine controls - Resetting or restarting virtual machine guests.....	435
Virtual machine controls - Suspending virtual machine guests.....	435
Virtual machine controls - Shutting down or stopping virtual machine guests.....	436
Virtual machine host performance.....	437
Virtual machine guest performance.....	438
System tab for clusters.....	440
Health Status.....	440
Identification.....	440
Product Description.....	440
System tab for a complex.....	441
Health Status.....	441
Product Description.....	441
Summary of Components.....	441
For a Complex Participating in iCOD:.....	441
For a Complex Not Participating in iCOD:.....	442
System tab for partitions.....	442
Identification.....	443
Product Description.....	443
Summary of Components.....	443
Associations.....	443
System tab for a storage host.....	443
Product Description.....	444
Host Bus Adapters.....	444
Properties.....	444

Ports.....	445
LUNs.....	445
System tab for a storage switch.....	445
Product Description.....	446
Ports.....	447
Status Summary.....	447
System tab for a storage array.....	447
Product Description.....	448
Ports.....	448
Port Details.....	449
Storage Volumes.....	449
Capacity Information.....	449
System tab for a tape library.....	450
Product Description.....	450
Ports.....	451
Media Access Devices.....	451
Changer Devices.....	452
Port types.....	452
Tools & Links tab.....	452
System Management Pages.....	453
System Web Application Pages.....	453
HP Systems Insight Manager Pages.....	453
Storage Essentials Pages.....	454
Essentials tab.....	454
Version Control.....	454
About the Version Control Agent.....	455
Additional resources.....	455
About the Version Control Repository Manager.....	456
Additional resources.....	456
About integration.....	457
About software repositories.....	457
About multiple system management.....	458
Accessing the Version Control Agent.....	458
Logging in to the VCA.....	459
Accessing the Version Control Repository Manager.....	459
Accessing VCRM from HP SIM.....	460
Accessing VCRM In-Place.....	460
Version Control status icons.....	460
Version Control status.....	460
HP Version Control Agent reports.....	461
Installing Software and Firmware.....	463
Firmware deployment to switches.....	464
Installing ROM firmware updates.....	465
Initial ProLiant Support Pack Install.....	466
WBEM-based tools	473
Property Pages.....	473
System Fault Management overview.....	474
WBEM providers overview.....	474
Available MSA tools.....	475
13 Partner applications.....	477
HP Integrity Essentials plug-ins.....	477
HP ProLiant Essentials plug-ins.....	478
HP Storage Essentials plug-ins.....	478
HP Infrastructure Resource Management plug-ins	479
HP Integrity Essentials overview.....	480
HP Integrity Essentials for HP-UX 11i.....	480
Software deployment.....	480

Configuration management.....	480
Workload management.....	481
Remote server management.....	481
HP Integrity Essentials for Windows.....	481
Deployment and configuration.....	481
Remote server management.....	481
HP Integrity servers with Linux.....	481
Central administration.....	481
HP Integrity Essentials for Linux.....	482
Deployment and configuration.....	482
Workload management.....	482
Remote server management.....	482
HP Integrity servers with OpenVMS.....	482
Central administration.....	482
HP Integrity Essentials for OpenVMS.....	482
Configuration management.....	482
Workload management.....	482
Remote server management.....	482
Event Monitoring Service overview.....	483
HP-UX Bastille overview.....	483
Features and benefits.....	483
GlancePlus overview.....	484
Ignite-UX overview.....	484
Integrated Lights-Out overview.....	484
Partition Manager overview.....	485
Security Patch Check overview.....	485
HP Serviceguard Manager overview.....	485
Software Distributor overview.....	486
Webmin overview.....	486
Workload Manager overview.....	487
HP OpenView Storage Data Protector overview.....	487
HP OpenView Performance Agent overview.....	488
HP Insight Power Manager overview.....	488
HP OpenView Storage Management Appliance overview.....	488
HP Process Resource Manager overview.....	489
Reasons to use PRM.....	489
Accessing Process Resource Manager from HP SIM.....	490
HP Virtual Server Environment overview.....	490
HP ProLiant Essentials applications.....	491
Monitor and Alert.....	491
Analyze and Control.....	491
Provision and Patch.....	491
Recovery and Scale.....	491
Remote Management.....	491
Enterprise Management.....	492
Other HP Management.....	492
Array Configuration Utility overview.....	492
HP BladeSystem overview.....	492
HP Client Manager overview.....	493
HP ProLiant Essentials Vulnerability and Patch Management Pack overview.....	493
Web JetAdmin overview.....	493
HP Storage Essentials overview.....	494
Storage device managers.....	494
HP StorageWorks Command View EVA overview.....	495
HP StorageWorks Command View SDM overview.....	495
HP StorageWorks Command View Tape Library overview.....	495
HP StorageWorks Command View XP overview.....	496
HP StorageWorks Command View XP Advanced Edition overview.....	496
HP StorageWorks 1000 Modular Smart Array overview.....	496

HP Service Essentials Remote Support Pack.....	496
Overview.....	496
Remote Support Software Manager.....	497
Remote Support tool.....	497
Remote Support Common Components.....	497
Open Service Event Manager.....	497
Using HP SIM with the Remote Support Pack.....	497
Viewing contract and warranty information.....	498
Introduction.....	498
Viewing contract and warranty information.....	498
Collecting contract and warranty data.....	499
Viewing contract and warranty status.....	500
Overview.....	500
System Information.....	500
Contract.....	500
Warranty.....	501
Contract and warranty status types.....	501
Suspending or resuming contract and warranty data collection for a single system.....	502
Suspending or resuming contract and warranty data collection for multiple systems.....	503
14 Reporting.....	505
HP Performance Management Pack reporting.....	505
System Information Reporting.....	505
Snapshot comparison.....	505
System reporting.....	506
Running an existing report in HTML format.....	506
Selecting the sort order.....	507
Viewing an existing report in XML format.....	507
Viewing an existing report in CSV format.....	507
Printing an existing report.....	507
Command line interface.....	507
Adding a report.....	507
Adding a new report.....	508
Selecting the sort order.....	510
Printing the report.....	510
Command line interface.....	510
Editing a report.....	510
Command line interface.....	511
Copying a report.....	511
Command line interface.....	512
Deleting a report.....	512
Showing SQL.....	512
Reporting views.....	513
Database views.....	513
R_ArrayControllers.....	513
R_Batteries.....	514
R_CellularSysCell.....	514
R_CellularSysParComplex.....	514
R_CellularSysPartition.....	515
R_CellularSysParIOChassis.....	515
R_ChangerDevices.....	515
R_CPU.....	515
R_deviceLicenseInfo.....	516
R_DIMMSlots.....	517
R_EventSummary.....	518
R_Fans.....	518
R_HPVMGuests.....	518
R_InstalledBoards.....	519

R_Inventory.....	519
R_lockdownStatus.....	520
R_LogicalDisks.....	520
R_MediaAccessDevices.....	520
R_NetworkInterface.....	521
R_OperatingSystem.....	521
R_PhysicalDisks.....	522
R_PowerSupply.....	522
R_Racks.....	523
R_Software.....	523
R_StorageDeviceInventory.....	523
R_StorageDeviceControllers.....	524
R_StorageHostBusAdapters.....	524
R_StoragePorts.....	525
R_StorageLogicalUnits.....	525
R_StorageDeviceCapacity.....	525
R_SWFWBaselineInformation.....	526
R_Process.....	526
R_UnixOSDetails.....	526
R_UnixLogicalMemory.....	527
R_UnixIODevices.....	527
R_WarrantyContract.....	528
R_UnixIPRoute.....	528
R_UnixSensors.....	528
R_HPUXFileSystem.....	528
R_HPUXVolumeGroup.....	529
R_HPUXLogicalVolume.....	529
R_HPUXPhysicalVolume.....	530
R_HPUXNetworkDetails.....	530
R_HPUXKernelParam.....	530
R_HPUXSoftwareBundle.....	530
R_HPUXSoftwareProduct.....	531
Snapshot comparison reporting.....	531
PMP reporting options.....	532

15 Administering systems and events.....535

Events.....	538
Example automatic event handling tasks.....	543
About administering events.....	540
Automatic event handling.....	540
Delete events.....	540
Event filter settings.....	541
Options for filtering events.....	541
SNMP trap settings.....	541
Status change event settings.....	541
Managing event handling tasks.....	542
Example automatic event handling tasks.....	543
Creating an automatic event handling task.....	544
Editing automatic event handling tasks.....	547
Copying automatic event handling tasks.....	548
Viewing task definitions.....	548
Viewing event task results.....	549
Enabling or disabling automatic event handling tasks.....	549
Configuring e-mail settings.....	550
Additional e-mail settings.....	550
EmailPrefixUserSubject.....	550
EmailKeywords.....	551
Configuring modem settings for paging.....	552

Clearing events.....	552
Deleting events	553
Configuring event filters for registered SNMP traps.....	553
Configuring SNMP traps.....	554
SNMP trap fields.....	554
Modifying traps.....	555
Configuring status change events.....	555
WBEM indications.....	556
Subscribing to WBEM indications.....	557
Unsubscribing to WBEM indications.....	557
Subscribing to health lifecycle events.....	558
Check event configuration.....	558
Examples of e-mail pages.....	559
Example of a standard e-mail page.....	559
Example of a Pager/SMS page.....	559
Example of an HTML page.....	560
Service notification events.....	560
Host configuration and setup.....	561
HP SIM handling of service event notifications.....	561
HP SIM Service Notification overview and setup information.....	561
Service trap notification details.....	562
OSEM port discovery.....	564
Examples of event tasks.....	564
Creating a paging task based on e-mail notification.....	564
Creating a task to delete all cleared events.....	565
Creating the event collection.....	566
Creating and scheduling the task.....	566
Creating a task to delete events older than 30 days.....	566
Creating the collection.....	566
Scheduling the task.....	567
Creating a task to send an e-mail when a system reaches a critical state.....	567
Creating the collection.....	567
Configuring HP SIM to send e-mail.....	568
Configuring status change events.....	568
Creating the task.....	568
Status polling.....	569
Software status polling.....	570
Hardware status polling.....	570
WMI Mapper Proxy.....	571
Adding a WMI Mapper Proxy.....	572
Editing a WMI Mapper Proxy.....	572
Deleting a WMI Mapper Proxy.....	573
Protocols.....	573
Setting global protocols.....	574
Setting protocols and credentials for a system or groups of systems.....	576
Setting protocols for a single system.....	577
Example XML file to add more than 10 WBEM username and password pairs.....	578
Global protocols.....	579
SNMP.....	579
DMI.....	580
HTTP.....	580
WBEM.....	581
Protocol functionality.....	581
Data collection.....	583
Append new data set (for historical trend analysis).....	584
Overwrite existing data set (for detailed analysis).....	584
Initial data collection.....	584
Bi-weekly data collection.....	584
Creating a data collection task.....	585

Command line interface.....	585
System properties.....	585
Editing system properties for a single system.....	586
Examples.....	586
System information.....	589
Contract and warranty information.....	590
Asset Information.....	590
Customer Company Information.....	591
Customer Contact.....	591
Reconfiguring system properties.....	592
Editing system properties for multiple systems.....	592
Suspending or resuming system monitoring for a single system.....	595
Suspending or resuming system monitoring for multiple systems.....	596
Version Control Repository.....	596
PMP administrative options.....	597
Managing SSH keys.....	597
Configuring SSH key security.....	598
Importing an SSH key.....	599
Exporting an SSH key.....	599
Deleting an SSH key.....	599
Configuring SSH bypass properties.....	600
Audit log.....	600
Configuring the HP SIM audit log.....	600
Configuring the tool definition files.....	601
Configuring the log.properties file.....	601
Viewing the Audit Log.....	601
Log content.....	601
Configuring the audit log file.....	602
Properties for globalsettings.props file.....	603

16 Troubleshooting.....611

Authentication.....	611
Automatic event handling.....	611
Blade.....	611
Browser.....	614
Certificates.....	618
CLI.....	619
CIMOM.....	620
Cluster.....	621
Collection.....	622
Configure or Repair Agents.....	623
Custom tools.....	624
Database.....	624
Discovery.....	624
Events.....	625
Event/SNMP trap.....	625
Firefox.....	625
Firmware upgrade.....	625
Generic.....	626
HP Service Essentials Remote Support Pack.....	626
HP SIM.....	626
HTTP event.....	628
Identification.....	628
Integrated Lights-Out (iLO).....	628
Internet Explorer.....	628
Installation.....	629
IP address.....	632
Logs.....	633

Menu.....	633
OpenSSH.....	633
Operating system.....	634
Paging notification.....	634
Passwords.....	634
Ping.....	635
Printing.....	635
Property pages.....	635
Protocol.....	636
Replicate Agent Settings.....	636
Response.....	636
Search.....	637
Security.....	637
Serviceguard Manager.....	638
Sign-in.....	639
SMI-S providers.....	644
SNMP Agent.....	647
Software status.....	647
Storage system.....	648
Switch.....	650
System.....	650
System Page.....	651
System properties.....	652
Task.....	652
Time zone.....	654
For Microsoft Windows CMS.....	654
For HP-UX or Linux CMS.....	654
Tools.....	654
VCRM.....	657
Virtual machine.....	658
Virtual Machine Management Pack.....	658
WBEM Indications.....	658
On the managed system:.....	658
On HP SIM:.....	658
Ensure that indications are generated by the managed system.....	659
Windows NT event log.....	660
WMIMapper.....	660

17 Reference information.....663

Predefined views.....	663
Database tables.....	663
AuthenticationMethods_values table.....	664
CIM_ActiveConnection table.....	665
CIM_Chassis table.....	665
CIM_ComponentCS table.....	666
CIM_ComputerSystemPackage table.....	666
CIM_ComputerSystem table.....	666
CIM_ControlledBy table.....	667
CIM_DeviceSAPImplementation table.....	667
CIM_DeviceSoftwareIdentity table.....	667
CIM_ElementCapabilities table.....	667
CIM_Fan table.....	667
CIM_HostedStoragePool table.....	668
CIM_IPProtocolEndpoint table.....	668
CIM_IPRoute table.....	669
CIM_iSCSICapabilities table.....	669
CIM_iSCSIConn_TCPProtoEnd table.....	670
CIM_iSCSIConnection table.....	670

CIM_iSCSI Session table.....	670
SCSIProtoEnd_iSCSI Session table.....	670
SCSIProtoEnd_NetworkPort table.....	670
CIM_LogicalDevice table.....	671
CIM_LogicalDisk table.....	671
CIM_LogicalPortGroup table.....	672
CIM_MediaAccessDevice table.....	672
CIM_NetworkAdapter table.....	673
CIM_MemberOfCollection table.....	675
CIM_NetworkPipeComposition table.....	675
CIM_NetworkPort table.....	675
CIM_OperatingSystem table.....	676
CIM_PhysicalElement table.....	678
CIM_PhysicalMedia table.....	679
CIM_PhysicalMemory table.....	680
CIM_PhysicalPackage table.....	681
CIM_PortController table.....	681
CIM_PowerSupply table.....	682
CIM_Process table.....	684
CIM_Processor table.....	685
CIM_Product table.....	687
CIM_RemoteServiceAccessPoint table.....	687
CIM_SCSIProtocolController table.....	687
CIM_SCSIProtocolEndpoint table.....	688
CIM_ProtoControlAccessesUnit table.....	688
CIM_ProtocolControllerForPort table.....	688
CIM_ProtocolControllerForUnit table.....	688
CIM_ProtocolEndpoint table.....	688
CIM_Rack table.....	689
CIM_Realizes table.....	689
CIM_Sensor table.....	689
CIM_SoftwareElement table.....	690
CIM_SoftwareIdentity table.....	691
CIM_StoragePool table.....	693
CIM_StorageVolume table.....	693
CIM_TCIPProtocolEndpoint table.....	694
Classifications_values table.....	694
ComputerSys_HAP table.....	694
ComputerSys_LogicalPortGroup table.....	695
ComputerSys_NetworkPort table.....	695
ComputerSys_PortController table.....	695
ComputerSys_SAP table.....	695
ComputerSys_SCSIProtoCont table.....	695
ComputerSys_SCSIProtoEndp table.....	695
ComputerSys_SoftwareIdent table.....	695
ComputerSys_StorageVol table.....	695
DB_DeviceInfo table.....	696
DB_DeviceInfoEx table.....	696
DC_Enclosure table.....	696
DC_ProliantHost table.....	697
Dedicated_values table.....	698
DeviceNames table.....	698
Device Extended Attributes database table.....	698
Devices table.....	699
DeviceProtocolInfo table.....	699
ExtentStatus_values table.....	700
DeviceSnmSettings table.....	700
HP_Cluster table.....	701
HP_Node table.....	701

HP_NParCabinet table.....	702
HP_NParCell table.....	702
HP_NParComplex table.....	703
HP_NParIOChassis table.....	704
HP_NParIOChassisSlot table.....	705
HP_NparPartition table.....	705
HPUX_BaseKernelParameter table.....	706
HPUX_Bundle table.....	706
HPUX_DNSService table.....	707
HPUX_Fileset table.....	708
HPUX_HFS table.....	710
HPUX_LogicalVolume table.....	711
HPUX_NISServerService table.....	712
HPUX_NTPTService table.....	712
HPUX_PhysicalVolume table.....	713
HPUX_Product table.....	713
HPUX_VolumeGroup table.....	715
HPVM_Guest table.....	716
HPVM_Host table.....	717
IPAddress table.....	717
IPProtocolEnd_NetworkPort table.....	717
IPXAddress table.....	717
OperationalStatus_SVvalues table.....	718
PhysicalPackage_Product table.....	718
SCSIProtoCont_SCSIProtoEnd table.....	718
SCSIProtocolCont_SoftwareId table.....	718
SCSIProtoEnd_SCSIProtoEnd table.....	718
NetworkAddresses_values table.....	718
NodeSnapshot table.....	719
NodeTypesEnum table.....	719
NodeSubTypesEnum table.....	719
Notices table.....	719
NoticeType table.....	720
OperationalStatus_CSvalues table.....	720
OperationalStatus_NPvalues table.....	721
operationalStatus_PCvalues table.....	721
Snapshot table.....	721
SPAllocatedFromStoragePool table.....	721
SVAllocatedFromStoragePool table.....	721
TCPPProtoEnd_IPProtoEnd table.....	721
Windows event log.....	722
Windows NT/2000 events.....	722
Windows NT/2000 event log error messages.....	722
Service and support.....	723
Service and support.....	723

glossary.....	725
---------------	-----

Index.....	739
------------	-----

List of Tables

4-1	Version Support Matrix for components used for install.....	71
12-1	Version Support Matrix for components used for install.....	307
12-2	Version Support Matrix for components used for install.....	384

1 Legal notices

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Warranty

A copy of the specific warranty terms applicable to your HP product and replacement parts can be obtained from your local Sales and Service Office.

Restricted rights legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this documentation and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and backup purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright notice

© Copyright 2003-2008 Hewlett-Packard Development Company, L.P.

Trademark notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95-branded products.

Intel, Celeron, Itanium, Pentium, and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a U.S. trademark of Sun Microsystems, Inc.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX is a registered trademark of The Open Group.

Release history

Edition 5.2, February 2008

To ensure that you receive the newest editions when they become available, subscribe to the appropriate product support service. See your HP sales representative for details.

2 Introduction

Online help

HP Systems Insight Manager (HP SIM) provides an online help system to help you become familiar with its management features. It provides general information about using and administering HP SIM. Click the question mark icon on any page or use the Help menu to view the online help.

HP SIM help categories

The HP SIM help system covers the following categories:

- **Product overview** Provides you with an overview of the features in HP SIM. See “Product overview” for more information.
- **Getting started** Describes procedures for how to begin using and administering HP SIM. See “Getting started” for more information.
- **Discovery and identification** Describes procedures for creating and managing discovery tasks, including identification, and managing hosts files, and discovery templates. See “Discovery and identification” for more information.
- **Users and authorizations** Describes procedures for creating and managing users, user groups, toolboxes, and authorizations. See “Users and authorizations” for more information.
- **Directory services** Describes procedures for configuring directory services and entering the distinguished name of container objects. See “Directory Services” for more information.
- **Networking and security** Describes procedures for networking and security, including setting up trust relationships. See “Networking and security” for more information.
- **Monitoring systems, clusters, and events** Describes procedures for monitoring systems and events. See “Monitoring systems, clusters, and events” for more information.
- **Storage integration** Describes procedures for discovering SNMP and Storage Management Interface - Specification (SMI-S) storage devices and viewing information about them. See “Storage integration using SNMP” and “Storage integration using SMI-S” for more information.
- **Managing with tasks** Describes procedures for managing systems and events by scheduling and executing tasks. See “Managing with tasks” for more information.
- **Tools that extend management** Describes procedures for using HP SIM default tools. See “Tools that extend management” for more information.
- **Partner applications** Describes partner applications and includes an overview of each application. See “Partner applications” for more information.
- **Reporting** Describes procedures for creating and generating custom reports. See “Reporting” for more information.
- **Administering systems and events** Describes how to manage and maintain HP SIM. See “Administering systems and events” for more information.
- **Troubleshooting** Describes troubleshooting procedures for HP SIM. See “Troubleshooting” for more information.
- **Reference** Includes database tables, Microsoft® Windows NT® error log messages, multiple-system aware (MSA) tools, and service and support information. See “Reference information” for more information.

3 Product overview

HP Systems Insight Manager (HP SIM) is the foundation for the HP unified server-storage management strategy. HP SIM is a hardware-level management product that supports multiple operating systems on HP ProLiant, Integrity and HP 9000 servers, HP StorageWorks MSA, EVA, XP arrays, and third-party arrays. Through a single management view of Microsoft® Windows®, HP-UX 11iv1, HP-UX 11iv2, HP-UX 11iv3, and Red Hat, and SuSE Linux, HP SIM provides the basic management features of system discovery and identification, single-event view, inventory data collection, and reporting. The core HP SIM software uses Web Based Enterprise Management (WBEM) to deliver the essential capabilities required to manage all HP server platforms.

HP SIM can be extended to provide systems management with plug-ins for HP clients, storage, power, and printer products. Plug-in applications for workload management, capacity management, virtual machine (VM) management, and partition management using HP Integrity Essentials enable you to choose the value-added software that delivers complete lifecycle management for your hardware assets.

Additional resources

For additional resources, go to the HP SIM website at <http://www.hp.com/go/hpsim>.

Related topics

- Features
- What's new?
- Product architecture
- Assistance
- Legal notices

Features

HP SIM management

- **Fault management and event handling** HP SIM provides proactive notification of actual or impending component failure alerts. Automatic Event Handling enables you to configure actions to notify appropriate users of failures through e-mail, pager, or Short Message Service (SMS) gateway, and enables automatic execution of scripts or event forwarding to enterprise platforms, such as [HP OpenView Network Node Manager](#) or [HP OpenView Operations](#).



NOTE: Pager support is only for Windows-based Central Management Server (CMS).

- **Consistent multisystem management** HP SIM initiates a task on multiple systems or nodes from a single command on the CMS. This functionality eliminates the need for tedious, one-at-a-time operations performed on each system.
- **Two user interfaces** HP SIM provides the option of a browser-based GUI or a command line interface (CLI) to make it easy to incorporate HP SIM into your existing management processes.
- **Web-Based Enterprise Management (WBEM) indications for HP-UX, Linux, and Storage Management Initiative Specification (SMI-S) devices** HP SIM enables you to use the GUI or CLI to subscribe and unsubscribe to WBEM indications.

Security

- **Role-based security** HP SIM enables effective delegation of management responsibilities by giving system administrators granular control over which users can perform specific management operations on specific systems.
- **Manage Secure Shell (SSH) keys** The **SSH Keys** feature enables you to view and manage, from the CMS, the public SSH keys stored in the `known_hosts` file. The SSH keys enable the CMS to authenticate a secure connection with a managed system.
- **Secure remote management** HP SIM leverages operating system security for user authentication and uses Secure Sockets Layer (SSL) and Secure Shell (SSH) to encrypt management communications.
- **Configure or Repair Agents** This feature enables you to repair credentials for SNMP settings, System Management Homepage, or Management HTTP Server trust relationships on Windows, Linux, and HP-UX systems supported by HP SIM. See “Configuring or repairing agents” for more information.

Installation

- **Easy and rapid installation.** HP SIM can be installed, quickly and easily, on HP-UX 11i v1, HP-UX 11i v2, or HP-UX 11i v3 on PA-RISC/Integrity server platforms, or on ProLiant platforms running Windows or Linux.
- **First Time Wizard** HP SIM provides you with step-by-step, online instructions for performing the initial configuration of HP SIM. The wizard helps you configure HP SIM settings on the Central Management Server (CMS).

Discovery

HP SIM can automatically discover and identify systems attached to the network. Discovery filters enable you to limit discovery to specific network segments or IP address ranges. Use discovery filters to prevent discovery of unwanted system types.

Custom tools

HP SIM defines tools using simple XML documents that enable you to integrate off-the-shelf or custom tools. These tools can be command line tools, web-based applications, or scripts. Access to these integrated tools is governed by role-based security.

Reporting

- **Data collection and inventory reports** HP SIM performs comprehensive system data collection and enables you to quickly produce detailed inventory reports for managed systems. Reports can be generated in HTML, XML, or CSV format. Data collection and reporting has been added for HP Superdome systems and other cellular complexes. Data that can be collected includes information on enclosures, cabinets, cells, memory, Integrity virtual machines, non-Integrity virtual machines, virtual partitions (vPars), and hard partitions (nPars). The type of data collected depends on what filters are selected, or what WBEM providers are installed.
- **Snapshot comparisons** HP SIM enables you to compare configuration snapshots of up to four different servers, or compare configuration snapshots of a single server over a period of time. This functionality assists IT staff in pinpointing configuration issues that can contribute to system instability. Snapshot comparisons can also be used to save a picture of a standard configuration for comparisons to other systems.

Partner applications

- **HP Version Control** HP SIM automatically downloads the latest BIOS, driver, and agent updates for HP ProLiant and HP Integrity servers running Windows and Linux, identifies systems running outdated

system software, and enables system software updates across groups of servers. For HP-UX systems, Software Distributor is integrated into HP SIM.

- **HP Service Essentials Remote Support Pack** HP SIM includes a new HP Service Essentials Remote Support Pack plug-in. This plug-in leverages elements of the HP Service Essentials Remote Support Pack (Remote Support Pack) technology and provides integrated HP SIM and Remote Support Pack capability. This capability deploys with your Windows-based Central Management Server (CMS) and includes the following:
 - Remote event monitoring to supplement the local monitoring of HP SIM
 - Real-time hardware event monitoring and secure event submission to HP Support to help identify and prevent potentially critical hardware problems
 - Faster restoration of your supported systems and devices to operational status
 - Less disruption to your company's revenue-generating activities and business productivity
 - The HP SIM single view of your data center is enhanced, with the addition of the following serviceability attributes
 - Contract and warranty details for your systems
 - Service event view, including remote support details such as HP case ID and service case status
 - CMS heartbeat polling, monitored by HP, allowing early notification to your IT team that event submission to HP is not working
- **Web-Based Enterprise Services and Open Service Event Manager** These analysis tools notify you when a significant system event will occur or has already occurred. Web-Based Enterprise Services (WEBES) System Event Analyzer (SEA) and Open Service Event Manager (OSEM) are used as part of the Remote Support Pack service offering and as standalone tools for HP Services customers. WEBES and OSEM generate service notifications to HP SIM through a specific SNMP trap type if analysis determines there are serviceable events. If the Remote Support Pack is installed, the service notification provided by WEBES and OSEM also provides status about the remote support incident.
- **System Management Homepage** The System Management Homepage provides a consolidated interface for single-system management. By aggregating the data from HP web-based agents and management utilities, the System Management Homepage provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server.
- **HP Performance Management Pack** HP SIM provides a software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers and HP StorageWorks Modular Smart Array (MSA) shared storage. The HP Performance Management Pack (PMP) tools that are available in HP SIM include Online Analysis, Offline Analysis, CSV File Generator Report, System Summary Report, Static Analysis Report, Configuration, Licensing, and Manual Log Purge. The PMP tools operate in conjunction with HP SIM. No software installation on the monitored servers is required, other than the Insight Management Agents. PMP 4.7 includes the following features:
 - Support for HP SIM 5.x (PMP 4.3 does not support HP SIM 4.x.)
 - Support for Oracle® databases (local or remote)

The following servers are supported on 4.3:

- ProLiant BL465c G1 servers
- ProLiant BL68c G1 servers
- ProLiant BL25p G2 servers
- ProLiant BL45p G2 VR1 servers
- ProLiant DL320 G5 servers
- ProLiant DL360 G5 servers
- ProLiant DL365 servers
- ProLiant DL585 G2 servers

- ProLiant ML310 G4 servers
- Integrity rx7620 servers
- Integrity rx7640 servers
- Integrity rx8620 servers
- Integrity rx8640 servers
- Integrity Superdome servers

Note: The Integrity Superdome includes support for the Intel Itanium 2 Montecito, M9M, and MX2 processors.

- Ultra 160 SCSI Adapter
- HP NC370i NIC
- rx8620 Gigabit LoM (5701) NIC
- rx8640 Gigabit LoM (5703) NIC
- LAN/SCSI Combo Card (Castor, AB290A)

The following new operating systems are supported on PMP 4.3:

- VMware ESX 2.5.2
- VMware ESX 2.5.3
- VMware ESX 2.5.4
- VMware ESX 3.0

Go to <http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/pmp/index.html> for more information about HP Performance Management Pack.

- **HP ProLiant Essentials Vulnerability and Patch Management Pack** HP ProLiant Essentials Vulnerability and Patch Management Pack identifies and provides advice to resolve security vulnerabilities. It delivers advanced patch management through automated acquisition, optimized deployment, and continuous enforcement of security patches. For more information about installation and setup, see the *HP ProLiant Essentials Vulnerability and Patch Management Pack Quick Setup Poster* and the *HP ProLiant Essentials Vulnerability and Patch Management Pack User Guide*, on the Management CD. For more information about the HP ProLiant Essentials Vulnerability and Patch Management Pack, go to the *HP ProLiant Essentials Vulnerability and Patch Management Pack* at <http://www.hp.com/servers/proliantessentials/vpm>.
- **HP ProLiant Essentials Virtual Machine Management Pack** Virtual machine management capabilities integrated into HP SIM extend its capabilities to deliver unified management of an IT infrastructure consisting of both physical and virtual server resources, and simplify and consolidate the provisioning, management, and migration of all server resources from one central interface.
The virtual machine management capabilities of HP SIM are enabled by the integration of the HP ProLiant Essentials Virtual Machine Management Pack and the HP Server Migration Pack - Universal Edition.
 - **HP ProLiant Essentials Virtual Machine Management Pack** The Virtual Machine Management Pack provides central management and control for the Microsoft's Virtual Server and the VMware's GSX Server or ESX Server virtual machines. Using the Virtual Machine Management Pack, all virtual machines and virtual machine (VM) hosts can be managed from the HP SIM console. The Virtual Machine Management Pack displays a tree view of the virtual machine hosts and virtual machine guests in the left pane of the HP SIM console. After selecting a system in the left pane tree, information for the system selected appears in the right pane. You can deploy, register, unregister, and upgrade the Virtual Machine Management Pack Agent. The Virtual Machine Management Pack is now integrated into HP SIM. See <http://www.hp.com/go/vmmanage> for documentation and more information about the Virtual Machine Management Pack.
 - **HP Server Migration Pack - Universal Edition** The HP Server Migration Pack - Universal Edition (SMP Universal) extends the functionality of the Virtual Machine Management Pack to provide integrated physical-to-virtual (P2V), virtual-to-virtual (V2V), virtual-to-ProLiant (V2P), and

physical-to-ProLiant (P2P) migrations. SMP Universal enables you to simplify the server consolidation process. To purchase additional licenses, see <http://www.hp.com/go/migrate>.

- **HP BladeSystem Integrated Manager in HP Systems Insight Manager** HP SIM delivers a blade environment designed to consolidate access to blade deployment, configuration, and monitoring tools. Picture views are available of racks and enclosures. The HP BladeSystem Integrated Manager is automatically installed with HP SIM. No license key is required. To access HP BladeSystem Integrated Manager, select **Tools**→**Integrated Consoles**→**HP BladeSystem**. See <http://h18004.www1.hp.com/products/servers/Integrity-bl/p-class/60p/index.html> for more information.
- **HP ProLiant Essentials Rapid Deployment Pack** The HP ProLiant Essentials Rapid Deployment Pack (RDP) is a multiserver deployment tool that enables IT administrators to easily deploy large numbers of servers in an unattended, automated fashion. The RDP is installed separately from HP SIM. It requires a license for each server managed. You must register your RDP product to purchase licenses or obtain a 10-node 30-day license before installing RDP (a 10-node 7-day evaluation license is built into the software). The RDP is installed from its own DVD. See <http://www.hp.com/servers/rdp> for information about RDP including a link to obtain evaluation licenses or register your product. See the RDP documentation for network environment setup, prerequisites for the deployment server, and installation instructions.
- **HP Storage Essentials** HP is changing the economics of managing the data center. HP Storage Essentials is the first open, standards-based suite of storage products designed to integrate into HP SIM. See <http://h18006.www1.hp.com/products/storage/software/esuite/index.html> for more information about HP Storage Essentials.
- **HP Insight Power Manager** HP Insight Power Manager (IPM) is an integrated power-monitoring and management application that provides centralized control of server power consumption and thermal output at the datacenter level. It extends the capacity of datacenters by enabling the user to control the amount of power and cooling required for ProLiant servers. Built on ProLiant Power Regulator technology, extends new server energy instrumentation levers into HP SIM for greater Unified Infrastructure Management.
- **Support for HP-UX Serviceguard clusters** HP SIM recognizes HP-UX Serviceguard clusters and displays them in the GUI. HP Serviceguard Manager opens when you click a Serviceguard cluster in a search list and provides information on the clusters.

Related topics

- [What's new?](#)
- [Product architecture](#)
- [Assistance](#)
- [Legal notices](#)
- [Getting started](#)

What's new?

Installation

- Replaced MSDE in HP SIM Windows installation with SQL 2005 Express Edition with Service Pack 2.
- Added Central Management Server (CMS) and managed system support for Windows Server 2008 and Windows Vista.
- Streamlined installation by removing HP ProLiant Essentials Vulnerability and Patch Management Pack and HP Performance Management Pack from the default installation set
- Added support for silent installation for Oracle database
- Added Central Management Server (CMS) and managed system support for Red Hat Enterprise Linux 5 for x86 with Update 1 and SUSE Linux Enterprise Server 10 for x86 with Service Pack 1

- Automatic installation of HP SIM is now supported for x64 bit operating systems
- Replaced Postgres SQL with HPSMDB

First Time Wizard

- Streamlined the application by enabling you to specify the operating systems that are managed in your environment, resulting in collections, reports, and tools for the selected operating systems only.
- Ability to automatically configure managed systems as discovery runs.
- Ability to test email configurations as e-mail settings are configured.

Security

Multiple names in SSL web server certificate to alleviate name mismatch errors by the browser when using different names for the system.

Users and authorizations

HP SIM allows for any user to be configured to have access to features like discovery, view audit logs, automatic event handling and more. In addition, there is a single setting to enable users to add or update security settings on HP SIM.

Discovery and identification

- Simple or Fully Qualified Domain Names (FQDN) host names can be included in ping inclusion and exclusion ranges for discovery.
- Discovering and identifying the HP Insight Management WBEM Providers for Windows Server 2003/2008 for getting a rich set of hardware information for HP ProLiant hardware.
- Ability to discover all nPars in a complex, including those not currently active, from information gathered in one nPar.
- Ability to discover all vPars in a vparmonitor, including those not currently active, from information gathered in one vPar.

Setting up managed systems

HP SIM features have been enhanced to make setting up managed systems an easier task.

- The Configure or Repair Agents feature now includes the following enhancements:
 - HP Insight Management Agents can be installed on ProLiant servers running Windows using the Initial HP ProLiant Support Pack task from a Windows Central Management Server (CMS).
 - SNMP traps can be sent from the managed systems to check the trap reception in HP SIM CMS.
 - WBEM indications can be sent from the managed systems that support WBEM providers and verifies reception in the HP SIM CMS running HP-UX.
 - Configure Single Sign on to managed systems.
 - Can install and configure HP Version Control Agent and Secure Shell (SSH) from Configure or Repair Agents.
 - Can install and configure WBEM providers from Configure or Repair Agents.
- The new Manage Communications feature enables you to troubleshoot communication problems between the CMS and the managed systems.

Data Collection

- You can now collect and display instant capacity (iCAP) properties for Cells and Processors, for an iCAP enabled Complex, using Web based enterprise management (WBEM) protocol.
- On ISS HP Insight Management WBEM Providers for Windows Server 2003/2008 enabled managed nodes, data collection will give preference to HP Insight Management WBEM Providers for Windows Server 2003/2008 over WMI/SNMP for certain attributes.



NOTE: Currently, there is limited SNMP support in HP Insight Management WBEM Providers for Windows Server 2003/2008. When data collection prefers over to HP Insight Management WBEM Providers for Windows Server 2003/2008, a few of the items in the report that were collected from SNMP earlier would be blank.

NOTE: The iCAP provider is available on HP-UX 11i v3 (11.31), HP-UX 11i v2 (11.23) and HP-UX 11i v1 (11.11) which can only be installed on HP 9000 and Integrity servers.

- Added Horizontal discovery of node partitions (nPars) for cell-based Integrity servers or HP 9000 servers.
- Added Horizontal discovery of virtual partitions (vPars) for cell-based HP-UX 9000 servers or procedure-based HP-UX 9000 servers.
- Added Data collection of software/firmware (sw/fw) baseline name and version for systems that have a Version Control Agent (VCA) installed.

Automatic event handling

- Support for new ProLiant WBEM indications Therefore, any event collection containing event type criteria having an SNMP trap that correlates to a WBEM indication will be upgraded and the WBEM indications will be selected.
- User pager information can be specified when creating or managing automatic event handling tasks.

License Manager

- Extended support for SSH and CLP to include iLO 2 specific extensions.
- Added license transfer with iLO 2 using the License Manager menu functions in the Graphical User Interface (GUI).
- Added a Graphical User Interface (GUI) for input of SSH credentials.

Reporting

- New HP Version Control Agent report that displays baseline information.
- Added data collection of software/firmware (sw/fw) baseline name and version for systems that have a Version Control Agent (VCA) installed.

Navigation

- The tool search feature provides a quick way to find a tool by entering text (often less than a single word) that is used to search and filter, textually, based on tool names, tool locations in the HP SIM cascading menu structure, and tool descriptions.
- The **Quick Launch** menu provides single click access to frequently used tools and can be customized to select which tools are displayed in the menu.
- **Go back to** link that returns you to the last viewed collection or tool, including the **System Page**.
- You can maximize the workspace so that the **System Status overview**, **Search**, **System and Event Collections** panels, and the HP SIM menus are collapsed, and the banner is minimized. You can also restore the workspace to the default size with a single click.

Task Wizard

- Improved performance.
- Added ability to select target systems using a search tool.

Miscellaneous features

- You can search software and firmware installed on HP-UX systems.
- Property pages are implemented for HP Insight Management WBEM Providers for Windows Server 2003/2008 and for OpenVMS providers. HP-UX Property pages have been updated to reflect new HP-UX providers.
- Support on **Property** pages for HP-UX 11i.x, Linux Itanium Processor Family (IPF), Windows Server 2003 and 2008, Windows XP, Windows Vista, Windows Longhorn, and OpenVMS.

Related topics

- Tool search
- Quick Launch menu
- Discovery and identification
- Assistance
- Features

Product architecture

HP Systems Insight Manager (HP SIM) leverages a distributed architecture that is divided into three types of systems: *Central Management Server* (CMS), *managed systems*, and web-browser clients.

The CMS with the managed systems together are called the *HP SIM management domain*.

Central management server

Each management domain has a single CMS. The CMS is the *system* in the management domain that executes the HP SIM software and initiates all central operations within the domain. In addition to the HP SIM software, the CMS maintains a *database* for storage of persistent objects that can reside locally or on a separate system. Typically, applications for the *multiple-system aware* (MSA) tools also reside on the CMS. However, these applications are not required to reside on the CMS. They can reside anywhere on the network.

Because the CMS is a system within the management environment, it manages itself as part of the domain. You can add the CMS as a managed system within another management domain if you want to manage the domain using a separate CMS.

Managed systems

Systems that comprise a management domain are called *managed systems*. A system can be any device on the network that can communicate with HP SIM, including servers, desktops, laptops, printers, workstations, hubs, *storage systems*, storage area networks (SANs), and routers. In most cases, these devices have an IP address associated with them. A managed system can be managed by more than one CMS, if desired.

Managed systems to be managed must have one or more *management agents* installed. There is a wide variety of agents, such as the ProLiant Insight Management Agents based on *SNMP*, or the *Windows Management Instrumentation* (WMI) for Windows systems, or *Web-Based Enterprise Management* (WBEM) providers, and System Fault Management providers for HP-UX. These agents provide management information and alerts (indications) to the CMS. The *SSH* agent (service) then enables the HP SIM CMS to log into the managed system to execute commands through scripts.

System collections

System collections provide a way to group systems in the HP SIM database. A collection can be used to filter systems that share common attributes, such as operating system or hardware type. System collections can also be arbitrary collections of systems. Systems can belong to one or more system collections. Many default shared system collections are provided, and you can create your own shared and private collections. Using system collections, you can, in a single step, perform a task on every system in a system collection. See "Shared system collections" for a complete list of all shared system collections.

Web-browser clients

HP SIM can be accessed from any supported browser client. The network client can be part of the management domain. However, you must be running a compatible browser to access the *GUI* or an *SSH* client application to securely access the *CLI*. Access to the web server on the CMS can be restricted to specific IP address ranges for specific users.

Related topics

- Features
- What's new?
- Assistance
- Legal notices
- Getting started

Assistance

Additional resources

For additional HP Systems Insight Manager (HP SIM) resources, see:

- HP SIM website at <http://www.hp.com/go/hpsim/> for general product information and links to software downloads, documentation, and troubleshooting information
- HP Technical Documentation website at <http://www.docs.hp.com/> for access to HP SIM manuals and release notes
- HP Software Depot website at <http://www.software.hp.com/> for access to HP SIM software downloads
- HP Business Support Center website at <http://www.hp.com/bizsupport/> for support information about HP SIM and HP Commercial products
- HP IT Resource Center website at <http://www.itrc.hp.com> for support information about HP SIM and HP Enterprise products
- HP SIM SMI-S Providers website at <http://www.hp.com/go/hpsim/providers> for information about device support and SMI-S providers
- Videos that showcase HP SIM and the Essentials at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>
- HP SIM forum at <http://forums1.itrc.hp.com/service/forums/categoryhome.do?categoryId=455> for discussions about HP SIM
- HP SIM tools and scripts forum at <http://forums1.itrc.hp.com/service/forums/categoryhome.do?categoryId=495> for contributing scripts to be used with HP SIM (these scripts are *not* supported by HP)

Technical support

Support for HP SIM is available through HP local Response Centers or through HP Technology Services:

- **HP Response Center for HP SIM on HP-UX**
1-800 HP Invent (1-800-474-6836) for North America, or contact your local HP Response Center
- **Technology Services for HP SIM on Windows or Linux**
First 90 days: HP provides warranty support for HP SIM for the first 90 days after installation
 - North America: **1-800 HP Invent** (1-800-474-6836)
 - Other countries: [Support phone numbers all other countries](#)

After 90 days: There are two support options following the first 90 days after installation

- Windows customers who have a Microsoft Operating System contract are entitled to support under the current Operating Environment. Call 1-800-633-3600 number for support.
- Linux customers or Windows customers who do not have a Microsoft Operating System contract can purchase support for the ProLiant Essentials products, including HP SIM, with Incident Packs. The Incident Packs can be purchased in three (3) call quantities both for 24x7 and 9x5 call windows. The part numbers are for Incident Packs are U8301E (24x7) and U8222E (9x5).

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Error messages
- Operating system type and revision level
- Detailed questions



NOTE: For continuous quality improvement, calls may be recorded or monitored.

Technical FAQs

<http://h18013.www1.hp.com/products/servers/management/hpsim/techsupport.html>

Related topics

- Resource library
- Features
- What's new?
- Product architecture
- Legal notices
- Getting started

4 Getting started

If you are getting started with HP Systems Insight Manager (HP SIM), you must first familiarize yourself with the software and set it up for your environment by reviewing the information in the “Product overview” section. Then, complete the following steps:

- Sign-in to the *GUI*. See “Signing in” for details.
- Familiarize yourself with the HP SIM **Home** page. See “Navigating the Home page” for details.
- If this is a new installation, perform the initial setup.

The First Time Wizard starts the first time an *administrative rights* signs in to HP SIM. The wizard provides step-by-step instructions for performing the initial configuration of HP SIM. Additional configuration options are available through the HP SIM GUI. See “Using the First Time Wizard” and “Performing initial setup” for details. Only users with administrative rights can configure HP SIM.

- Familiarize yourself with how to schedule and execute tasks. See “Managing with tasks” for details.
- Familiarize yourself with the HP SIM reporting features. See “Reporting” for details.
- If you intend to use the *command line interface* (CLI), review the HP SIM commands. See “Using command line interface commands” and the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for details.
- Customize the **Home** page and the **System Status** panel. See “Customizing the Home page” and “Customizing the System Status panel” for details.

Related procedures

- Signing in
- Signing out
- Product registration
- Navigating the Home page
- Performing initial setup
- Using command line interface commands
- Customizing the Home page
- Customizing the System Status panel

Related topics

- Product overview
- Monitoring systems, clusters, and events
- Managing with tasks
- Administering systems and events

Product registration

HP Systems Insight Manager (HP SIM) provides an option to register your HP SIM software with HP. Registration includes the following benefits:

- Notification of software updates
- Product support alerts
- Optional newsletters containing tips and tricks for using HP SIM



NOTE: You must be connected to the Internet to register HP SIM.

1. The **Registration** window appears automatically during installation on Windows systems, and when you sign-in to HP SIM if you have not already registered. If the **Registration** window is not already open, select **Options**→**Registration**.
2. Click **Register Now**. The **HP Systems Insight Manager License** page appears.
3. Click **Receive for free**. The **HP Systems Insight Manager Registration** page appears.
4. Enter the requested information. Items marked with an asterisk are required. You must read and accept the warranty and license terms before you can continue.
5. Click **next**. The receipt page appears.
6. Click the **HP SIM License Key** link in the **Download Software** column. An Adobe Reader file opens and displays the HP SIM license key information.

Note: You will also receive this file in an e-mail to the address you entered during the registration process. You must have Adobe Reader installed to view the license key file.

7. Click the icon for the Adobe Reader **Select** tool:



8. Select and copy the **License Key** number.
9. In the **Registration** window, position the cursor in any of the five fields forming the input box, and press the **Ctrl + V** keys to paste the license key. You can also right-click to paste. The license key is displayed with five characters in each of the five fields.
10. Click **Submit**. HP SIM notifies you that the license key has been added successfully. Close the **Registration** window.

Signing in

Access the *GUI* using a web browser or the *command line interface* (CLI) using a *Secure Shell* (SSH) client.

When you first sign-in to HP Systems Insight Manager (HP SIM), the **First Time Wizard** window appears. The First Time Wizard provides information and procedures for getting started with HP SIM. Click **Close** to exit the window. If you do not want this window to appear each time you sign-in to HP SIM, select **Do not automatically show this wizard again**, and then click **Close**. See the “Using the First Time Wizard” for more information.

Signing in to the GUI

You can access the HP SIM GUI from any network client using a web browser. For information about which browsers are supported, see the HP SIM installation guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>, and then select the appropriate guide for your operating system.



NOTE: After accessing HP SIM, if you open additional windows in the same browser using the same HP SIM URL, you do not need to sign back in to HP SIM. Any time you start a new instance of the browser and navigate to HP SIM, you must sign-in.

If you sign-in to HP SIM and then navigate to a different site entirely, the HP SIM session times out. If you use the same browser process to return to HP SIM within 20 minutes, you are not required to sign back in.

Manually signing in to HP SIM

There are several reasons to manually sign-in to HP SIM

- **If automatic sign-in fails, the sign-in page is displayed** This might occur if the user is logged in to the operating system using an account that is not an HP SIM account.
- **If automatic sign-in is not attempted** This might occur if the browser is not properly configured for automatic sign-in, or the feature is disabled in HP SIM.
- **If you click Sign Out from HP SIM** This enables the user to specify another user account to use if they are logged in to the operating system with a different account.

To manually sign-in to HP SIM

1. Open a supported web browser on any network client, and enter the address for the sign-in page by navigating to `http://hostname:280/`, where *hostname* is the host name of the CMS.
Note: If you are signing in directly on a Windows CMS, you can use the **HP SIM** desktop icon to access the sign-in page, or you can select **Start**→**Programs**→**HP Systems Insight Manager**→**HP Systems Insight Manager**.
2. Enter your user name, password, domain, and time zone if requested.
Note: If the browser can determine its time zone with certainty, then the **Time zone** selection field is not displayed.
3. Click **sign-in**.

Automatically signing in

You can sign-in to HP SIM using the same account with which you are logged in on your desktop, bypassing the HP SIM sign-in page. If user groups are configured for HP SIM, membership in these groups is accepted and treated the same as if you manually signed-in.

Certain conditions in your network environment must be met for this feature to function correctly:

- The CMS must be registered with a Service Principle Name (SPN) in the domain, which requires a domain administrator. From any system that is a member of the domain, the domain administrator can run the `setspn.exe` utility from the Windows Support Tools. For example:

```
setspn -a HTTP/<cms_fqdn> <sim_service_account>
```

Where HTTP is in all capital letters, *<cms_fqdn>* is the Fully Qualified Domain Name (FQDN) of the CMS, and *<sim_service_account>* is the domain account under which HP SIM service runs.



IMPORTANT: If you change the name of the HP SIM service account, you must first delete the SPN associated with the old service account name, then register the new service account name:

```
setspn -d HTTP/<cms_fqdn> <old_sim_service_account>
```

```
setspn -a HTTP/<cms_fqdn>  
<new_sim_service_account></new_sim_service_account>
```



NOTE: Local accounts cannot be used for HP SIM service account if automatic sign-in is desired.

- The feature must be enabled in HP SIM in the `globalsettings.props` file. This can be done by using the `mxglobalsettings` command, or by directly modifying the file. Set the value for the `AutomaticSignIn` property to 1. Restarting HP SIM is not necessary. See “Properties for `globalsettings.props` file” for information on modifying the `globalsettings.props` file.
- Both the browsing system and the CMS must be members of the Windows domain.
- You must be logged in to the Windows domain on the browsing system, and the HP SIM service must be running using a domain account that is registered with the SPN.



NOTE: Browsing locally from the CMS itself does not perform automatic sign-in; you must enter your credentials on the sign-in page.

- There must be no proxy servers between the browser and the CMS. Use the proxy bypass list in the browser, or use no proxy at all.
- The browser must be configured to support automatic sign-in. In Internet Explorer, enable **Integrated Windows Authentication** under **Tools**→**Internet Options**→**Advanced** tab. The CMS must be in the **Local Intranet** or **Trusted Sites** zone, which can be configured under the **Tools**→**Internet Options**→**Security** tab. If the CMS is in the Internet Explorer Local Intranet zone, select **Automatic Logon only in Intranet zone**. If the CMS is in the Internet Explorer Trusted Sites zone, select **Automatic logon with current user name and password**.

Firefox must be configured with a list of sites (for example, the CMS) where automatic sign-in can be performed, and should be restricted to local intranet sites. This list can be configured by entering `about:config` in the Firefox address bar. From the list of **Preference Names**, select **network.negotiate-auth.trusted-uris** and either double-click or right-click and select **Modify**. Here, you can specify a comma-separated list of URLs or domains, enter the list of URLs used to access HP SIM. For example: `https://cms_fqdn`, where `cms_fqdn` is the FQDN of the CMS.

When automatic sign-in occurs, an intermediate sign-in page is displayed that indicates automatic sign-in is occurring. If you click **Cancel** from this page, the manual sign-in page appears. You might want to cancel automatic sign-in if any unexpected network or domain errors occur. If any browser configuration errors are detected, automatic sign-in is cancelled and the manual sign-in page is displayed along with the configuration error.

Failures encountered during automatic sign-in are logged as normal sign-in failures in both the audit log and the event log. If automatic sign-in is not attempted, either because it's not enabled by HP SIM or the browser, no failure is detected or logged by HP SIM.

If automatic sign-in is configured, you can still manually sign-in to HP SIM.


- **If automatic sign-in fails, the manual sign-in page is displayed** This might occur if you are logged in to the operating system using an account that is not an HP SIM account.
- **If automatic sign-in is not attempted** This might occur if the browser is not properly configured for automatic sign-in, or the feature is disabled in HP SIM.
- **If you click Sign Out from HP SIM** This enables you to specify another user account to use if you are signed-in to the operating system with a different account.

Signing in using Secure Sockets Layer



CAUTION: If you are not certain that the HP SIM system to which you are browsing to is actually the HP SIM system you think it is, do not select either of the last two *Secure Sockets Layer (SSL)* options. You could be giving your sign-in credentials to a rogue system disguised as your HP SIM system, or you could be importing a certificate from a rogue system disguised as your HP SIM system, or importing a certificate from a rogue system disguised as your HP SIM system, giving your sign-in credentials to that rogue system.

If your browser is not configured with the SSL system *certificate* of the HP SIM system, a security alert regarding a certificate of untrusted origin might appear when first browsing to HP SIM using SSL. If a security alert appears, perform one of the following procedures:

- Use the browser to import the certificate into your browser. View the certificate by double-clicking the lock icon () , and then installing the certificate. See “Importing a server certificate” for more information.
- Export the HP SIM system certificate to a file by first browsing from a local browser on the HP SIM system, and then manually importing it into the remote browser. See “Exporting a server certificate” for more information.
- Sign-in to the HP SIM system this time without a trusted certificate, but be sure to import the certificate later. Your data is still encrypted.

After you have an SSL session established with HP SIM, all communications between the browser and HP SIM are secure through SSL.

Logging in to the CLI

You can access the HP SIM CLI directly from the Central Management Server (CMS) or from any network client using SSH client software.



NOTE: On an HP-UX or Linux CMS, you can log in to the operating system as any valid HP SIM user and use the CLI. Not all CLI functionality is available to all users; some functions are only available to users with *administrative rights* or *operator rights* on the CMS. On a Windows CMS, some commands require that the user be a member of the local Administrators group. These commands list includes:

- mxagentconfig
- mxauth
- mxcert
- mxcollection
- mxexec
- mxglobalprotocolsettings
- mxglobalsettings
- mxlog
- mxmib
- mxngroup
- mxnode
- mxquery
- mxreport
- mxstm
- mxtask
- mxtool
- mxtoolbox
- mxuser
- mxwbemsub

Logging in to the CMS directly

1. Log in to the CMS using a valid user name and password (*SSH system name*).
HP SIM grants authorizations based on your operating system user login.
2. Open a terminal window or a command prompt window to execute HP SIM commands.

Using an SSH client to log in remotely

The preferred way to log in remotely is using an SSH client. Telnet and rlogin work, but neither provides a secure connection.

1. Open an SSH client application on any network client.
2. Log in to the CMS through the SSH client software, using a valid user name and password.
HP SIM grants authorizations based on your operating system user login.

Related topics

- Getting started
- Signing out

- Using command line interface commands
- Networking and security

Signing out

Be sure to sign out from HP Systems Insight Manager (HP SIM) to prevent unauthorized access to your active session while you are away.

If you are monitoring HP SIM, your session remains active and continually refreshes, unless you close the browser or navigate to another website. If you navigate to another browser, HP SIM signs you out after 20 minutes.

As long as you are actively working in HP SIM, your session stays active. If the session is inactive for more than 20 minutes, HP SIM ends the session and signs you out after 20 minutes of inactivity. See “Configuring browser timeout options” for more information about keeping sessions active.

Signing out from the *GUI*

1. From the HP SIM banner, click **Sign Out**.
2. Close the web browser.

Logging out from the Command Line Interface

Log off of the CMS or the *Secure Shell* (SSH) client application.

Related topics

- Getting started
- Signing in

Using the First Time Wizard

The First Time Wizard is automatically launched the first time a user with administrative privileges signs in to HP Systems Insight Manager (HP SIM). The administrative account used to install HP SIM is the initial administrative account. If the wizard is canceled before completion, it restarts each time an administrative user signs in. You can cancel and disable the wizard from starting automatically by selecting the **Do not automatically show this wizard again** checkbox and clicking **Cancel**. The wizard can be started manually by selecting **Options**→**First Time Wizard**.

The First Time Wizard provides step-by-step instructions for performing the initial configuration of HP SIM. Additional configuration options are available in the HP SIM *GUI*.

The First Time Wizard helps you configure the following settings on the *Central Management Server* (CMS). After configuring a setting, click **Next** to continue the First Time Wizard setup procedure. The First Time Wizard does not apply any changes until you click **Finish** on the **Summary** page.



NOTE: The default settings in Firefox block the First Time Wizard. You must disable the pop-up blocker in Firefox to see the First Time Wizard.

NOTE: The selections you make in the First Time Wizard are not applied until you click **Finish** on the summary page.

The First Time Wizard includes the following options:

- **Introduction.** Describes the purpose of the First Time Wizard. You can cancel the First Time Wizard and disable the wizard from automatically starting when an administrative user signs in.
- **Managed Environment** Specifies all operating systems to be managed by the *Central Management Server* (CMS). The selections made here configure HP Systems Insight Manager (HP SIM) to show collections, tools, and reports only for managed environments that are selected.
- **WBEM** . Enter the default *Web-Based Enterprise Management* (WBEM) user names and passwords. This information is used to discover systems that use the WBEM *management protocol*.
Enter the mapper proxy system host name and port number to communicate with Windows systems using Windows Management Instrumentation (WMI).

- **SNMP** Enter the read community strings to use for all newly discovered systems. Community strings establish the authentication that enables communication between HP SIM and a managed system. This information is required to discover systems that use the SNMP management protocol.
See “Global protocols” for more information about WBEM and SNMP.
- **Discovery** Use the wizard to enable discovery, set up the discovery schedule, and enter the IP address ranges or host names of the systems you want to discover. Discovery is the process HP SIM uses to find and identify systems on your network and populate the database with that information. A system must be discovered to collect data and track *system health status*.
- **Configure Managed Systems** Configure managed systems as they are discovered, by configuring WBEM and *Windows Management Instrumentation* (WMI), SNMP, Secure Shell (SSH) access, and trust relationship.
- **E-mail** Enter the e-mail settings that the CMS will use to send e-mail notifications. You can set up Automatic Event Handling tasks that prompt HP SIM to send e-mails when the CMS receives a specific event.
- **Summary** Displays all First Time Wizard settings with the option to modify settings or to finish the First Time Wizard.



NOTE: The First Time Wizard configures only the basic settings of HP SIM. See the HP SIM installation guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>, and the **Related topics** section for more information.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring managed systems
- Configuring e-mail settings

Related topics

- Operating-system-specific collections, reports, and tools
- First Time Wizard summary
- Finishing the First Time Wizard
- Performing initial setup
- Administering systems and events
- Protocols
- Data collection
- Discovery and identification
- Events
- About administering events

Configuring the managed environment

From this page, select the operating systems that the Central Management Server (CMS) will manage. There are four options: Windows, Linux, HP-UX, and Other. The selections made here configure HP Systems Insight Manager (HP SIM) to hide collections, tools, and reports for operating systems you do not use. By default the CMS operating system is selected on this page.



NOTE: These settings can be changed at any time, and the hidden collections, tools, and reports can be made visible again. To change these settings from the HP SIM menu, select **Options**→**Managed Environment**.

1. Select the operating systems for the CMS to manage.
2. Click **Next** to go to the next First Time Wizard step, or click **Previous** to return to the previous step.

Related procedures

- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring managed systems
- Configuring e-mail settings
- First Time Wizard summary
- Setting global protocols

Related topics

- Operating-system-specific collections, reports, and tools
- Using the First Time Wizard

Entering WBEM settings

HP Systems Insight Manager (HP SIM) uses the *Web-Based Enterprise Management (WBEM)* protocol to communicate with managed *systems*. You can enter WBEM settings in the First Time Wizard or from the HP SIM menu bar. To disable WBEM communication or enter settings in the GUI, select **Options**→**Protocol Settings**→**Global Protocol Settings** from the HP SIM menu.

If you do not have WBEM systems in your network, you do not need to enter information here. If you have WBEM systems and you do not enter the user names and passwords for these systems, HP SIM will not discover them.



NOTE: See “Setting protocols and credentials for a system or groups of systems” for information about fine tuning protocol settings for a single system or a group of similar systems.

To enter WBEM settings using from the First Time Wizard **WBEM** page:

1. In the **User name**, **Password**, and **Confirm password** fields, enter a default user name and password as needed. To add additional default user name and password pairs, click **Add**. To delete user name and password pairs, click **Delete**. These defaults apply to all newly discovered systems.

HP recommends limiting WBEM user name and password pairs to 10 to reduce the overall discovery run time. To add more than 10 WBEM user name and password pairs, run the `mxnodesecurity -a -p wbem -c username:password` command for each additional set. You can also create an XML file that defines your system authorizations before running discovery. See “Example XML file to add more than 10 WBEM username and password pairs” for more information.

If your network includes *storage systems*, enter the user name and password of each *SMI CIMOM* in this section. For example, if you have an HP host bus adapter (HBA) (Emulex OEM) for Windows, enter the user name `cimadmin` and password `pwd580`. See your storage system's SMI-S provider documentation for information about the SMI CIMOM user name and password.

The system *identification* process attempts each user name and password pair until a successful response is obtained. Future WBEM requests to a system will use the user name and password that succeeded the system identification process. For Windows-based systems, the user name must include the domain name, for example, `domainname\username`.

Enter the user name and password pairs such that root and administrator passwords are listed first and user and guest passwords are listed second. This order minimizes the search time.

For UNIX, a root password is required for certain providers. The WBEM providers that require root passwords are:

- FC HBA
 - SCSI HBA
 - IOTree
 - LVM (root required only for Physical Volume Group information)
2. In the **WMI Mapper Proxy** section, enter the mapper proxy **Hostname** and **Port Number**. If a WMI Mapper Proxy has already been discovered, it appears here.
If you have selected not to manage Windows systems on the previous page, this section is not displayed.
 3. To go to the next First Time Wizard step, click **Next**, or to return to the previous step, click **Previous** to return to the previous step.
The users that are used for WBEM access do not need to be configured to sign-in.

Related procedures

- [Configuring the managed environment](#)
- [Entering SNMP settings](#)
- [Enabling automatic system discovery](#)
- [Configuring managed systems](#)
- [Configuring e-mail settings](#)
- [First Time Wizard summary](#)
- [Setting global protocols](#)

Related topics

- [Using the First Time Wizard](#)
- [Operating-system-specific collections, reports, and tools](#)
- [Global protocols](#)
- [Protocols](#)
- [Configuring HP SIM with storage systems](#)
- [Example XML file to add more than 10 WBEM username and password pairs](#)

Entering SNMP settings

HP Systems Insight Manager (HP SIM) uses *SNMP* to communicate with *managed systems*. Community strings establish the authentication that enables communication between HP SIM and a managed system. You can enter read community strings in the First Time Wizard, or from the HP SIM menu bar. To disable SNMP communication, enter community strings, or control other SNMP settings not available in the wizard, select **Options**→**Protocol Settings**→**Global Protocol Settings** from the HP SIM menu.

If you do not have SNMP systems in your network, it is not necessary to enter information here. If you have SNMP systems and you do not enter read community strings that match these systems, HP SIM does not discover them.

See “Setting protocols and credentials for a system or groups of systems” for information on fine tuning protocol settings for a single system or a group of similar systems.

To enter SNMP settings from the First Time Wizard **SNMP** page:

1. In the **Read community string** field, enter up to 10 read community strings. This value is case-sensitive. The identification process attempts communication with a system, using each of these communities in succession until a successful response is obtained. Future SNMP requests then use the community string that provided a successful response.
If you have SNMP systems and no read community string that match the systems are entered, the systems will not be discovered.
2. To go to the next First Time Wizard step, click **Next**, or to return to the previous step, click **Previous**.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Enabling automatic system discovery
- Configuring managed systems
- Configuring e-mail settings
- First Time Wizard summary
- Setting global protocols

Related topics

- Using the First Time Wizard
- Finishing the First Time Wizard
- Operating-system-specific collections, reports, and tools
- Global protocols
- Protocols

Enabling automatic system discovery

HP Systems Insight Manager (HP SIM) uses *automatic discovery* to find and identify systems on the network. The System Automatic Discovery task is the default discovery task and is disabled by default. You can enable and configure the System Automatic Discovery task in the First Time Wizard, or by selecting **Options**→**Discovery** from the HP SIM menu.

If the System Automatic Discovery task is enabled, it runs immediately when the First Time Wizard is finished to initially populate the HP SIM database.

You can create additional automatic discovery tasks by selecting **Options**→**Discovery** from the HP SIM menu and entering the details, and you can also run *manual discovery* to discover single systems. See “Configuring automatic discovery” and “Adding a system manually” for more information.

To enable automatic system discovery from the First Time Wizard **Discovery** page:

1. To configure HP SIM to run discovery immediately after you finish the First Time Wizard, select **Run discovery once after wizard finishes**.
2. To configure the System Automatic Discovery task to run on a regular schedule, select **Schedule** and enter the periodic run interval and time of day to run the task. See “Applying a time filter” for more information.
3. In the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field, specify the IP addresses to include for pinging. If you want to use this task to discover SMI-S *storage systems*, include the IP address of each *SMI CIMOM*. You can also enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. See “IP ranges” for more information about entering IP ranges. To use an existing hosts file, enter the hosts file name in the following format: `$HostsFileName`.

To discover SMI-S *storage systems*, you must add the IP address of each SMI CIMOM to the System Automatic Discovery task.

Alternatively, you can create a separate discovery task for your SMI CIMOMs. See “Editing a discovery task” and “Creating a new discovery task” for more information.

4. To go to the next First Time Wizard step, click **Next**, or to return to the previous step, click **Previous**.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Configuring managed systems
- Configuring e-mail settings

- First Time Wizard summary
- Configuring automatic discovery

Related topics

- Using the First Time Wizard
- Operating-system-specific collections, reports, and tools
- Discovery and identification
- Configuring automatic discovery general settings
- Configuring HP SIM with storage systems

Configuring managed systems

The **Configure Managed Systems** page in the First Time Wizard enables you to configure managed systems as they are discovered and to specify parameters for running the Configure or Repair Agents. All steps are optional and can be configured from the HP SIM **Options** menu at a later time. To skip this step, click **Next** to go to the next First Time Wizard step.

To configure managed systems from the First Time Wizard **Configure Managed Systems** page:

1. To use the First Time Wizard to configure managed systems when they are first discovered, select **Configure newly managed systems when Discovery runs for the first time**.
2. Enter the user name and password pair for an administrative user account on the managed systems.
3. Under **Configure WBEM/WMI**, select from the following:
 - **Create subscriptions for WBEM events**
 - **Send a test WBEM or WMI indication to this instance of HP Systems Insight Manager to ensure that events appear in HP Systems Insight Manager events lists**
 - **Deploy HP Systems Insight Manager WBEM certificate to the target systems to support client certificate authentication**
This option does not appear if there are no managed HP-UX systems.
4. Under **Configure SNMP**, select from the following:
 - **Set read community strings**
This string is pre-populated with settings from the **SNMP** page of the First Time Wizard.
 - **Set traps to refer to this instance of HP Systems Insight Manager**
 - **Send a test SNMP trap to this instance of HP Systems Insight Manager to make sure events appear in the HP Systems Insight Manager events lists**
5. Under **Configure secure shell (SSH) access**, select from the following:
 - **Host based authentication**
 - **Each user has to be authenticated on the managed system**
6. Select **Trust relationship** to set a trust relationship between managed systems and the Central Management Server (CMS).
7. To go to the next First Time Wizard step, click **Next**, or to return to the previous step, click **Previous**.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring e-mail settings

- First Time Wizard summary
- Setting global protocols

Related topics

- Using the First Time Wizard
- Operating-system-specific collections, reports, and tools
- Global protocols
- Protocols

Configuring e-mail settings

To use the First Time Wizard to configure HP SIM to send e-mail notifications through automatic event handling:

1. Enter the SMTP host name. The SMTP host is the outgoing e-mail server that the CMS uses to send e-mail notifications.
2. In the **Sender's e-mail address** box, enter the e-mail address that the management server uses when sending e-mail notifications.
3. (Optional) Select **Send test email** and enter recipients e-mail address.
Click **Send test email now**.
4. To authenticate your SMTP server, select **Server Requires Authentication**.
5. Enter the account user name and password in the corresponding boxes.

Note If you did not enter a valid Simple Mail Transfer Protocol (SMTP) host, HP SIM notifies you that it cannot send e-mail notifications. If you do not want to enter e-mail settings now, click **OK**, or to enter a valid SMTP host, click **Cancel**.



NOTE: If the **Server Requires Authentication** option is selected, and you enter incorrect account information, e-mail event notifications do not reach the intended recipients.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring managed systems
- First Time Wizard summary
- Setting global protocols

Related topics

- Using the First Time Wizard
- Operating-system-specific collections, reports, and tools
- Global protocols
- Protocols
- Configuring HP SIM with storage systems
- Example XML file to add more than 10 WBEM username and password pairs

First Time Wizard summary

When you are finished entering information in the HP Systems Insight Manager (HP SIM) First Time Wizard, review your selections on the **Summary Page**, and then click **Finish** to save them.

If you enabled automatic discovery or initiated Run discovery after the wizard finishes, discovery runs when you exit the First Time Wizard. If you did not enable automatic discovery or the Run discovery once after wizard finishes, discovery does not take place until you select **Options**→**Discovery** from the HP SIM menu,

and enable a discovery task or select a task and click **Run Now**. See “Configuring automatic discovery” for more information.

See “Performing initial setup” and “Setting up managed systems” for more information about setting up HP SIM and managed systems.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring managed systems
- Configuring e-mail settings
- Configuring HP SIM with storage systems

Related topics

- Operating-system-specific collections, reports, and tools
- First Time Wizard summary
- Finishing the First Time Wizard
- Performing initial setup
- Administering systems and events
- Protocols
- Data collection
- Discovery and identification
- Events
- About administering events

Finishing the First Time Wizard

When you click **Finish** in the First Time Wizard, the **Finish** page appears with a message stating *Your changes are being applied, please do not close the window.* If you selected **Run discovery once after wizard finishes** on the **Discovery** page, you are notified that discovery is running and where to go in the HP Systems Insight Manager (HP SIM) to monitor the progress of discovery. Also included on this page is information on where to go to see discovered systems that you are managing and where to go to better manage these systems. To close the First Time Wizard, click **Close**.

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring managed systems
- Configuring e-mail settings
- Setting global protocols
- Configuring automatic discovery
- Configuring HP SIM with storage systems

Related topics

- Setting up managed systems
- Discovery and identification
- Using the First Time Wizard

- First Time Wizard summary
- Operating-system-specific collections, reports, and tools
- Performing initial setup
- Administering systems and events
- Protocols
- Data collection
- Events
- About administering events

Operating-system-specific collections, reports, and tools

Operating-system-specific collections

The following collections are removed if the associated operating system is not selected on the **Managed Environment** page of the First Time Wizard or from the **Managed Environment** page in the HP Systems Insight Manager (HP SIM) UI (**Options**→**Managed Environment**). These collections are located in the **System and Event Collections** panel under **Systems by Operating System** and **Cluster by Type**, with the exception of **All VSE Resources** which is located under **Systems by Type**. The following table lists collections by operating system.

Windows	Linux	HP-UX	Other
Microsoft Windows Server 2003	Red Hat Linux	HP-UX	SCO Unix
Microsoft Windows 2000	SuSE Linux	HP Serviceguard (under Clusters by Type)	HP True64 UNIX
Microsoft Windows NT	Linux	All HP Integrity Virtual Machines*	HP OpenVMS
Microsoft Windows XP	All HP Serviceguard Clusters*	All Virtual Partition Servers*	HP NonStop Server
Microsoft Windows 95, 98, Me		All Resource Partitions*	HP TruClusters
MSCS Clusters		All Shared Resource Domains*	OpenVMS Clusters
Microsoft Vista		All HP Serviceguard Clusters*	Novell Netware
Microsoft Windows Server 2008		All Virtual Partitions*	
		HP Serviceguard (under Clusters by Type)	
		All HP Integrity Virtual Machines*	

* - Located under **All VSE Resources**.

Operating-system-specific reports

The following reports are specific to HP-UX and are added or removed depending on whether HP-UX is selected or not. There are no reports that are specific to Windows or Linux.

- Cellular Systems - Servers
- HP-UX File System - HP-UX
- HP-UX Kernel Parameters - HP-UX
- HP-UX Logical Volume - HP-UX
- HP-UX Network Details - HP-UX
- HP-UX Physical Volume - HP-UX
- HP-UX Software Bundle - HP-UX

- HP-UX Software Product - HP-UX
- HP-UX Volume Group - HP-UX
- I-O Devices - HP-UX
- Logical Memory Details - HP-UX
- Operating System Details - HP-UX

The following reports have no data for HP-UX and are removed if HP-UX is the only selection.

- Batteries
- System License Info
- Logical Disk Drives
- Installed Controllers
- Physical Disk Drives

Operating-system-specific tools

The following section lists HP SIM tools (by menu path) that by operating system.

Windows

- **Tools→Command Line Tools→Windows** and all tools listed here (copy, del, dir, net, netstat, rmdir, and type).
- **Deploy→Drivers, Firmware, Software.**
- **Configure→Disk Threshold.**
- **Configure→Replicate Agent Settings.**

Linux

- **Tools→Integrated Consoles→Webmin.**
- **Deploy→Drivers, Firmware, Software.**
- **Configure→Disk Threshold.**
- **Configure→Replicate Agent Settings.**
- **Deploy→RPM Package Manager** and all tools listed (Install Package, Query Package, Uninstall Package, Verify Package).
- **Tools→Command Line Tools→Unix/Linux** and all tools listed here (bdf, cat, cp, df, find, ls, my, ps, rm).

HP-UX

- **Configure→HP-UX Configuration** and all tools listed here (Kernel Configuration, Disks and File Systems, Accounts for Users and Groups, Auditing, System Security Policies, Authenticated Commands, Cards, Printers and Plotters, System Properties, Cards and Devices - pdweb, Kernel Configuration - kcweb).
- **Deploy→Software Distributor** and all tools listed here (View Installed Software, View Depot Software, CLI List Software, CLI Preview Install, CLI Verify Software).
- **Diagnose→Event Monitoring Service.**
- **Optimize→Process Resource Manager** and all tools listed here (Display Resource Usage and List Resource Manager Console).
- **Tasks & Logs→View SAM Log.**
- **Tasks & Logs→View Software Distributor Agent Log.**
- **Tasks & Logs→View Software Distributor Daemon Log.**
- **Tools→Command Line Tools→Unix/Linux** and all tools listed here (bdf, cat, cp, df, find, ls, my, ps, rm).

- **Configure**→**Management Processor**→**HP Integrity or HP 9000 iLO** and all tools listed here (New User, Modify User, Delete User, LAN Access, LDAP Settings, Firmware Upgrade, iLO Control, and Deploy SSH Public Key).
- **Tools**→**Integrated Consoles**→**Webmin**.

Other

- ▲ **Tools**→**Command Line Tools**→**Unix/Linux** and all tools listed here (bdf, cat, cp, df, find, ls, my, ps, rm).

Related procedures

- Configuring the managed environment
- Entering WBEM settings
- Entering SNMP settings
- Enabling automatic system discovery
- Configuring managed systems
- Configuring e-mail settings
- Configuring HP SIM with storage systems

Related topics

- First Time Wizard summary
- Finishing the First Time Wizard

Setting up managed systems

Overview

Setting up managed systems involves installing the required Management Agents software and configuring the supported protocols to communicate with the HP Systems Insight Manager software.

For steps to set up managed systems from the Central Management Server (CMS), see the following:

- “Linux CMS”
- “HP-UX CMS”
- “Windows CMS”

Linux CMS

Setting up managed systems from a Linux CMS

Use the following checklist as a guideline to assist you with setting up managed systems from a Linux Central Management Server (CMS):

1. Ensure that HP Systems Insight Manager (HP SIM) is installed on the CMS.
2. Ensure the First Time Wizard has been completed on the CMS. See “Using the First Time Wizard” for more information.

Important: Discovery must be run before setting up managed systems. See “Running a discovery task” for more information. Configuring automatic discovery is part of the First Time Wizard.

3. Install the ProLiant or Integrity Support Pack on the Central Management Server. See *Installing the ProLiant or Integrity Support Pack on a Linux system for the first time*.
4. Configure the managed system software. See *Configuring the managed system software*.

Installing the ProLiant or Integrity Support Pack on a Linux system for the first time

For Linux systems, use the Linux Deployment Utility to install the latest support pack with the preconfigured components to the local system. For more information regarding installing a support pack using the Linux Deployment Utility, see <http://www.hp.com/servers/psp>.

Configuring the managed system software

The HP SIM Configure or Repair Agents tool is a quick and easy way to configure Linux, HP-UX and Windows managed systems to communicate with HP SIM from a Linux CMS.



NOTE: It is possible to manually configure Linux systems. See [Setting up Linux managed systems manually](#).

To run Configure or Repair Agents remotely against multiple systems simultaneously, you must have authorizations to run the Configure or Repair Agents tool.

You must have full CMS configuration privileges to modify the HP SIM community strings in the node security file. In addition, you must enter root or administrator level user credentials for the target system.

To configure agents remotely:

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents tool can be configured to run automatically on a schedule, or you can run it manually. Only one instance of Configure or Repair Agents tool can run at a time.

Setting up Linux managed systems manually

You can use the HP SIM Configure or Repair Agents tool to configure Linux managed systems simultaneously, or you can configure each managed system manually.

To manually configure Linux managed systems, perform the following on each managed system:

1. Install and configure SSH.
 - a. Verify that SSH is installed on the managed system:

```
rpm -qa | grep ssh
```

If it is not installed, see your Linux provider for information about installing SSH.
 - b. On the CMS, copy the SSH generated public key from the CMS to the managed system, and place it in the authorized keys file of the execute-as user (root or administrator).

Important: On a non-English CMS, ensure that an administrator account (spelled exactly as follows, administrator) exists on the CMS, and that `mxagentconfig` has been run on the CMS for the created administrator account.

 - i. Launch the **Manage SSH Keys** dialog box from the CMS command prompt:

```
mxagentconfig -a -n hostname -u username -p Password
```
 - ii. Click **Connect**.
2. Configure the system to send SNMP traps.

Note: These steps might vary slightly, depending on your version of Linux. See your Linux provider for details if these file paths and file names do not exist on your system.

 - a. Verify that SNMP is installed:

```
rpm -qa | grep snmp
```

If it is not installed, see your Linux provider for information about installing SNMP.
 - b. Stop the HP Server and Management Drivers and Agents daemons on the platform where you are installing HP SIM using the following command:

```
/etc/init.d/hpsm stop
```

Note: If the HP Server Management Drivers and Agents daemon is not installed, omit this step and step F.
 - c. Stop the SNMP daemon:

```
/etc/init.d/snmpd stop
```

- d. Edit the `snmpd.conf` file using any text editor.
 For Red Hat Linux, run the following command for opening this file in the vi editor: `vi /etc/snmp/snmpd.conf`
 For SUSE SLES 8, run the following command for opening this file in the vi editor: `vi /usr/share/snmp/snmpd.conf`
 - i. Remove the comment symbol (`#`) from the `trapsink` line, and add the IP address of the CMS:
`trapsink IPaddress`
 where `IPaddress` is the IP address of the CMS.
 - ii. Add the CMS to the read only community by adding the line:
`rocommunity CommunityName IPaddress`
 where `CommunityName` is the SNMP community string used by the CMS and `IPaddress` is the IP address of the CMS.
 - iii. Save the changes to the file. To save and close this file using the vi editor, press the Esc key, enter `:wq!`, and press the Enter key.
 - e. Start the SNMP daemon:
`/etc/init.d/snmpd start`
 - f. Start the HP Server Management Drivers and Agents daemon if it is installed on your system:
`/etc/init.d/hpsasm start`
3. Install the Linux ProLiant Support Pack. To download this software and access installation information, see <http://www.hp.com/support/files>.
 4. Sign-in to the HP SIM GUI. See “Signing in” for assistance.
 5. Add the default WBEM user name and password to the **Global Protocol Settings** page in the HP SIM GUI.
Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system.
Note: This step can be performed once for all the managed systems you are setting up.
 - a. Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
 - b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name, password, and confirmation password.
 - c. Click **OK**.

Example: Setting up remote Linux systems from a Linux CMS

1. Sign-in to the HP SIM on the Linux CMS with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already. See “Using the First Time Wizard” for more information about running the First Time Wizard.
3. Run discovery if you have not already. See “Running a discovery task” for more information.
4. Preconfigure the System Management Homepage and version control components. For more information about preconfiguring the SMH component, see *System Management Homepage Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html> and for version control, see *HP Version Control Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
5. Install the ProLiant or Integrity Support Packs on remote system. Run the Linux Deployment Utility to install the latest Integrity Support Pack on Linux and HP-UX systems. For more information, download the *HP ProLiant Support Pack and Deployment Utilities User Guide* at <http://www.hp.com/servers/psp>.
6. Run the Configure or Repair Agents feature. For more information, see *Configuring the managed system software*.

HP-UX CMS

Installing the required software on an HP-UX system

Use the following checklist as a guideline to assist you with setting up managed systems from an HP-UX Central Management Server (CMS):

1. Understand the basic managed system software for HP-UX.

For HP-UX, the following software, shown with minimum recommended versions, is required for essential HP Systems Insight Manager (HP SIM) functionality to operate. This software is installed by default as part of the latest HP-UX 11i v2 operating environments, but it might need to be installed or updated on HP-UX 11i v1 or older HP-UX 11i v2 systems.

- T1471AA HP-UX Secure Shell
- B8465BA HP WBEM Services for HP-UX

Instant capacity (iCAP) properties for Cells and Processors for a Complex is collected and displayed using HP-UX Web-Based Enterprise Management (WBEM). For HP-UX, the following software is required for essential HP Systems Insight Manager (HP SIM) functionality to operate. This software is installed by default as part of the latest HP-UX 11i v3 (11.3), HP-UX 11i v2 (11.23) and HP-UX 11i v1 (11.11) which can only be installed on HP 9000 servers.

- ▲ B9073BA version 08.01.01 WBEM Services for HP-UX



NOTE: WBEM providers is only collected under the Web-Based Enterprise Management (WBEM).

This WBEM Services bundle contains basic system instrumentation displayed in the HP SIM **Property** pages, as well as supporting collection and reporting by HP SIM Inventory functionality. To maximize the value of HP SIM for properties, inventory, and events, see <http://www.hp.com/go/hpsim/providers> for the latest WBEM Services bundle.

See <http://www.hp.com/go/hpsim/providers> for the latest WBEM Services bundle.

2. Ensure the managed system software is installed.

To verify that the minimum required software is installed, log in to the remote system, and run the following command:

```
$ swlist -l bundle T1471AA B8465BA OpenSSL
```

To verify that the optional providers and System Management Homepage are installed, run commands such as:

```
$ swlist -l bundle LVMPProvider WBEMP-LAN-00 SysMgmtWeb SysFaultMgmt  
OnlineDiag
```

3. Acquire and install the managed system software if not previously installed.

The SecureShell, WBEM bundles are included on the HP-UX Operating Environment and Application Release media, as well as part of the HP SIM HP-UX depot downloaded from http://h18013.www1.hp.com/products/servers/management/hpsim/dl_hpux.html.

For the WBEM providers, see

http://h18013.www1.hp.com/products/servers/management/hpsim/dl_hpux.html.

After the depots containing the software have been acquired, they can be installed from the managed system using commands such as:

```
$ swinstall -s <depot_location> OpenSSL
```

Note: B8465BA and B9073BA version 08.01.01 depends on OpenSSL, so this must be installed first.

```
$ swinstall -s <depot_location> T1471AA
```

```
$ swinstall -s <depot_location> B8465BA
```

```
$ swinstall -s <depot_location> <names of WBEM providers being installed>
```

4. Configure the managed system software. See [Configuring the managed system software](#).

Configuring the managed system software

The HP SIM Configure or Repair Agents tool is a quick and easy way to configure Linux, HP-UX and Windows managed systems to communicate with HP SIM from an HP-UX CMS.



NOTE: It is possible to manually configure HP-UX systems. See [Setting up HP-UX managed systems manually](#).

To run Configure or Repair Agents remotely against multiple systems simultaneously, you must have authorizations to run the Configure or Repair Agents tool.

You must have full CMS configuration privileges to modify the HP SIM community strings in the system security file. In addition, you must enter root level user credentials for the target system.

To configure agents remotely:

1. Select **Configure**→**Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.
Note: The **Step 1: Verify Target Systems** page appears if the targets are selected before selecting a tool.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Configure or Repair Agents

Target: pbdemo Maximize ?

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:

Password:

Password (Verify):

Domain:

< Previous Next >

4. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Note: If you plan to **Configure secure shell (SSH) access** on a Windows target system, the account specified must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group if applicable.

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:

Password:

Password (Verify):

Domain:

< Previous

Next >

5. From the **Step 2: Enter credentials** page:
 - a. In the **User name** field, enter the system administrator name.
 - b. In the **Password** field, enter the system administrator's password for the user name previously entered.
 - c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.
6. Click **Next**. The **Step 3: Configure or Repair Agents** page appears.

Configure WBEEM and SNMP settings, SSH authentication mode, Version Control Agent settings, trust relationships, and for Insight Management Agents version 7.1 or earlier, the administrator password.

Configure WBEEM / WMI [Learn More..](#)

- Create subscription to WBEEM events
- Send a sample WBEEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM event lists.
- Use an HP SIM WBEEM certificate (good for 10 years) rather than username/password to manage the system. *This will deploy a WBEEM certificate to the managed system. This option is only valid for HP-UX systems.*
- Configure a non-administrative account for HP SIM to access WMI data. [Learn More..](#)
This option applies only to Windows Systems.
Administrative accounts can be used without further configuration. If non-administrative access to a managed system is desired, an existing domain account or one local to the managed system can be used by HP SIM to access WMI information over the network.
Enter the credentials for HP SIM to use to access the managed system:
User name:
Password:
Password (Verify):
Domain:

Configure SHIMP [Learn More..](#)

- Set read community string:
- Set traps to refer to this instance of HP Systems Insight Manager. *Note: A ReadWrite string will be created automatically on Windows systems.*
- Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM event lists.
- Configure secure shell (SSH) access authentication. [Learn More..](#)
 - Host based authentication. *Note: All users from this instance of HP SIM will be authenticated on the managed system.*
 - User based authentication for user: . *Each user has to be authenticated on the managed system.*
- Set Trust relationship to "Trust by Certificate". [Learn More..](#)
This enables HP SIM users to connect to the System Management Homepage, Onboard Administrators, Integrated Lights-Out (version 2 and later), and VCA using the HP SIM certificate for authentication.
- Configure Version Control Agent(VCA). [Learn More..](#)
This option applies only to Windows Systems.
The Version Control Repository Manager (VCRM) contains a repository that stores the software and firmware components used to support Windows and Linux platforms. The VCA can be configured to point to the VCRM, enabling easy version comparison and software updates.
Select the system where the VCRM is installed:

7. The **Step 3: Configure or Repair Agents** page enables you to select options to configure the target system.

The following options are available:

- **Configure WBEEM / WMI.** This section enables you to configure the target Linux, Windows or HP-UX system to send WBEEM indications or events to HP Systems Insight Manager.

For this section, the following must be considered:

- **Create subscription to WBEEM events, so that WBEEM events will be sent to the CMS.**
- **Send a sample WBEEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system.**

Note: The indication will appear as an **Informational Event** in the **Event List** of HP SIM. If you do not receive test WBEEM indications in the **Event List**, see "Troubleshooting".

Note: This is supported only on HP-UX and Windows managed systems with WBEEM provider installed.

- **Use an HP SIM WBEEM certificate (good for 10 years) rather than username/password to manage the system.** This option deploys a WBEEM certificate to the managed system and is only valid for HP-UX systems.
- **Configure a non-administrative account for HP SIM to access WMI data.** This option is applicable to Windows systems with HP WBEEM providers. The configuration of the managed system will be updated to allow the specified user to access WMI information over the network. This user will be used by HP SIM to read inventory and configuration information from the system, and will be configured as the WBEEM user in the System Protocol Settings. This configuration step is not necessary if HP SIM is configured with a user with administration rights. This user is not created by HP SIM; it should already exist as either a domain user or one local to the managed system.

The user will be added to the "DCOM Users" group on the managed system and will be given read-only access to WMI information, plus read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system and need not have logon rights. A special purpose domain account is recommended, and should be created by the domain administrator.

To enter the credentials for HP SIM to use to access the managed systems:

1. In the **User name** field, enter a user name.
2. In the **Password** field, enter the password for the user's name previously entered.
3. In the **Password (Verify)** field, reenter the password exactly as it was entered in the **Password** field.
4. In the **Domain** field, enter the Windows domain if the target belongs to a domain.

If configuring a non-administrative user is successful, then these credentials are saved as the System Protocol settings for WBEM access in HP SIM.

- **Configure SNMP.** This section enables you to configure *SNMP* settings.

For this section, the following must be considered:

- a. Select **Set read community string** to specify a community string. By default, HP SIM's first community string, that is not public, appears in the field. If no community string exists in HP SIM, you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you need not set this option. HP-UX enables read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over 30 characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP SIM over the network. Linux and HP-UX systems do not require a **Read Write** community string; hence the **Read Write** community is added on Windows systems only.

- b. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This setting enables the target systems to send *SNMP traps* to this instance of HP SIM.
- c. Select **Send a sample SNMP trap to this instance of the HP SIM to test that events appear in HP SIM event lists** to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

Note: A test trap can only be sent from a Windows managed system with HP Insight Management Agent installed. If you attempt to run this task on a Linux or HP-UX managed system, a message displays indicating the operation is not supported.

Note: The trap will appear as a Generic Trap from the system. This event will appear as an **Informational Event** in the **Event List** of HP SIM.

- **Configure secure shell (SSH) access.** Select this option to configure SSH access on managed systems.

If this option is selected, you must select one of the following options:

- **Host based authentication for SSH.**

Note: For this option to work, the user name and password provided in step 2 must be an administrative level account. For Linux or HP-UX targets, it must be the "root" account and password.

- **Each user has to be authenticated on the managed system**

Note: If you do not want all users that have login access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** as done in step three or by selecting the tool under **Deploy**→**Deploy Drivers**→**Firmware and Agents**→**Install Open SSH**.

- **Set Trust relationship to "Trust by Certificate".** Select this option to configure systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP SIM system certificate to the target system's trusted certificate directory. This option enables HP SIM users to connect to the System Management Homepage using the certificate for authentication. See "Trusted certificates" for more information.

Note: If you experience problems later setting the trust status on a Linux managed system, see "Troubleshooting" under **Certificate Problems** for assistance.

You can configure Single Sign-On (SSO) to management processors for Onboard Administrators and for Integrated Lights-Out 2 (iLO2). To configure SSO, select **Set Trust Relationship**. After SSO is configured, you are not continually prompted to supply the login credentials for the management processor.

Note: For systems with Management HTTP Server 4.x and earlier, Configure or Repair Agents adds the Administrator password in the Management HTTP Server store and modifies the SNMP settings but cannot change trust relationship information because Management HTTP Server 4.x and earlier did not deploy trust relationships.

- **Configure Version Control Agent (VCA).** Select this option to configure the VCA to point to the HP Version Control Repository Manager (VCRM), where the repository of software and firmware is located, enabling version comparison and software updates. This option is available only for Windows systems. This section can be accessed in the **Configuration** section of all CMS systems including Windows, Linux and HP-UX.

To configure VCA:

1. In the **Select the system where the VCRM is installed** field, select the server where the VCRM is installed from the dropdown list.
 2. In the **User Name** field, enter the user name to access the VCRM. This user cannot be the default "Administrator" user. It has to be an user with administrative privileges.
 3. In the **Password** field, enter the password to access the VCRM.
 4. In the **Confirm Password** field, reenter the password for the VCRM just as you entered it in the **Password** field.
- **Set administrator password for Insight Management Agents version 7.1 or earlier.** Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Do not set this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you need not set this option.

If this option is selected, you must complete the following steps:

 - a. In the **Password** field, enter the new administrator password.
 - b. In the **Confirm Password** field, reenter the new administrator password exactly as you entered it previously.

8. Click **Run Now**. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The log results indicate whether the repair attempt was successful.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed and for some to fail.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout tab.** This tab displays the output text information.
- **The stderr tab.** This tab displays information if the executable experienced an error.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

- a. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.

- b. Select which report to display.

- c. Click **OK** to display the report, or click **Cancel** to return to the **View Task Results** page.

9. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents tool can be configured to run automatically on a schedule, or you can run it manually. Only one instance of Configure or Repair Agents tool can run at a time.

Setting up HP-UX managed systems manually

You can use the HP SIM Configure or Repair Agents tool to configure HP-UX managed systems simultaneously, or you can configure each managed system manually.

To configure an HP-UX system manually:

1. On the CMS:
 - a. Configure the SSH keys for this system.
 - b. Configure the default WBEM user name and password if not previously done.
Note: SSH and WBEM are installed on HP-UX 11.23 systems by default. For 11.11 systems, verify that they are installed with this command:

```
swlist B8465BA T1471AA
```

- c. Subscribe to WBEM Indications/Events.
2. On each managed system:
 - a. Install SSH on the managed system if not previously installed.

```
swinstall -s /directory/depot T1471AA
```

 where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot T1471AA
```
 - b. Install WBEM on the managed system if not previously installed.
Note: OpenWBEM is not supported.

```
swinstall -s /directory/depot B8465BA
```

 where `directory` is the path to the depot file and `depot` is the name of the depot file. For example:

```
swinstall -s /tmp/HPSIM_download.depot B8465BA
```
 - c. Configure SNMP to send traps to the CMS:
 - i. Add the full host name or IP address of the CMS as a trapdest in the following file:

```
/etc/SnmpAgent.d/snmpd.conf
```



```
trap-dest: hostname_or_ip_address
```

- ii. Stop the SNMP Master agent and all subagents with the command:

```
/sbin/init.d/SnmpMaster stop
```
 - iii. Restart the SNMP Master agent and all subagents with the command:

```
/usr/sbin/snmpd
```
- d. Configure DMI on the managed system by adding the *Domain Name Service* (DNS) host name of the CMS.

Note: DMI must only be configured for HP-UX 11.0.

- i. Stop the DMI daemon on the managed system:

```
/sbin/init.d/Dmisp stop
```
 - ii. Edit `/var/dmi/dmiMachines` by adding the host name of the CMS to the end of this file. Save the file.
 - iii. Start the DMI daemon:

```
/sbin/init.d/Dmisp start
```
- e. On the CMS, copy the SSH-generated public key from the CMS to the managed system using the `mxagentconfig`:

Use one of the following commands:

- ```
mxagentconfig -a -n <hostname> -u root -f <file_with_root_password>
```

  
or
- ```
mxagentconfig -a -n <hostname> -u root -p <root_password>
```

Note: Using the `-p` option exposes the password through `ps` output, so use of the `-f` option (with a file only readable by root, and containing only the managed system root password) is highly recommended when using `mxagentconfig -a`. If the `-p` option is used, enclose the password in single quotes if the password has any special characters, such as `&` or `$`. For more information and options, see the `mxagentconfig` manpage with `man mxagentconfig`.

3. Sign-in to the HP SIM GUI. For assistance with this, see “Signing in”. Using the GUI, add the default WBEM user name and password to the **Global Protocol Settings** page.

Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system.

Note: This step can be performed once for all the managed systems you are setting up.

- a. Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
- b. In the **Default WBEM settings** section, ensure that the **Enable WBEM** checkbox is selected, and add the default WBEM user name, password, and confirmation password.
- c. Click **OK**.

Note: An account for at least one of the WBEM user name and password combinations must exist on each managed system. If the user in the Global Protocol Settings does not exist on the managed system you can set per-system WBEM user names and passwords from the **System Protocol Settings** page.

4. To subscribe to WBEM Indications/Events:

Note: For more information about HP-UX WBEM events, go to the *WBEM subscriptions in HP SIM* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- a. From the managed system, be sure WBEM is already installed.

Note: Subscribing to WBEM Indications/Events on managed systems is optional.

- b. Verify that **SysFaultMgmt** provider is installed.

Depending on the System Fault Management (SFM) configuration, run the following:

```
cimprovider -lm SFMProviderModule
```


The EMSWrapperProvider displays.

or

```
cimprovider -ls
```

The EMSWrapperProvider displays.

Note: For more information regarding SFM, see [HP System Fault Management Diagnostics](#).

- c. From the CMS:

To subscribe to WBEM Events, you must have **root** access. If the Global Protocol Setting does not match the managed system or does not contain **root** access, the subscription for WBEM Indications fails. You can verify what access WBEM has by running the following command line:

```
mxnodesecurity -l -p wbem -n <systemname>
```

If the managed system does not have a root level user credential configured, you can add it for the individual system.

Note: You can use the Configure or Repair Agents tool to perform this step without permanently recording a **root** password.

- To change the individual system:

```
mxnodesecurity -a -p WBEM -c \  
<username:password> -n <systemname>
```

- d. From the CMS, run the WBEM Indications/Events command line:

```
mxwbemsub -l -n <systemname>
```

See “Subscribing to WBEM indications” for more information.

Your managed systems are now ready to be managed by HP SIM.

Example: Setting up remote HP-UX systems from an HP-UX CMS

1. Sign-in to HP SIM on the HP-UX with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already. See “Running a discovery task” for more information.
3. Run discovery if you have not already. See “Using the First Time Wizard” for more information about running the First Time Wizard.
4. Ensure the managed system software is installed. For more information, see “Installing the required software on an HP-UX system”.
5. Run the Configure or Repair Agents feature to configure the managed system. For more information, see “Configuring the managed system software”.

Windows CMS

Setting up managed systems from a Windows CMS

Use the following checklist as a guideline to assist you with setting up managed systems from a Windows Central Management Server (CMS):

1. Ensure that HP Systems Insight Manager (HP SIM) is installed on the CMS.
2. Ensure the First Time Wizard has been completed on the CMS. See “Using the First Time Wizard” for more information.
Important: Discovery must be run before setting up managed systems. See “Running a discovery task” for more information. Configuring automatic discovery is part of the First Time Wizard.
3. Configure the managed system software. See [Configuring the managed system software using the Configure or Repair Agents feature from the CMS](#) for more information.

Configuring the managed system software using the Configure or Repair Agents feature from the CMS

The HP SIM Configure or Repair Agents tool is a quick and easy way to configure Linux, HP-UX and Windows managed systems to communicate with HP SIM from a Windows CMS.

To run Configure or Repair Agents remotely against multiple systems simultaneously, you must have authorizations to run the Configure or Repair Agents tool.

You must have full CMS configuration privileges to modify the HP SIM community strings in the system security file. In addition, you must enter administrator level user credentials for the target system.

To configure agents remotely:

1. Select **Configure**→**Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.
Note: The **Step 1: Verify Target Systems** page appears if the targets are selected before selecting a tool.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Note: If you plan to **Configure secure shell (SSH) access** on a Windows target system, the account specified must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group if applicable.

Configure or Repair Agents Maximize ?

Target: pbdemo

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:

Password:

Password (Verify):

Domain:

[< Previous](#) [Next >](#)

4. From the **Step 2: Enter credentials** page:
 - a. In the **User name** field, enter the system administrator name.
 - b. In the **Password** field, enter the system administrator's password for the user name previously entered.
 - c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

5. Click **Next**. The **Step 3: Install Providers and Agents (Optional)** page appears.

Step 3: Install Providers and Agents (Optional)

If agents or providers are already installed, skip this step and proceed to the configuration step.

By installing agents or providers on the managed systems, HP SIM will be able to collect inventory and status information from the systems. It will also enable HP SIM to receive event notifications from the system(s). In most cases, you will want to install either WBEM / WMI providers or SNMP agents, but not necessarily both.

This option applies only to ProLiant or Itanium-based Systems with Windows Operating Systems

- Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** [Learn More...](#)
- Install SNMP Agent (HP Insight Management Agents) for Windows** [Learn More...](#)
- Install Open SSH** SSH is used for running tools remotely on managed systems. [Learn More...](#)
- Install the Version Control Agent for Windows (VCA)** The VCA, in conjunction with the HP ProLiant Version Control Repository Manager, enables management of the HP ProLiant software and firmware on the managed systems. [Learn More...](#)

For selected installs:

- Force downgrade, or reinstall the same version
- Reboot system(s) if necessary after installation

Click "Next" to configure the providers and agents

< Previous Next >

6. You can install Insight Management Agents or providers, either *Web-Based Enterprise Management* or *Simple Network Management Protocol*, on managed systems so HP SIM can collect inventory and status information from these systems and receive event notifications from the systems. Installation is supported only on ProLiant or Itanium-based servers with Windows operating system.

From the **Step 3: Install Providers and Agents (Optional)** page:

- a. Select **Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** to install *WBEM* or *WMI* providers on Windows managed systems.
- b. Select **Install SNMP Agent (HP Insight Management Agents) for Windows** to install the *SNMP* agent on Windows managed systems. This Insight Management Agent allows network monitoring and control.
- c. Select **Install Open SSH** to install *OpenSSH* on Windows managed systems. See "Installing OpenSSH" for more information.
- d. Select **Install the Version Control Agent (VCA)** to install the *HP Version Control Agent*; (VCA) on Windows managed systems. The VCA enables you to view the HP software installed on a system and when updates for the software are available in the repository. See "About the Version Control Agent" for more information.

HP SIM determines the type of agent/provider to install based on the system type, subtype, and operating system description of the system.

Table 4-1 Version Support Matrix for components used for install.

Supported systems	HP WBEM Provider	HP ProLiant Agent	Open SSH	Version Control Agent
Unknown	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (64 bit)	7.90 (64 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating systems (2000)	Not supported	7.60 (32 bit)	3.71	2.1.8
Itanium-based systems with Windows operating system (2003)	Not supported	5.1.10	3.71	2.1.7.770

System Management Homepage version 2.1.7 is also installed, if necessary, with these agents.



NOTE: If you wish to install a 64 bit agent or provider, make sure the target system is identified as a 64 bit system in HP SIM.

If your system is not correctly identified, go to **System Page** → **Edit System Properties**. Select the correct system type, subtype and enter the operating system description manually.

Edit System Properties

blade31

Go back to [blade31](#)

System Information

Identification

Preferred system name: [Restore default name](#)

Prevent the Discovery process from changing this system name

Serial number:

Product Description

System type:

System subtype 1:

System subtype 2:

System subtype 3:

System subtype 4:

System subtype 5:

System subtype 6:

System subtype 7:

System subtype 8:

Product model:

Hardware description:

Operating system description:

Example: Installing Insight Management Agents on a ProLiant Windows 64 bit system:

1. Select system **Type**: server.
2. Select system **subtype 1**: ProLiant
3. Enter operating system description as Microsoft Windows Server 2003, x64 Enterprise Edition Service Pack 1 or the correct operating system description of your system.

If you want to configure the agents after installing, select the force reboot option. This allows the newly installed component to be completely initialized before configuring it.

Note: Installation with reboot typically takes about 8 minutes to complete.

7. Click **Next**. The **Step 4: Configure or Repair Agents** page appears.

Configure WBEM / WMI [Learn More..](#)

Create subscription to WBEM events

Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM event lists.

Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system. *This will deploy a WBEM certificate to the managed system. This option is only valid for HP-UX systems.*

Configure a non-administrative account for HP SIM to access WMI data [Learn More..](#)

This option applies only to Windows Systems with HP WBEM Provider installed.
Administrative accounts can be used without further configuration. If non-administrative access to a managed system is desired, an existing domain account or one local to the managed system can be used by HP SIM to access WMI information over the network.

Enter the credentials for HP SIM to use to access the managed system:

User name:

Password:

Password (Verify):

Domain:

Configure SNMP [Learn More..](#)

Set read community string:

Set traps to refer to this instance of HP Systems Insight Manager. *Note: A ReadWrite string will be created automatically on Windows systems.*

Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM event lists.

Configure secure shell (SSH) access authentication [Learn More..](#)

Host based authentication *Note: All users from this instance of HP SIM will be authenticated on the managed system.*

User based authentication for user: *Each user has to be authenticated on the managed system*

Set Trust relationship to "Trust by Certificate" [Learn More..](#)

This enables HP SIM users to connect to the System Management Homepage, Onboard Administrators, Integrated Lights-Out (version 2 and later), and VCA using the HP SIM certificate for authentication.

Configure Version Control Agent(VCA) [Learn More..](#)

This option applies only to Windows Systems.
The Version Control Repository Manager (VCRM) contains a repository that stores the software and firmware components used to support Windows and Linux platforms. The VCA can be configured to point to the VCRM, enabling easy version comparison and software updates.

Select the system where the VCRM is installed:

Enter the credentials for the VCA to use to access the VCRM:

User name:

Password:

Password (Verify):

Domain:

Set administrator password for Insight Management Agents version 7.1 or earlier [Learn More..](#)

This option applies only to ProLiant Systems

Password:

Password (Verify):

[< Previous](#) [Schedule](#) [Run Now](#)

8. The **Step 4: Configure or Repair Agents** page enables you to select options to configure the target system.

The following options are available:

- **Configure WBEM / WMI.** This section enables you to configure the target Linux, Windows or HP-UX system to send WBEM indications or events to HP Systems Insight Manager.

For this section, the following must be considered:

- **Create subscription to WBEM events, so that WBEM events will be sent to the CMS.**
- **Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system.**

Note: The indication will appear as an **Informational Event** in the **Event List** of HP SIM. If you do not receive test WBEM indications in the **Event List**, see "Troubleshooting".

Note: This is supported only on HP-UX and Windows managed systems with WBEM provider installed.

- **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system.** This option deploys a WBEM certificate to the managed system and is only valid for HP-UX systems.
- **Configure a non-administrative account for HP SIM to access WMI data.** This option is applicable to Windows systems with HP WBEM providers. The configuration of the managed system will be updated to allow the specified user to access WMI information over the network. This user will be used by HP SIM to read inventory and configuration information from the

system, and will be configured as the WBEM user in the System Protocol Settings. This configuration step is not necessary if HP SIM is configured with a user with administration rights. This user is not created by HP SIM; it should already exist as either a domain user or one local to the managed system.

The user will be added to the "DCOM Users" group on the managed system and will be given read-only access to WMI information, plus read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system and need not have logon rights. A special purpose domain account is recommended, and should be created by the domain administrator.

To enter the credentials for HP SIM to use to access the managed systems:

1. In the **User name** field, enter a user name.
2. In the **Password** field, enter the password for the user's name previously entered.
3. In the **Password (Verify)** field, reenter the password exactly as it was entered in the **Password** field.
4. In the **Domain** field, enter the Windows domain if the target belongs to a domain.

If configuring a non-administrative user is successful, then these credentials are saved as the System Protocol settings for WBEM access in HP SIM.

- **Configure SNMP.** This section enables you to configure *SNMP* settings.

For this section, the following must be considered:

- a. Select **Set read community string** to specify a community string. By default, HP SIM's first community string, that is not public, appears in the field. If no community string exists in HP SIM, you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you need not set this option. HP-UX enables read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over 30 characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP SIM over the network. Linux and HP-UX systems do not require a **Read Write** community string; hence the **Read Write** community is added on Windows systems only.

- b. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This setting enables the target systems to send *SNMP traps* to this instance of HP SIM.
- c. Select **Send a sample SNMP trap to this instance of the HP SIM to test that events appear in HP SIM event lists** to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

Note: A test trap can only be sent from a Windows managed system with HP Insight Management Agent installed. If you attempt to run this task on a Linux or HP-UX managed system, a message displays indicating the operation is not supported.

Note: The trap will appear as a Generic Trap from the system. This event will appear as an **Informational Event** in the **Event List** of HP SIM.

- **Configure secure shell (SSH) access.** Select this option to configure SSH access on managed systems. If this option is selected, you must select one of the following options:
 - **Host based authentication for SSH.**

Note: For this option to work, the user name and password provided in step 2 must be an administrative level account. For Linux or HP-UX targets, it must be the "root" account and password.
 - **Each user has to be authenticated on the managed system**

Note: If you do not want all users that have login access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** as done in step three or by selecting the tool under **Deploy**→**Deploy Drivers**→**Firmware and Agents**→**Install Open SSH**.
- **Set Trust relationship to "Trust by Certificate".** Select this option to configure systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP SIM system certificate to the target system's trusted certificate directory. This option enables HP SIM users to connect to the System Management Homepage using the certificate for authentication. See "Trusted certificates" for more information.

Note: If you experience problems later setting the trust status on a Linux managed system, see "Troubleshooting" under **Certificate Problems** for assistance.

You can configure Single Sign-On (SSO) to management processors for Onboard Administrators and for Integrated Lights-Out 2 (iLO2). To configure SSO, select **Set Trust Relationship**. After SSO is configured, you are not continually prompted to supply the login credentials for the management processor.

Note: For systems with Management HTTP Server 4.x and earlier, Configure or Repair Agents adds the Administrator password in the Management HTTP Server store and modifies the SNMP settings but cannot change trust relationship information because Management HTTP Server 4.x and earlier did not deploy trust relationships.
- **Configure Version Control Agent (VCA).** Select this option to configure the VCA to point to the HP Version Control Repository Manager (VCRM), where the repository of software and firmware is located, enabling version comparison and software updates. This option is available only for Windows systems. This section can be accessed in the **Configuration** section of all CMS systems including Windows, Linux and HP-UX.

To configure VCA:

 1. In the **Select the system where the VCRM is installed** field, select the server where the VCRM is installed from the dropdown list.
 2. In the **User Name** field, enter the user name to access the VCRM. This user cannot be the default "Administrator" user. It has to be an user with administrative privileges.
 3. In the **Password** field, enter the password to access the VCRM.
 4. In the **Confirm Password** field, reenter the password for the VCRM just as you entered it in the **Password** field.
- **Set administrator password for Insight Management Agents version 7.1 or earlier.** Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Do not set this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you need not set this option.

If this option is selected, you must complete the following steps:

- a. In the **Password** field, enter the new administrator password.
 - b. In the **Confirm Password** field, reenter the new administrator password exactly as you entered it previously.
9. Click **Run Now**. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The log results indicate whether the repair attempt was successful.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed and for some to fail.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout tab.** This tab displays the output text information.
- **The stderr tab.** This tab displays information if the executable experienced an error.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

- a. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.

- b. Select which report to display.

- c. Click **OK** to display the report, or click **Cancel** to return to the **View Task Results** page.

10. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents tool can be configured to run automatically on a schedule, or you can run it manually. Only one instance of Configure or Repair Agents tool can run at a time.

Example: Setting up Windows managed systems manually

1. Sign-in to the HP SIM on the Windows CMS with full CMS configuration privileges.
2. Run the First Time Wizard if you have not already. See "Running a discovery task" for more information.
3. Run discovery if you have not already. See "Using the First Time Wizard" for more information about running the First Time Wizard.
4. Preconfigure the System Management Homepage and version control components. For more information about preconfiguring the SMH component, see *System Management Homepage Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html> and for version control, see *HP Version Control Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
5. Run the Configure or Repair Agents feature. For more information, see "Configuring the managed system software using the Configure or Repair Agents feature from the CMS".

Performing initial setup

The initial setup involves setting up *managed systems*, configuring *discovery*, configuring event handling, adding *users*, and defining authorizations. It assumes that you just completed the installation of your *Central Management Server* (CMS). If you bypassed or canceled the First Time Wizard, the following steps assist you in setting up your environment to run HP Systems Insight Manager (HP SIM).



NOTE: The First Time Wizard starts the first time a user with *administrative rights* signs in to HP SIM. If the wizard is canceled before completion, it restarts each time a user with administrative rights signs in. You can cancel and disable the wizard from automatically starting by selecting the **Do not automatically show this wizard again** checkbox. The wizard can be manually started by selecting **Options**→**First Time Wizard**.

If you are a new administrator of an existing *management domain*, it might be useful for you to familiarize yourself with these steps, even though your CMS has already been through the initial setup. The steps in this process are common *tasks* that HP SIM administrators perform on a regular basis.

Initial setup process

When you first start HP SIM, the introductory page appears with a section called **Do this now to finish the installation**. To get started using HP SIM:

1. **Setting up managed systems** Setting up managed systems involves installing the required *management agents* and configuring HP SIM software. See “Setting up managed systems” for more information.
2. **Configure storage systems** If you have *storage systems* on your network, you must install and configure their *SMI-S providers* before HP SIM can discover them. See “Configuring HP SIM with storage systems” for more information.
3. **Configuring protocol settings** Configuring the protocol settings defines what *systems* are added to HP SIM using discovery in the next step. See “Setting global protocols” for more information.

If you ran the First Time Wizard, the protocol settings might already be configured.



IMPORTANT: If you have storage systems on your network, you must add the user name and password for each *SMI CIMOM* to the **Default WBEM settings** section of the **Global Protocol Settings** page. If you do not add this information, your storage systems will not be discovered.

4. **Configuring discovery: automatic or manual** Discovery is the process that HP SIM uses to find and identify the *systems* on your network and populate the *database* with that information. A system must first be discovered to collect data and track *system health status*. There are two ways to discover new systems:
 - **Automatic discovery.** Searches the network for systems running specific protocols. It runs automatically every 24 hours, but the process can be manually executed or scheduled to execute at other times. See “Configuring automatic discovery” for information about automatic discovery. If you ran the First Time Wizard, discovery might already be completed.
 - **Manual discovery.** Used to add a single system or a group of systems to the HP SIM database. See “Adding a system manually” for information about manual discovery.



IMPORTANT: If you have storage systems on your network, you must add each *SMI CIMOM* IP address to a discovery task. If an *SMI CIMOM* IP address is not included in a discovery task, the associated storage system will not be discovered.

5. **Adding new users** Any user with a valid network login can be added to HP SIM. See “Users and user groups” for more information. If you ran the First Time Wizard, new users might already be added.
6. **Configuring e-mail settings** Configuring e-mail settings enables users to receive e-mail notification of certain *events*. See “Configuring e-mail settings” for information about e-mail settings.
7. **Configuring paging settings** Configuring paging settings enables users to receive pages that notify them of certain events. See “Configuring modem settings for paging” for information about paging settings.
8. **Setting up automatic event handling** Automatic event handling enables you to define an action that HP SIM performs when an event is received. Automatic event handling can be set up to use the e-mail and paging settings that you specified in the previous sections. See “Creating an automatic event handling task” for more information.

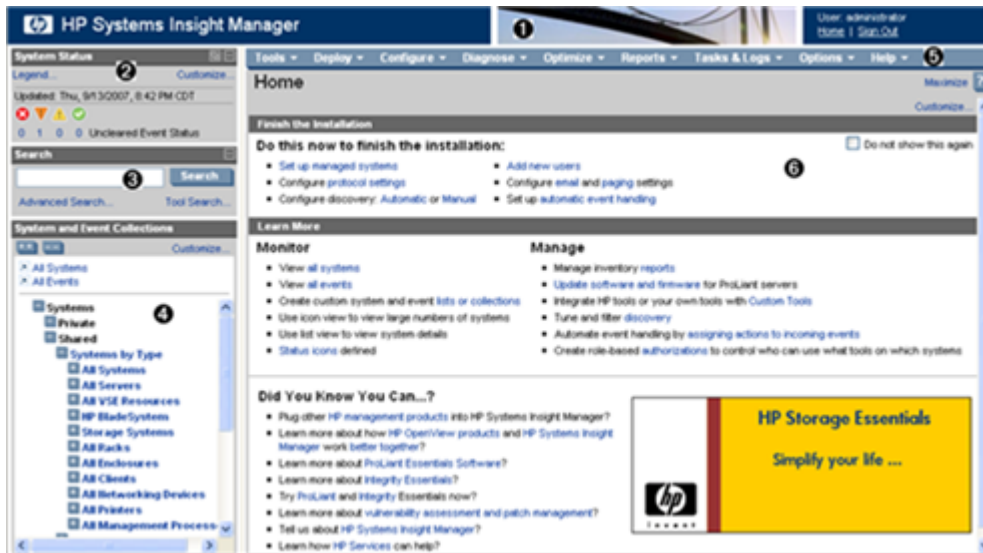
Related topics

- Signing in
- Signing out
- Navigating the Home page
- Configuring HP SIM with storage systems

Navigating the Home page

Graphical user interface features

This section describes the *GUI* features. The following figure is a sample screen shot of the GUI.



The GUI includes the following six regions:

1. **Banner** The banner provides a link to the **Home** page, a link to **Sign Out** of HP SIM, and displays the user that is currently signed-in. Click the minimize icon in the top right corner to minimize the banner. To maximize the banner, click the maximize icon.
2. **System Status panel** This panel provides uncleared event status, *system health status* information, and an alarm to notify you of certain events or statuses. The **System Status** panel can be customized for your environment. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign in the top right corner of the panel. To expand the panel, click the plus sign. If the **System Status** panel is collapsed and an alarm is received, the panel expands to show the alarm. The panel can be enlarged by clicking the **Open in new window** icon (☐) to display a separate large window that can be resized and viewed from across a room without sitting at the HP SIM terminal. See “[Enlarging the System Status panel](#)” for more information.
3. **Search panel** The search feature enables you to search for matches by system name and common system attributes. You can also perform an advanced search for matches based on selected criteria. To speed the search process, as you enter system information in the search box, a dropdown list appears listing systems that begin with the text you are entering. You can select from the dropdown list or continue to enter the information. See “[Search criteria](#)” for more information about the types of search criteria available. If you do not need to view this panel at all times, you can collapse it by clicking the minus sign (⊖) in the top right corner of the panel. To expand the panel, click the plus sign (⊕). See “[Basic and advanced search](#)” for more information.
4. **System and Event Collections panel** System and event collections enable you to view all known systems and events in a specific management environment. A collection can be private, visible only to its creator, or shared, visible to all users. HP SIM ships with default shared collections only. See “[Monitoring systems, clusters, and events](#)” for information about customizing and creating new collections. See “[Default shared collections](#)” for more information about the default shared collections shipped with HP SIM.

5. **Menus** The HP SIM menus provide access to tools, logs, software options, and online help. The **Options** menu is primarily for users who administer the HP SIM software. If you lack authorization to use these tools, you might not be able to access certain menus.
6. **Workspace** The workspace displays the results of your latest request. It can contain a collection, *tool*, or report. Some tools launch a separate browser window or X Window terminal instead of displaying in the *workspace*. This area contains the **Home** page when you sign-in to HP SIM. By default, the introductory page is the **Home** page. The introductory page provides information and tips about HP SIM and links to frequently used features. You can customize HP SIM to display a different page as the **Home** page. See “Customizing the Home page” for information about selecting a different introductory page.



NOTE: To maximize the workspace, click the **Maximize** link next to the Help icon (?). To restore the workspace to its original size, click **Restore Size**.

The four default sections on the introductory page include the following:

- **Do this now to finish the installation:** This section only appears if the following conditions are met:
 - The user has *administrative rights*.
 - The user has not disabled this section from the **Home Page Settings** page.
- **Monitor** This section provides links to common monitoring tasks, including locating and tracking *systems* and *events*.
- **Manage** This section provides links to frequently used tools and features available from the menus above the workspace. These links provide access to inventory reports, software and firmware deployment, *discovery*, event handling, integrating custom tools, and *authorizations*.
- **Did You Know You Can...?** This section provides useful tips and shortcuts, including where you can learn more about HP products, service offerings, and software.
This section appears if you have not disabled it from the **Home Page Settings** page.

Related topics

- Customizing the Home page
- Customizing the System Status panel

Customizing the Home page

Customize the **Home** page to select which pages display and customize the regions on the default **Home** page and introductory page.

To customize the **Home** page, perform the following procedure:

1. Click **Home** in the banner to display the **Home** page in the workspace.
2. Click **Customize** in the upper-right corner of the introductory page.

Note: If the **Home** page has been set to something other than the default introductory page, you can access the **Home Page Settings** page by selecting **Options**→**Home Page Settings**.

3. Specify which page you want to use as **Home** page:
 - Introductory page (default)
 - Plug-in (if installed) page



NOTE: This option is used by some HP SIM partner applications to point to their home page. However, if no partner application is using this, selecting this option displays the HP SIM default introductory page.

- Any specific *system*, *cluster*, or *event* collection view

Note: The default introductory page is only available when it is set as the **Home** page. If you want to view this page when it is not set as your home page, reselect it as the **Home** page.

4. (Optional) If the introductory page is selected as your home page, customize the content on the page by selecting or clearing the following options:
 - **Show "Do this now to finish the install" frame.** If selected, this section appears on the **Home** page.
 - **Show the "Did You Know?" image.** If selected, the image in the bottom right corner of the **Home** page appears.
5. (Optional) If you selected **This collection**, select a collection from the dropdown list, and then select **Automatically maximize workspace** if you want to automatically maximize the workspace when this collection is displayed as the home page.

Related topics

- [Navigating the Home page](#)
- [Customizing the System Status panel](#)

Customizing the System Status panel



NOTE: Customizations done to the **System Status** panel are also displayed in the system status pop-up window. To minimize the **System Status** panel, click the minimize icon (▢) in the upper right corner of the panel title bar. To maximize the **System Status** panel, click the maximize icon (⊕) in the upper right corner of the panel title bar. To open the **System Status** panel in a new window, click the Open in New Window icon.

Customize the **System Status** panel to display the following status information:

- **Uncleared Event Status** A count that indicates the number of *uncleared event statuses* that are Critical, Major, Minor, and Normal for any given system collection. Each number is a hyperlink to a detailed list of events with that particular status. By clicking the number, an event collection appears with those particular events and their corresponding systems.
- **Health Status** A count that indicates the number of systems, in a given system collection, that have a *system health status* that is Critical, Major, Minor, and Normal. Each number is a hyperlink to a detailed list of systems with that particular status. By clicking the number, a system collection appears with those particular systems. Health status is not shown by default but can be configured to appear.



NOTE: The **system health status information** displays only when it is customized to display the system health status.

- **Alarm** An alarm can be customized to appear for specific criteria for any given system collection. The alarm alerts you that a particular criterion has been met by one or more systems in that collection. For example, you might receive an alarm that a storage system has a critical uncleared event, or critical health status. Because the **System Status** panel is continually updated, the alarm appears until the event is cleared, the system is removed from the collection, or the alarm customization is changed so that it no longer applies. If the **System Status** panel is collapsed, and an alarm occurs, it opens automatically so that the alarm is visible. You can collapse the panel, but it continues to open as long

as the alarm is relevant. To have the panel remain collapsed, you must clear the offending event or system status or reconfigure the status display to no longer display alarms.

- **Legend of status icons** To display a list of status icons, click **Legend** in the **System Status** panel. Legend information appears in a separate window and remains open until you close it. See “System status types” for more information about default user templates.



NOTE: If the **System Status** panel is customized to have no status displayed, the timestamp does not display.

To customize the **System Status** panel:

1. Click **Customize** in the upper-right corner of the **System Status** panel. The **Customize System Status** page appears.
2. Select the first **Show summary of**, and then select **uncleared event status** or **health status**.
 - a. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - b. Edit the **Label** if desired.
3. Select the second **Show summary of**, and then select **uncleared event status** or **health status**.
 - a. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - b. Edit the **Label** if desired.
4. Select to **Show an alarm when any system meets the condition**.
 - a. Select the **Condition**.
 - b. Select the system collection **All Systems**, or select another system collection from the dropdown list.
 - c. Edit the **Label** if desired.
5. Click **OK** to save changes.

Note: Clicking **Restore Defaults** returns the customization screen to its default condition: only the *uncleared event status* appears in the banner. Health status and the alarm are disabled. All personalized information is removed.

Related topics

- [Enlarging the System Status panel](#)
- [Navigating the Home page](#)
- [Customizing the Home page](#)
- [System status types](#)

Enlarging the System Status panel

The **System Status** panel can be enlarged to enable you to monitor system and event statuses. Click the Open in New Window icon on the **System Status** panel title bar and the status panel pop-up window is displayed. The window can be resized by clicking and dragging the sides of the window. To close the window manually, click the Close Window icon. Otherwise, the window is closed if the HP Systems Insight Manager (HP SIM) window is closed or refreshed, or you sign out of HP SIM.

The enlarged status panel window mimics the **System Status** panel. Whenever a status changes there, the pop-up window is updated. Clicking one of the status values brings up the main HP SIM window and the corresponding collection is displayed. For example, if you clicked the Major status value, the **All Major Systems** table view page is displayed. This window can be customized using the options for customizing the **System Status** panel. See “Customizing the System Status panel” for more information.

The following are error messages that might be displayed:

- HP Systems Insight Manager is not configured to display any status.
To resolve this issue, close the window, customize the display of the **System Status** panel, and re-launch.
- This window does not have a connection with the main HP Systems Insight Manager window.
To resolve this issue, close the window.



NOTE: The status panel pop-up window might not be displayed if you have a pop-up blocker configured and running on your system. You must disable the pop-up blocker or configure it to allow the HP SIM application to use pop-up windows.

NOTE: If HP SIM is configured to enable session timeout, the status pop-up window no longer displays the status when the session expires.

Utilizing RSS capabilities

Really Simple Syndication (RSS) is a data format based on eXtensible Markup Language (XML) that can be used by applications and websites to provide content to other applications. HP SIM uses RSS to publish **System Status** panel information that can be viewed in newsfeed programs.

RSS capabilities can be enabled in HP SIM by changing the *rssFeedEnabled* property in the `globalsettings.props`. By changing this value, you can view the **System Status** panel information in newsreaders and applications. Perform the following to enable RSS:

1. Stop the HP SIM service.
2. In the `globalsettings.props` file, set the *rssFeedEnabled* property to **True**. The file is located at:
 - **On Windows** It is typically located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`.
 - **On HP-UX and Linux** It is located at `/etc/opt/mx/config/globalsettings.props`.
3. Restart the HP SIM service.
4. Browse to `http://server_name:280/RSS` to view the XML output for the current HP SIM status values.

The URL in step 3 can be used in RSS readers to view the same data.

Related procedure

- ▲ [Customizing the System Status panel](#)

Related topics

- [Navigating the Home page](#)
- [Customizing the Home page](#)

Setting language locale

You can set the language or locale in your operating system, in a command shell, or in your web browser to English or Japanese and run HP Systems Insight Manager (HP SIM). Both the *Central Management Server* (CMS) and the managed systems must support all the desired languages. The language is used to present all the labels, menus, and status and error messages in HP SIM in the requested language. The *GUI* shown in your browser appears in the preferred language of the web browser. Also, tools and tasks executed interactively through the CMS have the same language used as the language the tool command line is executed with on the target system. This enables your web browser to run tools, create scheduled tasks, and manually run scheduled tasks in the preferred language. Likewise, the language setting of your command shell is forwarded through the `mxexec` and `mxtask` command line commands to set the language for executing a tool, manually executing a task, or creating a scheduled task when the command line for the tool is executed on the target systems.

The CMS also has another locale independent from any user sessions (see “Configuring HP SIM”), the CMS Locale. Some of the features inherit this locale, such as logging files and e-mail messages sent by Automatic Event Handling, which are neutral from any session.

Setting the web browser language or locale

When you configure your web browser and select the language you prefer, the HP SIM GUI displays the date and time in the language requested by the browser, although the overall HP SIM GUI is displayed in English or Japanese. The browser locale is also used to set the language and encoding in the *Secure Shell* (SSH) command shell in which the tool command executes. The browser locale is saved on a scheduled task when it is created and is used to set the language and encoding on the target system for *Single-system Aware (SSA)* tools and on the execution system for *Multiple-system Aware (MSA)* tools. When you manually execute a task, the current browser locale overrides the locale set in the scheduled task for this single manual execution of the task (for SSA and MSA tools).

Configuring the language settings in Internet Explorer for Japanese

To set the preferred language settings to Japanese in Internet Explorer:

1. Select **Tools**→**Internet Options**→**[Languages]**. The **Language Preference** window appears.
2. Click **Add**. The **Add Language** window appears.
3. Select **Japanese** from the list.
4. Click **OK** to add it to the language preference list.
5. Select **Japanese** in the language preference list and click **Move Up** until it is at the top of the list, or select and remove any other languages listed here.
6. Click **OK**. Continue to click **OK** until you have closed all windows.

Configuring the language settings in Mozilla for Japanese

To set the preferred language setting to Japanese in Mozilla:

1. Select **Edit**→**Preferences**. The **Preferences** window appears.
2. In the **Category** list on the left, select and open the **Navigator** dropdown list and select **Languages**. The **Languages** view appears on the right.
3. Click **Add**. The **Add Languages** window appears.
4. Select **Japanese** from the list.
5. Click **OK** to add it to the language preferences list.
6. Select **Japanese** in the language preferences list and click **Move Up** until it is at the top of the list, or select and remove any other languages listed here.
7. Click **OK** to save preferences and close the window.

Configuring the language or locale settings in Windows

To install and run HP SIM in Japanese mode, you must first set the **Locale** for the current user to **Japanese**. See “Configuring Windows XP language settings for Japanese” or “Configuring Windows 2000 locale settings for Japanese” for more information. After you have completed these steps, install HP SIM and it will run in Japanese language mode. For more information about installing HP SIM, see the HP SIM user guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>, and then select the appropriate guide for your operating system.

Configuring Windows XP language settings for Japanese

1. Select **Start**→**Control Panel**→**Regional and Language Options**→**Advanced**.
2. Under **Language to use for non-unicode programs**, select **Japanese**.
3. Click **Apply** to apply changes.
4. Reboot the system.

After rebooting the system, open a command prompt window and execute the `chcp 932` (Japanese) and `chcp 437` (English) to toggle between the two languages. The HP SIM CLI commands use the Code page to determine what locale and encoding to output, as do the Command Prompt commands, such as `dir`.

Configuring Windows 2000 locale settings for Japanese

1. Select **Start**→**Settings**→**Control Panel**→**Regional Options**→**General**.
2. Click **Set default**. The **Select System Locale** window appears.
3. From the dropdown list, select **Japanese**.
4. Click **OK**.
5. Click **Apply**.
6. Reboot the system.

After rebooting the system, open a command prompt window and execute the `chcp 932` (Japanese) and `chcp 437` (English) to toggle between the two languages. The HP SIM CLI commands use the Code page to determine what locale and encoding to output, as do the Command Prompt commands, such as `dir`.

Configuring HP-UX and Linux language settings

Ensure that support for the desired languages and character map encodings are installed on the managed systems (for SSA tools) and execution system (for MSA tools, usually the CMS). To verify the language settings, execute:

```
locale -a
```

to see if the language and character map encodings you need are listed. Furthermore, if you want to run command tools of the *x-window* command type, ensure that the X Display you select to display the X-Window application has been configured to use the font lists required for that application and the requested language. For Motif X Window applications (X clients), it might be enough to have the Common Desktop Environment (CDE) configured for the language you want to display. It should have all the X11 resource file properties for X11 Motif or Gnome widget set font lists configured with fonts that support the language and encoding you want to use (for example, Japanese and SJIS), or you must configure the X resource file of your X clients to set the specific font lists you want to use for each application. This process usually means running `xlsfonts` to find out what fonts are installed, knowing what languages the X application supports, seeing how the application sets fonts in its `app-defaults` file, and then editing the X Resource file properties on the X clients to configure the application font list properties.

Configuring HP SIM

HP SIM has a configuration file that can be modified to override locale settings that control:

- **CMS locale** The *locale* of the CMS, which affects the language used in the CMS logs and e-mails sent by Automatic Event Handling tasks
- **Target locale** The *locale*, *character map encoding*, *code page*, and *LANG* variables used when executing a command on a remote system through SSH

This configuration file is `globalsettings.props` and is located:

- **On Windows** `C:\ProgramFiles\HP\System Insight Manager\config\globalsettings.props`.
- **On HP-UX and Linux** `/etc/opt/mx/config/globalsettings.props`.

CMS locale

By default, the CMS Locale is determined by the environment. On an HP-UX CMS, it looks for "`LANG=`" in "`/etc/rc.config.d/LANG`" and uses that setting. On a Linux CMS, it looks for "`LANG=`" in "`/etc/sysconfig/i18n`" and "`/etc/sysconfig/language`" and uses that setting. On a Windows CMS, it uses the default locale setting of the Java™ Virtual Machine, which is based on the locale setting of the user account used to install HP SIM.

If the locale used by the CMS is not the desired locale, you can manually edit `globalsettings.props` and add a line, such as `CMSLocale=en_US`, or whatever locale you want to override the CMS locale.

Target locale

For HP SIM, the character map encoding for a locale might be different for each target operating system and each language. To enable HP SIM to select the encoding to use for each target system (for SSA tools)

or each execution system (for MSA tools, usually the CMS), HP has defined the format of some properties that can be added to the `globalsettings.props` file. These properties provide the character map encoding to use for each language on each operating system, what Code Page code to use for each language on a Windows target and execution system, and the string that defines that encoding in the `LANG` environment variable on a Linux or HP-UX system. Also, some properties define what to use for unsupported languages on each operating system. The format of the property names are:

```
"TargetCharacterMapEncoding_" + language + "_" + os_name + "=" + encoding
"TargetCodePage_" + language or encoding + "_" + os_name + "=" + code page
number "TargetLangEncoding" + encoding + "_" + os_name + "=" + encoding string
```

where *language* is the two-character code for a language, *os_name* is the uppercase keyword for the supported operating system (for example, LINUX, HPUX, WINNT), and *encoding* is the canonical name for character map encoding for that language on the operating system. The supported names can be found in column 2 of the web page <http://java.sun.com/j2se/1.4.2/docs/guide/intl/encoding.doc.html>.

The entries look like:

```
TargetCharacterMapEncoding_ja_LINUX=EUC_JP
TargetCharacterMapEncoding_??_LINUX=ISO8859_1-
TargetCharacterMapEncoding_ja_HPUX=SJIS
TargetCharacterMapEncoding_??_HPUX=ISO8859_1
TargetCharacterMapEncoding_ja_WINNT=SJIS
TargetCharacterMapEncoding_??_WINNT=ISO8859_1
TargetCodePage_ja_WINNT=932
TargetCodePage_??_WINNT=437
```

For the Windows target and execution systems, these properties are used to choose the `chcp` command to execute in the SSH command prompt shell, to force the language and encoding to set to execute the Windows command line command. For example:

```
chcp 932 (forces the language to Japanese Shift-JIS)
chcp 437 (forces the language to US English with at least ISO-8859-1 support)
```

For Linux and HP-UX target and execution systems, the encoding is used with the locale to define the `LANG` environment variable to be defined in the SSH environment on the target and execution systems. Example values can be found by executing the `locale -a` command on these operating systems. For example:

```
LANG=en_US.iso88591
(US English language, ISO-8859-1 encoding on HP-UX)
LANG=ja_JP.SJIS
(Japanese language, Shift-JIS encoding on HP-UX)
LANG=ja_JP.eucjp
(Japanese language, EUC-JP encoding on Linux)
LANG=en_US.utf8
(US English language, UTF-8 encoding on Linux)
```

Using command line interface commands

HP Systems Insight Manager (HP SIM) provides a *command line interface* (CLI) in addition to the *GUI*. Many functions available in the GUI are also available through the CLI.

HP SIM commands are installed in the following locations on the Central Management Server (CMS):

- **HP-UX and Linux:** `/opt/mx/bin/`
- **Windows:** `C:\Program Files\HP\System Insight Manager\bin\`



NOTE: The Windows path varies if HP SIM is not installed in the default location.

See the *Infrastructure management using the HP SIM command line interface* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> and the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more detailed information on CLI commands.

manpages

Viewing manpages on UNIX systems

You can use the `man` utility on HP-UX and Linux systems to format and display CLI command line usage manpages. Use the following format to specify a manpage to view: `# man [sectionNumber] ManpageName`.

HP-UX

- CLI command line usage manpages are specified as section 1M.
- CLI Extensible Markup Language (XML) usage manpages are specified as section 4.

Examples: To view the command line usage or XML usage for the `mxtask` CLI, enter one of the following:

- `% man mxtask` displays the command line usage for the `mxtask` CLI.
- `% man 1m mxtask` displays the command line usage for the `mxtask` CLI.
- `% man 4 mxtask` displays the XML usage for the `mxtask` CLI.

Linux

- CLI command line usage manpages are specified as section 8.
- CLI XML usage manpages are specified as section 4.

Examples: To view the command line usage or XML usage for the `mxtask` CLI, enter one of the following:

- `# man mxtask` displays the command line usage for the `mxtask` CLI.
- `# man 8 mxtask` displays the command line usage for the `mxtask` CLI.
- `# man 4 mxtask` displays the XML usage for the `mxtask` CLI.

Viewing manpages on Windows systems

The HP SIM Windows manpages are available in the following folder:

`Manager\hpwebadmin\webapps\mxhelp\mxportal\en\man`. Double-click a manpage file to view the contents in a web browser.

Commands

The following table provides a complete list of HP SIM commands. For a detailed explanation of these commands, click the manpage link to view an associated manpage or see the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>. Use your browser's back button to return to this page.



NOTE: In the following table, the manpage section numbers for CLI command line usage manpages are different for each operating system. The CLI command line usage manpage section number is 1M for HP-UX.

and Windows, and 8 for Linux systems. The CLI XML usage manpage section number is 4 for all operating systems.

Command	Functionality	Available manpages
mcompile	Compiles an <i>SNMP Management Information Base (MIB)</i> file into an intermediate format configuration (CFG) file for importing into HP SIM using the <code>mxmib</code> command.	mcompile(1M, 8)
mxagentconfig	Configures Secure Shell (SSH) on a managed system by copying the <i>Central Management Server</i> public key to a user's SSH key directory and then appending that key to the authenticated keys file. The user must be a valid SSH user on the managed system before running this command.	mxagentconfig(1M, 8)
mxauth	Enables <i>administrative rights</i> users to manage HP SIM authorizations.	mxauth(1M, 8) , mxauth(4)
mxcert	Creates a new certificate, imports a signed or trusted certificate, removes a certificate, lists certificates, generates a certificate signing request, notes whether to require trusted certificates, upgrades certificate from HP SIM 4.x, and synchronizes public certificate with the System Management Homepage share directory.	mxcert(1M, 8)
mxcollection	Adds, modifies, removes, and lists collections. Note: <code>mxcollection</code> XML file components and tags are case-sensitive.	mxcollection(1M, 8) , mxcollection(4)
mxexec	Executes HP SIM tools, with associated arguments, on specific HP SIM managed systems or system groups, verifies the status of running tools, and enables a administrative rights user to kill or cancel a running task.	mxexec(1M, 8)
mxgetdbinfo	Displays information about the HP SIM database.	mxgetdbinfo(1M, 8)
mxgethostname	Prints the name, IP address, or information about the local host in HP SIM.	mxgethostname(1M, 8)
mxglobalprotocolsettings	Manages global protocol settings from an XML file or the command line. This command lists global protocol settings in detailed or XML format.	mxglobalprotocolsettings(1M, 8) mxglobalprotocolsettings(4)
mxglobalsettings	Manages the global settings in HP SIM.	mxglobalsettings(1M, 8)
mxinitconfig	Performs initial configuration for the CMS. Note: For best performance, running <code>mxinitconfig</code> is not recommended after HP SIM is configured.	mxinitconfig(1M, 8)
mxlog	Logs an entry to the log file or standard out.	mxlog(1M, 8)
mxmib	Adds, deletes, and processes a list of <i>MIBs</i> for HP SIM and lists registered MIBs and traps for a specific registered MIB.	mxmib(1M, 8)
mxngroup	Enables you to create, modify, remove, and list system groups in HP Systems Insight Manager.	mxngroup(1M, 8) , mxngroup(4)
mxnode	Adds, modifies, identifies, removes, or lists systems in HP SIM.	mxnode(1M, 8) , mxnode(4)

Command	Functionality	Available manpages
mxnodesecurity	Adds, modifies, or removes security credentials for SNMP and <i>Web-Based Enterprise Management</i> (WBEM) protocols. Also verifies the certificate used for WBEM.	mxnodesecurity(1M, 8) , mxnodesecurity(4)
mxoracleconfig	Enables you to configure HP SIM to use an Oracle database. This command does not initiate the database.	mxoracleconfig(1M, 8)
mxpassword	Adds, lists, modifies, or removes passwords stored in HP Systems Insight Manager. The passwords are displayed in clear text for readability.	mxpassword(1M, 8)
mxquery	Adds, lists, modifies, or removes queries in HP Systems Insight Manager. Note: The use of categories in mxquery has been deprecated in favor of mxcollection. Using cat works for mxquery in this release, but you should use mxcollection for creating and manipulating collections (previously known as queries).	mxquery(1M, 8) , mxquery(4)
mxreport	Enables users with sufficient privileges to run reports and add, delete, and list reports and report categories.	mxreport(1M, 8) , mxreport(4)
mxstart	Starts the HP SIM daemons.	mxstart(1M, 8)
mxstm	Adds, removes, and lists System Type Manager rules.	mxstm(1M, 8)
mxstop	Stops the HP SIM daemons.	mxstop(1M, 8)
mxtask	Lists, executes, removes, creates, and changes ownership for HP SIM scheduled tasks using the command line or an external XML file.	mxtask(1M, 8) , mxtask(4)
mxtool	Enables you to add, list, modify, or remove HP SIM <i>tools</i> .	mxtool(1M, 8) , mxtool(4)
mxtoolbox	Enables administrative rights users to add, rename, describe, disable, enable, remove, and list HP SIM toolboxes.	mxtoolbox(1M, 8) , mxtoolbox(4)
mxuser	Adds, modifies, removes, or lists <i>users</i> in HP SIM. Enables you to assign authorizations for created users and user groups.	mxuser(1M, 8) , mxuser(4)
mxwbemsub	Enables you to add, list, delete, or move WBEM event subscriptions from systems managed by the CMS. This command requires access to a file that only allows administrative rights user access.	mxwbemsub(1M, 8)

Entering commands

Permissions

On an HP-UX or Linux CMS, you can log in to the operating system as any valid HP SIM user and use the CLI (not all CLI functionality is available to all users; some functions are only available to users with administrative rights or operator configuration rights on the CMS). On a Windows CMS, some commands require that the user be a member of the local Administrators group. This list includes:

- mxagentconfig
- mxauth
- mxcert

- mxcollection
- mxexec
- mxglobalprotocolsettings
- mxglobalsettings
- mxlog
- mxmib
- mxngroup
- mxnode
- mxquery
- mxreport
- mxstm
- mxtask
- mxtool
- mxtoolbox
- mxuser
- mxwbemsub

On a Windows CMS, if you are not a member of the local Administrators group, add the options `--user username` and `--pass password` when running any of the listed CLI commands. For example, to list information about one or more authorizations in compact or table form, enter `mxauth [-lt] --user username --pass password`.

On a Linux or HP-UX CMS, you can add the options `--user username` and `--pass password` to a command to run it under a different account from the one that is signed-in. For example, if you have operator rights, and you want to remove multiple authorizations by specifying an input file, which requires administrative rights, enter `mxauth -a|r -f filename --user username --pass password` and use the sign-in information of a administrative rights user.

Quotation marks

When you enter a CLI command with a string that includes spaces or special characters, you must enclose the string in quotation marks. For example: `mxreport -l -x report -n "Inventory - Servers"`.

Related topics

- [Signing in](#)
- [Signing out](#)

Resource library

This section provides HP Systems Insight Manager (HP SIM) documentation links to help you perform tasks, troubleshoot problems, learn more about various features, and more.

- **Automating Software Maintenance in an HP Environment**

See the *Automating Software Maintenance in an HP Environment* white paper at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Changing the HP SIM system name**

See the *Changing the HP SIM 5.x system name* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Compiling and Customizing SNMP MIBs with HP SIM**

See the *Compiling and customizing SNMP MIBs with HP SIM* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **Configuring or Repairing Agents**
For more information, see “Configuring or repairing agents”.
- **Creating custom tool definition files for HP SIM**
See *Creating custom tool definition files for HP SIM* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Deploying HP SIM on MSCS Clusters**
See the *Deploying HP SIM 5.x on MSCS Clusters* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Getting Started with HP SIM 5.0 in a smaller Windows environment**
See the *Getting started with HP SIM in a smaller Windows environment* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Installing the System Management Homepage individually (without using HP SIM)**
See the *System Management Homepage Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
- **Installing version control individually (without using HP SIM)**
See the *HP Version Control Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.
- **Installing and using the HP ProLiant Essentials HP Performance Management Pack Data Migration Tool**
See the *HP ProLiant Essentials Performance Management Pack Data Migration Tool Installation and User Guide* at <http://www.hp.com/products/pmp>.
- **Installing HP SIM**
See the HP SIM user guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>, and then select the appropriate guide for your operating system.
- **Using the HP SIM command line interface**
See the *.HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Learning more about the ProLiant or Integrity Support Packs**
 - To read about the HP ProLiant Support Pack, see <http://h18013.www1.hp.com/manage/psp.html>.
 - To download the HP ProLiant Support Pack, see <http://www.hp.com/servers/swdrivers>.
 - To download the Integrity Support Pack, see <http://www.hp.com/support/itaniumservers>.
- **Learning more about the ProLiant Remote Deployment Utility**
To read about the ProLiant Remote Deployment Utility, see <http://h18013.www1.hp.com/manage/rdp.html>.
- **Managing WBEM Event Subscriptions for HP-UX Systems with HP SIM**
See the *WBEM subscriptions in HP SIM* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Managing HP servers through firewalls with HP SIM**
See the *Managing HP servers through firewalls with HP SIM 5.x* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Manually Migrating to HP SIM**
See the *Migrating from Insight Manager 7 to HP SIM 4.2* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- **MIB Support - Out of the Box**
See the *HP Insight Management MIB update kit for HP SIM* at http://h18013.www1.hp.com/products/servers/management/hpsim/dl_windows.html#windows.
- **Moving HP SIM to a new system**
See the *Moving HP SIM 5.1 to a new Windows system* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Receiving HP driver, support, and security alerts, plus software updates customized to your HP products**
See <http://www.hp.com/go/subscribe-gate1>.
- **Setting up managed systems**
See "Setting up managed systems".
- **Technical documentation**
See *Technical documentation* at <http://docs.hp.com/en/index.html>.
- **Transitioning to HP SIM**
See the *Migrating from Compaq Insight Manager (WIN32) to HP SIM* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Understanding HP SIM Security**
See the *Understanding HP SIM 5.0 security* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Using the HP ProLiant Essentials Server Migration Pack**
See the *HP ProLiant Essentials Server Migration Pack User Guide* at <http://www.hp.com/products/pmp>.
- **Using Secure Shell (SSH) in HP SIM**
See the *Secure Shell (SSH) in HP SIM 5.x* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Using HP OpenView**
See the *HP SIM 5.1 and HP OpenView Select Access* white paper at <http://h18000.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Using HP SIM with HP StorageWorks Management Software**
See the *Using HP Systems Insight Manager with HP StorageWorks Management Software* white paper at <http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00057439/c00057439.pdf>.
- **Viewing the entire HP SIM Online Help System in a PDF**
See the *HP Systems Insight Manager 5.2 User Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Viewing the HP SIM Read Me file online**
See the *HP SIM Readme* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.
- **Viewing the entire System Management Homepage Online Help in a PDF**
See the *System Management Homepage Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Viewing the entire HP Version Control Agent Online Help in a PDF**

See the *HP Version Control Agent Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- **Viewing the entire HP Version Control Repository Manager Online Help in a PDF**

See the *HP Version Control Repository Manager Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

Related topics

- Troubleshooting
- Getting started
- Partner applications

5 Discovery and identification

Discovery is the process of finding systems in the management domain so that they can be managed from the Central Management Server (CMS) by HP Systems Insight Manager (HP SIM).

There are two types of discovery:

- **Automatic discovery** The process that HP SIM uses to find and identify systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status. The primary source for automatic discovery is ping sweeps configured in the automatic discovery tasks page. Other sources might include receiving events from unknown systems or from a management processor that has information about a server. Identification automatically runs on discovered systems.
- **Manual discovery** Manual discovery is the process that enables you to bypass a full automatic discovery and add single or multiple systems to the database, create or import the HP SIM database hosts file, and create or import a generic hosts file.

You can only perform discovery if you have *administrative rights*.

Automatic discovery

The option **Automatically discover a system when an event is received from it** is disabled by default, but can be enabled by selecting it in the **General Settings for All Discoveries** section. For discovery to run, you must enable the default System Automatic Discovery task by selecting **Options**→**Discovery**, selecting the default task, and then clicking **Enable**. HP recommends editing this task to ensure that the IP range is correct.

To access the **General Settings for All Discoveries** section, select **Options**→**Discovery**, click the **Automatic** tab, and then click **Configure general settings**. In the section, **Do this now to finish the installation**, on the introductory page, click **Automatic**, or from the **Manage** section of the **Homepage**, click **discovery**.

Alternatively, you can click **Edit**, instead of **Enable**, to edit and save the task. In the **Schedule** section, select **Automatically execute discovery every**, and then set the discovery time. If you disable automatic discovery, no new automatic discovery is performed until you enable automatic discovery by visiting the **Discovery** page and making your selections. You can also perform a manual discovery any time that you choose. See “Configuring automatic discovery” for more information about scheduling automatic discovery.

HP SIM performs *automatic discovery* using the *Internet Protocol* (IP).

Internet Protocol

HP SIM discovers systems running the IP when it pings systems in a listed range of addresses. It defaults to the local *subnet*, a range that corresponds to the IP addresses assigned to the system where HP SIM is running. You can change the address list to indicate other systems or segments of the network that you want HP SIM to discover.

Web Agents are not discovered unless HTTP is enabled on the **Global Protocol Settings** page in the **HTTP settings (default)** section. To enable HTTP, see “Setting global protocols” for information. To ensure that *clusters* are discovered in automatic discovery, the cluster IP address and all node addresses must be listed in the section, **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files**. To access the **Configuration** section, click the **Automatic** tab, and then click **New** for a new discovery task, or click **Edit** to edit an existing discovery task.

HP SIM uses a globally unique system identifier obtained from the system to help identify HP systems with multiple IP addresses. If no unique identifier can be obtained, the fully qualified *Domain Name Service* (DNS) names of the systems are used for each IP. To ensure systems are resolved, for each IP address, the fully qualified DNS names must match.

Event-based automatic discovery

Event-based automatic discovery is disabled by default. You can enable this feature by selecting **Automatically discover a system when an event is received from it**. Event-based automatic discovery

adds any systems that send *SNMP traps*, *WBEM* indications, or other *events* to HP SIM that do not have a matching IP address in the database. The option, **Ping exclusion ranges, templates, and/or hosts files**, allows the entry of any IP addresses that you want excluded from event-based automatic discovery. If SNMP is disabled on the **Global Protocols Settings** page under **Options**→**Protocol Settings**→**Global Protocol Settings**, then SNMP traps are ignored. If WBEM is disabled, WBEM indications are also ignored.



NOTE: With the exception of the SNMP Authentication Failure trap, all traps trigger an automatic discovery.

Discovery templates

Discovery templates are files that can be used by automatic discovery instead of typing addresses directly into the fields, **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files**. The templates can be used as a way to quickly change the scope of automatic discovery and are used each time discovery runs. To access the discovery template section, click the **Automatic** tab from the **Discovery** page and then click **Manage templates**.

For example, you can configure a discovery template with a broad range of addresses that are discovered infrequently when you want to issue a broad range ping. When necessary, the template can be used to input the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field of the **Edit Discovery** section. To access this section, select **Options**→**Discovery**, click the **Automatic** tab, and then click **Edit**. The templates also enable you to quickly change the scope of discovery without having to cut and paste addresses or manually reenter the ranges.

After creating a discovery template, to reference it in automatic discovery, enter `@template_name` in the fields **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** or **Exclusion ranges, templates and/or hosts files**. See “IP ranges” for more information.



NOTE: Because discovery now supports multiple schedules and configurations (ranges), the need for templates is significantly reduced. HP recommends that you leverage several different discovery schedules and configurations instead of using discovery templates.

NOTE: A single discovery template cannot include both included and excluded ranges. You must create a separate template for use in each field of automatic discovery. Template files cannot be nested, that is, a template file cannot contain another template file name through the `@template_name` reference.

When configuring automatic discovery, the format of a discovery template is the same as that used in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** and **Ping exclusion ranges, templates and/or hosts files**.

Access discovery templates by clicking **Manage templates** under the section, **For all automatic discoveries** section on the **Discovery** page. See “Managing discovery templates” for information about creating a discovery template file.

First discovery

You can start a discovery in the following ways:

- Execute discovery immediately from the **Discovery**→**Automatic** page, select the discovery task, click **Edit** to configure the discovery task for your environment, and then click **Run Now**. The discovery process starts immediately. The discovery progress is updated as the systems are discovered, until the discovery process is complete.
- Allow sufficient time for a complete discovery and *identification* to be performed. Times vary, depending on your network, bandwidth, and discovery settings. In most cases, the discovery process finds all systems by pinging the network.

Subsequent discoveries

You can run discovery any time from the **Discovery**→**Automatic** page. For subsequent discoveries, you can specify the subnets or systems to interrogate and the schedule to follow.

For the most comprehensive discovery and identification, always select SNMP, *Desktop Management Interface* (DMI), *Web-Based Enterprise Management* (WBEM), and HTTP as the protocols on the **Options**→**Protocol**

Settings→**Global Protocol Settings** page. Configure default community strings and WBEM passwords on the **Global Protocol Settings** page. See “Global protocols” for additional information.

Status indicators let you know when discovery is running, and the column, **Last Run**, displays **running**, the percentage of completion, the number of **pings attempted**, and the systems **processed**. A processed system is one in which the IP address has been either identified or found unresponsive. However, a processed system is not always added to the database.

Manual discovery

Manual discovery enables you to bypass a full discovery. With manual discovery, you can:

- Add a single system to the HP SIM database
- Add multiple systems to the HP SIM database through hosts files
- Create and import an HP SIM hosts file
- Import a hosts file that was created or exported from Insight Manager (WIN32); the hosts file automates the process of adding systems or restoring system information
- Create or import a generic hosts file to automate the process of adding systems or restoring system information
- Set up systems before they are physically connected to the network

The system is added to the database using the IP address as the system name. After the system is connected to the network and identification runs, the system name is updated with the system name instead of the IP address.

To access the manual discovery page by:

- Select **Options**→**Discovery** and click the **Manual** tab
- Click **Manual** in the **Do this now to finish the installation** section of the introductory page
- Click **discovery** in the **Manage** section of the **Home** page

Hosts files

Hosts files are used by manual discovery to manually add multiple *systems* to the HP Systems Insight Manager (HP SIM) *database*, and are usually used only one time to import systems. You can use an existing *hosts file*, a file created from the HP SIM database, or an HP SIM exported hosts file as the basis for adding systems. Typically, the file contains a listing of the names of systems, system IP addresses, and any alias names that are used for the system.

Importing the hosts file bypasses the need for immediate discovery. For example, in the case of a catastrophic system failure, you could import a backup hosts file as the basis for reconfiguring your management environment and automatically repopulating the database. Adding the systems using the hosts file utility does not replace systems in the database. For example, if a system listed in the hosts file has the same IP address as an existing system, the duplicate is ignored. Any systems that previously existed in the database are not modified.

You can import hosts files from the following sources:

- The HP SIM database, which imports the system data, creates a hosts file, and sorts the data types according to your selection
- Another system that has an existing hosts file

To create and manage hosts files, click the **Hosts Files** tab on the **Discovery** page.

Options for adding a single system

- Know the IP address or host name of the system. If you know at least one of these, HP SIM can find the other by validating the information with the *Domain Name Service* (DNS) for the network.
- To add a *cluster* and its nodes, enter each IP address separately.
- Decide if you want to set the *system type*, subtypes, or *Web-Based Enterprise Management* credentials as well as the product model.

- Specify the **Web-Based Enterprise Management Settings** for the system on the **System Protocol Settings** page. You can override the default user name and passwords by selecting **use values specified below** and entering appropriate user names and passwords.
- Specify the SNMP settings for this system to be unique or match the global discovery settings. The current system default settings are displayed. If you override the default and specify a different value, that community string must be supported on the system. If it is not and one of the defaults is supported, HP SIM reverts back to the default value. When manually adding a single system, you can modify the following settings:

timeout	The amount of time HP SIM waits for an SNMP response when it sends a request to the system. The default timeout value appears. If a response is not received within time interval, HP SIM might determine that the system does not support SNMP. Decreasing this value can cause increased network traffic because the rate of retry attempts is increased. Use caution when changing this value. A value of three seconds usually works for a LAN. However, if systems are connected through a WAN, try a higher value, for example, 10 seconds.
retries	The number of additional times after the first attempt is made to communicate with a system before the attempts stop.
community strings	A community string sets up authentication that enables or prohibits communication between the managed system and the CMS. The CMS community string of the must match the community string of the managed system. Use the read-only community string to read variables. Use the write community string to modify variables. Although only one community is valid for a communication attempt, a system can belong to multiple communities. However, HP SIM uses only one community string when communicating with a system.



NOTE: If an IP address is used to manually add a single system, it must be properly resolved to a system name for the name to be displayed in the GUI.

See “Adding a system manually” for the steps to add a single system to the database.

Related procedures

- [Configuring automatic discovery](#)
- [Configuring automatic discovery general settings](#)
- [Creating a new discovery task](#)
- [Editing a discovery task](#)
- [Disabling or enabling a discovery task](#)
- [Deleting a discovery task](#)
- [Running a discovery task](#)
- [Creating a new discovery template file](#)
- [Editing a discovery template](#)
- [Deleting a discovery template](#)
- [Adding a system manually](#)
- [Creating a new hosts file](#)
- [Editing a hosts file](#)
- [Deleting a hosts file](#)
- [Adding systems in a hosts file to the HP SIM database](#)

Related topics

- [Managing hosts files](#)
- [Managing discovery templates](#)
- [Identification](#)

- Discovery filters
- Data collection
- Status polling
- Protocols
- Discovery and identification

Configuring automatic discovery

When you access the **Automatic** tab on the **Discovery** page, a table displays a list of all available discovery tasks. You can configure multiple instances of discovery with each instance having its own schedule and set of inclusion ranges. When a discovery task is executed, the **Last Run** column is updated to display its progress, including the percentage of completion.

Automatic discovery and completion percentages are calculated by weighting two factors: the ping sweep (performed on each host) is 10% of the process; the system identification is 90% of the process. If no host is found on an IP address, the system identification is considered complete. For example, you have 100 hosts in your discovery range. If 50 hosts have been pinged, but only 10 identified, you have: $50/100 * .10 = 0.05$ (ping sweep) $10/100 * .90 = 0.09$ (identification) $0.05 + 0.09 = 0.14 * 100 = 14\%$ (total completed percentage).



NOTE: Only one discovery task can run at a time. If you select to run more than one discovery task, the percentage in the **Last Run** column remains at 0% until the currently running task is complete.

Under the **For all automatic discoveries** section, the following options are available:

- **Configure general settings** Used to configure settings that apply to all discovery tasks. See “Configuring automatic discovery general settings” for more information.
- **Manage templates** Used to manage discovery templates. See “Managing discovery templates” for more information.
- **Configure global protocol settings** Used to configure global protocol settings. See “Setting global protocols” for more information.

Note: To discover clusters correctly, SNMP must be enabled with the correct security settings on HP Systems Insight Manager (HP SIM) and running on the target systems.

Note: *Desktop Management Interface* (DMI) identification is only supported on Windows and HP-UX-based *Central Management Server* (CMS) installations and only like operating systems are identified. For example, a Windows-based CMS identifies only Windows-based DMI systems, and an HP-UX-based CMS identifies only HP-UX-based DMI systems.

From the **Automatic** tab, you can also:

- **Create a new discovery task** Click **New** and the **New Discovery** section appears. See “Creating a new discovery task” for more information.
- **Edit an existing discovery task** Select a task from the table, and click **Edit**. The **Edit Discovery** section appears. See “Editing a discovery task” for more information.
- **Enable or disable a discovery task** Select a task and click **Disable** to disable the schedule of an enabled task. If a task is disabled, the button changes to **Enable**. To resume automatic execution of the task, click **Enable**. See “Disabling or enabling a discovery task” for more information.
- **Delete an existing discovery task** Select a task from the table and click **Delete**. See “Deleting a discovery task” for more information.
- **Run a discovery task** Select the task you want to run and click **Run Now**. When a task is running, the **Run Now** button changes to a **Stop** button. See “Running a discovery task” for more information.



NOTE: Two discovery tasks cannot be running at the same time. The second task displays 0% completion until the first task is completed.

- **Stop a discovery task from running** Select the running task and click **Stop**. See “Running a discovery task” for more information.
- **View HP Storage Essentials discovery status** When HP Storage Essentials is installed, its discovery status is displayed with a link to the HP Storage Essentials discovery log.
- **Configure HP Storage Essentials global application settings** When HP Storage Essentials is installed, the **Automatic** tab includes a link to the HP Storage Essentials global application settings configuration page.

Related procedures

- Configuring automatic discovery general settings
- Creating a new discovery task
- Editing a discovery task
- Disabling or enabling a discovery task
- Deleting a discovery task
- Running a discovery task
- Creating a new discovery template file
- Editing a discovery template
- Deleting a discovery template
- Setting global protocols

Related topics

- Discovery and identification
- Managing discovery templates
- IP ranges

Creating a new discovery task

HP Systems Insight Manager (HP SIM) ships includes one default discovery task (System Automatic Discovery). However, you can create a new discovery task to discover specific systems. For example, if you want to discover systems in a specific IP address range. You can set the task to run at scheduled times using specific ping inclusion ranges, templates, or hosts files.

To create a discovery task:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. To create a new discovery task, click **New**. The **New Discovery** section appears.

New Discovery

Required field *

Name: *

Schedule:

Automatically execute discovery every:

days PM

Ping *inclusion* ranges, system (hosts) names, templates, and/or hosts files:

3. In the **Name** field, enter a name for the task. This field is required.
4. In the **Schedule** section, select **Automatically execute discovery every**, and then enter how often the task should run. The default frequency, is once per day. If you clear the **Automatically execute discovery every** option, the task is disabled after it is created.
5. In the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field, specify the IP addresses to include for pinging. If you want to use this task to discover SMI-S *storage systems*, include the IP address of each *SMI CIMOM*. You can also enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. See "IP ranges" for more information about entering IP ranges. To use an existing hosts file, enter the hosts file name in the following format: `$HostsFileName`.

If a hosts file is used, only the systems that are accessible and match the discovery filter criteria are added to the database.

6. To save the task, click **OK**, or to close the **New Discovery** section and not save any settings, click **Cancel**.

Note: If you have selected a large number of systems, the following message appears, stating The automatic discovery task is configured with a large number of addresses: [NUM]. Click **OK** to continue, or click **Cancel** to change the IP address range.

Note: The **OK** button is disabled until you enter text in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** box.

Creating an automatic discovery task using the command line interface

Users with *administrative rights* can use the `mxtask` command to create an automatic discovery task from the command line interface (CLI).

See "Using command line interface commands" for information about accessing the manpage.

Related procedures

- Configuring automatic discovery general settings
- Editing a discovery task
- Disabling or enabling a discovery task
- Deleting a discovery task
- Running a discovery task

Related topics

- Discovery and identification
- IP ranges

Editing a discovery task

When editing an existing discovery task, because all fields are prepopulated with existing information, you can edit only the fields that you want to edit.

To edit an existing discovery task:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the task to be edited and then click **Edit**. The **Edit Discovery** section appears.
3. In the **Name** field, enter a name for the task. This field is required.
4. In the **Schedule** section, select **Automatically execute discovery every**, and then enter how often the task should run. The default frequency, is once per day. If you clear the **Automatically execute discovery every** option, the task is disabled after it is created.
5. In the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field, specify the IP addresses to include for pinging. If you want to use this task to discover SMI-S *storage systems*, include the IP address of each *SMI CIMOM*. You can also enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. See “IP ranges” for more information about entering IP ranges. To use an existing hosts file, enter the hosts file name in the following format: `$HostsFileName` .

If a hosts file is used, only the systems that are accessible and match the discovery filter criteria are added to the database.

6. To save the task, click **OK**, or to close the **New Discovery** section and not save any settings, click **Cancel**.

Note: If you have selected a large number of systems, the following message appears, stating The automatic discovery task is configured with a large number of addresses: [NUM] . Click **OK** to continue, or click **Cancel** to change the IP address range.

Note: The **OK** button is disabled until you enter text in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** box.

Related procedures

- [Configuring automatic discovery general settings](#)
- [Creating a new discovery task](#)
- [Disabling or enabling a discovery task](#)
- [Deleting a discovery task](#)
- [Running a discovery task](#)

Related procedures

- [Discovery and identification](#)
- [IP ranges](#)

Disabling or enabling a discovery task

You can disable or enable an existing discovery task.

If you disable a task, the **Schedule** column displays a message that the task is disabled. You might want to disable a task if you know your network is not going to change, or if you want to limit network traffic.

If a task is enabled, the **Schedule** column displays the schedule for the task.



NOTE: Manually running a disabled task by selecting the task and then clicking **Run Now** does not enable the task for future discoveries.

To disable or enable a discovery task:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the task to disable or enable.
3. Click **Disable** to disable a task, or if the task is already disabled, click **Enable** to resume the automatic execution of a task.

Related procedures

- Configuring automatic discovery general settings
- Creating a new discovery task
- Editing a discovery task
- Deleting a discovery task
- Running a discovery task

Related topics

- ▲ Discovery and identification

Deleting a discovery task

You can delete *discovery* tasks that are no longer necessary. You cannot delete the **Default Discovery** task. If you select the **Default Discovery** task, the **Delete** button is disabled.

To delete a discovery task:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the tasks to delete, and then click **Delete**. A confirmation box appears.
3. To delete this task, click **OK**, to cancel the deletion process, click **Cancel**.

Related procedures

- Configuring automatic discovery general settings
- Creating a new discovery task
- Editing a discovery task
- Disabling or enabling a discovery task
- Running a discovery task

Related topics

- Discovery and identification
- IP ranges

Running a discovery task

You can manually select and run any existing *discovery* task at any time. For example, if you add a new system that has not been discovered, you can manually run a discovery task to discover and begin managing the system. You can also stop a task that is running.

To run or stop a discovery task:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. Select the discovery task that you want to run, and then click **Run Now**. The task runs immediately.

The **Run Now** button changes to **Stop** when a task is running. To stop a task, select the task and click **Stop**.

Related procedures

- Configuring automatic discovery general settings
- Creating a new discovery task
- Editing a discovery task
- Disabling or enabling a discovery task
- Deleting a discovery task
- Creating STM rules

Related topics

- Discovery and identification
- IP ranges

System types

There are many different *system types* in HP Systems Insight Manager (HP SIM). All of these types are available on the **General Settings for All Discoveries** page, with the exception of clusters, complexes, racks, and enclosures. These types are not listed because they are not discovered directly. For example, a cluster is typically discovered through a cluster node. If you enable discovery filters and select some system types, HP SIM attempts to discover systems that fit those types the next time *automatic discovery* run. The following is a list of system types recognized by HP SIM during discovery.

- **Application** An application references an application running on a server. HP SIM currently does not create systems of this type, but HP SIM or an HP Essential might do so in the future.
- **Cluster** A cluster is a virtual computer usually made up of several servers clustered together with special software. Clusters are typically part of a fault-tolerant configuration. If a system is expected to be a cluster but not identified as such, ensure that the agents are properly configured on the cluster nodes and that it is a supported cluster environment.
- **Complex** Computer systems that support multiple hardware partitions are referred to as a complex. For example, the HP Integrity Superdome systems support multiple hardware partitions within a single complex.
- **Desktop** A small computer system typically located at a user's desk.
- **Enclosure** A physical container for a set of blades servers. An enclosure contains a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the processor and server power supplies.
- **Environmental Monitor** A device that monitors the environment around a system, rack, or other hardware component. These systems typically monitor temperature, the presence of smoke, and security.
- **Handheld** A Personal Digital Assistant (PDA) or small computer that fits in your hand.
- **Hub** Also called a *repeater*, this simple device is used to extend the number of ports available on the network.
- **KVM switch** A keyboard, video, and mouse switch that is used to enable a single keyboard, video monitor, and mouse to be shared by multiple systems that can be network-enabled.
- **Management Processor** Usually a small firmware-based system that is embedded in a server or other server-related hardware (such as an enclosure), and typically provide only management capabilities. The Integrated Lights-Out (iLO) card is an example of a management processor.
- **Notebook** A computer that is portable.
- **Partition** Certain systems and operating environments can be flexibly configured into partitions, each of which can run a separate instance of the operating system. Partitions provide protection that prevents software errors in one partition from interfering with another partition. Server systems that allow hardware partitions can also keep hardware errors from interfering with another partition.
- **Power Distribution Unit** A device that provides power to multiple systems in a rack, and can remotely control powering systems on or off.
- **Power supply** A device that supplies power to the servers on your network.
- **Printer** A device typically attached to the network that is used for printing.
- **Rack** A nonaddressable piece of hardware used to house servers, enclosures, or networking equipment. A rack created by HP SIM usually contains several enclosures.
- **Resource Partition** Set by users through the RPM Package Manager. This partition is limited to specific resource quantities and rules that allow the dynamic reallocation of processors and memory.
- **Remote Access Device** A device used to enable remote users to dial into an intranet through a phone line or over a LAN to an intranet.

- **Router** A networking device used to route network packets.
- **Server** A computer on a network that is dedicated to a particular purpose. For example, saving files, running print jobs, or housing a database server.
- **Shared Resource Domain** A collection of compartments, all of the same type, that share system resources. The compartments can be npars, vpars, psets, or fss groups.
- **Storage Device** A disk drive array that usually supports RAID levels and is accessed over a Fibre Channel Storage Area Network (SAN).
- **Switch** A network device, similar to a router, that uses hardware-based switching technology to route packets quickly on the network.
- **Tape library** A storage device that contains one or more tape drives, usually for backup purposes.
- **Thin client** A remote system connecting to a terminal server, which is a computer that has no disk or local storage and enables you to connect through terminal server packages to a central server or remote desktop.
- **Uninterruptible Power Supply (UPS)** A battery backup that provides power for servers or other computers.
- **Unknown** In HP SIM, Unknown is a status indicating that none of the built-in or System Type Manager (STM) based tasks could identify the system. However, some management protocol was detected on the system. Servers might be listed as Unknown for the following reasons:
 - You must be able to ping the system from the server where HP SIM is running. You can issue the ping command from a command or terminal window, or you can ping from HP SIM by selecting the unknown server, selecting the **Diagnose** and **Ping** options, and then following the on-screen instructions.
 - Try running the Configure or Repair Agents settings tool located in the **Configure** menu.
 - If the system supports SNMP, it might be that the type is new or is a third-party system that is not identified by default. See “Global protocols” and “System tab” for more information. You can use the System Type Manager (STM) tool to add a new type. See “Creating STM rules” for more information.
 - Community strings in HP SIM must match the ones used for the remote device. Ensure that HP SIM and the systems to be identified are using the same community string. Note that community strings are case-sensitive. From HP SIM, select **Options**→**Protocol Settings**, and then select **Global Protocol Settings** or **System Protocol Settings** to change the community strings.
 - In Windows NT and Windows 2000, one community name on the system must be set to *Read Create*. You are not required to use this community string in HP SIM (a community string set to *Read* is all that is required). The Management Agents connect to themselves using *Simple Network Management Protocol* and require one string set to *Read Create*.
 - The HP SIM system must be allowed to make SNMP requests to the managed systems. Ensure that the *Simple Network Management Protocol* security settings are not preventing these requests. In Windows NT and Windows 2000, ensure that the **Allow SNMP packets from any host** is selected, or that the address of the HP SIM server is in the list of allowed hosts.
 - If you are using IP-specific security, *localhost (127.0.0.1)* must also be allowed to make SNMP requests to the host. The *localhost* entry enables the Management Agents to connect to themselves using SNMP.
 - The ProLiant Management Agents must be installed and running properly on the ProLiant servers you are managing. For Windows systems, look at the Event Log to verify that the Management Agents are running (you should see a few *Agents started* messages and no errors).
 - Routers and switches in the network must allow SNMP traffic to pass on UDP port 161 or 162.
- **Unmanaged** A system type that was found with an IP address, but without any detected management protocols. If this is not the expected type, ensure that the *Web-Based Enterprise Management* user name and password, or the SNMP community name, is correct. Install agents if possible (for example, for

Windows, install the Initial ProLiant Support Pack). See “Initial ProLiant Support Pack Install” for information about installing the Initial ProLiant Support Pack.

- **Virtual Connect Domain** The system that represents the virtual connect configuration and is used to manage virtual connect information and licensing.
- **Workstation** A high-end personal computer system that is sometimes used for graphics or other design work.

System discovered by HP SIM

The table below lists systems that can be discovered by HP Systems Insight Manager (HP SIM) along with the prerequisites required for each.

HP BladeSystem Integrated Manager systems discovered by HP SIM

Pre-requisites for systems to be managed by HP BladeSystem Integrated Manager in HP Systems Insight Manager:

- SNMP agents running on the system, which must be the Insight Management Agents
- HP ProLiant Support Pack installed on all supported blades
- Latest supported firmware version on all the Integrated Lights-Out (iLO)s and Onboard Administrator
- Latest supported firmware on all switches

Prerequisites for Consolidated Client Infrastructure (CCI) to be managed by HP BladeSystem Integrated Manager in HP Systems Insight Manager:

- The *Windows Management Instrumentation* (WMI) proxy configured in HP SIM
- *Web-Based Enterprise Management* (WBEM) and SMI-S installed on the system
- WBEM credentials supplied in HP SIM

HP ProLiant BL465c	HP ProLiant BL685c	HP ProLiant BL6460c
HP ProLiant BL448c G1c	HP ProLiant BL860c	HP ProLiant BL680c
HP ProLiant xw460c	Cisco Catalyst Blade Switch 3020 for HP c-Class BladeSystem	GbE2c Ethernet Blade Switch for HP
HP 1Gb Ethernet Pass-Thru Module for HP c-Class BladeSystem	Fibre Channel Switch for HP c-Class BladeSystem	4x DDR IB Switch
HP 1Gb VC-Enet	HP StorageWorks SB40c for HP c-Class BladeSystem	HP StorageWorks TapeBlade
AiO SB600c Storage	ProLiant BL20p /G2/G3/G4	ProLiant BL30p
ProLiant BL35p	ProLiant BL40p	ProLiant BL45p G1/G2
la64 hp server BL 60p	ProLiant xw25p Blade Workstation	ProLiant BL25p G1/G2
Brocade 4GB SAN Switch for HP p-class Blade system	McDATA 4GB SAN Switch for HP p-class Blade system	HP ProLiant BL p-Class F-GbE Interconnect Switch x
HP ProLiant BL p-Class C-GbE2 Interconnect Switch y	Integrated Lights-Out	Integrated Lights-Out 2 (iLO 2)
ProLiant BL e-Class Integrated Administrator	BladeSystem c7000 Onboard Administrator	HP ProLiant BL1000
HP ProLiant BL1500	HP ProLiant BL2000	HP ProLiant BL2500
ProLiant BL 10e	ProLiant BL 10e G2	HP ProLiant BL1000
HP BladeSystem e-Class/CCI		

Storage devices discovered by HP SIM

For information on the prerequisites for these systems, go to <http://h18006.www1.hp.com/storage/smispviders.html>.

StorageWorks XP

StorageWorks XP128

StorageWorks XP1024

StorageWorks XP10000	StorageWorks XP12000
StorageWorks XP48	StorageWorks XP512
StorageWorks XP 2400 (Kodiak)	

StorageWorks VA

StorageWorks VA7100	StorageWorks VA7110
StorageWorks VA7400	StorageWorks VA7410

StorageWorks EVA

StorageWorks EVA3000	StorageWorks EVA5000
StorageWorks EVA4000	StorageWorks EVA6000
StorageWorks EVA8000	

StorageWorks MSA

MSA1000	MSA1500
MSA 1500 active/active	MSA 1510i
MSA1000 active/active	MSA 1500cs
500 G2 Modular Smary Array	iSpitfire
ThunderBolt	

StorageWorks Tape Library

EML	ESLE
ESL 9xxx	EML E-series (AG104A, et al)
ESL E-series (AA934B, et al)	MSL 5xxx
MSL 6xxx	MSL 6000 Series (AD609A, et al)
MSL 4048	

EMC Array

Symmetrix DMC 800	Symmetrix DMC 1000
Symmetrix DMC 2000	Symmetrix DMC 3000
Symmetrix 3xxx	Symmetrix 5xxx
Clariion CX200	Clariion CX300
Clariion CX400	Clariion CX500
Clariion CX600	

HDS Array

9200	9920-E
9500V	9960
9970V	9980V

StorageWorks EVA

4000	6000
8000	4100
6100	8100

Network Appliance NAS

Netapp FASxxx	
---------------	--

StorageWorks NAS

DL310-SS	DL380G4-SS
DL58x-SS	ML310-SS
ML35x-SS	ML370-SS
NAS 2xxx/4xxx/9xxx	

Fibre Channel

394757-B21 and 394588-B21 (Mezzanine)	A5158A
A6795A	A6826A
A7298A	A7387A
A7388A	A9782A
A9784A	FCA2101
FCA2214	FCA2214DC
FCA2355	FCA2404 (AB232A)
FCA2404DC	FCA2408
A7538A	A7560A
AB378A	AB379A
AB465A	AB466A
AB467A	FC1142 (AE311A)
FC1242 (AE312A)	FC2142SR (A8002A)
FC2242SR (A8003A)	FCA2684
FCA2684DC	AB378A
AB379A	FC1143 (AB429A)
FC1243 (AB379A)	FC2143 (AD167A)
FC2243 (AD168A)	Q2300
FCA2257P	FCA2684
FCA2684DC	

Obtaining, installing, and configuring providers and agents

- **Web-Based Enterprise Management (WBEM)** An Industry initiative to provide management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM client applications.

For HP-UX, WBEM is included in the operating system install. For Linux Itanium Processor Family (IPF), WBEM must be manually installed. Go to the HP Software Depot (<http://www.software.hp.com/>) to download. The WBEM download from the openPegasus website does not include the hardware specific data for HP SIM to manage Linux x86 systems.



NOTE: *Windows Management Instrumentation* (WMI) is the implementation of WBEM from Microsoft. See *WMI* for more information.

To install the HP Insight Management WBEM Provider, which is an HP extension of WBEM providers for managing ProLiant systems running Windows 2003, from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install WBEM/WMI Provider (HP Insight Management WBEM Provider) for Windows** .



NOTE: The WBEM providers cannot be installed on HP-UX or Linux systems.

NOTE: A Common Information Model Object Manager (CIMOM) acts as the interface for communication between WBEM providers and management applications such as HP SIM.

The CMS must have the correct credentials to authenticate to WBEM and WMI. There are two ways to authenticate HP SIM to a client:

- Basic authentication to WBEM Services or WMI using user name and password.
- Using the CMS certificate to authenticate is available only for HP-UX WBEM Services 02.05.00, which supports client certificate authentication. Use the Configure or Repair Agents **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system** option to deploy a WBEM certificate to the managed system and is only valid for HP-UX systems.
- **WMI** An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled.

The WMI Mapper Proxy is a configuration setting for WMI. The WMI Mapper receives client CIM/XML WBEM requests and converts the requests to *Windows Management Instrumentation* (WMI) requests. The WMI results are converted to CIM/XML format and returned to the Central Management Server (CMS). The *discovery* and *Identification* task uses the proxies in the WMI Mapper Proxy list to discover whether a *system* is a WMI-enabled system. If the system is WMI-enabled, then the identification information for that system based on that specific proxy is returned.

The WMI Mapper makes it possible to retrieve WMI instrumented data on a Windows machine through WBEM requests. The Windows version of HP SIM installs this WMI Mapper locally so that it can make WMI requests across the network to the systems without the need to install the WMI Mapper on the managed Windows systems.

The WMI Mapper is included in a Typical install of HP SIM on a Windows CMS (optional in a Custom install) . For HP-UX and Linux-based CMS's, the WMI Mapper is not available.

- **Simple Network Management Protocol (SNMP)** One of the management protocols supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.

If SNMP is not part of the Windows operating system install, you can install it from the Windows CD as a component. Verify on the target system that the SNMP service allows a remote connection from the CMS. If there are different read community sets on the target system, ensure that the read community string is configured in CMS SNMP protocol. To ensure that the **Set read community string** option in Configure or Repair Agents is set to **public**, select **Configure**→**Configure or Repair Agents**. Step 4 of Configure or Repair Agents enables you to configure the **Set read community string** option. See “Windows CMS” for additional information.

To install the HP Insight SNMP agents for ProLiant systems running on Linux x86 operating system, go to www.software.hp.com and select the ProLiant Support Pack 7.90.



NOTE: The SNMP agents cannot be installed on HP-UX systems.

To install the SNMP provider from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install SNMP Agents (HP ProLiant Insight Management Agents) for Windows**.

To configure the write community string on the CMS, select **Options**→**Protocol Settings**→**System Protocol Settings** from the HP SIM menu. To configure the community string for multiple systems, select **Options**→**Protocol Settings**→**Global Protocol Settings** and set the write community string.

- **Desktop Management Interface (DMI)** An industry-standard protocol, primarily used in client management, established by the Desktop Management Task Force (DMTF). DMI provides an efficient

means of reporting client system problems. DMI-compliant computers can send status information to a central management system over a network.

For HP-UX and Linux-based systems, you can download DMI from the HP Software Depot (<http://www.software.hp.com/>).

- **OpenSSH** A set of network connectivity tools providing encrypted communication sessions over a computer network using SSH. It was created as an open source alternative to the proprietary SSH software suite offered by SSH Communications Security.

You can download OpenSSH from the HP Software Depot (<http://www.software.hp.com/>).

To install OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**. To configure OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**→**Configure secure shell (SSH) access**.



NOTE: OpenSSH can also be installed from the HP SIM menu by selecting **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install OpenSSH**.

- **Secure Shell (SSH)** SSH is used to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

You can download SSH from the HP Software Depot (<http://www.software.hp.com/>).

To install the SSH provider from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**. To configure OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**→**Configure secure shell (SSH) access**.

To retrieve the most recent version of the HP Insight Management Agent for Windows ProLiant systems, go to the HP Software Depot (<http://www.software.hp.com/>), and enter **HP SIM Insight Management Agents for Windows** in the **Search** box.

Configuring management protocols

Management protocols can be configured through the First Time Wizard, through the Replicate Agent Settings, globally through the **Global Protocol Settings** page, or for individual or groups of systems from the **System Protocol Settings** page. See the following sections for additional information:

- Entering WBEM settings
- Entering SNMP settings
- Windows CMS
- HP-UX and Linux CMS
- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols

Sending test traps and indications

To verify that SNMP traps and WBEM indications can be sent, send test traps and indications.

You can send test traps and indications from Replicate Agent Settings on Windows and HP-UX systems, with the WBEM provider installed, from the **Step 4: Configure or Repair Agents** page, under **Configure WBEM / WMI**. Select **Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system**. See “Windows CMS” for more information.

You can also send test indications from HP-UX by running the following procedure:

1. From the HP-UX managed system, run `/ect/opt/resmon/lbin/send_test_event monitor name` . For example, `/etc/opt/resmon/lbin/send_test_event disk_em`.

Possible monitor names:

- `dm_memory`
 - `lpmc_em`
 - `disk_em`
 - `dm_chassis`
 - `dm_core_hw`
 - `ia64_corehw`
 - `fpl_em`
2. Confirm that the test indication is shown in the HP SIM event table view after you trigger it.
 3. Additionally, on the HP-UX managed system, you can run `/opt/sfm/bin/evweb eventviewer -L` to verify that indications are generated and received on the local system. This command lists all of the WBEM events that have been generated on the system.

Related procedures

- [Adding a WMI Mapper Proxy](#)
- [Deploying OpenSSH to multiple systems using RDP](#)
- [Installing OpenSSH](#)
- [Creating an OpenSSH task through the CLI](#)
- [Configuring DMI access](#)
- [Configuring SNMP access](#)

Related topics

- [Global protocols](#)
- [WMI Mapper Proxy](#)
- [Configuring or repairing agents](#)

Configuring automatic discovery general settings

Configure *automatic discovery* to customize the *discovery* process for your environment.



NOTE: All steps are optional.

To configure general settings for automatic discovery:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Configure general settings**. The **General Settings for All Discoveries** section appears.
3. Select from the following options:
 - **Automatically discover a system when an event is received from it.** This option enables systems to be discovered when a trap or some other supported event is received by HP Systems Insight Manager (HP SIM). It uses the discovery filters and IP address exclusion ranges for additional filtering of these events. This option is not selected by default.
 - **Automatically discover a server blade when its Integrated Lights Out management processor is identified.** This option adds servers indirectly discovered through the server's management processor, which are discovered when the server's iLO is discovered. The discovered servers are identified as Disabled on the system table view page. The only information displayed is the system serial number and the association to iLO and the enclosure. If the iLO is in a c-Class enclosure, the option **Discover systems in an enclosure when Onboard Administrator is discovered** should also be enabled.

- Select **Discover systems in an enclosure when Onboard Administrator is discovered**. This option adds systems identified by the Onboard Administrator even if the systems are not in the configured discovery range. This option is selected by default.
 - Select **Automatically discover VM guest(s) when the host is identified**. This option adds all HP Integrity Virtual Machine (HPVM) guest systems to the HP SIM database when the HPVM host system is discovered and identified. This option is selected by default.

Note: For automatic identification of virtual machine guests running on a virtual machine host, the IP address of the guest is required. To acquire the IP address from *Web-Based Enterprise Management* (WBEM) Providers, VMWare tools must be installed on the virtual machine guests.
 - **Automatically discover other virtual partitions within the same vPar Monitor when one of the virtual partitions is identified**. This option is selected by default.
 - **Automatically discover all nPars within the same complex when one of the nPars is identified**. This option is selected by default.
4. In the **Ping exclusion ranges, templates and/or hosts files** field, specify the IP addresses, templates, or hosts files containing IP addresses to exclude from the automatic discovery process. You can also enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. This field applies to both range-pinging and event-based automatic discovery. See “IP ranges” for more information.
- Important:** When discovering clusters, the ping inclusion range must include the IP addresses of the cluster and the cluster members.
5. Select **Enable discovery filters**. See “Discovery filters” for more information.
6. In the section, **Discover the following system types**, select the type of systems to be discovered. See “System types” for more detailed information about the system types listed.
- Important:** When discovering clusters, you must include the server system type, so that the cluster members are not filtered out.
- Note:** This option is available only when you select **Enable discovery filters**.
7. In the **Limit discovery to systems that meet the following criteria** section, select from the following:
- **Any system that matches the above filter**
 - **All manageable systems (WBEM, SNMP, DMI, WMI, or HTTP support)**
 - **Manageable systems with HP agents only**
- Note:** The option, **Limit discovery to systems which meet the following criteria** is available only when you select **Enable discovery filters**.
8. To save settings, click **OK**, or to close the **General Settings for All Discoveries** section without saving changes, click **Cancel**.
- If you click **OK** when discovery filters are enabled but have not selected any system types, the following error message appears:

You must make at least one system type selection when enabling filters.

The **Discovery** page **General Settings for All Discoveries** section is not protected from multiple users accessing the page at the same time. The last user to save the settings has his or her settings take affect. If discovery is in progress and the settings are applied by a different user or the same user, any remaining systems to be processed have the new settings applied.

Related topics

- [Discovery and identification](#)
- [IP ranges](#)
- [Discovery filters](#)
- [System types](#)
- [Global protocols](#)

Discovery filters

Discovery filters are a mechanism to prevent or enable certain *system types* from ever being added to the *database* through *automatic discovery*. When you want to discover systems of a certain type, using filters is much easier than specifying the IP addresses of each individual system. Discovery filters do not apply to manually added systems.

You can access discovery filters in one of the following ways:

- From the **Discovery** page, select **Options**→**Discovery**. From the **Automatic** tab, click **Configure general settings**, and then select **Enable discovery filters**.
- From the **Home** page, in the **Manage** section, click **discovery**. The **Discovery** page appears. From the **Automatic** tab, click **Configure general settings**, and then select **Enable discovery filters**.
- From the introductory page, in the **Do this now to complete the installation** section, click **Automatic**. The **Discovery** page appears. From the **Automatic** tab, click **Configure general settings**, and then select **Enable discovery filters**.

To disable filters, clear the **Enable discovery filters** checkbox. To enable filters, select the **Enable discovery filters** checkbox, and then select the system types that you want to discover.

To access and modify discovery filters, you must have *administrative rights*. If discovery filters are enabled, only systems of the selected types are added to the database through automatic discovery. Because all *tasks* operate on systems that exist in the database, tasks do not run on any system until the filter criteria has been met and that system has been added to the database. Filters do not affect any systems already discovered, even if the systems change to a type that no longer matches the current filter. If discovery filters are disabled, automatic discovery discovers systems according to the **General Settings for All Discoveries** section on the **Discovery** page in the **Automatic** tab. See “Configuring automatic discovery general settings” for more information about configuring discovery filters.

If you do not discover the HP systems that you expect to find, ensure that the *HP Insight Management Agents* are installed and running correctly on the target systems. In addition, verify that the SNMP Community Strings settings and WBEM user name and passwords in HP Systems Insight Manager (HP SIM) and on the agents for systems that are not discovered are configured correctly. See “Setting global protocols” for more information.

Related procedure

- ▲ [Configuring automatic discovery general settings](#)

Related topic

- ▲ [Discovery and identification](#)

Managing discovery templates

Discovery templates are files that can be used by *automatic discovery* instead of entering the addresses directly in to the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields. You can also add Simple or Fully Qualified Domain Names (FQDN) host names to discovery templates. However, you cannot enter a range of host names. Discovery templates can be used as a quick way to change the scope of automatic discovery. See the “Discovery templates section in “Discovery and identification” section for more information.



NOTE: Saved discovery template files are located in the directory <install directory>\config\discovery\templates directory.

From the **Managing Templates** section, you can:

- **Create new discovery template files** Click **New**. The **Create New Template** section appears. See “Creating a new discovery template file” for more information.
- **Edit existing discovery template files** Select the discovery template file you want to edit, and then click **Edit**. The **Edit Template** section appears. See “Editing a discovery template” for more information.
- **Delete existing discovery template files** Select the discovery template file you want to delete, and then click **Delete**. A confirmation box appears. See “Deleting a discovery template” for more information.

Related procedures

- [Creating a new discovery template file](#)
- [Editing a discovery template](#)
- [Deleting a discovery template](#)

Related topic

- ▲ [Discovery and identification](#)

Creating a new discovery template file

You can create new discovery template files instead of entering addresses directly into the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields.

To create a new discovery template file:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
 2. In the **For all automatic discoveries** section, select **Manage templates**. The **Manage Templates** section appears.
 3. Click **New**. The **Create New Template** section appears.
 4. In the **Discovery template name** field, enter a name for the new template. This field is required.
 5. To import a file, complete one of the following steps:
 - Click **Browse** to select an existing discovery template file that is present on the local client (the system from which you are browsing) and click **Import**
 - or
 - Enter the discovery range information into the **Contents** area. You can enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. See “IP ranges” for information about the correct syntax for entering IP ranges.
- Note:** Because template files cannot be nested, only ranges are allowed.
6. To save the discovery template file, click **OK**, or to close without saving changes, click **Cancel**.

After creating a discovery template, you can reference it in automatic discovery by using `@template_name` in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** or **Ping exclusion ranges, templates and/or hosts files** fields. See “IP ranges” for more information.

Template file format

```
#
# use @<file_name> in the automatic discovery IP inclusion range
# to reference this template
#
# Example:
#
# 2.0.0.0 :NOBROADCAST
# 2.0.0.0 - 2.0.2.0
# 3.0.0.0 - 3.0.0.254 : 255.255.255.0
```

Related procedures

- [Editing a discovery template](#)
- [Deleting a discovery template](#)

Related topics

- IP ranges
- Discovery and identification
- Managing discovery templates

Editing a discovery template

You can edit an existing discovery template file. All fields are optional except for the **Discovery template name** field. Edit only the fields that you want to change.

To edit a discovery template file:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
 2. In the **For all automatic discoveries** section, select **Manage templates**. The **Manage Templates** section appears.
 3. Select a discovery template file to edit, and then click **Edit**. The **Edit Template** section appears.
 4. The **Discovery template name** field cannot be edited. You must use the existing template name.
 5. To import a file, complete one of the following steps:
 - Click **Browse** to select an existing discovery template file that is present on the local client (the system from which you are browsing) and click **Import**
 - or
 - Enter the discovery range information into the **Contents** area. You can enter Simple or Fully Qualified Domain Names (FQDN) host names. However, you cannot enter a range of host names. See “IP ranges” for information about the correct syntax for entering IP ranges.
- Note:** Because template files cannot be nested, only ranges are allowed.
6. To save the discovery template file, click **OK**, or to close without saving changes, click **Cancel**.

Related procedures

- Creating a new discovery template file
- Deleting a discovery template

Related topics

- Discovery and identification
- Managing discovery templates

Deleting a discovery template

You can delete existing discovery template files. If you delete a discovery template file, the file is permanently deleted and cannot be retrieved again. Ensure that you only delete discovery template files if you no longer need them or you are creating a new discovery template file.



NOTE: Ensure that the discovery template is not currently in use. A template is not in use when the following conditions are met:

- There are no references to the template in the **Ping exclusion ranges, templates and/or hosts files** field in the **General Settings for All Discoveries** section.
 - There are no references to the template in the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field of all existing discovery tasks.
-

To delete a discovery template file:

1. Select **Options**→**Discovery**. The **Discovery** page appears with the **Automatic** tab selected.
2. In the **For all automatic discoveries** section, select **Manage templates**. The **Manage Templates** section appears.
3. Select a discovery template file to delete.
4. Click **Delete**. A confirmation box appears.
5. To delete the discovery template file, click **OK** to cancel the deletion process, click **Cancel**.

Related procedures

- Creating a new discovery template file
- Editing a discovery template

Related topics

- Discovery and identification
- Managing discovery templates

Adding a system manually

Use *manual discovery* to add a *system* to the HP Systems Insight Manager (HP SIM) *database* between scheduled *discoveries*.

To add a system using manual discovery:

1. Select **Options**→**Discovery**, and then click the **Manual** tab. The **System Information** section appears.
2. Enter the system name or IP address. Simple or Fully Qualified Domain Name (FQDN) host names can be entered. However, ranges of host names are not allowed.
3. Click **Add System** to add the system to the database. If you have not entered the *SNMP* or *Web-Based Enterprise Management* (Wbem) credentials for this system previously, click **More Settings**. Enter the credentials, then click **Add System**, or click **More Settings** and enter the following information:

The screenshot shows the 'Discovery' section of the HP SIM interface. At the top, there is a header 'Discovery' with the instruction 'Indicate the systems you want HP Systems Insight Manager to manage.' Below this are three tabs: 'Automatic', 'Manual', and 'Hosts Files'. The 'Manual' tab is selected. Underneath, there is a sub-header 'System Information' and a 'Required field *' label. A text input field is labeled 'Enter the system's name or IP address: *'. Below this is a section titled 'Specify additional system properties to use only if Identification fails on this system'. This section contains several dropdown menus for 'System type' (set to 'Unmanaged'), 'System subtype 1' through 'System subtype 8' (all set to 'None'), and a text input field for 'Product model'.

WBEM Settings

Use default (User names)
 Use custom

Port #	User name	Password	Confirm password
Default 1:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Default 2:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Default 3:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Default 4:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Default 5:	<input type="text"/>	<input type="text"/>	<input type="text"/>

SNMP Settings

Timeout (in seconds)

Use default (currently: 5)
 Use custom

Retries

Use default (currently: 3)
 Use custom

Read-only community string

Use default (currently: public)
 Use custom

Write community string

Use default (currently: private)
 Use custom

- **Specify additional system properties to use only if Identification fails on this system.**
Includes:
 - **System type** Click the down arrow and select the appropriate System type.
 - **System subtype** Click the down arrow and select the appropriate System subtype. You can input up to eight different system subtypes.
 - **Product model** Enter the system model number here. This field is free form.
- **WBEM Settings**
 - **User name**
 - **Password** If you do not want to use the default global values for the WBEM user name and password, select **Use Custom**, and then enter custom values.
If you are manually discovering a *storage system*, ensure that the user name and password of the SMI CIMOM are present in the global protocol settings, or enter them here as custom values. To view the global settings, select **Options**→**Protocol Settings**→**Global Protocol Settings**.
For Windows-based systems, the user name should include the domain name. For example, *domainname\username*.
Note: OpenWBEM is not supported.
- **SNMP Settings** If you do not want to use the default global values for the SNMP settings, select **Use Custom**, and enter custom values.
 - **Timeout (in seconds)** The amount of time HP SIM waits for an SNMP response when it sends a request to the system. If a response is not received within this time interval, HP SIM might determine that the system does not support SNMP. Decreasing this value can cause increased network traffic because the rate of retry attempts is increased. Use caution when changing this value. A value of three seconds usually works for a LAN.

However, if systems are connected through a WAN, try a higher value, for example, 10 seconds.

- **Retries**

The number of additional times after the first attempt is made to communicate with a system before the attempts stop.

- **Read-only community string and Write community string**

Note: The **Write community string** is optional and is required only for firmware updates on a GbE switch. If you must update the GbE switch firmware, you must first set the write community string from this page and then run the existing switch update task. Do not set this feature if the network is not trusted.

A community string sets up authentication that enables or prohibits communication between the managed system and the Central Management Server (CMS). The community string of the CMS must match the community string of the managed system. Use the read-only community string to read variables. Use the write community string to modify variables. Although only one community is valid for a communication attempt, a system can belong to multiple communities. However, HP SIM only uses one community string when communicating with a system.

Hosts files can be used to manually add multiple systems to the HP SIM database. See “Managing hosts files” for more information.

Command line interface

Use the `mxnode` command to add, delete, modify, identify, or list systems in HP SIM from the command line interface (CLI). For assistance with this command, see the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

Related procedure

- ▲ Creating a new hosts file

Related topics

- Discovery and identification
- IP ranges
- Using command line interface commands

Managing hosts files

Hosts files are used by manual discovery to manually add multiple *systems* to the HP Systems Insight Manager (HP SIM) *database* and are generally used only one time to import systems.

To use a hosts file to specify systems for an automatic discovery, add the hosts file name to the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** section of the **Discovery** page under the **Configure general settings** section of the **Automatic** tab. Enter the following statement: `$Hosts_filename` where *Hosts_filename* is the name of the hosts file that you want to use.

See “Adding a system manually” for information about adding a single system to the database. See the “Hosts files” section in the “Discovery and identification” section for more information about hosts files.

From the **Hosts Files** section, you can:

- **Create new hosts files** Click **New**. The **New Hosts File** section is displayed. See “Creating a new hosts file” for more information.
- **Edit a hosts file** Select the hosts file to edit, and then click **Edit**. The **Edit Hosts File** section is displayed. See “Editing a hosts file” for more information.

- **Delete a hosts file** Select the hosts file to delete, and then click **Delete**. A confirmation box is displayed. See “Deleting a hosts file” for more information.
- **Add a hosts file to the HP SIM database** Select the hosts file to add, and then click **Add system now**. See “Adding systems in a hosts file to the HP SIM database” for more information.

Related procedures

- Creating a new hosts file
- Editing a hosts file
- Deleting a hosts file
- Adding systems in a hosts file to the HP SIM database
- Creating a task to import a hosts file for HP SIM integration
- Batch-adding systems using the CLI

Related topic

- ▲ Discovery and identification

Creating a new hosts file

This procedure enables you to create a new hosts file for use in HP Systems Insight Manager (HP SIM).



NOTE: For keywords that contain more than one word, such as "management processor," enclose the full keyword in double quotation marks. Quotation marks are optional for single keywords, like server.

NOTE: For clusters, ensure that the cluster and its members are defined in the hosts file.

To create a hosts file:

1. Select **Options**→**Discovery**, and then click the **Hosts Files** tab.
2. Click **New** to create a new hosts file. The **New Hosts File** section appears.

New Hosts File

Required field *

Name:

Initialize contents with:

Template file

Systems loaded from the central management server, sorted by:

Systems loaded from hosts file:

Contents:

```
# Title:      [title here]
# Author:    [author here]

# Example:
##$IMXE_DEFAULT: Type = server
# 1.1.1.1   myServer1.mysite.com   myServer1
# 1.1.1.2   myServer2.mysite.com   myServer2
#
##$IMXE_DEFAULT: Type = desktop
# 1.1.1.3   myClient1.mysite.com   myClient1
# 1.1.1.4   myClient2.mysite.com   myClient2
```

3. In the **Name** field, enter a name for the new hosts file. This field is required.

4. Under **Initialize contents with**, select one of the following:
 - **Template file.** Loads the contents into the **Contents** window.
 - **Systems loaded from the central management server, sorted by:** From the dropdown list, select one of the following: **IP address**, **System name**, **System type and then by IP address**, or **System type and then by system name**. This option loads the systems managed by HP SIM into the **Contents** window.
 - **Systems loaded from hosts file.** Enter the file name and location (for example, `c:\ doc.txt`), or click **Browse** to locate the hosts file. This option reads the contents of the specified file and displays it in the **Contents** window.
5. If you did not select **Template File**, click **Initialize Now** to install the hosts file. Otherwise, enter the contents of the hosts file in the **Contents** section. Simple or Fully Qualified Domain Name (FQDN) host names can be entered in the hosts file. However, no range of host names are allowed.
6. To save the hosts file, click **OK**, or to cancel any changes you have made, click **Cancel**.

Hosts file format

The format for a valid hosts file line is:

```
IP_ADDRESS [DNS_NAME] SYSTEM_NAME
```

Where:

<i>IP_ADDRESS.</i>	Is a valid IP address
<i>DNS_NAME.</i>	Specifies an optional DNS name parameter
<i>SYSTEM_NAME.</i>	Is the name of the system

With this format, the following hosts file lines are valid:

```
1.2.3.4 mySystem.mydomain.com mySystem
```

```
2.3.4.5 mySystem
```

The following lines are not valid:

```
1.2.3.4/
```

```
mySystem/
```

```
mySystem.mydomain.com/
```

Precede comment lines with the # character:

```
# This is a comment line
```

```
1.2.3.4 mySystem.mydomain.com mySystem #This is an end-of-line comment
```

See "Hosts file extensions" for information about hosts file extensions.

Related procedures

- [Editing a hosts file](#)
- [Deleting a hosts file](#)
- [Adding systems in a hosts file to the HP SIM database](#)
- [Batch-adding systems using the CLI](#)

Related topics

- [IP ranges](#)
- [Discovery and identification](#)
- [Managing hosts files](#)

Editing a hosts file

To edit a hosts file:

1. Select **Options**→**Discovery**, and then click the **Hosts Files** tab.
2. Select an existing hosts file, and then click **Edit**. The **Edit Hosts File** section appears.

3. In the **Replace contents with** section, select one of the following:
 - **Template file.** Loads the contents into the **Contents** window.
 - **Systems loaded from the central management server, sorted by:** From the dropdown list, select one of the following: **IP address**, **System name**, **System type and then by IP address**, or **System type and then by system name**. This option loads the systems managed by HP SIM into the **Contents** window.
 - **Systems loaded from hosts file.** Enter the file name and location (for example, `c:\ doc.txt`), or click **Browse** to locate the hosts file. This option reads the contents of the specified file and displays it in the **Contents** window.
4. Click **Replace Now**, or enter the changes in the **Contents** section.
5. To save the hosts file, click **OK**, or to cancel any changes you have made, click **Cancel**.

Related procedures

- [Creating a new hosts file](#)
- [Deleting a hosts file](#)
- [Adding systems in a hosts file to the HP SIM database](#)
- [Batch-adding systems using the CLI](#)

Related topics

- [Discovery and identification](#)
- [Managing hosts files](#)

Deleting a hosts file

Ensure that the selected hosts file is not in use. A hosts file is not in use when:

- There are no references to it in the **Ping exclusion ranges, templates and/or hosts files** section of the general settings page.
- There are no references to it in the **Ping inclusion ranges, templates, and/or hosts files** section of every existing discovery task.



NOTE: Only delete hosts files if you no longer need them or if you are creating a new hosts file.

To delete a hosts file:

1. Select **Options**→**Discovery**, and then click the **Hosts Files** tab.
2. Select hosts files to delete, and then click **Delete**. A confirmation box appears.
3. Click **OK** to delete the hosts files, or click **Cancel** to cancel the delete process.

Related procedures

- [Creating a new hosts file](#)
- [Editing a hosts file](#)
- [Adding systems in a hosts file to the HP SIM database](#)

Related topics

- [Discovery and identification](#)
- [Managing hosts files](#)

Adding systems in a hosts file to the HP SIM database

1. Select **Options**→**Discovery**, and then click the **Hosts Files** tab.
2. Select an existing hosts file.
3. Click **Add Systems Now**.

HP SIM reads in the hosts file and adds the systems.

Related procedures

- Creating a new hosts file
- Editing a hosts file
- Deleting a hosts file

Related topics

- Discovery and identification
- Managing hosts files

Creating a task to import a hosts file for HP SIM integration

Users with *administrative rights* who are using both HP Systems Insight Manager (HP SIM) and its companion Windows management application, Insight Manager (WIN32), can import Insight Manager (WIN32) system *database* files for easy transition from the Windows client/server environment to a web-based environment.

Insight Manager (WIN32) creates a system database file that stores the names and *IP* addresses of *discovered systems* in the file `cim_ip.dat`. The file is formatted like a *hosts file* that HP SIM recognizes. The file is dynamically updated as systems are discovered or deleted in Insight Manager (WIN32). The `cim_ip.dat` file is located in the directory where Insight Manager (WIN32) is installed.

Insight Manager (WIN32) supports systems that include spaces in their names. In the `cim_ip.dat` file, these system names contain an asterisk (*) instead of a space. Any *system* name that contains a space is invalid in HP SIM.

Importing the .dat file



NOTE: If the hosts file contains a cluster name or address, the HP SIM discovery IP range must be changed to include the cluster members because it is possible that the imported hosts file does not include the cluster members. See “Creating a new discovery task” for information about changing the IP range.

1. Select **Options**→**Discovery**, click the **Manual Discovery** tab, and then click **Hosts Files** at the top of the page. The **Manual Discovery - Hosts Files** page appears.
2. Click **New**. The **New Hosts File** section appears.
3. In the **Hosts file name** field, enter a name for the file, such as `cim_ip.dat`.
4. Select **Systems loaded from hosts file**, and perform one of the following steps:
 - Enter the full path name for the file.
 - Locate the `cim_ip.dat` file by clicking **Browse**. When the file is located, click **Open** to enter the file name in the **Systems loaded from hosts file** field.
5. Click **Initialize Now** to initialize the file and display the contents in the **Contents** area.
6. To save the file as a hosts file for future reference, click **OK**.
7. On the **Manual Discovery - Hosts File** page, ensure that the file you added is selected, and then click **Add Systems Now** to insert the systems into the *database*.

Displaying the systems

Within a short time, the systems inserted through a hosts file are added to the database. When the next discovery and identification tasks run, full system information is added to the system.

To display the systems in the **System and Event Collections** panel, select **All Systems**. The system table view page displays, and the systems added are displayed along with all other discovered systems.

Exporting Insight Manager (WIN32) files

There are two ways to export Insight Manager (WIN32) `.dat` files from within Insight Manager (WIN32):

- Use the Insight Manager (WIN32) Export feature
- Use the `cim_ip.dat` file, which compared to the previous method, contains abbreviated system information.

See <http://h10018.www1.hp.com/wwsolutions/misc/hpsim-helpfiles/win32sim.pdf> for more information about exporting the Insight Manager (WIN32) .dat file.

Related procedure

- ▲ Creating a new hosts file

Batch-adding systems using the CLI

You can batch-add systems by host name using the command line interface (CLI). To do this, you must first create an .xml file, and then run the `mxnode` command from the command line.

1. Create and save an .xml file. For example,

```
<?xml version="1.0" encoding="windows-1252"?>
<node-list>
  <node name="system1"/>
  <node name="system2"/>
  <node name="system3"/>
</node-list>
```

2. From the command line, run:

```
mxnode -a -f mysystems.xml
```

Where *mysystems.xml* is the name of the file you created.

Related procedure

- ▲ Creating a new hosts file

Hosts file extensions

Hosts files typically contain IP addresses, system names, system name aliases, and user comments. The hosts file that you create can contain additional information about *systems*. The information appears as one or more comments that precede the hosts file entry for the system. Unless other values are specified, the default values are used. The following table lists default values are provided for the following parameters:

Parameter	Keyword
system type	TYPE
SNMP timeouts	SNMP_TIM
SNMP retries	SNMP_RET
SNMP read community	SNMP_MON
SNMP write community	SNMP_CON

You can modify the hosts file to substitute a value for the defaults for one entry or change the default for all subsequent entries. To change values for a single-system entry in a hosts file, add a statement to the hosts file as a comment on the line before the host entry, as shown in the following example. The statement applies only to the system it precedes. In the following example, the default TYPE is changed to "server" for the system EngProliant.

Keyword statement	Hosts file entries
#\$IMXE:< Keyword=value >	#\$IMXE: TYPE=server
For example: #\$IMXE: TYPE=server	16.26.176.92 EngProliant.compaq.com EngProliant #user comments

To change the default globally so that it affects the next file entry and all subsequent entries, use a statement similar to the following example. The default is changed to "router" for the next entry. Router remains the default for all entries until another #`$IMXE_DEFAULT` statement changes that value. If a single instance of `TYPE` is changed by a #`$IMXE` statement, the default is not used only for the next entry and then reverts to back "router".

Keyword statement	Hosts file entries
# <code>\$IMXE_DEFAULT: < Keyword=value></code>	# <code>\$IMXE_DEFAULT: TYPE=router</code>
For example: # <code>\$IMXE_DEFAULT: TYPE=router</code>	16.26.176.92 BldRtr6.compaq.com BldRtr6 #user comments



NOTE: If a keyword parameter is omitted on a commented entry, the current default value is used. The current default is always the standard default unless a new default value was set using the #`$IMXE_DEFAULT` statement. Enclose keywords containing more than one word, such as "management processor," enclose the full keyword in double quotation marks. Quotation marks are optional for single keywords like "server."

The following text quoted from a hosts file illustrates several statements. The explanations, which begin with the pound sign (#), are not displayed in the hosts file.

```
# Title: Systems in database
# Sorted by: IP address
# Date: 28-Mar-00 2:29:31 PM
# Author: administrator
```

The system EngProliant uses all current defaults. There are no additional comments.

```
16.26.176.92 EngProliant.compaq.com EngProliant #user comments
```

The system testServer in the following example defaults for `TYPE`. The defaults for `SNMP Timeouts` and `Retries` were restored for this system but only apply to testServer. The `SNMP write community string` default was changed and only applies to testServer.

```
#$IMXE: TYPE=Server
#$IMXE: SNMP_TIM=0 SNMP_RET=0 SNMP_MON=public
SNMP_CON=private
16.26.160.20 testServer.compaq.com testServer
```

All defaults in the following example for the system BldRtr1 are the same as for testServer, but had to be specified because they are not the global defaults. These changes apply only to BldRtr1.

```
#$IMXE: TYPE=Router
#$IMXE: SNMP_TIM=0 SNMP_RET=0 SNMP_MON=public
SNMP_CON=private
16.26.160.23 BldRtr1.compaq.com BldRtr1
```

For the system BldRtr5, the `TYPE` and protocols used for discovery were changed from the current defaults. Because the remaining keyword entries are missing, the standard defaults are applied for the `SNMP timeouts`, `retries`, and `community strings`.

```
#$IMXE: TYPE=Router
```

```
16.26.160.24 BldRtr5.compaq.com BldRtr5
```

For the system AcctServer, only the TYPE was changed from the current defaults.

```
#$IMXE: TYPE=Server
16.26.176.36 AcctServer.compaq.com AcctServer #user comments
```

The global default for TYPE was changed from Unknown to Router. All subsequent entries will be identified as routers until a TYPE statement is used to specify another type or restore the default.

```
#$IMXE_DEFAULT: TYPE=Router
16.25.176.38 FloorRtr2a.compaq.com FloorRtr2a #user comments
```

The default for the next host entry was changed to management processor, which is enclosed in quotes. # \$IMXE: TYPE="Management Processor" AcctSvriLo.compaq.com
16.25.176.37 AcctSvriLo #user comments

...

Default values

If a parameter is missing in the hosts file, the default is applied. The following lists the parameters that can be used in hosts files:

Keyword	Value	Description
TYPE	Application, Cluster, Complex, Desktop, Enclosure, Environmental Monitor, Handheld, Hub, KVM Switch, Management Processor, Notebook, Partition, Power Distribution Unit, Power Supply, Printer, Rack, Resource Partition, Remote Access Device, Router, Server, Shared Resource Domain, Storage Device, Switch, Tape Library, Thin Client, UPS, Unknown, Unmanaged, and Workstation See "System types" for more information about each system type.	Unknown (Default)
DMI	0 1	Disabled (Default) Enabled
SNMP	0 1	Disabled (Default) Enabled
HTTP	0 1	Disabled (Default) Enabled
SNMP_TIM	0 Greater than 0	System default (Default)
SNMP_RET	0 Greater than 0	System default (Default)
SNMP_MON	Public <Community String >	Read only (Default)
SNMP_CON	<Community String>	No default

Related procedure

- ▲ Managing hosts files

Related topic

- ▲ Discovery and identification

IP ranges

You can specifically include or exclude IP addresses individually for *discovery* or as part of a range. Because the IP address range entries also affect *cluster* discovery, IP ranges must include the addresses of the cluster and its nodes. Enter one *system* or range per line. When entering IP address ranges, use the guidelines in the following table:

IP range	Range to enter
Your local subnet IP ranges from 1 to 254, the default Ping inclusion ranges	172.25.76.1-172.25.76.254
A single system as a range in the Ping inclusion ranges or Exclusion ranges fields	172.25.76.114-172.25.76.114 or 172.25.76.114
A group of systems within a subnet in the Ping inclusion ranges or Exclusion ranges fields	172.25.76.38-172.25.76.48
Systems included in a discovery template file	@DiscoveryTemplate_filename
Systems included in a hosts file	\$filename
No broadcast node in this subnet	172.25.76.255:NOBROADCAST
Broadcast node determined by the subnet mask	172.25.76.0-172.25.76.255:255.255.255.0 or 172.25.76.114:255.255.255.0

Discovery assumes you do not want to ping the subnet network ID (typically the zero node), or the subnet broadcast address (typically node 255), because these settings would unnecessarily use network resources. If the system 255 is not a broadcast address on your network, you can indicate this in the **Ping inclusion ranges** section as shown in the preceding table or exclude the specific system in the **Exclusion ranges** section. HP Systems Insight Manager (HP SIM) uses the subnet mask to determine the broadcast system. If you do not specify a mask, HP SIM uses the default mask for the class of network. If your subnet mask is not the default for the class, the broadcast system can be included, generating much more network traffic than necessary.

Related procedure

- ▲ Configuring automatic discovery

Related topic

- ▲ Discovery and identification

Identification

The *Identification* process follows automatic or manual system *discovery* and identifies the following information about the discovered system:

- Management protocol the system uses (for example, *Simple Network Management Protocol* (SNMP), *Desktop Management Interface* (DMI), *Web-Based Enterprise Management* (WBEM), HTTP, Secure Shell (SSH), or WS-Management).



NOTE: OpenWBEM is not supported.

NOTE: By default, HP SIM supports WS-Management identification on the standard SSL port 443. The addition of WS-Management support does not affect existing identification or discovery of Integrated Lights Out (iLO) using other protocols such as *Web-Based Enterprise Management* or SNMP. **WSMAN:1.0**

appears as a Management Protocol along with all other supported management protocols on the system page **System** tab of the **System** page.

- Type of system (for example, server, client, management processor, storage, switch, router, or cluster)
 - Product name of the system
 - Operating system name, type, and version
 - Associations, such as *iLO in server*
-



NOTE: During identification, remote *enclosures* have a generic name (format: Encl_SerialNumber) assigned to them until one server from every enclosure is discovered and identified. Then, the enclosures contain the name of the enclosure assigned to the enclosure.

HP SIM collects and recognizes the product ID and serial number, and most importantly, how to handle the server-to iLO associations using the Universally Unique Identifier (UUID) instead of the serial number. The following processes occur sequentially for each system that is identified by HP Systems Insight Manager (HP SIM):

- Identify the type of system, supported protocols, and limited attributes (such as the operating system type)
- Filter out systems that do not meet the filter criteria (if the system is new)
- Obtain additional data, such as license data or Web agents that might be written to the database directly, and queryable attributes that can be queried (such as CPU and memory data)
- Runs association algorithms based on system type identified in the first step.

For newly found *automatically discovered* systems, before the system is added to the *database*, any *discovery filters* that are configured are applied. If a system does not match the discovery filter, it is not added to the database, and no additional tasks or requests are made to that system. After the system passes the filter, it is added to the database. At this time, the system is available to any polling tasks, lists, or other operations.



NOTE: Discovery filters do not apply to manually discovered systems.

HP SIM performs initial hardware and software status polling and initial data collection on newly added systems. See “Hardware status polling”, “Software status polling”, and “Data collection” for more information about each task. The information about the systems is stored in the database.

The time to complete the discovery and identification processes varies with the network size and resources. All necessary tasks are predefined in HP SIM. Predefined tasks cannot be removed from the system, but they can be disabled if necessary. You can also create a new identification task and schedule it to run when you want to update identification information from systems.

By default, HP SIM runs the *System Identification* task once per day and when new systems are discovered. Most users do not need to schedule identification tasks to run more than once per day.

Note: For automatic identification of virtual machine guests running on a virtual machine host, the IP address of the guest is required. To acquire the IP address from *Web-Based Enterprise Management* (WBEM) Providers, VMWare tools must be installed on the virtual machine guests.

If VMware tools are installed on the guest, the UUID, host name, and primary IP address of the virtual machine host are collected. If VMware tools are not installed, only the UUID is collected. In this case, the virtual machine guest is named as *>VMHost_Name<_>Display Name<*, where *VMHost_Name* is the name of the guest host system and *Display Name* is the display name of the guest in VMware Virtual Infrastructure Client.

Initial identification

After a system is newly discovered or rediscovered, HP SIM attempts to identify it. The discovery task is not 100% complete until all the systems discovered or rediscovered have been identified.

Identifying systems

To identify systems in between discoveries, select **Options**→**Identify Systems**. The **Identify Systems** page appears. From this page, select target systems to add. See “Creating a task” for more information about selecting targets.

Related procedure

- ▲ Adding a system manually

Related topic

- ▲ Discovery and identification

Managing system types

The *System Type Manager* (STM) is a utility that modifies the default behavior of *identification*. STM enables you to customize the type and product name of third-party systems using rules based on responses to *SNMP* and *Desktop Management Interface* (DMI) (Windows only) lists from systems on your network.



IMPORTANT: For most HP *systems*, the *system type* and product name cannot be modified. Identification can be customized based on SNMP System Object Identifiers (OIDs) for all other fields. Manufacturers assign unique system OIDs to their SNMP-instrumented products. STM enables you to customize identification by creating rules that map these system OIDs to product categories and names that you choose. You must have *administrative rights* to use STM.

To access the **Manage System Types** page, select **Options**→**Manage System Types**. From this page, you can:

- **Create a New Rule.** Click **New**. The **New rule** section appears. See “Creating STM rules” for more information.
- **Edit an Existing Rule.** Select the rule you want to edit, and then click **Edit**. See “Editing STM rules” for more information.
- **Delete an Existing Rule.** Click **Delete**. A confirmation box appears. To delete the rule, click **OK**, or to cancel the deleting and return to the **Manage System Types** page, click **Cancel**. See “Deleting STM rules” for more information.

Related procedures

- Creating STM rules
- Editing STM rules
- Deleting STM rules

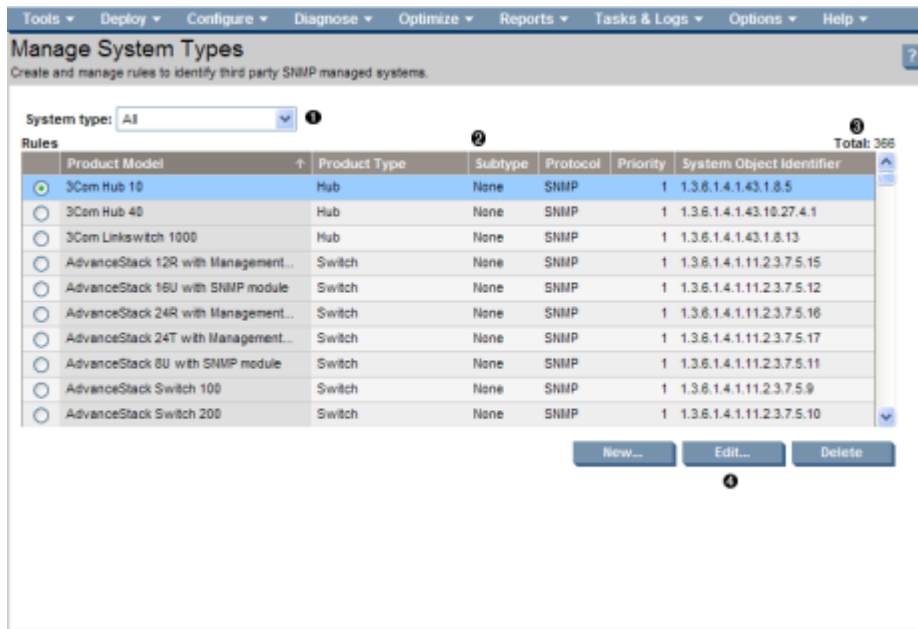
Related topics

- Navigating the Manage System Types page
- Additional information for creating STM rules
- About System Type Manager

Navigating the Manage System Types page

The **Manage System Types** page lists rules currently defined in HP Systems Insight Manager (HP SIM) including the following:

1. System type
2. Columns
3. Total
4. Available buttons



To access the **Manage System Types** page, select **Options**→**Manage System Types**.

System type

The list on the **Manage System Types** page can be filtered by *system type* by selecting a type from the **System Type** dropdown list. Click the down arrow, and then select a system type for which to filter the list.

Columns

The following columns appear on the **Manage System Types** page:

- Product Model
- Product Type
- Sub Type
- Protocol
- Priority
- System Object Identifier

Click a column heading to sort the column in ascending or descending order.

Total

The **Total** field displays the total number of *systems* that meet the System Type criteria selected in the **System type** dropdown list.

Available buttons

The following buttons are available on the **Manage System Types** page:

- **New**. Used to create a new rule.
- **Edit**. Used to edit existing rules. Select the rules to edit, and then click **Edit**.
- **Delete**. Used to delete an existing *SNMP* or *DMI* rule. Select the rule, and then click **Delete**. In the confirmation box, click **OK** to delete the rule, or **Cancel**, to return to the **Manage System Types** page without deleting the rule.

Related procedures

- Creating STM rules
- Editing STM rules
- Deleting STM rules

Related topics

- [Managing system types](#)
- [About System Type Manager](#)

About System Type Manager

Manufacturers assign unique System Object Identifiers (OIDs) to their *Simple Network Management Protocol* (SNMP)-instrumented products. System Type Manager (STM) enables you to customize *identification* by creating rules that map these OIDs to product categories and names of your choosing. HP Systems Insight Manager (HP SIM) *discovers* and applies information from the rule when an unknown system matches a rule that you specify. Rules contain OIDs, and an optional, additional object identifier, that are compared with responses from a target *system*. When a rule meets the comparison criteria, the system is identified using information from the rule.



NOTE: SNMP rules can be created from the **Manage System Types** page of HP SIM or from the *CLI* using the `mx:stm` command. Additionally, on Windows systems, you can create rules based on the *Desktop Management Interface* (DMI) protocol using the CLI `mx:stm` command in the CLI.

NOTE: SNMP rules require a OID and product name. Optionally, a compare rule (match or starts with), MIB OID with value and compare rule, product type, subtype, custom management page, and priority can also be specified. DMI rules are specified by selecting a product name and at least one, or at the most three, DMI elements with response values and compare rules.

Why add or modify system identification?

The following are situations in which you might want to add or modify system identification:

- You might have third-party systems on your network that are not included in the HP SIM *database*, and you want them identified by unique product names based on location or use.
- You have systems of a known type that you want to identify in another way. For example, you have laptops that you want to classify on some other basis.

Options for creating a System Type Manager rule

Systems are identified and classified using specific rules and are assigned a corresponding system type and a product name.

For SNMP systems, STM uses the system OID and an optional MIB variable OID with its value and data type. Identification is based on the system OID returned from the system to be identified. If there is a matching rule for the system OID, identification proceeds based on whether the response value matches the criteria in the rule.

For DMI systems, STM uses requests consisting of one to three DMI elements, attribute, and value pairs. For a rule to be applied, the returned response values must match values in the rule in a manner defined by the corresponding compare rules.

The custom management page is a link on the **System Page** under the **Tools & Links** tab. The link appears with other system links for the system if it is unique. You can specify a URL address that opens an HTML page. For example, enter: `http://support.networkingcompany.com/model123` .

New system types are displayed in system collections after a full discovery runs and identifies systems that match rules you created.

You can modify and delete rules as the systems in your network change.

Related procedures

- [Creating STM rules](#)
- [Editing STM rules](#)
- [Deleting STM rules](#)

Related topics

- Managing system types
- Navigating the Manage System Types page

Creating STM rules

The following procedure instructs you how to create a new *SNMP* rule through *System Type Manager (STM)*. The STM is a utility used to modify the default behavior of *identification*. STM enables you to customize the type and product name of *systems* using rules based on responses to *Simple Network Management Protocol (SNMP)* and *Desktop Management Interface (DMI)* (Windows only) collections from systems on your network.



NOTE: DMI rules can only be created from the command line interface.

NOTE: The following fields are required to create an STM rule:

- System Object Identifier, including the Compare Rule
- System Type
- Product Name

To create a new SNMP rule:

1. Select **Options**→**Manage System Types**. The **Manage System Types** page appears.
2. Click **New**. The **New rule** section appears.

The screenshot shows the 'Manage System Types' dialog box with the 'New rule' section active. The dialog has a title bar 'Manage System Types' and a subtitle 'Create and manage rules to identify third party SNMP managed systems.' Below the subtitle, there is a 'Required field *' label and a note: 'Use the following criteria to create a new system type.' The form contains several fields and buttons:

- 'System object identifier:*' text box with a 'Retrieve from system...' button to its right.
- 'Compare rule:*' dropdown menu set to 'match'.
- 'MIB variable object identifier:' text box with a 'Retrieve from MIB...' button to its right.
- 'Object value:' text box with a 'Retrieve from system...' button to its right.
- 'Data type:' dropdown menu set to 'string'.
- 'Compare rule:' dropdown menu set to 'any value'.
- 'Priority (1 is highest):' text box containing the number '1'.
- 'Assign the following properties to systems identified by the above criteria.' section with:
 - 'System type:*' dropdown menu set to 'Server'.
 - 'Subtype:' dropdown menu set to 'None'.
 - 'Product model:*' text box.
 - 'Custom management page:' text box with a 'Launch' button to its right.
- 'OK' and 'Cancel' buttons at the bottom right.

3. Enter the **System object identifier** information. Retrieve the system object identifier from a target system on your network by clicking **Retrieve from system**. The **Retrieve from system** section appears. The **System object identifier** field is required.

Retrieve from system:

Enter an object identifier, community string and target hostname or IP address and click on the 'Get response' button to view details below. Clicking 'OK' will transfer this value to the system object identifier field above.

Object identifier:	<input type="text" value="1.3.6.1.2.1.1.2"/>
Community string:	<input type="text" value="public"/>
Target hostname or IP address:	<input type="text"/>
<input type="button" value="Get response"/>	
Response SNMP data type:	
Response value:	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- In the **Object identifier** field, enter the object identifier.
 - In the **Community string** field, enter the community string if other than public, which is the default. To retrieve data, the community string of the target system and the HP Systems Insight Manager (HP SIM) server must match to retrieve data.
 - In the **Target hostname or IP address** field, enter the IP address of the system you want to search.
 - Click **Get response** to show the **Response SNMP data type** and the **Response value**.
 - To close the **Retrieve from system** section, click **OK**, and place the response value in the **System object identifier**, or **Object value** fields, or both.
- Enter the **System object identifier compare rule**. Click the down arrow and select the appropriate rule. In most cases, this rule is **match**. You can set it to **starts with** if you know that a class of systems has system object identifiers that start with the value you have entered.
 - (Optional) Specify **MIB variable object identifier** by clicking **Retrieve from MIB**. The **Retrieve from MIB** section appears.

You might need to perform this action if you have systems that return the same system object identifier that you would like to classify as different products based on an SNMP variable that returns a different value for each class. For example, if you have Windows NT servers from different vendors that return the same Windows NT system object identifier, you can specify rules using the Windows NT System Object Identifiers (OID) as the OID and a vendor-specific MIB variable and value combination to create separate rules for each vendor.

Retrieve from MIB:

Select a MIB file and MIB variable to view the MIB variable details below. Clicking 'OK' will transfer this value to the MIB Variable OID field above.

MIB definition file name:	<input type="text" value="rfc1213.mib"/>
MIB variable name:	<input type="text" value="sysDescr"/>
MIB variable object identifier:	1.3.6.1.2.1.1.1
MIB variable access:	READ-ONLY
MIB variable status:	MANDATORY
MIB variable type:	DISPLAYSTRING
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- Click the down arrow in the **MIB definition file name** box to select the MIB definition file.
 - Click the down arrow in the **MIB variable name** box to select the MIB variable name.
 - To close the **Retrieve from MIB** section, click **OK**, and place the **MIB variable object identifier** information in the field.
- Select the **Object value** by clicking **Retrieve from system**. The **Retrieve from system** section appears.
 - Enter the **Object identifier**, **Community string**, and **Target hostname or IP address**.
 - Click **Get response** to view the **Response SNMP data type** and the **Response value**.
 - To close the **Retrieve from MIB** section, click **OK**, and place the information in the **Object value** field.
 - Select the **Object value Data type** by clicking the down arrow and selecting either **string** or **integer**.
 - Select the **Object value Compare rule** by clicking the down arrow.
 - Enter a **Priority** (applies only if there is more than one rule with the same system object identifier).
 - In the **System type** field, click the down arrow, and then select the system type.

11. In the **Subtype** field, click the down arrow, and then select the system subtype.
12. In the **Product name** field, enter the product name for the new rule.
13. In the **Custom management page** field, enter a URL. The URL displays this web page as a system link on the **System Page** of systems identified using this rule. Enter the special keywords *\$ipaddress* and *\$hostname* anywhere in this URL. They are replaced by the actual IP address or host name of the system when the link is placed on the **System Page**.
14. Click **Launch** to verify that you can browse to the URL.
15. To save the new rule, click **OK**, or to cancel all changes and close the **New rule** section, click **Cancel**.

Command line interface

Use the `mxstm` command to add SNMP and DMI (Windows only) rules from the command line. For assistance with this command, see the HP-UX or Linux manpage by entering `man mxstm` at the command line. See “Using command line interface commands” for more information about the command and how to access the manpage.

Related procedures

- [Editing STM rules](#)
- [Deleting STM rules](#)

Related topics

- [Managing system types](#)
- [About System Type Manager](#)
- [Navigating the Manage System Types page](#)

Editing STM rules

Edit an existing *SNMP* rule using *System Type Manager (STM)* to change the priority, *system type*, subtype, or custom management page.



NOTE: Changing the priority on this page reorders the priorities of all other rules with the same system Object Identifier (OID) such that all rules with the same system OID have a unique priority ranging from one to the number of rules with the same system OID.

NOTE: All steps are optional.

To edit an SNMP rule:

1. Select **Options**→**Manage System Types**. The **Manage System Types** page appears.
2. Click **Edit**. The **Edit rule** section appears.
3. In the **Priority** field, change the priority.
4. In the **System type** field, click the down arrow to change the system type.
5. In the **Subtype** field, click the down arrow to change the subtype.
6. In the **Custom management page** field, change the URL. Click **Launch** to verify that you can browse to the URL launch page.
7. To save changes and return to the **Manage System Types** page, click **OK**, or to return to the **Manage System Types** page without saving any changes, click **Cancel**.

Related procedures

- [Creating STM rules](#)
- [Deleting STM rules](#)

Related topics

- [Managing system types](#)
- [About System Type Manager](#)
- [Navigating the Manage System Types page](#)

Deleting STM rules

1. Select **Options**→**Manage System Types**. The **Manage System Types** page appears.
2. Select the rule to delete.
3. Click **Delete**. A confirmation box is displayed.
4. Click **OK** to delete the rule, or click **Cancel** to cancel the deletion process.

Related procedures

- [Creating STM rules](#)
- [Editing STM rules](#)

Related topics

- [Managing system types](#)
- [About System Type Manager](#)
- [Navigating the Manage System Types page](#)

Additional information for creating STM rules

Manufacturers assign unique system Object Identifiers (OIDs) to their SNMP-instrumented products. In addition, *systems* supply information about themselves using variables described in files called *Management Information Bases* (MIBs). These values are enumerated using an industry-standard structure. MIBs are provided by vendors for their systems and must be registered with HP Systems Insight Manager (HP SIM) to be accessible and usable from *System Type Manager* (STM). HP preregisters all HP MIBs and many third-party MIBs. You can register the remaining MIBs using the MIB compiler, if you have the related systems on your network. See “[Registering a MIB](#)” for information about registering MIBs. If you examine a MIB, you will find modules, or groups of variables. Some variables have multiple values. Each of these values has an OID as well. You can use these OIDs to determine which system you have and its current behavior by querying these OIDs.

Things you should know about DMI identification

Desktop Management Interface (DMI) identification is based on how a system responds to a DMI request. Systems supply information about themselves as defined in files called MIFs. MIFs are vendor-specific. Simply having a *Management Information Format* (MIF) file on a target system does not guarantee DMI identification. MIFs cannot be registered the way MIBs are registered in HP SIM. If you examine a MIF (for example, the generic `Win32s1.MIF`), you will find groups of attributes. The values returned in response to requests for MIF attributes can be used to determine which system you have and its current behavior.

For example, the following extract is part of the `Win32s1.MIF`. Notice the group named *Component ID*, followed by several attributes that identify one aspect of a DMI system (such as *Manufacturer*, *Product*, *Version*, and *Serial Number*). Other MIFs have different groups and specify other aspects of a system. The information in the MIFs is the information supplied to STM when you create a rule. STM can request a value from a specific target for a specific attribute.



NOTE: DMI identification is only supported on Windows and HP-UX-based *Central Management Server* (CMS) installations. In addition, only like operating systems can be identified. For example, a Windows-based CMS can identify a Windows-based DMI, while HP-UX-based Central Management Server can only identify HP-UX-based DMI systems.

```
Start Group
Name = "ComponentID"
ID = 1 Class = "DMTF|ComponentID|001"
Description = "This group defines the attributes common to
all components. This group is required."
```

```
Start Attribute
Name = "Manufacturer"
ID = 1 Description = "Manufacturer of this system."
```



```

Access = Read-Only
Storage = Common
Type = String(64)
Value = "Intel Corporation"
End Attribute

Start Attribute
Name = "Product"
ID = 2
Access = Read-Only
Storage = Common
Type = String(64)
Value = "Win32 DMI Service Layer"
End Attribute

Start Attribute
Name = "Version" ID = 3
Description = "Version number of this component."
Access = Read-Only
Storage = Common
Type = String(64)
Value = "2.32" End Attribute

Start Attribute
Name = "Serial Number" ID = 4 Access = Read-Only
Storage = Common Type = String(64)
Value = "unsupported"
End Attribute ...

```

Adding new DMI rules (from Windows CMS only)

You can create a new DMI-based rule using the command line utility (`mxstm`). DMI system information originates in MIF files. MIF files contain elements that have attributes and corresponding values. See “Using command line interface commands” for information about accessing the `mxstm` manpage.

Adding new SNMP rules

You can create a new SNMP-based rule using the command line utility (`mxstm`) or by selecting **Options**→**Manage System Types** from the HP SIM user interface. Within the SNMP framework, manageable network systems (routers, bridges, servers, and so on) contain a software component called a *management agent*. The agent monitors the various subsystems of the network element and stores this information in a MIB. The agents enable the system to generate traps, which can be configured to be sent to a trap destination server that is running HP SIM.

Related procedures

- Creating STM rules
- Editing STM rules
- Deleting STM rules

Related topics

- Managing system types
- About System Type Manager
- Navigating the Manage System Types page

6 Users and authorizations



NOTE: *Users* that have been added to the *Central Management Server* (CMS) cannot view or manage systems until *authorizations* have been configured for them.

NOTE: Command line tools provided by HP-UX and Linux (such as `ls` and `df`) are run as root by default. For security reasons, you might want them to run as a specific user to avoid inadvertently allowing unauthorized access to a user.

HP Systems Insight Manager (HP SIM) enables you to configure authorizations for specific users or user groups. Authorizations give the user access to view and manage systems. Each authorization specifies a user or user group, a toolbox, and a system or system group. The specific set of tools that can be run on a system that is specified in the assigned toolbox.

It is important that you plan which systems each user will manage and which specific set of *tools* each user is authorized to execute on managed systems. A user with no toolbox authorizations on a particular system cannot view or manage that system.

Authorizations are cumulative. If a user is authorized for Toolbox1 and Toolbox2 on the same system, the user is authorized for all tools in both Toolbox1 and Toolbox2 on that system. Similarly, a user authorized for the **All Tools** toolbox on a system requires no other toolbox authorizations on that system because the **All Tools** toolbox always includes all tools.

See the following guidelines for setting up user names and authorizations in the following sections:

- “Configuring automatic discovery”
- “Creating new users”
- “Creating new user groups”
- “Creating new toolboxes”
- “Creating new authorizations”

Users authorization templates

The **Users and Authorizations** tabs offer the following options:

- **Add, edit, and delete users and user groups, and view and print user reports.** Select **Options**→**Security**→**Users and Authorizations**→**Users**.
- **Add, edit, and delete toolboxes, and view and print toolbox reports.** Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**.
- **Add, update, and delete authorizations, and view and print authorization reports.** Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**.



NOTE: By default, users created in HP SIM can access HP Storage Essentials with limited read privileges. You can change the permission settings by following the instructions and links on the **Users**, **Toolboxes**, and **Authorizations** tabs.

Related procedures

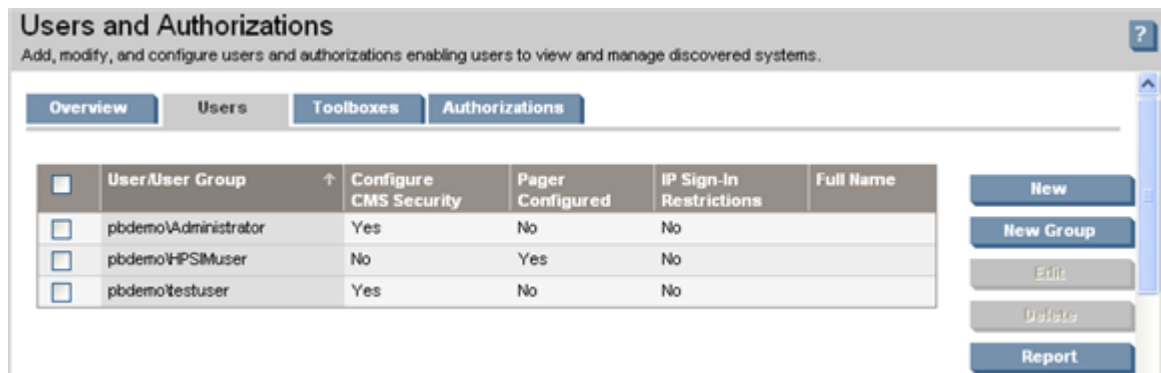
- Creating new users
- Creating new user groups
- Creating new toolboxes
- Creating new authorizations
- Editing user accounts and user groups
- Editing toolboxes
- Deleting user accounts and user groups
- Deleting toolboxes
- Deleting authorizations
- User and user group reports
- Toolbox report
- Authorizations report

Related topics

- Users and user groups
- Toolboxes
- Authorizations

Users and user groups

Administering *users* involves adding, editing, deleting, and reporting. After you have added a user or user group, you can assign predefined authorizations from the **Authorizations** tab.



Users and user groups must exist in the operating system. For Windows, this includes Active Directory. When a user group is configured in HP Systems Insight Manager (HP SIM), any user that is a member of the user group in the operating system can sign-in to HP SIM without having to be configured as a user in HP SIM. The user can subsequently create tasks and run tools based on the user group's authorizations and configuration rights as configured in HP SIM.

The **Users** tab displays a table with the following information:

- **User/User Group** This column includes all users and user groups. A user group is displayed in bold type, while group-based user accounts (members of a configured user group) are displayed in italics.
- **Configuration CMS Security** This column indicates if the user has been given the right to configure CMS security. This option is set when you select or clear the **User can configure CMS security access such as creating, modifying or removing other users** checkbox when creating or editing users. The column displays either **Yes** or **No**.
- **Pager Configured** This column indicates if the user has a pager configured (**Yes** or **No**.) and is blank for user groups.
- **IP Sign-In Restrictions** This column indicates if there are any IP restrictions applied to the user or user group.
- **Full Name** This column displays the full name of the user or group if this information was entered during the creation of the user or user group.

The **Users** tab provides the following options:

- **Create new users.** Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then click **New**. The **New User** section appears.
- **Create new user groups.** Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then click **New Group**. The **New User Group** section appears.
- **Edit existing users or user groups.** Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then select a user or user group. Click **Edit**. The **Edit User** or **Edit User Group** section appears. You can edit group-based (in italics) users to convert them to individually configured users.
- **Delete users or user groups.** Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then select users or user groups. Click **Delete**. A confirmation box appears. To delete the users or user groups, click **OK**, or to cancel the deletion, click **Cancel**.
- **View and print user reports.** Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then click **Report**. The **Users Report** window appears. To print the report, select **File**→**Print**.



NOTE: To sort the information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the list is sorted. If the

arrow is pointing up, the list is sorted in ascending order. If the arrow is pointing down, the list is sorted in descending order.

- **Run SE user security configuration** By default, users created in HP SIM can access HP Storage Essentials with limited read privileges. To edit user roles and give users additional privileges, click the **Run SE user security configuration** link.

Related procedures

- Creating new users
- Creating new user groups
- Editing user accounts and user groups
- Deleting user accounts and user groups
- User and user group reports

Related topics

- Users and authorizations
- Toolboxes
- Authorizations
- Default user templates

Creating new users

Create a new *user* account to sign-in to HP Systems Insight Manager (HP SIM). The account must be valid on the operating system (including Active Directory on Windows) on the *Central Management Server* (CMS) and is authenticated by the CMS. You must know the operating system *user account* name of the user you are adding, but it is not necessary to know the password.

To create a new user:

1. Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then click **New**. The **New User** section appears.
2. (Required) In the **Sign-in name [on central management server(CMS)]** field, enter the operating system login account name to be used to sign-in to HP SIM. This field is required.
Note: The user cannot sign-in to HP SIM if the account is not a valid login. The account is not validated until the user attempts to sign-in to HP SIM.
3. (Optional) In the **Domain (Windows® domain for sign-in name)** field, enter the Windows domain name for the login name if the CMS is running a Windows operating system. If left blank, the CMS system name is used as the domain.
Note: If the user account was migrated from Insight Manager 7, the **Domain (Windows® domain for login name)** field associates a placeholder domain with the user. If the user receives pages, this field must be edited to include a valid domain on your network.
4. (Optional) In the **Full name** field, enter the user's full name.
5. (Optional) If you are using Windows, in the **Phone** field of the **Pager Information** section, enter the pager phone number. If the **Phone number** field is left blank, the paging information is not saved. This field does not apply to user groups..
6. (Optional) In the **E-mail address** field, enter the user's e-mail address.
7. In the **Copy all authorizations of this user or [template]** field, select a template (administrator-template, operator-template, or user-template) or sign-in account that already has the predefined authorizations that you want to assign to the sign-in account you are creating. See "Default user templates" for more information about default user templates.
8. For user accounts that must be able to create, modify, or delete other accounts in the **Central management server security configuration right** section, select **User can configure CMS security access such as creating, modifying or removing other users**. If you selected an existing user with administrative rights or the administrator template in the previous step, this option is automatically selected.

9. Under the **Sign-In IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems you want this user to be able to use as a client browsing this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted decimal notation, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in the dotted decimal notation. Enter 0.0.0.0 to prevent a user from logging in through a remote system.
Important: If browsing from the CMS, ensure all IP addresses of the CMS are properly included. If browsing to `localhost`, ensure the loopback address 127.0.0.1 is also included.
10. In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from management by this user or user group. Use the same format as in the previous step for **Inclusion ranges**. Enter 0.0.0.0 to prevent a user from logging in through a remote system.
Note: Ensure that your inclusion and exclusion ranges do not overlap.
Note: The following five steps are only for a CMS running Windows.
11. Under the **Pager Information** section, in the **Phone number** field, enter the pager phone number of the user associated with this user account if you are using a Windows operating system. If the **Phone number** field is left blank, the paging information is not saved. This field does not apply to user groups.
12. In the **PIN number** field, enter the PIN number associated with the pager phone number. This field does not apply to user groups.
13. In the **Message length** field, select how many characters can be accepted in the paging message from the dropdown list. This field does not apply to user groups.
14. In the **Baud rate** field, select the appropriate baud rate for the pager from the dropdown list. This field does not apply to user groups.
15. In the **Data format** field, select the appropriate data format for the pager from the dropdown list. This field does not apply to user groups.
16. To save and close the **New User** section, click **OK**. The new user account is created. To save and keep the **New User** section open, click **Apply**, or to cancel the creation of this user, click **Cancel**.

Command line interface

Users with *administrative rights* can use the `mxuser` command to create users from the *command line interface (CLI)*



NOTE: Users must have the **User can configure CMS security access such as creating, modifying or removing other users** option selected when their account is set up for them to be able to use the `mxuser` command.

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- [Editing user accounts and user groups](#)
- [Deleting user accounts and user groups](#)
- [User and user group reports](#)

Related topics

- [Users and authorizations](#)
- [Users and user groups](#)
- [Default user templates](#)

Creating new user groups

User groups must exist in the operating system. For Windows, they must also exist in Active Directory. Members of user groups in the operating system can sign-in to HP Systems Insight Manager (HP SIM) and inherit the group's attributes for configuration rights, sign in IP address restrictions, and authorizations. When

a group's configuration rights, sign in IP address restrictions, or authorizations are changed, this change is immediately reflected for all current members of the group.

With configuration rights, the user inherits the highest setting. With sign-in IP address restrictions, the user inherits all entries. With authorizations, the user inherits all authorizations.



NOTE: A user's group membership is determined at sign-in. If a user's group membership changes in the operating system, it is not reflected in HP SIM until the next time the user signs in to HP SIM.

To create a new user group:

In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from management by this user or user group. Use the same format as in the previous step for **Inclusion ranges**. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

1. Select **Options**→**Security**→**Users and Authorizations**→**Users**, and then click **New Group**. The **New User Group** section appears.
2. In the **Group name (on central management server)** field, enter the operating system group name to be used for signing in to HP SIM. This field is required.
3. If the *Central Management Server* (CMS) is running a Windows operating system, in the **Domain (Windows domain for login name)** field, enter the Windows domain name for the group .
4. In the **Full name** field, enter the full name for the group. This name appears in the table under the **Users** tab.
5. In the **Copy all authorizations of this user or [template]** field, select a template or sign in that already has the predefined authorizations that you want to assign to the group you are creating. See “Default user templates” for more information about default user templates.
6. For user accounts that must be able to create, modify, or delete other accounts in the **Central management server security configuration right** section, select **User can configure CMS security access such as creating, modifying or removing other users**. If you selected an existing user with administrative rights or the administrator template in the previous step, this option is automatically selected.
7. Under the **Sign-In IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems you want this user to be able to use as a client browsing this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted decimal notation, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes are ignored. Spaces are not allowed within a single IP address in the dotted decimal notation. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Important: If browsing from the CMS, ensure all IP addresses of the CMS are properly included. If browsing to `localhost`, ensure the loopback address 127.0.0.1 is also included.

8. To save and close the **New User Group** section, click **OK**. To save and keep the **New User Group** section open, click **Apply**, or to cancel to close the **New User Group** section without saving the new group, click **Cancel** .

Command line interface

Users with *administrative rights* can use the `mxuser` command to create a user group from the *command line interface (CLI)*



NOTE: Users must have the **User can configure CMS security access such as creating, modifying or removing other users** option selected when their account is set up for them to be able to use the `mxuser` command.

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Editing user accounts and user groups
- Deleting user accounts and user groups
- User and user group reports

Related topics

- Users and authorizations
- Users and user groups
- Default user templates

Editing user accounts and user groups

In the event a *user account* or user group must be modified, you can edit it from the **Users** tab on the **Users and Authorizations** page.



NOTE: If a group's configuration rights or sign-in IP address restrictions are changed, these changes are immediately applied to all current members of the group. If a group name is edited, none of its current members are affected, other than displaying the new group name.

NOTE: A group-based user account can be edited only to convert to an individual user account and is not reversible.

To edit a user account or user group:

1. Select **Options**→**Security**→**Users and Authorizations**→**Users**.
2. Select the user or user group you want to edit, and then click **Edit**. The **Edit User** or **Edit User Group** section appears.
3. Change the appropriate setting.

Note: Steps d through e and i through m do not apply to user groups.

- a. (Required) In the **Sign-in name [on central management server(CMS)]** field, enter the operating system login account name to be used to sign-in to HP SIM. This field is required.

Note: The user cannot sign-in to HP SIM if the account is not a valid login. The account is not validated until the user attempts to sign-in to HP SIM.

- b. (Optional) In the **Domain (Windows® domain for sign-in name)** field, enter the Windows domain name for the login name if the CMS is running a Windows operating system. If left blank, the CMS system name is used as the domain.

Note: If the user account was migrated from Insight Manager 7, the **Domain (Windows® domain for login name)** field associates a placeholder domain with the user. If the user receives pages, this field must be edited to include a valid domain on your network.

- c. (Optional) In the **Full name** field, enter the user's full name.
- d. (Optional) If you are using Windows, in the **Phone** field of the **Pager Information** section, enter the pager phone number. If the **Phone number** field is left blank, the paging information is not saved. This field does not apply to user groups..
- e. (Optional) In the **E-mail address** field, enter the user's e-mail address.
- f. For user accounts that must be able to create, modify, or delete other accounts in the **Central management server security configuration right** section, select **User can configure CMS security access such as creating, modifying or removing other users**. If you selected an existing user with administrative rights or the administrator template in the previous step, this option is automatically selected.
- g. Under the **Sign-In IP Address Restrictions** section, in the **Inclusion ranges** field, enter the IP addresses of the systems you want this user to be able to use as a client browsing this CMS. If you list multiple IP addresses, separate them with a semicolon (;). Each range is a single IP address or two IP addresses separated by a dash (-). The IP addresses must be entered in the standard dotted decimal notation, for example, 15.1.54.133. Any spaces surrounding the semicolons or dashes

are ignored. Spaces are not allowed within a single IP address in the dotted decimal notation. Enter 0.0.0.0 to prevent a user from logging in through a remote system.

Important: If browsing from the CMS, ensure all IP addresses of the CMS are properly included. If browsing to `localhost`, ensure the loopback address 127.0.0.1 is also included.

- h. In the **Exclusion ranges** field, enter the IP address of the systems that should be excluded from management by this user or user group. Use the same format as in the previous step for **Inclusion ranges**. Enter 0.0.0.0 to prevent a user from logging in through a remote system.
 - i. Under the **Pager Information** section, in the **Phone number** field, enter the pager phone number of the user associated with this user account if you are using a Windows operating system. If the **Phone number** field is left blank, the paging information is not saved. This field does not apply to user groups.
 - j. In the **PIN number** field, enter the PIN number associated with the pager phone number. This field does not apply to user groups.
 - k. In the **Message length** field, select how many characters can be accepted in the paging message from the dropdown list. This field does not apply to user groups.
 - l. In the **Baud rate** field, select the appropriate baud rate for the pager from the dropdown list. This field does not apply to user groups.
 - m. In the **Data format** field, select the appropriate data format for the pager from the dropdown list. This field does not apply to user groups.
4. To save and close the **Edit User** section, click **OK**. The new user account is created. To save and keep the **Edit User** section open, click **Apply**, or to cancel the modifications for this user, click **Cancel**.
The user or group changes are saved.

Command line interface

Users with *administrative rights* can use the `mxuser` command to modify users or user groups from the *command line interface* (CLI).



NOTE: Users must have the **User can configure CMS security access such as creating, modifying or removing other users** option selected when their account is set up for them to be able to use the `mxuser` command.

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- [Users and authorizations](#)
- [Creating new users](#)
- [Creating new user groups](#)
- [Deleting user accounts and user groups](#)
- [User and user group reports](#)

Related topics

- [Users and authorizations](#)
- [Users and user groups](#)

Deleting user accounts and user groups

If an HP Systems Insight Manager (HP SIM) *user account* or user group is deleted from the operating system, or disabled or locked out, and the *user* is already signed in to HP SIM, the signed-in user is not affected. Therefore, to remove a signed in user from HP SIM, the user account must be deleted from within HP SIM. Deleting the user account from HP SIM forces the user to sign out if he or she is already signed in to HP SIM.

When deleting a user group, all members of the group lose membership in that group, which causes those users' authorizations, configuration rights, and login IP address restrictions to be updated based on their new group memberships. Users that are no longer members of any user group are deleted from HP SIM.



CAUTION: Deleting a user or user group prevents the user or group from signing-in and removes all associated *authorizations* and *tasks* that are owned by that user or user group.



NOTE: You cannot remove the last user account with *administrative rights*.

To delete a user account or user group:

1. Select **Options**→**Security**→**Users and Authorizations**→**Users**.
2. Select the users or groups to be deleted.
3. Click **Delete**. A confirmation box appears.
4. to delete the selected users or user groups, click **OK**, or to cancel the deletion process and return to the **Users** section, click **Cancel** . Deleting a user group also deletes all members of the group, and a second confirmation box appears, listing which users will be deleted. To continue and delete all listed users, click **OK**, or to cancel the deletion process and return to the **Users** section, click **Cancel**.

The users, user groups, associated authorizations, and tasks are permanently deleted.

Command line interface

Users with *administrative rights* can use the `mxuser` command to modify users and user groups from the *command line interface* (CLI).



NOTE: Users must have the **User can configure CMS security access such as creating, modifying or removing other users** option selected when their account is set up for them to be able to use the `mxuser` command.

Users with *operator rights* can use the `mxexec` command to launch command tools on one or more systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- [Creating new users](#)
- [Creating new user groups](#)
- [Editing user accounts and user groups](#)
- [User and user group reports](#)

Related topics

- [Users and authorizations](#)
- [Users and user groups](#)

User and user group reports

For detailed information about *users* and user groups, you can generate and print a report.



NOTE: To sort information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the report is sorted. If the arrow is pointing up, the report is sorted in ascending order. If the arrow is pointing down, the report is sorted in descending order.

The following summary of user information appears in the **Users Report** window, along with the date and time of the report:

- **User/User Group**
- **Configuration Rights**

- **Pager Configured**
- **IP Login Restrictions**
- **Full Name**

To generate and print a user account or user group report:

1. Select **Options**→**Security**→**Users and Authorizations**→**Users**.
2. Click **Report**.
The **Users Report** window appears.
3. To print the report, select **File**→**Print**.
The user report is printed.

Command line interface

Users with *administrative rights* can use the `mxuser` command to create user and user group reports from the *command line interface* (CLI).

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new users
- Creating new user groups
- Editing user accounts and user groups
- Deleting user accounts and user groups

Related topics

- Users and authorizations
- Users and user groups

Default user templates

The default templates have predefined authorizations that are assigned to the new sign-in account you are creating. This authorization gives the user access to systems and creates a relationship between toolboxes and discovered systems. Separate tools are provided for each access level, and the user can be authorized for these user access tools in the **Monitor Tools** toolbox, while administrative access tools are assigned in the **All Tools** toolbox.

The following default user templates are available in HP Systems Insight Manager (HP SIM):

- **Administrator-template** This template automatically gives the user administrative rights on the *Central Management Server* (CMS) and includes the **All Tools** toolbox for the CMS and for **All Managed Systems**.
- **Operator-template** This template gives the user operator rights on the CMS and includes authorizations for the **Monitor Tools** toolbox on the CMS and the **All Tools** toolbox on **All Managed Systems**.
- **User-template** This template gives the user user rights on the CMS and includes authorizations for the **Monitor Tools** toolbox for the CMS and **All Managed Systems**.

Related topics

- Creating new users
- Creating new user groups
- Toolboxes

Toolboxes

The **Toolboxes** section enables you to configure groups of *tools*. The following toolboxes are created during the installation process::

- The **All Tools** toolbox contains all tools in the *Central Management Server* (CMS).
- The **Monitor Tools** toolbox contains tools that display the state of the *managed systems* but not tools that change the state of the managed systems. For example, the **Monitor Tools** toolbox permits viewing installed software but does not permit installing software.
- The **Full Rights** toolbox contains all tools in the *Central Management Server* (CMS).
- The **Limited Rights** toolbox contains only the create and edit both reports and tools.
- When HP Storage Essentials is installed, a Toolbox for Storage Essentials tools is added to this page. See your HP Storage Essentials documentation for more information.

The **Toolboxes** tab provides the following options:

- **Create new toolboxes.** Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**, and then click **New**. The **New Toolbox** section appears.
- **Edit existing toolbox.** Select a toolbox to edit, select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**, and then, click **Edit**. The **Edit Toolbox** section appears.
- **Delete toolboxes.** Select toolboxes to delete, and then select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**. A confirmation box appears. To delete the toolboxes, click **OK**, or to cancel the deletion, click **Cancel**.
- **View and print toolbox reports.** Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**, and then click **Report**. The **Toolboxes Report** appears. To print the report, select **File**→**Print**.



NOTE: To sort information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the list is sorted. If the arrow is pointing up, the list is sorted in ascending order. If the arrow is pointing down, the list is sorted in descending order.

- **Run SE user security configuration** Toolboxes defined in HP SIM are not automatically shared with HP Storage Essentials. Click **Run SE role security configuration** to create a toolbox equivalent (role) in HP Storage Essentials. By default, HP SIM users have limited read access to all HP Storage Essentials managed systems and features.

Related procedures

- [Creating new toolboxes](#)
- [Editing toolboxes](#)
- [Deleting toolboxes](#)
- [Toolbox report](#)

Related procedures

- [Users and user groups](#)
- [Authorizations](#)
- [Default user templates](#)

Creating new toolboxes

Create a *toolbox* to configure a group of *tools* for each *user* has access. Toolboxes are set up so that some users can use certain tools but not others. For example, an administrator has access to more tools than a user.



NOTE: The toolbox name must start with an alphabetic character followed by alphanumeric characters, embedded blank characters, underscore (_), or dash (-) and must be less than or equal to 16 characters in length.

To add a toolbox:

1. Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**, and then click **New**. The **New Toolbox** section appears.
2. In the **Name** field, enter a name for the new toolbox. This field is required.
3. In the **Description** field, enter a description for the toolbox.
4. To enable the toolbox and all authorizations created with this toolbox, select **Toolbox is enabled**.
5. To display a list of tools in the available tools list, in the **Show tools in category** field, select a category. In the available tools list, select the tools to be assigned to this toolbox, and then click **>>**.

The selected tools appear in the **Toolbox contents** list. To remove a tool from the associated tools list, you can select a tool displayed in the **Toolbox contents** list, and then click **<<**.

Note: The **HP SIM Tools** category includes tools that are related to configuration rights on the HP SIM server itself. In previous versions of HP SIM, these rights were only enabled to full configuration rights users. With HP SIM 5.2, any user can be granted these rights if needed based on an authorization. These tools include: Delete Systems in HP SIM, Edit any user tasks in HP SIM, Edit HP SIM Notification Settings, Edit HP SIM Reports, Edit Shared Collections in HP SIM, Edit Systems in HP SIM, Modify HP SIM Events, Run HP SIM Discovery, and View HP SIM Audit Log.

Note: For users with *operator rights* and user rights to clear, delete, assign events, and add comments to events, you must select **Configuration Tool** from the **Show tools in category** dropdown list. Then, select **Clear Events**, **Delete Events**, **Assign Events**, and **Comment Events** as necessary, and then click **>>** to add them to the **Toolbox contents**.

6. To save the new toolbox and close the **New Toolbox** section, click **OK**. To save the settings without closing the **New Toolbox** section, click **Apply**, or to cancel the new toolbox creation and return to the **Toolboxes** section, click **Cancel**.

Command line interface

Users with *administrative rights* can use the `mxtoolbox` command to add toolboxes from the *command line interface* (CLI).

Users with *operator rights* can use the `mxexec` command to launch command tools on one or more systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Editing toolboxes
- Deleting toolboxes
- Toolbox report

Related topics

- Users and authorizations
- Toolboxes


Editing toolboxes

You can change *toolboxes* to modify the contents, name, and description of the toolbox.



NOTE: The *All Tools toolbox* cannot be edited. While, the *Monitor Tools toolbox* can be edited, but only the set of *tools* contained in the toolbox can be changed.

To modify a toolbox:

1. Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**.
2. Select the toolbox to edit, and then click **Edit**. The **Edit Toolbox** section appears.
Note: For users with *operator rights* and user rights to clear, delete, assign events, and add comments to events, you must select **Configuration Tool** from the **Show tools in category** dropdown list. Then, select **Clear Events**, **Delete Events**, **Assign Events**, and **Comment Events** as necessary, and then click  to add them to the **Toolbox contents**.
3. Change the appropriate setting. See “Creating new toolboxes” for more detailed information about each field.
Note: New custom tools are located under **Tools**→**Custom Tools**.
4. To save changes, click **OK**, or to cancel the changed, click **Cancel**.

Command line interface

Users with *administrative rights* can use the `mxttoolbox` command to modify toolboxes from the *command line interface* (CLI).

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new toolboxes
- Deleting toolboxes
- Toolbox report

Related topics

- Users and authorizations
- Toolboxes

Deleting toolboxes



CAUTION: When a *toolbox* is deleted, all of the associated *authorizations* are also deleted.



NOTE: The *All Tools toolbox* and the *Monitor Tools toolbox* cannot be deleted.

To delete a toolbox:

1. Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**.
2. Select the toolboxes to be deleted.
3. Click **Delete**. A confirmation box appears.
4. To delete the toolboxes, click **OK**, or to cancel the deletion process, click **Cancel**.
The toolbox and all associated authorizations are permanently deleted.

Command line interface

Users with *administrative rights* can use the `mxttoolbox` command to delete toolboxes from the *command line interface* (CLI).

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new toolboxes
- Editing toolboxes
- Toolbox report

Related topics

- Users and authorizations
- Toolboxes

Toolbox report

For detailed information about a *toolbox*, you can generate and print a toolbox report.



NOTE: To sort the report information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the report is sorted. If the arrow is pointing up, the report is sorted in ascending order. If the arrow is pointing down, the report is sorted in descending order.

The following information about all toolboxes appears in the **Toolboxes Report** window, along with the date and time of the report:

- **Toolbox**
- **Enabled**
- **Tools**
- **Description**

To print a toolbox report:

1. Select **Options**→**Security**→**Users and Authorizations**→**Toolboxes**.
2. Click **Report**.

The **Toolboxes Report** window appears.

3. Select **File**→**Print** to print the report.

The toolbox report is printed.

Command line interface

Users with *administrative rights* can use the `mxttoolbox` command to generate and run reports from the *command line interface* (CLI).

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new toolboxes
- Editing toolboxes
- Deleting toolboxes

Related topics

- Users and authorizations
- Toolboxes

Authorizations

Authorizations give *users* access to view and manage *systems*. An authorization is composed of users, *toolboxes*, and discovered systems. When you first access the **Authorizations** tab, a table appears listing all authorizations and includes the following information:

- **User/User Group** This column includes all valid users and user groups. A user group is displayed in bold type. Group-based users are not displayed in this table. However, they are listed in the **authorizations for users** table and are displayed in italics.
- **Toolbox** This column displays the toolboxes assigned to the user or user group for each authorization.

- **System** This column displays the systems on which the user or user group has authorizations. A system group is displayed in bold type.
- **Auto** This column displays **Auto** if the authorization is set to automatically update when the collections that the authorization is based upon are updated.

The screenshot shows the 'Users and Authorizations' management interface. It has tabs for Overview, Users, Toolboxes, and Authorizations. A dropdown menu shows 'Authorizations for all authorizations'. Below is a table with columns: checkboxes, User/User Group, an arrow icon, Toolbox, Systems, and Auto. The table contains four rows of authorization data. To the right of the table are buttons for New, Update, Delete, and Report.

<input type="checkbox"/>	User/User Group	↑	Toolbox	Systems	Auto
<input type="checkbox"/>	nimbusdemo\Administrator		All Tools	CMS	
<input type="checkbox"/>	nimbusdemo\Administrator		All Tools	All Managed Systems	
<input type="checkbox"/>	NIMBUSDEMO\testuser		All Tools	CMS	
<input type="checkbox"/>	NIMBUSDEMO\testuser		All Tools	All Managed Systems	

A system group is a group of systems based on a system collection that is used for authorizations. Authorizations that use system groups are updated automatically when a change is made to the system collection that the system group is based upon. For authorizations to be updated automatically, the option, **Do not track changes. If this collection changes, the authorization will not change** must not be selected.

You can view all authorizations, or you can view filtered authorizations for users, user groups, toolboxes, system groups, and individual systems. Select the option from the **Authorizations for** box, and then select the name from the **Select name** box.

The **Authorizations** tab provides the following options:

- **Creating new authorizations** Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**, and then click **New**. The **New Authorizations** section appears. This option is not available for group-based users. Instead, create authorizations for the user group of the group-based user.
- **Deleting authorizations** Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**, select authorizations to delete, and then click **Delete**. A dialog box appears. To delete the authorizations, click **OK**, or to cancel the deletion, click **Cancel**. This option is not available for group-based users. Instead, delete authorizations for the user groups of the group-based user.
- **Viewing and printing authorization reports** Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**, and then click **Report**. The **Authorizations Report** window appears. To print the report, select **File**→**Print**.
- **Updating authorizations** Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**, select an authorization using a system group based on a collection, and then click **Update**. The **Update Authorizations** section appears.



NOTE: To sort the information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the list is sorted. If the arrow is pointing up, the list is sorted in ascending order. If the arrow is pointing down, the list is sorted in descending order.

- **Run SE user security configuration** Authorizations defined in HP SIM are not automatically shared with HP Storage Essentials. To update user security in HP Storage Essentials, click the **Run SE user security configuration** link.

- You can define separate authorizations in HP Storage Essentials on the **Users** page.
- By default, HP SIM users have limited read access to all HP Storage Essentials managed systems and features. You can modify access privileges on the **Roles** page.
- Use the **Organizations** page to control the HP Storage Essentials managed systems that are visible to HP SIM users.

Related procedures

- Creating new authorizations
- Deleting authorizations
- Updating authorizations
- Authorizations report

Related topics

- Users and authorizations
- Users and user groups
- Toolboxes
- Default user templates

Creating new authorizations



NOTE: To create *authorizations* with individual *systems*, be sure the systems have been *discovered* and are accessible in the *database*.

NOTE: You cannot directly create new authorizations for group-based users.

To add a new authorization:

1. Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**, and then click **New**. The **New Authorizations** section appears.
2. In the **Select** dropdown list, select **User(s)** or **UserGroup(s)**, and then select the users or groups in the box. This field is required.
3. In the **Enter authorizations for the selected user(s)** section, select one of the following options:
 - **Copy all authorizations of this user or [template]**
Select a user or template from the dropdown list.
 - **Manually assign toolbox and system/system group authorizations**
 - a. In the **Select Toolbox(es)** section, select the toolboxes to include.

Users and Authorizations

Add, modify, and configure users and authorizations enabling users to view and manage discovered systems.

Maximize ?

New Authorizations

Required field:*

Select : *
0 selected

pbdemo\Administrator

Enter authorizations for the selected user(s)

- Copy all authorizations of this user or [template]: [administrator-template] ▼
- Manually assign toolbox and system/system group authorizations:

Select Toolbox(es): *
0 selected

All Tools

Full Rights

iLO Tools

Limited Rights

Monitor Tools

Select Systems: *
0 selected

[Add...](#)

All Managed Systems

CMS

OK

Cancel

Apply

- b. In the **Select Systems** list box, the two default system groups (**All Managed Systems** and **CMS**) are displayed. Select one of these groups, or to select systems for the authorization, click **Add** to display the **Add Systems** section.
- c. In the **Add systems by selecting from** section, select one of the following:
 - i. **Collection** Select a collection and click **View contents**.

If you want to use the entire collection as your selection, select **Select "collection name" itself**. This option creates a system group based on the currently displayed contents of the collection.

- a. (Optional) To enable the authorization to automatically be updated, without user intervention when a collection is changed, select **Automatically track changes. If this collection changes, so does the authorization**.
- b. (Optional) Select **Do not track changes. If this collection changes, the authorization will not change**. If this option is selected, you must manually update the authorization after a collection has changed by using the **Update** button on the **Authorizations** tab.

Note: These two selections are only available if a collection of systems is selected and the **Select "collection name" itself** option is selected. You must select one option or the other. The default selection is based on the *DynamicAuthorizations_AutoUpdateDefaultValue* property setting in the *globalsettings.props* file. The default is set to **Yes**. This is reflected in the **Select Systems** list box in the **New Authorizations** section with [Auto] appended to the entry. For example, if you selected **All Systems** and chose to have it automatically updated, **All Systems 001 [Auto]** would be displayed in the **Select Systems** box.

You can continue to add systems and collections and can enable automatic updates for each selected collection. Since automatic updates for any authorization apply to all authorizations using the same selected collection, changing the setting for one affects any other authorization using the same collection. Therefore, during system selections, if you select a group already associated with an automatically updating authorization, the option **Automatically track changes. If this collection changes, so does the authorization** is preselected. Likewise, if an authorization that does not automatically update is associated with a collection, the option **Do not track changes. If this collection changes, the authorization will not change** is preselected.

- c. If you want to select all individual systems from the collection, select the checkbox at the top of the table view in the column heading to select all systems.
Note: This action creates a separate authorization for each selected system.
- d. To save system selections, click **Apply**, or to return to the **New Authorizations** section without saving changes, click **Cancel**.

After clicking **Apply**, a message appears based on the options selections. To return to the **New Authorizations** section, click **OK**.

- ii. **Search** Enter a system name and click **Search**, or select a system from the list and click **Search**.
 - a. Select systems.
 - b. Click **Apply**, or to return to the **New Authorizations** section without saving changes, click **Cancel**.
After clicking **Apply**, a message appears based on the options selections. Click **OK** to return to the **New Authorizations** section.

A system group is a group of systems based on a system collection that is used for authorizations. Authorizations that use system groups are updated automatically when a change is made to the system collection that the system group is based upon. The option **Do not track changes. If this collection changes, the authorization will not change** must not be selected for the authorizations to be updated automatically.

If you selected individual systems of a collection, each selection populates the list box and is selected for inclusion in the authorization. If you selected a collection and the collection has been used previously in an authorization, a message appears stating that a system group for the collection exists and will be updated with current source collection content. This condition affects all authorizations associated with that collection. When a collection is used for the first time, no message appears. A system group with the name of the collection followed by three numbers, usually (001) is displayed in the **Select Systems** dropdown list and is selected.

4. To save the new authorization and close the **New Authorizations** section, click **OK**, or, if you do not want to create the authorization, click **Cancel**.



NOTE: You you add CMS tools to any other system, a warning appears alerting you, that the authorization just added contains an HP SIM-based tool in the toolbox and that the CMS server was not selected. It also states that the authorization was created but might not authorize the user on all the selected tools. Some tools in HP SIM are used to manage HP SIM itself. For example, discovery or viewing the HP SIM audit log. This error means that one or more of these tools were in a selected toolbox and the CMS was not one of the selected systems. To correct this error, select the CMS as one of the target systems.

NOTE: When upgrading to HP Systems Insight Manager (HP SIM) 5.x from any other version of HP SIM, any system groups that the user created are migrated, but become top-level collections. To manage these system groups, use the feature to edit a collection and update an authorization. See “Editing system or cluster collections” and “Updating authorizations” for more detailed information.

Command line interface

Users with *administrative rights* can use `mxngroup` to create and manage system groups from the command line interface (CLI).

Users with administrative rights can use the `mxauth` command to add authorizations from the CLI.



NOTE: Users must have the **User can configure CMS security access such as creating, modifying or removing other users** option selected when their account is set up for them to be able to use the `mxngroup` and `mxauth` commands.

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Deleting authorizations
- Authorizations report
- Updating authorizations

Related topics

- Users and authorizations
- Authorizations

Updating authorizations

This option is only available for authorizations using system groups based on a collection. It enables the contents of a system group to be updated to the current contents of its source collection. All authorizations using this system group (collection) are updated.

To update an authorization:

1. Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**, select an authorization based on a system group, and then click **Update**. The **Update Authorizations** section appears.
2. In the **Show** dropdown list, select **changes**, **current contents**, or **updated contents**.
 - **changes** Describes the specific changes that occur to the system group if updated. **Systems to Add** shows new systems to be added to the system group and added to all authorizations based on the system group. **Systems to Remove** shows current systems to be removed from the system and removed from all authorizations using the system group. **Systems Unchanged** shows a list of systems that are unaffected by the update. They remain unchanged in the system group and all authorizations based on the system group.



- **current contents** Shows the current contents of the system group.
 - **updated contents** Shows what the contents of the system group will be after updating. This option applies to authorizations based on this system group.
3. To update the authorization, click **Update Contents**, or to cancel the update, click **Cancel**.

Command line interface

Users with *administrative rights* can use `mxngroup` to update system groups from the command line interface (CLI). However, if there are edits to the system group from the CLI, there is no affect on the source collection. See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new authorizations
- Deleting authorizations
- Authorizations report

Related topics

- Users and authorizations
- Authorizations

Deleting authorizations



CAUTION: If all authorizations are deleted, no user, not even a user with *administrative rights*, can view or manage any systems.

To delete an authorization:

1. Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**.
2. Select the authorizations to be deleted.
3. Click **Delete**. A confirmation box appears.
4. To delete the authorizations, click **OK**, or to cancel the deletion process and return to the **Authorizations** section, click **Cancel**.

Authorizations cannot be directly deleted for group-based users. Instead, delete the authorizations for the user group of the group-based user.



NOTE: When deleting the last authorization using a system group, other than the default **All Managed Systems** of **CMS** system groups, the system group is also deleted.

Command line interface

Users with *administrative rights* can use the `mxngroup` command to delete system groups using the *command line interface* (CLI).

Users with *administrative rights* can use the `mxauth` command to delete authorizations using the *command line interface* (CLI).

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new authorizations
- Authorizations report
- Updating authorizations

Related topics

- Users and authorizations
- Authorizations

Authorizations report

Generate an **Authorizations Report** to view and print authorizations. The **Authorizations Report** is tailored to the current filtered view. For example, if **user** is selected in the **Authorizations for** box, a report

is generated for only for the user selected. If **(none)** is selected in the **Select name** dropdown list, a report is generated for everything selected in the **Authorizations** box.



NOTE: To sort the report information in ascending or descending order, click the appropriate column heading. The column heading that includes the arrow is the column by which the report is sorted. If the arrow is pointing up, the report is sorted in ascending order. If the arrow is pointing down, the report is sorted in descending order.

The following information about authorizations appears in the **Authorizations Report** window, along with the date and time of the report:

- **User/User Group**
- **Toolbox**
- **System**

To view and print an authorizations report:

1. Select **Options**→**Security**→**Users and Authorizations**→**Authorizations**.
2. Select an *authorization* from the **Authorizations for** dropdown list.
3. (Optional) Select a name from the **Select name** dropdown list.
4. Click **Report**.

The **Authorizations Report** appears.

5. to print the report, select **File**→**Print**.
The **Authorizations Report** is printed.

Command line interface

Users with *administrative rights* can use the `mxngroup` command to generate and run system group reports from the *command line interface* (CLI).

Users with *administrative rights* can use the `mxauth` command to generate and run reports from the CLI.

Users with *operator rights* can use the `mxexec` command to launch command tools on systems from the CLI. For assistance with this command, see the associated manpage.

See “Using command line interface commands” for information about accessing the manpage.

Related procedures

- Creating new authorizations
- Deleting authorizations
- Updating authorizations

Related topics

- Users and authorizations
- Authorizations

System groups

A system group is a group of systems used solely for authorizations. System groups can be managed directly from the *command line interface* (CLI) using the `mxngroup` command, or they can be managed indirectly through the GUI.

Managing system groups from the GUI

A system group is created when an authorization is created using a system collection. This system group is named after the collection with three digits appended, usually 001 (for example, All Racks 001). The system group contains the systems that were displayed during system selection and is saved when the authorization is created.



NOTE: Any additional changes to the system collection do not affect the system group or authorizations unless updated by one of the following options.

The content of the system group is updated with the current contents of the collection when:

- Another authorization is created using the collection
- An authorization using the system group is updated
- Using `mxngroup` from the CLI

In the first two cases, the current contents of the collection are displayed for verification.

When deleting authorizations, a system group no longer used in any authorization is deleted.

Managing system groups from the CLI using `mxngroup`

System groups can be created directly using the `mxngroup` command. When system groups are created using the CLI, a top-level collection is created and named after the system collection with three digits appended, usually 001. The collection contains the systems in the system group only when the system group is first added. Later modifications are not reflected in the collection.



NOTE: Any additional changes to the system group or collection do not affect the other, unless updated by one of the following options or by using the GUI as previously described. This means that changes to the collection do not affect authorizations, and changes to the system group do not affect the collection view unless specifically updated.

The contents of the system group can be updated with the current contents of the collection by using the `-u` parameter for `mxngroup`:

```
mxngroup -m -g <groupname> -u
```



CAUTION: This command does not display the systems in the collection. To display the updated contents of the system group, use `mxngroup -lm -g <groupname>`.

CAUTION: Setting up a periodic task to dynamically update a system group is not recommended. A collection based on system attributes can be compromised, adversely affecting authorizations in HP Systems Insight Manager (HP SIM) if those attributes are based on a nonsecure protocol (such as SNMP) or are maintained by a user with user rights. Additionally, the collection itself can be modified by a user with user rights, which also adversely affects authorizations.

When deleting authorizations, a system group no longer used in any authorizations is deleted.

Related procedures

- Creating new authorizations
- Updating authorizations

Related procedures

- ▲ Users and authorizations

7 Directory Services

The Directory Groups tool is used to determine a system's membership in a Windows domain, organizational unit (OU), or group. Before using the Directory Groups tool, you must first configure the directory server parameters on the **Directory Server Configuration** page. After you configure the directory server, the Directory Groups tool must be configured with the distinguished name (DN) of the desired container objects in the directory.

- **Directory Server Configuration** Used to configure directory server settings, including the network name, port, and credentials to access the directory server. To access, select **Options**→**Directory Services**→**Directory Server Configuration**.
- **Directory Groups** Used to enter the complete distinguished name (DN) of one or more containers, organizational units (OU), or group objects in the directory. To access, select **Options**→**Directory Services**→**Directory Groups**.

Related procedures

- [Configuring directory servers](#)
- [Configuring directory groups](#)

Related topic

- ▲ [Users and authorizations](#)

Configuring directory servers

1. Select **Options**→**Directory Service**→**Directory Server Configuration**. The **Directory Server Configuration** page appears.
2. (Required) Enter the network name or IP address of the directory server in the **Name** field. Multiple systems can be specified by separating each system with a semicolon (;). This action enables a backup to be specified if a system cannot be contacted. For example, if the first system cannot be contacted, the second system in the list is tried.
3. Select either **Use SSL** or **Use Global Catalog** for the **Port Configuration** setting.

The port configuration flag is preset to use SSL and to specify the default Lightweight Directory Access Protocol (LDAP) SSL port of 636 in the **Port** field. The global catalog flag is cleared by default. Selecting and clearing the SSL or global catalog flags changes the port number to the default values.

The global catalog communicates through LDAP, but it does so over a different set of ports: 3368 and 3269 for SSL. The global catalog contains a read-only copy of all objects in the Active Directory, spanning multiple domains, but only a small subset of object attributes. Configuring a global catalog here can provide a simple solution for multidomain sites. You can configure the directory attributes replicated to the global catalog, but the desired attributes are enabled by default.

Note: HP recommends selecting **Use SSL** so that user name and password credentials are encrypted. If this option is cleared, the directory server certificate is treated as a trusted system certificate and can be imported using the existing HP SIM GUI or command line interface (CLI).
4. (Required) Enter the port number of the directory server.

The port number is preset to use SSL in the **Port Configuration** field and to specify the default LDAP SSL port of 636 in the **Port** field.
5. In the **User Name** field, enter the user name to authenticate to the directory server. Write access for this account is not required. An empty field indicates that an anonymous connection should be used. Any password entered is ignored.
6. In the **Password** field, enter the password for the user name specified.
7. In the **Confirm** field, reenter the password for the user name specified.

After configuring the directory server parameters, you must configure the containers and groups that contain the computer objects of interest. See “Configuring directory servers” for information about configuring directory server parameters.

Related procedure

▲ Configuring directory groups

Related topics

- Users and authorizations
- Directory Services

Configuring directory groups

After configuring the directory server parameters, you must configure the containers and groups that contain the computer objects of interest. A container is like a branch, where systems in the container are child objects of the container object in the directory tree. For example, consider a computer container, with a distinguished name (DN) of *CN=Computers, DC=insight, DC=lab*. Another type of container is the Organizational Unit (OU). This function is expected to exist in enterprise-class environments because it can be used to apply Group Policy settings, whereas CN containers cannot (at least, not easily). Lastly, a directory group object contains a list of member systems. The list is static and consists of each system's DN in the directory.

Configuration of a container or group requires the DN of the group object, which specifies the fully qualified location of the object in the directory.

To determine the name of the Windows domain specified by the container, the directory domain object is determined from the container DN. This domain object is the DC components of the DN. For example, *DC=Insight, DC=lab*. This object is required to determine the Windows domain name. If a plain container object (not an OU) is specified, only the Windows domain is discovered for member systems. The default computer container (*CN=Computers, DC=Insight, DC=lab*) falls into this category. If an OU container object (object class is *organizationalUnit*) is specified, the OU name is determined through the OU directory attribute, and both the OU and Windows domain attributes are discovered for member systems.

To determine a system's membership in a directory group object, the group object is queried for the system's DN (if available in HP SIM from a container search). If the DN is not available in HP SIM, the list of members in the directory group is read, and each object's *Domain Name Service* (DNS) name is queried from the directory (based on DN of the object). This object lookup is performed because the object might not have been included in any of the configured containers. The HP SIM system is matched against this list, also using the full DNS name.

When a system is considered to be a member of a configured container or group, its attributes (in HP SIM) are modified accordingly, adding Windows domain, OU, and directory group attributes as appropriate. If a system previously had these attributes, and the system is found to no longer be a member of the corresponding container or group, the attribute is removed.

To configure a directory group:

1. Select **Options**→**Directory Service**→**Directory Groups**. The **Directory Groups** page appears.
2. Select target systems. See "Creating a task" for more information.
3. Click **Next**. The **Specify Group Locations** page appears.
4. Enter the **Distinguished Name (DN)** for the **Group 1**.
5. (Optional) If you want to search subtrees, select **Search**. This applies only to container and OU objects, not directory group objects, and only to those OU objects that are more than one level deep. If this option is selected, HP Systems Insight Manager (HP SIM) searches the entire depth of the specified branch. A match is based on the full DNS name of the system. If HP SIM does not have the full DNS name of a system, a match is considered successful if the short system name matches (using the CN attribute of the object) and no other partial match occurs. Systems having only an IP address available as the system name will fail unless the IP address is the name in the directory object.
6. (Optional) To add additional groups, click **Add**. Repeat steps 4 through 6 for each group.
7. (Optional) To delete a group, click **Delete** next to the group to be deleted.
8. Click **Run Now**.
9. In the **Confirm** field, reenter the password for the user name specified.

Related procedure

▲ Configuring directory groups

Related topics

- Users and authorizations
- Directory Services

8 Networking and security

HP Systems Insight Manager (HP SIM) provides the following security options:

- **User and Authorizations.** Select **Options**→**Security**→**Users and Authorizations**.
- **Server Certificate.** Select **Options**→**Security**→**Certificates**→**Server Certificate**.
- **Trusted Certificate.** Select **Options**→**Security**→**Certificates**→**Trusted Certificate**.
- **Login Event Settings.** Select **Options**→**Security**→**Login Event Settings**.
- **System Link Configuration.** Select **Options**→**Security**→**System Link Configuration**.

Secure Sockets Layer and certificates

Secure Sockets Layer (SSL) is used between the browser and HP Systems Insight Manager (HP SIM) to ensure data integrity and privacy. An integral part of SSL is a *certificate*, which is a public document used to identify the HP SIM server. When HP SIM is installed, it creates a *self-signed certificate*. Your browser might initially display a security alert when you browse to HP SIM, describing the certificate as untrusted. This designation occurs because the certificate is self-signed (signed by the HP SIM server) and the signer is not in the browser's list of *Certification Authorities* (CA). By securely importing the HP SIM server certificate into the browser, the browser can authenticate the HP SIM server to which you are browsing. See "Server certificates" for more information about importing certificates into your browser.

HP SIM also supports the ability to use a certificate from a third-party CA or your own internal CA or Public Key Infrastructure (PKI). In this case, you can import the CA certificate into your browser. See "Importing a CA-signed certificate" for more information.

Sign-in and accounts

A user name, domain name (for Windows CMS), and password are required before you can access any feature of HP SIM. HP SIM uses the user authorizations of the underlying operating system (Windows, Linux, or HP-UX) and relies on the operating system to authenticate users.

The user that is installing HP SIM must be either a system administrator (for Windows) or root user (for Linux and HP-UX). This user is given administrative access to HP SIM.

After signing in with this account, create additional accounts for other users. Each account can be set up with different configuration rights and authorizations. You can also restrict the IP addresses from which each account can sign-in. See "Users and authorizations" for more information.

Audit settings can also be configured to log a notice for different types of security events, including sign-in and sign out events. See "Configuring sign-in events" for more information.

Single Login, Replicate Agent Settings, and Install Software and Firmware

To take advantage of *single login* or to execute Replicate Agent Settings or Install Software and Firmware tasks on the managed systems, set up a trust relationship between HP SIM and the desired managed systems. A trust relationship enables the managed system to specify which HP SIM servers can issue commands to the system. Without an established trust relationship, these commands fail. See "Setting up trust relationships" for more information.

Setting up a trust relationship on the managed system requires that you browse to the system, set the trust mode, and add HP SIM to the Trusted System Certificates list. Managed systems can also be set up with an appropriate certificate during deployment. See "Initial ProLiant Support Pack Install" for more information. At the HP SIM server, you must also specify the user authorization for the managed system and have executed a System Identification task. If you have enabled the **Require** option on the **Trusted System Certificates** page, you must import the certificates of trusted managed systems into HP SIM, or a root CA certificate. See "Trusted certificates" and "Server certificates" for complete details.

Certificates

HP SIM allows secure and authorized management from the *Central Management Server* (CMS). User authorizations for managed systems and the CMS can be configured, helping ensure that only authorized users perform state-changing operations. Communication between the CMS, managed systems, and the browser is secured using SSL and certificates, helping to authenticate systems and protect user credentials and management data.

A new SSL certificate is created during CMS initialization that is used as a client credential in *Web-Based Enterprise Management* (WBEM) requests (instead of the CMS certificate). To authenticate using the WBEM certificate, select **Use certificate instead** in the **WBEM settings** section of the **System Protocol Settings** page. See “Setting protocols and credentials for a system or groups of systems” for more information. To configure the WBEM certificate, use the Configure or Repair Agents task. See “Windows CMS” for more information.



NOTE: The WBEM client certificate authentication feature is only supported on HP-UX systems, that have WBEM Services 2.5 installed for HP SIM.

Related procedures

- Configuring the system link
- Configuring sign-in events
- Changing the HP SIM default SSL port
- Setting protocols and credentials for a system or groups of systems
- Windows CMS
- HP-UX and Linux CMS

Related topics

- Server certificates
- Trusted certificates
- Possible certificate errors
- Users and authorizations
- About login
- About secure task execution

About login

Single Login

Single Login allows a link within an HP Systems Insight Manager (HP SIM) page to establish an authenticated browser session to a *managed system* that supports Single Login without requiring *users* to re-enter their user names and passwords. However, if you are trying to establish an authenticated browser session with another instance of HP SIM running on another system, you must re-enter your user name and password. Single Login links exist wherever there is a link to another system.



NOTE: HP SIM is the initial point of authentication, and browsing to another managed system must be from within HP SIM.

If you browse to a managed system using any method other than the links within HP SIM, Single Login is not supported, and you are required to enter the appropriate user name and password for each managed system. Managed systems must be set up to trust an HP SIM system before accepting a Single Login command. Trust is set up at the system by importing the HP SIM system certificate into the Trusted Management Servers List of the system. See “Setting up trust relationships” for more information.



IMPORTANT: If you browse to a managed system using any method other than the links within HP SIM, Single Login is not supported, and you are required to enter the appropriate user name and password for each managed system.



NOTE: Single Login does not work on a Virtual Cluster System. However, it does work on the physical systems which compose the cluster.

Signing in

Signing in to HP SIM allows access to HP SIM and determines what authorizations you have in HP SIM. Browsing to HP SIM using Secure Socket Layer (SSL) encrypts all information between the browser and HP SIM, including sign in credentials. SSL securely encrypts the password and helps prevent someone from capturing and replaying a valid sign-in sequence.

The sign-in page has three fields:

- **User Name.** The name of the user.
- **Password.** The password for the user name.
- **Domain Name.** The Windows domain of the user. This field appears in Windows environments only.



NOTE: In a Windows environment, administrators are selected from the operating system during the HP SIM installation. To sign in to HP SIM, enter the appropriate information for the account in the fields provided. The **User Name** field specifies the user name, and the **Domain Name** specifies the Windows domain. These fields are required in a Windows environment.

After the credentials are securely received by HP SIM, HP SIM validates the account, verifies that browsing is being done from a valid IP address for that account, and authenticates the credentials against the Windows domain. See “Users and authorizations” for details about accounts.

Some sign in failures are caused by failure in the operating system, and some are caused by failure within HP SIM. Use the operating system User Management tools to address these potential login failures:

- Sign in credentials are not entered correctly. Passwords are case-sensitive.
- The account being entered has been deleted or has been disabled or locked out.
- The password for the account has expired or must be changed.

The following reasons for sign in failure within HP SIM can be addressed on the **Users and Authorizations** pages:

- The account being entered is not an account for HP SIM.
- You are attempting to sign in from an IP address that is not valid for the specified account. The browser systems can also cause sign in failures.
- The browser is not configured to accept cookies.



NOTE: For more information, see the HP SIM user guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>, and select the appropriate guide for your operating system.

- A cookie blocker is installed.



NOTE: HP SIM can be configured to log an *event* in the HP SIM Event Database when a login attempt fails or succeeds and when a sign out occurs.

Sign in authentication on Linux and HP-UX

HP SIM uses Pluggable Authentication Modules (PAM) to authenticate users who log in to the web server interface on Linux and HP-UX.

Configuring PAM on a Linux system

The administrator of a Linux CMS can customize the PAM that HP SIM uses. The file `/etc/pam.d/mxpamauthrealm` contains the authentication steps for the HP SIM web server interface. The default for this file is:

- `##PAM-1.0`
- `auth required /lib/security/pam_unix.so`
- `account required /lib/security/pam_unix.so`
- `session required /lib/security/pam_unix.so`

This default setup directs PAM to use the standard UNIX authentication module to authenticate users attempting to sign in to the HP SIM web server interface. Standard calls from the system libraries are used to access account information usually read from `/etc/passwd` or `/etc/shadow`.

The administrator of the system can adjust these requirements to conform to the security requirements of the system. For example, if the security policy on the system is time dependent and `/etc/security/time.conf` is configured, you could adjust `mxpamauthrealm` to:

- `##PAM-1.0`
- `auth required /lib/security/pam_unix.so`
- `account required /lib/security/pam_unix.so`
- `session required /lib/security/pam_unix.so`

Configuring PAM on an HP-UX system

Customizing PAM security on HP-UX is similar. All of the PAM configurations are stored in `/etc/pam.conf`. The lines for HP SIM on HP-UX 11i are:

- `mxpamauthrealm auth required /usr/lib/security/libpam_unix.1`
- `mxpamauthrealm account required /usr/lib/security/libpam_unix.1`
- `mxpamauthrealm session required /usr/lib/security/libpam_unix.1`

The lines for HP SIM on HP-UX 11i 2.0 are:

- `mxpamauthrealm auth required /usr/lib/security/$ISA/libpam_unix.1`
- `mxpamauthrealm account required /usr/lib/security/$ISA/libpam_unix.1`
- `mxpamauthrealm session required /usr/lib/security/$ISA/libpam_unix.1`

If you want the HP SIM web server login model to match what is configured for your other login methods (telnet, rlogin, login, ssh, and so on), configure the same plug-in modules that are used by these other login methods. These modules should be defined by the login service name in the `/etc/pam.conf` file or the `/etc/pam.d/login` file.

Related topics

- Networking and security
- About secure task execution
- Installing OpenSSH
- Managing SSH keys

About secure task execution

HP Systems Insight Manager (HP SIM) *tasks* that cause state or configuration changes on *managed systems* use *secure task execution* (STE) to issue commands to the system. STE enables an HP SIM system to securely request execution of a task from a managed system, ensuring that the *user* requesting the task has the appropriate rights to perform the task. The request includes a digital signature to uniquely identify the HP SIM system making the request. *Secure Sockets Layer* (SSL) is then used to encrypt the request and protect the data from alteration or eavesdropping. See “Setting up trust relationships” for more information.



NOTE: STE requires a Trusted Management Servers List at each managed system to ensure that only specified HP SIM systems can execute tasks on the system.

NOTE: On the managed system, only a Trust by Certificate ensures that the request came from the specified HP SIM system. Other options, such as Trust by Name or Trust All, do not verify the *digital signature* of the HP SIM system and; therefore, these options cannot reliably verify the sender of the request.

NOTE: Tasks using STE, such as Replicate Agent Settings and Install Software and Firmware, cannot be executed on a Virtual Cluster System. However, they can be executed directly on each individual system in the *cluster*.

Related topics

- Exporting a server certificate
- Setting up trust relationships
- Requiring trusted certificates
- Creating a server certificate
- Installing OpenSSH
- Managing SSH keys

Configuring the system link

To choose the name format used when creating links to *managed systems*. The System Link Configuration setting defines how HP Systems Insight Manager (HP SIM) creates browser links to remote systems and how it communicates with remote systems for certain requests.



NOTE: When you are browsing to *systems* using *Secure Sockets Layer* (SSL), the system name should match the name in the system *certificate* to prevent browser warnings.

To configure the system link:

1. Select **Options**→**Security**→**System Link Configuration**. The **System Link Configuration** page appears.
2. Select from the following options:
 - **Use the system name.** Select this option to use the system name.
 - **Use the system IP address.** Select this option to use the system IP address. For systems with multiple addresses, multiple links can be entered.
 - **Use the system full DNS name.** Select this option to use the full system *Domain Name Service* (DNS) name.

Note: On an HP-UX or Linux Central Management Server (CMS), the default value is **Use the system full DNS name** on new HP SIM installations. New installations on Windows defaults to **Use the system name** and upgrades maintain the existing setting regardless of the operating system.

Note: During *discovery*, the full system DNS name is used as the primary lookup key (if it is available). Otherwise, the IP address is used.

Note: In the case of systems with multiple network interfaces, selecting the **Use the system name** provides only one link per destination to the system, whereas **Use the system IP address** provides multiple links to the system.

3. To save and apply the changes, click **OK**.

Related topics

- Networking and security
- Server certificates
- Installing OpenSSH
- Managing SSH keys

Configuring sign-in events

Configure sign-in events to create actionable *events* for sign-in and sign-out activities.



NOTE: Configuring sign-in events does not affect the HP Systems Insight Manager (HP SIM) Audit Log. Sign-in events are always logged in the HP SIM Audit Log.

To configure sign-in events:

1. Select **Options**→**Security**→**Sign-in Event Settings**. The **Sign-in Event Settings** page appears.
2. Select from the following options:
 - **All sign-in and sign-out activities**. Select this option to create events for all sign-in and sign-out actions.
 - **Only failed sign-in attempts**. Select this option to create events only for sign-in attempts that are unsuccessful.
 - **None**. Select this option if you do not want to create any events for sign-in or sign-out activities.
3. To save and apply changes, click **OK**.

Related topics

- Networking and security
- Users and authorizations
- Installing OpenSSH
- Managing SSH keys

Configuring browser timeout options

HP Systems Insight Manager (HP SIM) enables you to configure the browser timeout settings to one of the following. These settings affect the browser session while signed-in to the HP SIM GUI.

Monitor When the timeout option is configured to monitor, the HP SIM session remains alive and is continually refreshed unless you close the browser or navigate to another site. If you close the browser, the session is immediately closed. If you navigate to another site, HP SIM logs you out after 20 minutes. This option is the default and appears in the `globalsettings.props` file as `EnableSessionKeepAlive=true`.

Active When the timeout option is configured to remain active, the HP SIM session remains alive as long as you are actively working in HP SIM. However, HP SIM ends your session and logs you out after 20 minutes of inactivity.

You can change the timeout settings to monitor or active by editing the `globalsettings.props` file.

To configure the timeout setting to active:

1. Open the `globalsettings.props` file.
 - On a Windows operating system, the `globalsettings.props` file is located in the `install directory/config` folder.
 - On an HP-UX or Linux operating system, the `globalsettings.props` file is located in the `/etc/opt/mx/config` directory.
2. Change `EnableSessionKeepAlive=true` to `EnableSessionKeepAlive=false`.
3. Select **File**→**Save**.

The updates are saved.
4. Close the `globalsettings.props` file.

To change the default timeout:

1. From the HP SIM directory, navigate to:

Windows:
`install directory\jboss\server\hpsim\deploy\jbossweb-tomcat50.sar\conf\web.xml`

Linux and HP-UX:

```
/opt/mx/jboss/server/hpsim/deploy/jbossweb-tomcat50.sar/conf/web.xml
```

2. Edit the `<session-timeout>` value from the default of 20 minutes to the number of minutes you want.
3. Save the `globalsettings.Props` and the `web.xml` files.

The updates are saved.

4. Close the `web.xml` file.

Related topics

- [Signing in](#)
- [Networking and security](#)
- [Users and authorizations](#)

Changing the HP SIM default SSL port

If the HP Systems Insight Manager (HP SIM) SSL port conflicts with an application, you can change the default port number. See the *Understanding HP SIM 5.0 security* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for a list of ports in use. To change the default SSL port for HP Systems Insight Manager (HP SIM), complete the following:

1. In the `server.xml` file (located in the `jboss\server\hpsim\deploy\jbossweb-tomcat50.sar` directory), change the two occurrences of 50000 to the desired port.

```
<Connector port="280" maxThreads="50" minSpareThreads="5"
maxSpareThreads="15" enableLookups="false" redirectPort="50000"
acceptCount="10" debug="0" connectionTimeout="60000" />
```

2. For the first port entry, enter the following and replace 50000 with the port of your choice:
3. For the second port entry, enter the following and replace 50000 with the port of your choice:

```
<Connector address="{jboss.bind.address}" port="50000" scheme="https"
secure="true" maxThreads="200" minSpareThreads="10" maxSpareThreads="25"
enableLookups="false" acceptCount="10" debug="5" URIEncoding="utf-8"
useBodyEncodingForURI="true" clientAuth="false"
keystoreFile="C:\bullwinkle\target\Windows\stage\SIM\config\certstor\hp.keystore"
keystorePass="removed" sslProtocol="TLS" />
```

Related topic

- ▲ [Networking and security](#)

Server certificates

The **Server Certificate** page enables you to view and manage the *SSL* server certificate of the *Central Management Server* (CMS). HP Systems Insight Manager (HP SIM) supports two types of certificates; *self-signed* and *Certificate Authority (CA)-signed*. While a self-signed certificate is created by default during installation, enabling you to browse to HP SIM, both the self-signed and CA-signed certificates can be created after installation. The CA-signed certificate requires an internal certificate server or an external CA to sign the certificate.



HP SIM provides the following security certificate options:

- **Export server certificate** Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Export**.
- **Edit server certificate** Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Edit**.
- **Create new server certificate** Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **New**.
- **Import server certificate** Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Import**.

Related procedures

- Exporting a server certificate
- Editing a server certificate
- Creating a server certificate
- Importing a server certificate
- Synchronizing certificates
- Creating a certificate signing request
- Submitting a certificate signing request
- Importing a CA-signed certificate

Related topics

- Networking and security
- Replicating trusted certificates
- Possible certificate errors
- Installing OpenSSH
- Managing SSH keys

Creating a server certificate

Users with *administrative rights* can create a new *self-signed certificate* when they replace the HP Systems Insight Manager (HP SIM) *Secure Sockets Layer (SSL) server certificate* and *private key* in the following situations:

- The integrity of the HP SIM server certificate private key is compromised
- The existing HP SIM server certificate expires

This self-signed certificate is configured to expire 10 years from the date of creation.

Create a new self-signed certificate when you must replace the HP SIM SSL server certificate and private key. The public key is included in the certificate that goes out to the client. The private key is kept secure in the keystore database on the HP SIM server file system. The public and private key pair of the System Management Homepage (residing on the same system) is overwritten with the new HP SIM public and private key pair.



IMPORTANT: Replacing the SSL server certificate and private key invalidates the existing HP SIM server certificate and the System Management Homepage certificate wherever they might be imported, such as browsers and the Trusted Management Servers List in other System Management Homepages. Replace the previous server certificate with the new server certificate in accordance with your security practices to return to the same level of functionality you had before.



NOTE: On Windows and Linux, this process also affects the local System Management Homepage certificate and private key on HP-UX systems, it affects the *Web-Based Enterprise Management (WBEM) Services* certificate and private key.

NOTE: Valid characters for each of these fields are letters a through z (lowercase), A through Z (uppercase), numbers 0 through 9, and the following special characters: ' () + , - . / : ? space _ and ~. Each field must contain at least one non-white space character.

Server Certificate
View and manage the SSL server certificate

New Server Certificate

Create a new server certificate. This will create a new private key for the central management server and invalidate all trust relationships based on the existing certificate.

required field *

Subject:

Common Name (CN):*	psystems Insight Job
Alternative Names:	psystems Insight Job,psystems
Organizational Unit (OU):*	Hewlett-Packard Network Management Software
Organization (O):*	Hewlett-Packard Company
Locality (L):*	Palo Alto
State (ST):*	California
Country (C):*	US

OK Cancel

To create a new certificate:

1. Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **New**. The **New Server Certificate** section appears, and the fields are automatically populated with default values.
2. (Optional) Change the following fields:

- a. The **Common Name (CN)** field holds the parameter that the browser uses for name comparison when browsing to the Central Management Server (CMS). This field can be updated with other name formats, such as fully qualified names, and can contain up to 255 characters.
 - b. (Optional) In the **Alternative Names** field, enter multiple system names separated by a comma. If a name identical to the CN is specified in the **Alternative Names** field, it is not duplicated in the certificate.

Alternative names are case-sensitive. Therefore, if a duplicate case-sensitive name is entered, they are not duplicated in the certificate. For example, if SYS1, sys1, and SYS1 are entered, SYS1 is only listed once in the certificate.

The alternative names might be displayed in a different order from the order you enter them. However, this does not affect their usage.
 - c. In the **Organization (O)** field, enter the name of your organization. This field can contain up to 64 characters.
 - d. In the **Organizational Unit (OU)** field, enter the name of your department. This field can contain up to 64 characters.
 - e. In the **Locality (L)** field, enter the name of your city. This field can contain up to 128 characters.
 - f. In the **State (S)** field, enter the name of your state. This field can contain up to 128 characters.
 - g. In the **Country (C)** field, enter the name of your country. This field can contain up to two alphanumeric characters, using the two-letter country codes.
3. After changes are made, click **OK**. If you click **Cancel**, you are returned to the **Server Certificate** page without creating a new server certificate. A warning appears, reminding you about the effects of changing the certificate and private key. If you click **OK** in the warning box to continue, a new 1,024-bit key-pair and a new self-signed certificate are generated. The old key-pair and certificate are not retrievable unless a backup was created manually before this process. The new certificate and private key take effect the next time HP SIM is restarted.
 4. Reboot the HP SIM server to ensure the new certificate is properly synchronized with the local System Management Homepage and any applications or components using the certificate sharing directory. After creating a new server certificate, reboot the HP SIM server for the HP SIM server certificate to be synchronized with the HTTP server certificate. Synchronizing the certificates prevents repeated browser security alerts when browsing to HP Insight Management Agent on the HP SIM server.

Related procedures

- [Exporting a server certificate](#)
- [Importing a server certificate](#)
- [Editing a server certificate](#)
- [Synchronizing certificates](#)

Related topics

- [Server certificates](#)
- [Installing OpenSSH](#)
- [Managing SSH keys](#)

Editing a server certificate

Edit a server *certificate* to change fields in an existing certificate. This modification might be required if you are submitting a certificate signing request (CSR) to an external *Certificate Authority (CA)*.



NOTE: On Windows and Linux, this process also affects the local System Management Homepage certificate and private key on HP-UX systems, it affects the *Web-Based Enterprise Management (WBEM) Services* certificate and private key.

NOTE: Valid characters for each of these fields are letters a through z (lowercase), A through Z (uppercase), numbers 0 through 9, and the following special characters: ' () + , - . / : ? space _ and ~. Each field must contain at least one non-white space character.

To edit a server certificate:

1. Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Edit**. The **Edit Server Certificate** section appears.
2. Edit the following fields as necessary:

Note: The **Common Name (CN)** field and the key pair cannot be modified, so the trust relationships with any System Management Homepages remain in tact. However, the browser trust must be re-established by importing the modified certificate and deleting the old certificate from the browser.

 - a. (Optional) In the **Alternative Names** field, enter multiple system names separated by a comma. If a name identical to the CN is specified in the **Alternative Names** field, it is not duplicated in the certificate.

Alternative names are case-sensitive. Therefore, if a duplicate case-sensitive name is entered, they are not duplicated in the certificate. For example, if SYS1, sys1, and SYS1 are entered, SYS1 is only listed once in the certificate.

The alternative names might be displayed in a different order from the order you enter them. However, this does not affect their usage.
 - b. In the **Organization (O)** field, enter the name of your organization. This field can contain up to 64 characters.
 - c. In the **Organizational Unit (OU)** field, enter the name of your department. This field can contain up to 64 characters.
 - d. In the **Locality (L)** field, enter the name of your city. This field can contain up to 128 characters.
 - e. In the **State (S)** field, enter the name of your state. This field can contain up to 128 characters.
 - f. In the **Country (C)** field, enter the name of your country. This field can contain up to two alphanumeric characters, using the two-letter country codes.
3. Click **OK**. A warning message appears, indicating that the certificate is about to be modified. You can click **Cancel** to abort the modify operation.

Related procedures

- [Creating a server certificate](#)
- [Exporting a server certificate](#)
- [Importing a server certificate](#)
- [Synchronizing certificates](#)

Related topics

- [Server certificates](#)
- [Networking and security](#)
- [Installing OpenSSH](#)
- [Managing SSH keys](#)

Importing a server certificate

Import a *Certificate Authority* (CA)-signed server certificate to replace the existing server *certificate* in the following situations:

- You have installed HP Systems Insight Manager (HP SIM) and want to replace the default *self-signed certificate* with a certificate created by a third-party CA or your own internal CA.
- The integrity of the HP SIM server certificate *private key* is compromised.
- The existing HP SIM server certificate has expired.



CAUTION: Replacing the *SSL* server certificate and private key invalidates the existing server certificate wherever it might be imported, such as browsers and the Trusted Management Servers Lists of managed

systems. Replace the previous server certificate with the new server certificate in accordance with your security practices to return to the same level of functionality you had before.



NOTE: On Windows and Linux, this process also affects the local System Management Homepage certificate and private key on HP-UX systems, it affects the *Web-Based Enterprise Management (WBEM) Services* certificate and private key.

To import a server certificate:

1. Create a certificate signing request (CSR). See “Creating a certificate signing request”. The CSR uses parameters from the existing certificate, including any alternative names. If you want to change those parameters, edit the server certificate (see “Editing a server certificate”) or create a new server certificate (see “Creating a server certificate”).
2. Submit the request to a CA. See “Submitting a certificate signing request” for more information. The CA returns a signed certificate.
3. Import the signed certificate reply into HP SIM. See “Importing a CA-signed certificate” for more information.

Related procedures

- Creating a server certificate
- Exporting a server certificate
- Editing a server certificate
- Synchronizing certificates
- Creating a certificate signing request
- Importing a CA-signed certificate
- Submitting a certificate signing request

Related topics

- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Exporting a server certificate

Export the HP Systems Insight Manager (HP SIM) server *certificate* to a file to facilitate deployment of the certificate to your browsers. This certificate enables a browser to properly identify the HP SIM server. The HP SIM server certificate is a public document, so it does not need to be kept private. However, because the certificate is kept publicly accessible, you must ensure that it cannot be modified.



NOTE: The system certificate can be exported as a Base64-encoded certificate. The exported certificate can be imported into a browser or the Trusted Management Servers List.

To export the server certificates from HP SIM:

1. Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Export**.
The Internet Explorer **File Download** dialog box appears.
2. To export and save the file, click **Save**, or to abort the file download operation and return to the **Server Certificate** page, click **Cancel**.

Related procedures

- Creating a server certificate
- Importing a server certificate
- Editing a server certificate
- Synchronizing certificates

Related topics

- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Creating a certificate signing request

Create a certificate signing request (CSR) to replace the HP Systems Insight Manager (HP SIM) *Secure Sockets Layer* (SSL) server certificate and *private key*.

The CSR includes any alternative names that exist in the certificate. If this causes issues for any desired Certificate Authorities (CA), the certificate might need to be modified to remove alternative names.

To create a certificate signing request:

1. Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Import**. The **Import Server Certificate** section appears.
2. Click **more** next to **Create a Certificate Signing Request (CSR)**.

The **Create Certificate Signing Request** section follows the **Import Server Certificate** section.

Note: The current certificate parameters are shown. Selecting to create a CSR does not create a new key-pair or change any certificate parameters. If you want to create a new key-pair, create a new certificate. If you want to modify the certificate parameters, click **Edit** (instead of **Import**) on the **Server Certificate** page.

3. To create a PKCS #10 signing request that is downloaded through a standard browser, click **Create**. In Internet Explorer, use the **File Download** dialog box. In Mozilla, save the text in the new browser window to a file.
4. Send the certificate file to a *Certificate Authority (CA)*, which can be internal or external.

Note: The existing *self-signed certificate* is still valid, so the SSL web server remains operational for browsing until the signed certificate is received from the CA.

Related procedures

- Importing a server certificate
- Importing a CA-signed certificate
- Submitting a certificate signing request

Related topics

- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Submitting a certificate signing request

After creating the certificate signing request (CSR), the CSR must be submitted to the desired *Certificate Authority (CA)* for signing.



NOTE: You must complete the CSR creation procedure before continuing with this procedure. See “Creating a certificate signing request” for more information.

To submit the request to a CA:

1. Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Import**. The **Import Server Certificate** section appears.
2. Click **more** next to **Submit CSR to Certificate Authority (CA)**.
3. Send the PKCS #10 (CSR) data to a CA.

After the CA has returned PKCS #7 data, import it into the HP Systems Insight Manager (HP SIM).

Related procedures

- Importing a server certificate
- Creating a certificate signing request
- Importing a CA-signed certificate

Related topics

- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Importing a CA-signed certificate

After creating a certificate signing request (CSR) and having it signed by a *Certificate Authority (CA)*, you can import the signed *certificate*.

The only importable certificate format is PKCS #7. If the certificate reply received from the CA is a single certificate, then first import a *self-signed root certificate* from the issuing CA into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List. After importing the CA root certificate, the certificate reply can then be imported to serve as the HP SIM server certificate.



NOTE: On Windows and Linux, this process also affects the local System Management Homepage certificate and private key on HP-UX systems, it affects the *Web-Based Enterprise Management (WBEM) Services* certificate and private key.

NOTE: HP SIM only supports importing certificates that have a public key size of 2,046 bits or less.

To import the signed certificate reply from a CA:

1. Select **Options**→**Security**→**Certificates**→**Server Certificates**, and then click **Import**. The **Import Server Certificate** section appears.
2. Click **more** next to **Import signed certificate reply from CA**. The **Import Signed Certificate Reply** section follows the **Import Server Certificate** section.
3. Click **Browse** next to the **Certificate filename** field. The **Choose file** dialog box appears.
 - a. Navigate to the location where the signed certificate is stored.
 - b. Select the correct file name, and then click **Open**.
The file name appears in the **Certificate filename** field.
4. Click **Import**. The signed certificate is imported.

After creating a CSR or importing the server certificate, reboot the HP SIM server for the HP SIM server certificate to synchronize it with the System Management Homepage certificate and the certificate sharing directory. Synchronizing the certificates prevents repeated browser security alerts when browsing to HP Insight Management Agent on the HP SIM server, which enables HP SIM and the local System Management Homepage to update their *Secure Sockets Layer (SSL)* server certificates and private *keys*.

Related procedures

- Importing a server certificate
- Creating a certificate signing request
- Submitting a certificate signing request

Related topics

- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Synchronizing certificates

When the HP Systems Insight Manager (HP SIM) server certificate is created or modified, the public and private *certificate key*-pair of the System Management Homepage certificate is overwritten with the HP SIM public and private key-pair.



NOTE: This feature is available in the unlikely event that the certificates become unsynchronized for an unknown reason.

NOTE: For the certificate sharing feature to work in HP-UX, OpenSSL must be installed in the `/OPT/APACHE/SSL/BIN/` directory (default for HP-UX installations). For the certificate sharing feature to work in Linux, OpenSSL must be installed in the `/USR/BIN/` directory (default for Linux installations).

Related procedures

- Creating a server certificate
- Exporting a server certificate
- Importing a server certificate
- Editing a server certificate

Related topics

- Server certificates
- Networking and security
- Replicating trusted certificates
- Installing OpenSSH
- Managing SSH keys

Replicating trusted certificates

System administrators that have the HP Systems Insight Manager (HP SIM) **Require** or **First Time Accept** features enabled can replicate the trusted certificates list to other HP SIM systems. If you do not use the **Require** or **First Time Accept** features of HP SIM as a two-way trust solution, this procedure is not necessary.

Migrating trusted system certificates from the Source *Central Management Server* (CMS) to the target CMS

Two options are available to migrate the trusted certificates from a source CMS to a target CMS. The first option can be used when the source CMS has many trusted certificates and the second option can be used when a source CMS has fewer of trusted certificates.

Migrating certificates when the source CMS has many trusted certificates



WARNING! When migrating certificates, you lose the existing SSL Server Key and certificate on the target CMS and must reestablish the trust relationship with any agents configured to trust the target CMS. See Step 13.

To migrate a trusted certificate from a source to a target CMS with many trusted certificates:

1. Sign-in with administrative rights HP SIM on the source CMS system.
2. Go to `<HPSIM Install folder>\Systems Insight Manager\config\certstor`.
3. Copy the files named `hp.keystore` and `keyfile.3`.
4. Log in with administrative privileges to the target CMS system.
5. Go to the `<HPSIM Install folder>\Systems Insight Manager\config\certstor` directory.
6. Replace the `hp.keystore` and `keyfile.3` files with the files copied in step 3.
7. On the target CMS system, select **Start**→**Settings**→**Control Panel**→**Administrative Tools**→**Services**.
8. Restart the HP SIM service.

Note: You might see a browser warning indicating that the name in the certificate does not match the name of the site. This result is expected because you are temporarily using the certificate from the source

CMS, but you can view the certificate displayed by the browser to ensure its authenticity before signing in.

9. Sign-in with administrative rights to HP SIM on the target CMS. Select **Options**→**Security**→**Certificates**→**Server Certificate**.
10. To create a new server certificate, click **New**.
11. On the target CMS system, select **Start**→**Settings**→**Control Panel**→**Administrative Tools**→**Services**.
12. Restart the HP SIM service.
13. Install the new server certificate on the required managed systems using the Replicate Agent Settings feature. For more information, see “Using the Replicate Agent Settings feature”.

Migrating certificates when the source CMS has a lower number of trusted certificates

1. Log in to the source CMS system with administrative privileges.
2. Select **Options**→**Security**→**Certificates**→**Trusted Certificate**.
3. Select a certificate, and then click **Export**.
4. Save the certificate locally.
5. Repeat steps 2 and 3 for all certificates listed on the **Trusted System Certificates** page.
6. Copy all exported certificates to the target CMS system.
7. Sign-in with administrative rights to HP SIM on the target CMS.
8. Select **Options**→**Security**→**Certificates**→**Trusted Certificate**.
9. Click **Import**.
10. Click **Browse**, and then select a certificate.
11. Click **OK**.
12. Repeat steps 9 through 11 for all certificates.

Using the Replicate Agent Settings feature



NOTE: This section assumes agents are already configured to trust the source CMS.

NOTE: This process configures the agents to trust only the new target CMS. If trust for the original source CMS is still necessary, perform steps 5, 6, and 13 (or 16) using the source CMS.

1. Log in to the System Management Homepage on the target CMS.
2. Select **Settings**→**Security**→**Trust Mode**.
3. Select **Trust by Certificate**, and then click **Save Configuration**.
4. Select **Settings**→**Security**→**Trusted Management Servers**.
5. Enter the IP address of the target CMS in the field adjacent to **Add Certificate From Server**.
6. Click **Add Certificate From Server**.
7. Sign-in with administrative rights to HP SIM on the source CMS.
8. Select **Configure**→**Replicate Agent Settings**.
9. From the **Select Target Systems** page, select all managed systems that are configured to trust the source CMS.
10. Click **Apply Selections**, and then click **Next**.
11. Select the target CMS as source and click **Next**.
Note: If the source system does not have HP SIM installed, proceed to step 15.
12. In the source configuration settings page, click **System Management Homepage**→**Settings**→**Configuration Options Properties**, and then select **Trust Mode**.
13. Click **System Management Homepage**→**Settings**→**Trusted Certificate Properties**, and then select **Trusted Certificate** for the target CMS.
14. In the source configuration settings page, click **HTTP Server**→**Configuration**→**Options Properties**, and then select **Trust Mode**.
15. Click **HTTP Server**→**Trusted Certificates Properties**, and select **Trusted Certificate** for the target CMS.
16. Click **Run Now**. The CMS certificates are replicated on the selected managed systems.

Related procedures

- Creating a Replicate Agent Settings task
- Exporting a server certificate
- Editing a server certificate
- Creating a server certificate
- Importing a server certificate
- Synchronizing certificates
- Creating a certificate signing request
- Submitting a certificate signing request
- Importing a CA-signed certificate

Related topics

- Networking and security
- Installing OpenSSH
- Managing SSH keys

Possible certificate errors

Possible certificate error messages include:

- `Invalid Certificate Format` is displayed in the debug log files followed by the system this error message corresponds to.

The certificate was being sent from a program residing on a port that one of the HP SIM HP Insight Management Agent should reside on. Another possible cause of this error is that the certificate sent to the Central Management Server (CMS) was corrupt.

To correct this issue, verify that the Insight Management Agent running on the client system has not been tampered with and is running as expected. Verify that no other programs on the client are using the ports used by HP SIM. If this error continues, contact HP technical support. For information about the ports that are used by HP SIM and its partner applications, see the *Understanding HP SIM 5.0 security* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>.

- `Certificate has expired` followed by the system name.

The expiration date of the certificate is past the current date.

To correct this issue, verify the certificate expiration date. If the expiration date is past the current date, then a new certificate must be generated for this system. Otherwise, check the system date and time on the Central Management Server (CMS). If the CMS is out of date, then correct the date and time and try importing the certificate again. See “Creating a server certificate” for information about generating a new certificate. See “Importing a server certificate” for information about importing the certificate.

Related topics

- Networking and security
- Server certificates
- Trusted certificates

Trusted certificates

Trusted *certificates* provide the highest level of security. Users with *administrative rights* can import certificates from other systems into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List.

The purpose of the Trusted System Certificates List in HP SIM is to maintain a list of certificates in the HP SIM *keystore*. Certificates include the HP SIM system certificate and the certificates of *managed systems* that are trusted by the HP SIM system. These imported certificates are placed in the keystore and are displayed in the Trusted System Certificates List.

The **Trusted System Certificate List** page includes the following options:

- **Always Accept** If **Always Accept** is selected, SSL always accepts the certificate presented by a system in the SSL connection. This setting is the default and is vulnerable to man-in-the-middle attacks, but it is the easiest option to use.
- **Require** If **Require** is selected, you must set up the trust by manually installing the system's certificate into the HP SIM Trusted System Certificate List. This option is the most secure, but it is the most difficult to implement.

HP SIM provides the following trusted certificate options:

- **Import trusted certificate.** Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, and then click **Import**.
- **Export certificate** Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, and then click **Export**.
- **Delete trusted certificate** Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, select the certificates to be deleted, and then click **Delete**.

Related procedures

- Importing trusted certificates
- Exporting trusted certificates
- Deleting trusted certificates

Related topics

- Requiring trusted certificates
- Administering systems and events
- Server certificates
- Requiring trusted certificates
- Setting up trust relationships
- Replicating trusted certificates
- Possible certificate errors
- Installing OpenSSH
- Managing SSH keys

Importing trusted certificates

If you have selected **Require** on the **Trusted System Certificates** page, you must import certificates that represent the *managed systems* you want to trust to the Trusted Certificates List. You can import the *certificate* of the system itself on a per-system basis. You can also import the signing certificate of the *Certificate Authority (CA)* or intermediate CA used to sign and issue certificates for groups of systems, which simplifies the maintenance of this list.



NOTE: Only users with *administrative rights* can import certificates into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List.

NOTE: HP SIM only supports importing certificates that have public key sizes of 2,048 bits or less.

To import certificates into the Trusted System Certificates List:

1. Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, and then click **Import**. The **Import Trusted System Certificate** section appears.
2. Next to the **Certificate filename** field, click **Browse**.
The **Choose file** dialog box appears.
3. Navigate to the location of the certificate to be imported, and then select the file name. Click **Open**.
The certificate is imported.

Related procedures

- Exporting trusted certificates
- Deleting trusted certificates

Related topics

- Trusted certificates
- Setting up trust relationships
- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Exporting trusted certificates

Export the HP Systems Insight Manager (HP SIM) server *certificate* to a file to facilitate deployment of the certificate into your browser, enabling the browser to properly identify the HP SIM server. This certificate is a public document, so it does not need to be kept private. However, because the certificate is kept publicly accessible, you must ensure that it cannot be modified.

Only HP SIM users with *administrative rights* can export the HP SIM system certificate from HP SIM.



NOTE: The system certificate can be exported as a Base64 encoded certificate. The exported certificate can be imported into a browser or a system's or the Trusted Management Systems List.

Exporting the system certificate from HP SIM

To export the system certificate from HP SIM using Microsoft Explorer:

1. Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, and then click **Export**.
The **File Download** dialog box appears.
2. Select the location for the file to be saved.
3. Enter a file name and click **Save** to save the certificate as a Base64-encoded X.509 certificate. This file can be imported into a browser or managed system for authentication of the *Central Management Server (CMS)* during a *Secure Sockets Layer (SSL)* connection. You can click **Cancel** to cancel the save operation and return to the **System Certificate** page.

To export the system certificate from HP SIM using Mozilla:

1. Display the certificate in a new browser window.
2. Select the entire contents of the browser window that includes the certificate.
3. Copy the selected text to the clipboard.
4. Paste the text into a text editor, and save the file with a `.CER` file extension.

Exporting the system certificate from the browser (Microsoft Internet Explorer only)

1. View the HP SIM system certificate using one of the following methods:
 - From the Internet Explorer browser menu, select **File**→**Properties**→**Certificates**.
 - Double-click the **Lock** icon in the lower right portion of the browser to display the **Certificate** dialog box.
The **Certificate** dialog box appears.
2. Click the **Details** tab in the **Certificate** dialog box.
The **Details** tab appears.
3. Click **Copy to File**.
The Certificate Export Wizard launches.

4. Click **Next**.
The **Export File Format** dialog box appears.
5. Select **Base-64 encoded X.509** for the export file format. Click **Next**.
The **File to Export** dialog box appears.
6. In the **File name** field, enter the file you want to export. Click **Next**.
The **Completing the Certificate Export Wizard** dialog box appears.
7. Click **Finish**. You can click **Back** to return to the previous page or click **Cancel** to cancel the export operation.
A message appears indicating that the export is completed.
8. Click **OK**.

Related procedures

- Importing trusted certificates
- Deleting trusted certificates

Related topics

- Trusted certificates
- Setting up trust relationships
- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Deleting trusted certificates

Delete *certificates* from the Trusted System Certificates List to remove them from the HP Systems Insight Manager (HP SIM) keystore.



CAUTION: The delete process is irreversible. Use this feature with caution!

To delete certificates from the Trusted System Certificates List:

1. Select **Options**→**Security**→**Certificates**→**Trusted Certificates**.
2. Select the certificates to be deleted.
3. Click **Delete**. A dialog box appears.
4. To delete the certificates, click **Yes**, or to cancel the delete process and return to the **Trusted System Certificates** page, click **Cancel**.

The certificates are deleted from the Trusted System Certificates List.

Related procedures

- Importing trusted certificates
- Exporting trusted certificates
- Requiring trusted certificates

Related topics

- Trusted certificates
- Server certificates
- Networking and security
- Installing OpenSSH
- Managing SSH keys

Requiring trusted certificates

Trusted system certificates are certificates that represent managed systems. Enabling the **Trusted System Certificate** option enables HP Systems Insight Manager (HP SIM) to authenticate the remote managed system. For ease of use, this option is disabled; this scenario is typical and maintains a high level of security. For maximum security, this option should be enabled, which requires extra configuration.

If **Require** is enabled, when HP SIM attempts to make a Secure Sockets Layer (SSL) connection to a managed system, a certificate representing that system must be found in the HP SIM keystore or the SSL connection and attempted operation fails. The attempted operation fails as well. The certificate representing the system can be the system's SSL system certificate or the Certificate Authority (CA) level certificate that was used to sign the system's certificate. For large numbers of systems, using having a handful of CA-level certificates to sign all the system certificates can simplify the management and maintenance of the system certificates. However, this option requires the presence of a certificate system in your environment, or the services of a third-party security company.



CAUTION: If you select the **Require** option, a warning message appears, indicating that certain features work only for systems whose certificates are represented in the **Trusted Certificate List**.

The HP SIM Trusted System Certificates List is only used when the **Require** option is enabled.



IMPORTANT: Changing the **Require** option can adversely affect the operation of HP SIM. Carefully read and understand the warning described in this section.

When using a CA-level certificate, any valid certificate signed by the CA-level certificate is accepted by HP SIM, whether it is already issued or issued at some point in the future.

To enable the **Require** option:

1. From the **Administer** tab, select **Options**→**Security**→**Certificates**→**Trusted Certificates**.
The **Trusted Certificates** page appears.
2. Select **Require**. This setting restricts the CMS from accepting any connections other than SSL connections with managed systems. The managed systems must have a certificate in the **Certificate List**. This option does not affect browsing to the CMS.
A warning message appears indicating that certain features work only for systems whose certificates are represented in the **Trusted System Certificates List**.
3. To require trusted certificates, click **OK**. To disable the **Require** option and return to the **Trusted System Certificates** page, click **Cancel**.

To disable the Trusted System Certificates option:

1. From the **Administer** tab, select **Options**→**Security**→**Certificates**→**Trusted Certificates**.
The **Trusted Certificates** page appears.
2. Select another option.
3. Click **OK**, or to leave the **Require** option enabled and return to the **Trusted System Certificates** page, click **Cancel**.

Related topics

- [Importing trusted certificates](#)
- [Exporting trusted certificates](#)
- [Deleting trusted certificates](#)
- [Installing OpenSSH](#)
- [Managing SSH keys](#)

Setting up trust relationships

The following sections detail how to set up a trust relationship between an HP Systems Insight Manager (HP SIM) CMS and a managed system.

Configuration of the managed system

For *Single Login* and *Secure Task Execution* (STE) to function properly, the *managed system* must be running a supported agent and be configured to trust the HP SIM server. The trust mode is configured from the System Management Homepage (SMH). The following trust modes are available:

Trust By Certificate. The **Trust by Certificate** mode sets the **System Management Homepage** to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of a digital signature and certificates. This mode provides the highest level of security because it verifies the digital signature before allowing access. HP recommends this option.



NOTE: If you do not want to enable any remote configuration changes by HP SIM, leave **Trust by Certificate** selected, and leave the list of trusted systems empty.

Trust By Name. The **Trust By Name** mode sets the **System Management Homepage** to accept certain configuration changes only from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure, and prevents nonmalicious access. For example, you might use this option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server name submitted, not the digital signature.

Trust All. The **Trust All** mode sets the **System Management Homepage** to accept configuration changes from any system. For example, you could use the **Trust All** option if you have a secure network, and everyone in the network is trusted.



NOTE: For **Trust By Certificate**, the certificate from the HP SIM system can be installed during the initial support pack deployment. See “Initial ProLiant Support Pack Install” for more information.

Importing the HP SIM certificate over the network

If you prefer importing the HP SIM certificate from a file, see [Importing the HP SIM certificate from a file](#) for more information.

1. From a web browser, navigate to the managed server using the address:
https://managed-server:2381. The **System Management Homepage** appears.
2. Log in to the **System Management Homepage**.
3. On the **Settings** tab, select **System Management Homepage**→**Security**.
4. Click **Trust Mode**. The **Trust Mode** page appears.
5. To require trusted certificates, select **Trust by Certificate**.
6. To save the trust mode, click **Save Configuration**, or to cancel all changes, click **Reset Values**.
7. Click the browser **Back** button to return to the **Trust Mode** page.
8. To access the Trusted Management server certificate, click **Trusted Certificate**.
9. In the text box next to **Add Certificate From Server**, enter the name of the HP SIM server that contains the certificate to be added.
10. Click **Add Certificate From Server**. The certificate information is presented for verification before it is added to the list.
Note: Because this is a nonsecure request over HTTP, a malicious party could intercept the request and substitute an untrusted certificate in response to the request. A more secure method for obtaining the HP SIM certificate is described in the “[Importing the HP SIM certificate from a file](#)” section.
11. Verify the certificate information. , If you want to add it to the Trusted Certificate List, click **Add Certificate to Trust List**.

Note: If you are setting up a trusted certificate on a cluster, see “[Cluster](#)” for more information.

Importing the HP SIM certificate from a file

1. Export the HP SIM server certificate from the HP SIM server to a file. See “[Exporting a server certificate](#)” for more information.
2. Place the certificate file in a file location that is accessible by the file system of the managed system.

3. Browse to the managed system, and using a text editor (such as Notepad), open the HP SIM server certificate created in step 1.
4. Highlight the entire contents of the file, including the **Begin Certificate** and **End Certificate** lines. Copy the highlighted contents of the certificate file to the clipboard.
5. Return to the managed system browser and then select the **HP SIM Certificate Data** box.
6. Paste the contents of the certificate file into this box, and then click **Add Cert**. A confirmation window appears with three links at the top.
7. Click **Options**, and scroll down to the **Trusted Certificates** section. The **Trusted Certificates:** list appears with the server name and links to **View Certificate** and **Remove Certificate** for the HP SIM certificate that was just added.

Setting up the managed server running Management HTTP Server

Importing the HP SIM certificate

1. Export the HP SIM server certificate from the HP SIM server to a file. See “Exporting a server certificate” for more information.
2. Place the certificate file in a file location that is accessible by the file system of the managed system.
3. Browse to the managed system, and using a text editor (such as Notepad), open the HP SIM server certificate created in step 1.
4. Highlight the entire contents of the file, including the **Begin Certificate** and **End Certificate** lines. Copy the highlighted contents of the certificate file to the clipboard.
5. Return to the managed system browser and select the **HP SIM Certificate Data** box.
6. Paste the contents of the certificate file into this box, and then click **Add Cert**. A confirmation window appears with three links at the top.
7. Click **Options**, and scroll down to the **Trusted Certificates** section. The **Trusted Certificates:** list appears with the server name and links to **View Certificate** and **Remove Certificate** for the HP SIM certificate that was just added.

Requesting the HP SIM certificate

Enter the HP SIM server name in the appropriate field, and then click the corresponding **Get Cert** button. The managed system makes an HTTP request directly to the HP SIM server for its certificate.

Note: Because this is a nonsecure request over HTTP, a malicious party could intercept the request and substitute an untrusted certificate in response to the request. A more secure method for obtaining the HP SIM certificate is described in “Importing the HP SIM certificate” for more information.

Onboard Administrator configuration

To enable Single Login support in Onboard Administrator 1.20 or later, see the Onboard Administrator documentation.

HP StorageWorks Command View EVA configuration

To enable Single Login support in HP StorageWorks Command View EVA 6.0 or later, see the *HP StorageWorks Command View EVA user guide*.

With HP SIM 5.2 and later, the `cv-tools.xml` file is automatically installed and configured. An account in HP SIM based on the default administrator template will have administrator rights in Command View EVA and an account based on the default user template will have user rights in Command View EVA.

HP SIM configuration

System identification

A system identification task must be run at least once on any managed system for HP SIM to know that the system supports Single Login and Secure Task Execution, or these features do not function.

Certificates for trusted systems

If you have enabled **Require** on the **Trusted System Certificates** page (select **Options**→**Security**→**Certificates**→**Trusted Certificate**), import certificates that represent the managed

systems you want the HP SIM server to trust into the Trusted System Certificates List of HP SIM. For the managed system certificate, you can use the system certificate, or, if applicable, the certificate the Certificate Authority (CA), used to sign the system certificate.



NOTE: If **Require** is disabled on the **Trusted Certificates** page, then Trusted System Certificates List is not used, all certificates are accepted, and you can omit this section.

Before importing system certificates into the HP SIM Trusted System Certificates List, export the certificates to a file in Distinguished Encoding Rules (DER) or Base64-encoded format. To obtain the system certificate, you can:

- For Windows system with which you have access to the file system, copy the certificate from the file `c:\compaq\wbem\cert.pem` in Base64-encoded format, to some place accessible by HP SIM or access it directly if it is already accessible by HP SIM.
- Export the system certificate while browsing to the system. Select **File**→**Properties** from the browser menu. Click **Certificates**. Click the **Details** tab, and then click **Copy to File**. Export the certificate as a Base64-encoded X.509 file.

To obtain the CA certificate, contact your CA, or see the documentation provided with your certificate server software. To import managed system certificates into the HP SIM Trusted System Certificates List:

1. Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, and then click **Import**. The **Import Trusted System Certificate** section appears.
2. Next to the **Certificate Filename** field, click **Browse**.
The **Choose file** dialog box appears.
3. Navigate to the location of the certificate to be imported, and then select the file name. Click **Open**.
The certificate is imported.

Note: If you are setting up a trusted certificate on a cluster, see “Cluster” for more information.

Suppressing browser warning messages

To suppress browser warnings regarding untrusted certificates when browsing to an HP SIM managed system import the certificates into the browser.

1. Open Internet Explorer, and browse to the managed server at **https://managed_server:2381** or HP SIM at **https://sim_server:50000**.
2. On the Internet Explorer **Security Alert**, click **View Certificate**.
3. After reviewing the certificate, click **Install Certificate**.
4. Click **Next**.
5. Click **Place all certificates in the following store**.
6. Click **Browse**.
7. Select **Trusted Root Certificate Authorities**, and then click **OK**.
8. Click **Next**.
9. Click **Finish**.
10. Click **OK**.

Related procedures

- Creating a certificate signing request
- Submitting a certificate signing request
- Importing a CA-signed certificate
- Exporting a server certificate
- Setting up managed systems

Related topics

- Server certificates
- Trusted certificates

- Networking and security
- Creating a Replicate Agent Settings task
- Installing OpenSSH
- Managing SSH keys

9 Monitoring systems, clusters, and events

You can monitor *systems*, *clusters*, and *events* using the tools in the **System and Event Collections** panel. These tools enable you to locate more information about systems and events and quickly select systems to perform *tasks*. From **System and Event Collections** panel, you can quickly access the **System Overview** page, the **All Systems** page, and the **All Events** page. You can also save searches in private collections under **Systems** or **Events**. See “Saving collections” for more information.



NOTE: If you upgraded from HP Systems Insight Manager (HP SIM) 4.x to HP SIM 5.x and you used the My Favorites feature, the My Favorites subfolders and folder contents are migrated under the **Private** collections.

About collections

Systems and events are grouped into collections based on information from the HP SIM database. After a collection is defined, you can display the results or associate the collection with a task. You can also save an edited or unedited collection as a collection with another name.

You can use collections to organize large numbers of systems into smaller, more meaningful groupings. For example, your organization might have five system administrators who are responsible for 100 different systems in six different buildings. You can create a collection for each administrator that includes only his or her systems, or you can create a collection for each building that includes only the systems located in that building.

Types of collections

The following types of collections available in HP SIM:

- **By member** When creating a collection, you can select exactly which specific systems or collections you want to include. From the **Customize Collections** page, click **New**. The **New Collection** section appears. Select **Choose members individually**. When creating event collections, you cannot select individual events. You can select other event collections only to create a convenient hierarchy.

When creating event collections, you cannot select individual events. You can select event collections only to create a convenient hierarchy.

- **By attribute** When creating a collection, you can describe the contents of the collection by the attributes of its members. Collections defined by attributes are dynamic because each time they are invoked, the contents are determined again. Many attributes can be used to create collections, including: system name (full or partial), operating system, system type, and so on. For event collections, attributes could be cleared status, type, severity, time, and so on. See “Saving collections” for more information about search criteria and attributes. Multiple attributes can be combined to create the exact group of systems or events required. You create collections by attribute when you click **Save As** from the **Advanced Search** page. See “Searching for systems and events” for more information about performing a system or event search.

Complex collections that contain individual collections or a number of search criteria require more system resources to run. Therefore, it is important to keep the collection as simple as possible to minimize the performance impacts of individual tasks. This advice applies to collections by attributes only.



NOTE: In HP SIM releases prior to version 5.1, you could specify system attributes when creating event collections. If you upgrade to HP SIM 5.1 from any previous version of HP SIM, and you have event collections that include system attributes, the collection is divided into three different collections: one with the same contents as the original collection, one that includes the system attributes only, and one that includes the event attributes only. The original collection becomes a combination collection that contains an event collection with only the original event information, and a system collection with only the original system information. For example, if you had a collection named MyServersEvents in

previous versions of HP SIM that included system attributes, this collection would be migrated into three new collections: MyServersEvents-combination, MyServersEvents-systems, and MyServersEvents-events.

- **Combination collections** This form of collections enables you to bind together a system collection and an event collection. These collections enable you to reuse and recombine system and event collections you have created.

See the *Collections in HP Systems Insight Manager* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about collections.

Related procedures

- Customizing the cluster table view page
- Deleting clusters from the database
- Printing a cluster collection view
- Entering comments on events
- Assigning events to users
- Clearing events from the collection
- Customizing the event table view page
- Deleting events from the database
- Printing an event collection view
- Setting properties for an event collection
- Creating event collections
- Performing an advanced search for events
- Deleting event collections
- Editing event collections
- Moving event collections
- Copying event collections
- Setting properties for a system or cluster collection
- Creating system or cluster collections
- Performing an advanced search for systems
- Deleting system or cluster collections
- Editing system or cluster collections
- Moving system or cluster collections
- Copying system or cluster collections
- Performing a basic search
- Performing an advanced search for clusters
- Saving collections
- Customizing the system table view page
- Deleting systems from the HP SIM database
- Moving system or cluster collections
- Copying system or cluster collections
- Moving event collections
- Copying event collections
- Printing a system collection view

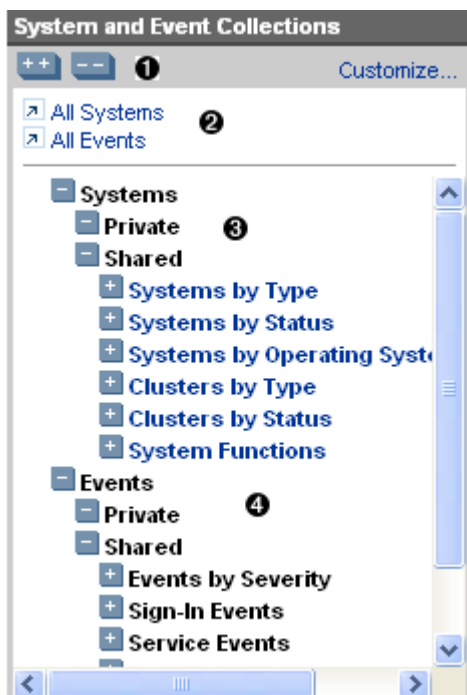
Related topics

- System table view page
- Cluster table view page
- Event table view page
- Customizing event collections
- Customizing system or cluster collections
- Searching for systems and events
- Navigating the System and Event Collections panel
- Reference
- Default shared collections
- Service notification events

Navigating the System and Event Collections panel

The **System and Event Collections** panel contains the following features:

1. Tree controls and customization
2. Overviews
3. Systems
4. Events



Selecting a collection displays a view of its contents. From the **System and Event Collections** panel, you can launch several types of collection view pages. Select one of the pages in the following list to view more information about the types of views available:

- Navigating the system table view page
- Navigating the event table view page
- Navigating the Cluster Table View Page
- Navigating the picture view page
- Navigating the tree view page

In the **System and Event Collections** panel, the **Private** and **Shared** collections are created by default. Collections in **Shared** can be viewed by any valid HP Systems Insight Manager (HP SIM) user. However,


only users with *administrative rights* can edit or delete these collections and their contents. Private collections can only be viewed, edited, or deleted by the user that created the collection. Collections can be placed in **Private** or **Shared** collections. To place a collection in the **Shared** folder, you must have administrative rights. Private collections can be placed into a shared collection, but shared collections cannot be placed into a private collection.


If a collection is placed in both **Shared** and **Private**, any user that has administrative rights can modify the collection stored in the **Shared** collection. When the collection is modified in one place, changes are reflected in the other collection. If the user that created the collection has his or her user rights reduced from administrative rights to operator rights, he or she can no longer modify the collection that is located in the **Shared** collection, and can only edit the collection located in the **Private** collection, which is not be reflected in the collection located in the **Shared** collection.

Collections and members of collections can be set to hidden in the user interface. You might want to do this to remove the clutter of unused collections from the **System and Event Collections** panel. See “Setting properties for a system or cluster collection” and “Setting properties for an event collection” for more information.


Tree controls and customization

The following controls are available to navigate the tree view in the **System and Event Collections** panel:

 Expands all branches of the tree

 all branches of the tree to first-level branches

 Expands a branch of the tree

 Collapses a branch of the tree

The **Customize** link in the **System and Event Collections** panel enables you to customize the **System and Event Collections** panel tree to your own preferences. Any *user* can customize his or her **Systems**, **Events**, and **Private** collections, but only a user with administrative rights can customize the shared **Systems** and **Events** collections. Click **Customize** to display the **Customize Collections** section.

Overviews

The **System and Event Collections** panel includes:

- **All Systems** Displays the **All Systems** page. See “Navigating the system table view page” for information about the system table view page.
- **All Events** Displays the **All Events** page. See “Navigating the event table view page” for information about the event table view page.

Systems

A system collection logically groups systems into a group based on information in the HP SIM *database*. After a collection is defined, you can display the results in the workspace or associate it with a management *task*.

In addition to using the collections provided by HP SIM, you can create, edit, or delete your own collections. Collections must follow specific naming conventions. See “Collection naming conventions” for more information about naming collections.

Collections can be used to organize large numbers of systems into smaller, more meaningful groups. For example, your organization might have five system administrators who are responsible for 100 different systems in six different buildings. You can create a collection for each administrator that includes only his or her systems, or you can create a collection for each building that includes only the systems located in a particular building.

Events

An event collection logically groups multiple event collections into a single collection based on information in the HP SIM database. After a collection is defined, you can display the results in the workspace or associate it with a management task.

Related procedures

- Customizing system or cluster collections
- Customizing event collections

Related topics

- Monitoring systems, clusters, and events
- Navigating the tree view page
- System types

Customizing system or cluster collections

The **System and Event Collections** panel contains a **Systems** collection. The **Systems** collection contains additional system, cluster, and **System Functions** collections.



NOTE: Cluster collections are only created by attributes, not by members.

Collections can be private or shared. Shared collections are visible to all users, while private collections are personal collections you create that only you can view. HP Systems Insight Manager (HP SIM) includes several predefined shared collections. For example, **Systems by Status** is a default shared collection is included with HP SIM. See “Shared system collections” for information about default shared collections.

To customize system collections, click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears, and includes the following options:



1. Displaying collection type
2. Expanding or collapsing collections
3. Customize collections table
4. Available buttons

Name	Visible	Status displayed
<input type="radio"/> Private	Yes	-
<input type="radio"/> Shared	Yes	-
<input type="radio"/> Systems by Type	Yes	-
<input type="radio"/> All Systems	Yes	No
<input type="radio"/> All Servers	Yes	No
<input type="radio"/> All Virtualized Infrastructure	Yes	-
<input type="radio"/> HP BladeSystem	Yes	-
<input type="radio"/> Storage Systems	Yes	-
<input checked="" type="radio"/> All Racks	Yes	Yes
<input type="radio"/> All Enclosures	Yes	No
<input type="radio"/> All Clients	Yes	No
<input type="radio"/> All Networking Devices	Yes	No
<input type="radio"/> All Printers	Yes	No

Displaying collection type

Select the type of collection you want to customize by selecting **Systems** from the **Show collections of** dropdown box.

Expanding or collapsing collections

You can select to view all collections included in the **Shared** and **Private** collections, or to view only the **Shared** and **Private** collection titles. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.

Customize collections table

When the **Customize Collections** page appears, if the collection and system status is displayed in the **System and Event Collections** panel, a table is displayed that includes the names of all the collections.

Available buttons

On the **Customize Collections** page, the following options are available:

- **New** This enables you to create a new system or cluster collection. If you have *administrative rights*, you can save the new collection as a shared collection. Otherwise, you can only save it as a private collection. See “Performing an advanced search for systems” for more information about creating a system collection by attributes.
- **Edit** This enables you to modify an existing collection name and its contents. See “Editing system or cluster collections” for more information about editing system or cluster collections.
- **Move** This enables you to move collections from one collection to another. See “Moving system or cluster collections” for more information about moving system collections.
- **Copy** This enables you to copy a collection as another collection. See “Copying system or cluster collections” for more information.
- **Delete** This enables you to delete an existing system or cluster collection, or system and event combination collections. Only empty system collections can be deleted. If you have administrative rights, you can delete a shared system or cluster collection. See “Deleting system or cluster collections” for more information.
- **Set Properties** This enables you to set the display status, collection visibility, and the default view. See “Setting properties for a system or cluster collection” for more information.

Related procedures

- Performing an advanced search for systems
- Editing system or cluster collections
- Creating system or cluster collections
- Deleting system or cluster collections
- Setting properties for a system or cluster collection
- Moving system or cluster collections
- Copying system or cluster collections

Related topics

- Monitoring systems, clusters, and events
- Default shared collections
- System status types
- Software status types

Creating system or cluster collections

Perform the following procedure to create a new private or shared *system* or *cluster* collection.



NOTE: Users with *administrative rights* can create a shared collection. Users with *operator rights* can view shared collections, but can only create their own private collections.

To create a new system or cluster collection:

1. In the **System and Event Collections** panel, click **Customize**. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Systems**. All available system or cluster collections are displayed.
3. Click **New**. The **New Collection** section appears.
4. Select **Choose members individually**, **Choose members by attributes**, or **Choose members from existing system and event collections**. See “Types of collections” for more information about the different collection types.
 - a. If you selected **Choose members individually**, complete the following steps:
 - i. In the **Choose from** dropdown list, select an individual collection.

Note: When a collection is selected from the dropdown list, the first-level members of that collection are displayed in the **Available Items** box.
 - ii. From the **Available Items** box, select items to place in the collection by highlighting the item and clicking **>>**. You can click the up and down arrows to change the position of an item in the collection, or click **Remove** to remove items from the **Selected Items** box.
 - iii. Click one of the following:
 - **Save As Collection** To save the collection. See “Saving collections” for more information.
 - **Cancel** To close the **New Collection** section without saving changes.
 - b. If you selected **Choose members by attributes**, complete the following steps:
 - i. In the **Search for** dropdown list, select **systems** or **clusters**.
 - ii. Enter the search criteria for the collection. See “Performing an advanced search for systems” for more information about system search criteria, or see “Performing an advanced search for clusters” for more information about cluster search criteria.
 - iii. Click one of the following:
 - **[View]** To run the search and display results immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.
 - c. If you selected **Choose members from existing system and event collections**, complete the following steps:
 - i. In the **Select system collection** dropdown list, select a system collection.

Note: Combination collections are not displayed in the dropdown list.
 - ii. In the **Select event collections** dropdown list, select an event collection.
 - iii. Click one of the following:
 - **View** To run and display the search immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.

Note: If a collection is created with a system collection and an event collection on the **Customize Collections** page, the collection is saved as a system collection and is placed in the **Systems** branch location that you specify.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to create new collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for systems
- Editing system or cluster collections
- Deleting system or cluster collections
- Setting properties for a system or cluster collection
- Moving system or cluster collections
- Copying system or cluster collections

Related topics

- Monitoring systems, clusters, and events
- Customizing system or cluster collections
- Navigating the System and Event Collections panel

Editing system or cluster collections

Users with *administrative rights* can edit a shared collection. Users with *operator rights* can view shared collections, but can only edit their own private collections.

To edit a system or cluster collection:

1. In the **System and Event Collections** panel, click **Customize**. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Systems**. All available system or cluster collections are displayed.
3. Select a system or cluster collection to edit, and then click **Edit**. The **Edit Collection** section appears. Depending on how the collection was created, the following appears:
 - a. If the collection was created using the **Choose members individually** option, complete the following steps:
 - i. In the **Choose from** dropdown list, select an individual collection.

Note: When a collection is selected from the dropdown list, the first-level members of that collection are displayed in the **Available Items** box.
 - ii. From the **Available Items** box, select items to place in the collection by highlighting the item and clicking **>>**. You can click the up and down arrows to change the position of an item in the collection, or click **Remove** to remove items from the **Selected Items** box.
 - iii. Click one of the following:
 - **Save As Collection** To save the collection. See “Saving collections” for more information.
 - **Cancel** To close the **New Collection** section without saving changes.
 - b. If the collection was created using the **Choose members by attributes** option, complete the following steps:
 - i. In the **Search for** dropdown list, select **systems** or **clusters**.
 - ii. Enter the search criteria for the collection. See “Performing an advanced search for systems” for more information about system search criteria, or see “Performing an advanced search for clusters” for more information about cluster search criteria.
 - iii. Click one of the following:
 - **[View]** To run the search and display results immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.
 - c. If the collection was created using the **Choose members from existing system and event collections** option, complete the following steps:
 - i. In the **Select system collection** dropdown list, select a system collection.

Note: Combination collections are not displayed in the dropdown list.
 - ii. In the **Select event collections** dropdown list, select an event collection.
 - iii. Click one of the following:
 - **View** To run and display the search immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to edit existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for systems
- Creating system or cluster collections
- Deleting system or cluster collections
- Setting properties for a system or cluster collection
- Moving system or cluster collections
- Copying system or cluster collections

Related topics

- Monitoring systems, clusters, and events
- Customizing system or cluster collections
- Navigating the System and Event Collections panel

Saving collections

Perform the following procedure to save a system, event, or cluster collection with a new name or to a specific location.



NOTE: For a system search, the name can contain no more than 40 characters (no special characters) and must be unique so that a duplicate collection name cannot be assigned to the new collection, and cannot include special characters.

To save a collection:

1. In the **Name** field, enter a name for the collection.
2. Under **Place in**, select one of the following options to save the collection:
 - **Existing collection** Select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.
 - **New collection** Enter a name for the new collection and select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Related procedures

- Performing an advanced search for systems
- Performing an advanced search for events
- Performing an advanced search for clusters
- Performing a basic search
- Customizing the system table view page
- Deleting systems from the HP SIM database
- Printing a system collection view
- Customizing the cluster table view page
- Deleting clusters from the database
- Printing a cluster collection view



Related topics

- Searching for systems and events
- Basic and advanced search
- Search criteria
- System table view page
- Cluster table view page

Moving system or cluster collections

This procedure enables you to move a collection from one collection to another. *Users with administrative rights* can move a shared collection.

To move a collection:

1. In the **System and Event Collections** panel, click **Customize**. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select the collection to move, and then click **Move**. The **Move Collection** section appears.
4. Under **Move to**, select one of the following:
 - **Existing collection** Select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.
 - **New collection** Enter a name for the new collection and select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Command line interface

Users with administrative rights can use the `mxcollection` command to move existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.



NOTE: *Users with administrative rights* can move a shared collection. You cannot move shared and private root collections, and you cannot move a shared collection into a private collection.

Related procedures

- Performing an advanced search for systems
- Creating system or cluster collections
- Deleting system or cluster collections
- Setting properties for a system or cluster collection
- Moving system or cluster collections
- Copying system or cluster collections

Related topics

- Monitoring systems, clusters, and events
- Customizing system or cluster collections
- Navigating the System and Event Collections panel

Copying system or cluster collections



You can copy a collection as a new collection. When you copy a collection that was created by members, you are copying the collection and its members into the new collection. If the original collection is edited after it is copied to the new collection, the newly copied collection is not updated. For example, if the original collection has two members, the same two members are copied to the new collection. If the original collection is edited to add another member after it is copied, the newly copied collection is not modified.

When you copy a collection that was created based on attributes, you are copying the collection attributes into the new collection. If the original collection is edited after it is copied to the new collection, the newly copied collection does not reflect these edits.

When you copy a combination collection, the newly created collection has the same system collection and event collection. If the original collection is edited after it is copied to the new collection, the newly copied

collection is not updated. See the *Collections in HP Systems Insight Manager* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about collections.

To copy a collection:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select the collection to copy, and then click **Copy**. The **Copy Collection** section appears.
4. In the **Collection name** field, enter a name for the new collection.
5. Under **Place in**, select a location to save the collection, and then, depending on the type of collection, do one of the following:
 - **Existing collection** Select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.
 - **New collection** Enter a name for the new collection and select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to copy existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for systems
- Creating system or cluster collections
- Deleting system or cluster collections
- Setting properties for a system or cluster collection
- Moving system or cluster collections
- Editing system or cluster collections



Related topics

- Monitoring systems, clusters, and events
- Customizing system or cluster collections
- Navigating the System and Event Collections panel

Deleting system or cluster collections



NOTE: Users with *administrative rights* can delete a shared collection. Users with *operator rights* can view shared collections, but, can only delete their own private collection.

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select the collection to be deleted.
4. Click **Delete**. A dialog box appears. To continue with the deletion, click **OK**, or to cancel the operation, click **Cancel**. If the selected collection is not empty or is in use by a task (such as **Home** page, reports,

and so on) an error message appears. However, if the collections contents are based on attributes, the collection can be deleted even if it is not empty.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to delete existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for systems
- Editing system or cluster collections
- Creating system or cluster collections
- Setting properties for a system or cluster collection



Related topics

- Monitoring systems, clusters, and events
- Customizing system or cluster collections
- Navigating the System and Event Collections panel

Setting properties for a system or cluster collection

You can use the **System and Event Collections** panel to set collection properties such as hiding or showing collections, system status, and cluster status, and selecting the default view for a collection.

To set properties for system or cluster collections:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Systems**. All available system or cluster collections are displayed. Click  to expand all system and cluster collections in the table, or click  to collapse all system and cluster collections in the table.
3. Select a collection, and then click **Set Properties**. The **Set Properties** section appears.
4. Under **Visible**, select **Yes, show collection and its members in the user interface** or select **No, do not show collection and its members in the user interface**. If you have collections that are unused, you might want to select **No, do not show collection and its members in the user interface** so that the collections do not clutter the **System and Event Collections** panel.
5. If you want to see the system health status, under **Status Displayed**, select **Yes, show status in System and Event Collections panel**, or to keep the panel uncluttered, select **No, do not show the status in System and Event Collections panel**.

Note: This option is available only for collections based on attributes and for combination collections.

Note: For a collection, the most critical status of its members is displayed. If you open the collection, the status for each individual member is shown.

Note: To conserve system resources, try to limit the display of status to only those collections that you view the most.

6. In the **Default View** field, select the default view from the dropdown list.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to set properties for collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for systems
- Editing system or cluster collections
- Creating system or cluster collections
- Deleting system or cluster collections

Related topics

- Monitoring systems, clusters, and events
- Customizing system or cluster collections
- Navigating the System and Event Collections panel

Customizing event collections

The **System and Event Collections** panel contains an **Events** collection. This collection contains collections of different types of *events*.

Collections can be private or shared. Shared collections are visible to all *users*, while private collections are personal collections you create that only you can view. HP Systems Insight Manager (HP SIM) includes several predefined shared collections. For example, **Events by Severity** is a default shared collection included with HP SIM. See “Shared event collections” for information about default shared collections.

To customize system collections, click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears and includes the following options:

1. Displaying collection type
2. Expanding or collapsing collections
3. Customize collections table
4. Available buttons

Name	Visible	Status displayed
<input type="radio"/> Private	Yes	-
<input type="radio"/> Shared	Yes	-
<input type="radio"/> Events by Severity	Yes	-
<input type="radio"/> All Events	Yes	-
<input checked="" type="radio"/> Important Events	Yes	-
<input type="radio"/> Important Uncleared Events	Yes	-
<input type="radio"/> Informational Events	Yes	-
<input type="radio"/> Sign-In Events	Yes	-
<input type="radio"/> Service Events	Yes	-
<input type="radio"/> Events by Time	Yes	-

Displaying collection type

Select **Events** from the **Show collections of** dropdown box to customize event collections.

Expanding or collapsing collections

You can select to view all collections included in the **Shared** and **Private** collections, or to view only the **Shared** and **Private** collection titles. Click to expand all system and cluster collections in the table, or click to collapse all system and cluster collections in the table.

Customize collections table

When the **Customize Collections** page appears, if the collection and system status is displayed in the **System and Event Collections** panel, a table is displayed that includes the names of all the collections.

Available buttons

The following options are available on the **Customize Collections** page for events:

- **New** This enables you to create a new event collection. If you have administrative rights, you can save the new collection as a shared collection. Otherwise, you can only save it as a private collection. See [“Performing an advanced search for events”](#) for more information about creating an event collection by attributes.
- **Edit** This enables you to modify an existing collection name and its contents. See [“Editing event collections”](#) for more information about editing event collections.
- **Move** This enables you to move collections from one collection to another, either from a private to a shared collection, or from a shared to a private collection. See [“Moving system or cluster collections”](#) for more information about moving system collections.
- **Copy** This enables you to copy a collection as another collection. See [“Copying system or cluster collections”](#) for more information.
- **Delete** This enables you to delete an existing event collection or system and event combination collections. If you have administrative rights, you can delete a shared event collection. Only empty event collections can be deleted. See [“Deleting event collections”](#) for more information.
- **Set Properties** This enables you to set the visibility of the collection and its members. See [“Setting properties for a system or cluster collection”](#) for more information.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to set properties for collections from the *command line interface* (CLI).

See [“Using command line interface commands”](#) for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- [Performing an advanced search for events](#)
- [Editing event collections](#)
- [Creating event collections](#)
- [Deleting event collections](#)
- [Moving event collections](#)
- [Copying event collections](#)
- [Setting properties for an event collection](#)

Related topics

- [Monitoring systems, clusters, and events](#)
- [Default shared collections](#)
- [Service notification events](#)

Creating event collections



NOTE: By default, all newly created collections are private.

NOTE: *Users with **administrative rights** can create a new shared event collection. Users with **operator rights** or **user rights** view shared collections, but can only create their own collections.*

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Events**. All available event collections are displayed.
3. Click **New**. The **New Collection** section appears.
4. Select **Choose members individually**, **Choose members by attributes**, or **Choose members from existing event and system collections**. See “Types of collections” for more information about the different collection types.
 - a. If you selected **Choose members individually**, complete the following steps:
 - i. In the **Choose from** dropdown list, select an individual collection.

Note: When a collection is selected from the dropdown list, the first-level members of that collection are displayed in the **Available Items** box.
 - ii. From the **Available Items** box, select items to place in the collection by highlighting the item and clicking **>>**. You can click the up and down arrow to change the position of an item in the collection, or click **Remove** to remove items from the **Selected Items** box.
 - iii. Click one of the following:
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.
 - b. If you selected **Choose members by attributes**, the **New** section appears. Complete the following steps:
 - i. In the **Search for** dropdown list, select **events**.
 - ii. Enter the search criteria for the collection. See “Performing an advanced search for events” for more information about event search criteria.
 - iii. Click one of the following:
 - **View** To run the search and display the results immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information.
 - **Cancel** To close the **New Collection** section without saving changes.
 - c. If you selected **Choose members from existing event and system collections**, complete the following steps:
 - i. In the **Select event collection** dropdown list, select an event collection.

Note: Combination collections are not displayed in the dropdown list.
 - ii. In the **Select system collections** dropdown list, select a system collection.
 - iii. Click one of the following:
 - **View** To run the search and display the results immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to create new collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for events
- Editing event collections
- Deleting event collections
- Moving event collections
- Copying event collections
- Setting properties for an event collection

Related topics

- Monitoring systems, clusters, and events
- Customizing event collections
- Navigating the System and Event Collections panel

Editing event collections

The **Event Collections** section enables you to add, delete, and reorder the position of members of an existing collection. This section is similar to the **New Collection** section.



NOTE: *Users with administrative rights* can edit a shared collection. *Users with operator rights* can edit only their own collections.

To edit an existing event collection:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Events**. All available event collections are displayed.
3. Select the event collection to edit, and then click **Edit**. The **Edit Collection** section appears. Depending on how the collection was created, the following appears:
 - a. If the collection was created with the **Choose members individually** option, complete the following steps:
 - i. In the **Choose from** dropdown list, select an individual collection.
Note: When a collection is selected from the dropdown list, the first-level members of that collection are displayed in the **Available Items** box.
 - ii. From the **Available Items** box, select items to place in the collection by highlighting the item and clicking **>>**. You can click the up and down arrow to change the position of an item in the collection, or click **Remove** to remove items from the **Selected Items** box.
 - iii. Click one of the following:
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.
 - b. If the collection was created with the **Choose members by attributes** option, complete the following steps:
 - i. In the **Search for** dropdown list, select **events**.
 - ii. Enter the search criteria for the collection. See “Performing an advanced search for events” for more information about event search criteria.
 - iii. Click one of the following:
 - **View** To run the search and display the results immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information.
 - **Cancel** To close the **New Collection** section without saving changes.
 - c. If the collection was created with the **Choose members from existing system and event collections** option, complete the following steps:
 - i. In the **Select event collection** dropdown list, select an event collection.
Note: Combination collections are not displayed in the dropdown list.
 - ii. In the **Select system collections** dropdown list, select a system collection.
 - iii. Click one of the following:
 - **View** To run the search and display the results immediately.
 - **Save As Collection** To save the collection. See “Saving collections” for more information about saving collections.
 - **Cancel** To close the **New Collection** section without saving changes.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to edit existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for events
- Creating event collections

- Deleting event collections
- Moving event collections
- Copying event collections
- Setting properties for an event collection



Related topics

- Monitoring systems, clusters, and events
- Customizing event collections
- Navigating the System and Event Collections panel

Moving event collections

This procedure enables you to move a collection from one collection to another. *Users with administrative rights* can move a shared collection.

To move a collection:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show collections of** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select the collection to move, and then click **Move**. The **Move Collection** section appears.
4. Under **Move to**, select one of the following:
 - **Existing collection** Select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.
 - **New collection** Enter a name for the new collection and select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to move existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for events
- Creating event collections
- Deleting event collections
- Setting properties for an event collection
- Moving event collections
- Copying event collections

Related topics

- Monitoring systems, clusters, and events
- Customizing event collections
- Navigating the System and Event Collections panel

Copying event collections



You can copy a collection as a new collection. When you copy a collection that was created by members, you are copying the collection and its members into the new collection. If the original collection is edited after it is copied to the new collection, the newly copied collection is not updated. For example, if the original

collection has two members, the same two members are copied to the new collection. If the original collection is edited to add another member after it is copied, the newly copied collection is not modified.

When you copy a collection that was created based on attributes, you are copying the collection attributes into the new collection. If the original collection is edited after it is copied to the new collection, the newly copied collection does not reflect these edits.

When you copy a combination collection, the newly created collection has the same system collection and event collection. If the original collection is edited after it is copied to the new collection, the newly copied collection is not updated. See the *Collections in HP Systems Insight Manager* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about collections.

To copy collections:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select the collection to copy, and then click **Copy**. The **Copy Collection** section appears.
4. In the **Collection name** field, enter a name for the collection.
5. Under **Place in**, select a location to save the collection.
 - **Existing collection** Select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.
 - **New collection** Enter a name for the new collection and select an existing private or shared collection from the dropdown list. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to copy existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for events
- Creating event collections
- Deleting event collections
- Setting properties for an event collection
- Moving event collections
- Editing event collections



Related topics

- Monitoring systems, clusters, and events
- Customizing event collections
- Navigating the System and Event Collections panel

Deleting event collections



NOTE: Users with *administrative rights* can delete a shared collection. Users with *operator rights* or *user rights* can view shared collections, but can only delete their own private collections.

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select the collection to be deleted.
4. Click **Delete**. A dialog box appears. To continue with the deletion, click **OK**, or to cancel the operation, click **Cancel**. If the selected collection is not empty or is in use by a task (such as **Home** page, reports, and so on) an error message appears. However, if the collections contents are based on attributes, the collection can be deleted even if it is not empty.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to delete existing collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for events
- Editing event collections
- Creating event collections
- Setting properties for an event collection
- Moving event collections
- Copying event collections



Related topics

- Monitoring systems, clusters, and events
- Customizing event collections
- Navigating the System and Event Collections panel

Setting properties for an event collection

You can use the **System and Event Collections** panel to set event collection properties such as hiding or showing collections.

To set properties for event collections:

1. Click **Customize** in the **System and Event Collections** panel. The **Customize Collections** page appears.
2. In the **Show collection of** dropdown list, select **Events**. All available event collections are displayed. Click  to expand all event collections in the table, or click  to collapse all event collections in the table.
3. Select a collection, and then click **Set Properties**. The **Set Properties** section appears.
4. Under **Visible**, select **Yes, show collection and its members in the user interface** or select **No, do not show collection and its members in the user interface**. If you have collections that are unused, you might want to select **No, do not show collection and its members in the user interface** so that the collections do not clutter the **System and Event Collections** panel.

Command line interface

Users with *administrative rights* can use the `mxcollection` command to set properties for collections from the *command line interface* (CLI).

See “Using command line interface commands” for more information about accessing the manpage, which includes detailed information for this command.

Related procedures

- Performing an advanced search for events
- Editing event collections
- Creating event collections
- Deleting event collections

Related topics

- Monitoring systems, clusters, and events
- Customizing event collections
- Navigating the System and Event Collections panel

System table view page

Users with *administrative rights* can manage all shared system collections from the system table view page. Users can also manage their own private collections from this page. They can:

- **Save selections** See “Saving collections” for more information.
- **Delete systems from the *database*** See “Deleting systems from the HP SIM database” for more information.
- **Print a system collection results** See “Printing a system collection view” for more information.
- **Customize the view** See “Customizing the system table view page” for more information.

The system table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab “remembers” the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

Related procedures

- Saving collections
- Customizing the system table view page
- Deleting systems from the HP SIM database
- Printing a system collection view

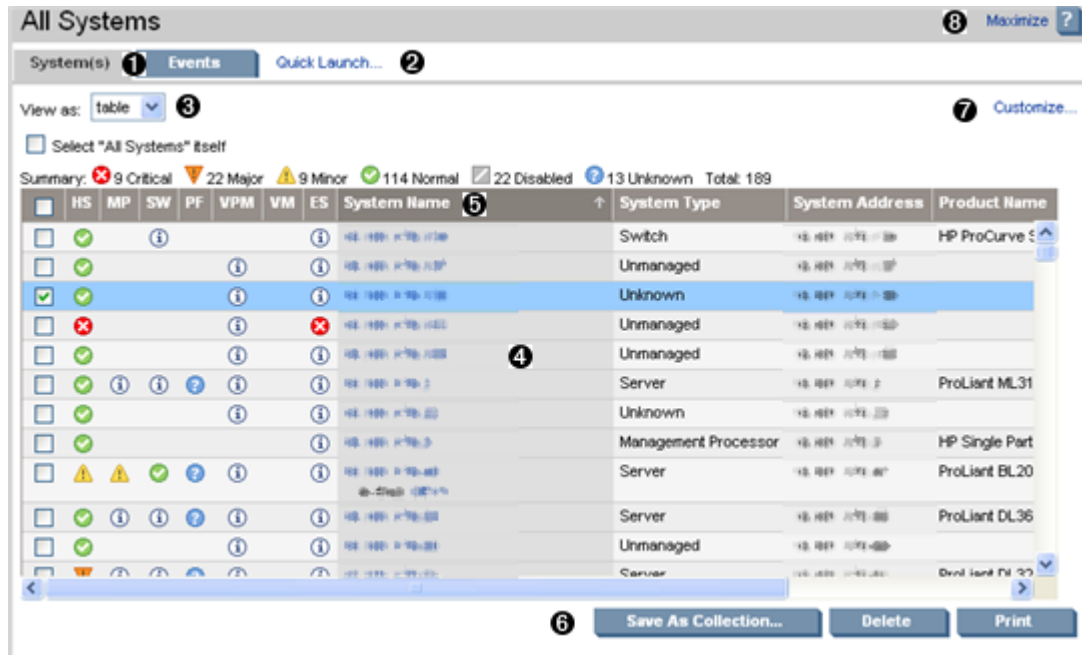
Related topics

- Navigating the system table view page
- Navigating the picture view page
- System status types
- Software status types
- Monitoring systems, clusters, and events

Navigating the system table view page

The system table view page is the default view for an attribute-based system collection and displays a list of systems that meet common *criteria*. The system table view page is divided into the following sections:

1. Tabs
2. Quick Launch
3. View as
4. Table information
5. System view columns
6. System table view page buttons
7. Customizing the view



From this page, you can view *systems* in a list, table, or tree, and save system collections, delete systems, and print the system collection.

If a collection includes more than 500 members, the first 500 members are displayed on the first page. Systems selected on one page remain selected as you navigate to a different page in the collection. Whenever a column is selected as the column to sort by, the entire collection is sorted, not just the items on the currently viewed page.

Tabs

The system table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab "remembers" the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

Quick Launch

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

View as

This **View as** dropdown list is used to select either **table**, which displays the system results in a table form, **icons**, which displays only the **HS** status icon and the **System Name** for each system, and **tree**, which displays the **HS** status icon and the System Name for each system in a tree format. See “[Navigating the tree view page](#)” for more detailed information about the tree view. See “[Navigating the icon view page](#)” for more information about the icon view.

System health status summary

The summary shows how many systems in the view have a status of: Critical, Major, Minor, Normal, Disabled, and Unknown. See “[System status types](#)” for more information.

Table information

To access a systems view or picture view of a system, click a link in the **System Name** column. Typically, the **System Page** is displayed when a system is clicked. However, *Racks* link to the rack picture view page, and *enclosures* link to the enclosure picture view page. These links are both types of container views. See [System Name](#) for more information.

System view columns

Sort columns by clicking the column header to switch between ascending and descending order. The column that the table is sorted by includes an up or down arrow in the column heading. Place your cursor over a column name to display a brief description of the column. The columns are not available when you select the **icons**, **picture**, or **tree** views. The following are the columns located on the system table view page:

- Selection
- Health status
- Management processor
- Software status
- HP Performance Management Pack
- HP ProLiant Essentials Vulnerability and Patch Management Pack
- HP ProLiant Essentials Virtual Machine Management Pack
- Contract and Warranty status
- Aggregate Event status
- System Name
- System Type
- System Address
- Product Name
- Operating system name

See “[Customizing the system table view page](#)” for more information about customizing columns.

Selection

Select the checkbox in this column to select a system. You can select more than one system. This option is available in the table view, tree view, and icon view. Select the checkbox in the column heading or select **Select "*collection name*" itself** to select or deselect all displayed systems.

Health status

The **HS** column displays the overall system health status, which is determined by the default Hardware Status Polling task and is a roll up of all the status sources, which can be SNMP, WBEM, DMI, HTTP, and cluster status. By clicking the status icon in this column, the **HP Management Agents** or the **HP Instant Toptools for Servers** page is displayed. If the system does not have Web Agents or Instant Toptools installed, the **System Page** is displayed. See “[System status types](#)” for more information.

The hardware status that is displayed for container systems, such as Serviceguard or a complex, is the actual hardware status for the container itself. For clusters, the hardware status is the ping status.



NOTE: The status of a complex is collected only when VSE Manager is registered with HP SIM. In addition, the status update is collected every 30 minutes from the nPar or Complex outside of HP SIM.

Management processor

The **MP** column displays the status icon of the management processor if the system has an Integrated Lights-Out (iLO) board installed. Otherwise, the Informational icon is displayed. Clicking the status icon displays the management processor login page.

Software status

The **SW** column, available for servers only, indicates both the availability of software updates and if they are considered critical they are. See “Software status types” for more information about the software status types.

If you click an Unknown status, HP SIM displays the **Legacy Version Control** page.

If HP Version Control Agent (VCA) is installed on the system, clicking the software status icon for that system displays **HP Version Control Agent Software Inventory** page. If you hold your cursor over the status icon and the VCA is not installed on the system, the following message appears that states `Version Control Agent not found`.

HP Performance Management Pack

If HP Performance Management Pack (PMP) is installed, this column (indicated by **PF**) displays the cumulative performance status of all monitored subsystems for the system. By clicking the status icon in this column, the **HP Performance Management Pack** page for the selected system is displayed, providing more detailed performance information.

The status is considered Unknown if one of the following conditions are met:

- PMP is not licensed
- PMP is licensed but is not monitoring a server
- If licensing and monitoring are started, but there are insufficient samples

If you click the status link, the PMP displays a page with information about purchasing a license to monitor that system, or shows notification that PMP monitoring is not supported on that system.



NOTE: For the **PF** column, status is displayed for all systems from the **All Servers** list. If the status cannot be determined for some reason, the status is displayed as Unknown.

HP ProLiant Essentials Vulnerability and Patch Management Pack

If installed, HP ProLiant Essentials Vulnerability and Patch Management Pack vulnerability information is displayed in the **VPM** column of the HP SIM console. Initially, the icon in the column indicates Vulnerability and Patch Management Pack eligibility information for the target system in the row. After target servers are licensed and a vulnerability scan is performed, the column displays the combined status of the last vulnerability scan on the target system (patch status is not displayed in the column). Click the icon to display detailed information about the system status with regard to the Vulnerability and Patch Management Pack. Clicking the Normal, Minor, or Major icons opens a new informational page from which you can access the last scan results for the system. A new scan can also be launched from this page. Clicking the Unknown icon for a system displays an explanatory page listing possible reasons why Vulnerability and Patch Management Pack is inaccessible and offers possible solutions to the correct the problem.



NOTE: If the Vulnerability and Patch Management Pack is not installed on the HP SIM system, the Informational icon appears in the **VPM** column on the system table view page. Clicking this icon displays information about how to install the Vulnerability and Patch Management Pack and purchase licenses.

If the system is not licensed, or has not yet been scanned by the Vulnerability and Patch Management Pack, the Informational icon appears in the **VPM** column. Clicking this icon displays details about licensing the target system, a link to the HP SIM License Manager or information about vulnerability scanning, and a link to scan for patch vulnerabilities on the target system.

HP ProLiant Essentials Virtual Machine Management Pack

If HP ProLiant Essentials Virtual Machine Management Pack is installed, the **VM** status column displays the cumulative status of all virtual machine hosts and virtual machine guests. Clicking the status icon on the **VM** status column displays in the **HP ProLiant Essentials Virtual Machine Management Pack** page for the selected system, providing more information about the status of the virtual machine.

For systems with Server type and Virtual Machine Host or Virtual Machine Guest subtype, HP SIM populates the **VM** status column with the appropriate status icons.

Contract and Warranty status

The **CW** column is available when a Windows CMS and the HP Service Essentials Remote Support Pack is installed. To view the **Contract and Warranty Status** page for a system, click the **CW** status icon. See “Contract and warranty status types” for more information about contract and warranty status types.



NOTE: If you receive an incorrect response for a particular HP brand system after clicking the **CW** icon on the system table view page, there might be an entitlement issue with the system. This is not a Remote Support or an HP SIM issue. Please contact HP support. You must have a valid serial number and product ID along with any contract or Care Pack numbers that are applicable.

NOTE: There is no status icon in this column for management processors, instead see the contract and warranty status for the server where the management processor is physically located.

Aggregate Event status

The **ES** column is a summary of all of a system's uncleared events. This status is updated whenever an event is added, updated, or removed. To view all of the events for a system, including cleared events, click the **ES** status icon.

System Name

This column contains the actual system name of all discovered systems. Systems can be shown as a single system or as a system in a container. When you place the cursor over the system name, the full system *Domain Name Service (DNS)* name is displayed, which helps differentiate between two or more systems that share the same system name. If you click the system name link, the **System Page** is displayed. See “System Page” for more information. If you click a system that is a container (rack or enclosure), the picture view for that object is displayed. See “Navigating the picture view page” for more information. See “About racks and enclosures” for more information about racks and enclosures.

The **System Name** column displays systems and associated devices. The following are the associations available in HP Systems Insight Manager (HP SIM):

- Management processor to server
- Management processor to server for nPar
- Management processor to complex

Note: After upgrading HP SIM, for this association to be displayed, you must rediscover the complex if you have appropriate XML, *Web-Based Enterprise Management (WBEM)*, and SNMP instrumentation on the management processor and partition-able cells.

Note: For a high-end HP Integrity Superdome, rerunning discovery works only if you have an sx2000 Superdome and the latest firmware. Mid-range servers must have either sx1000 or sx2000 chipsets and the latest firmware.

- Management processor to enclosure
- Server to *enclosure*
- Enclosure to rack
- Switch to enclosure
- System to *cluster*
- Logical server to server

The following system types are containers:

- Rack
- Enclosure
- Cluster

When servers and management processors in racks and enclosures are *discovered* and *identified*, associations are made between the systems and the racks and enclosures where systems reside. This association is displayed in the **System Name** column on the system table view page by showing *name* in *system type container name*. The following are examples of the different associations available:

- When switches in blade enclosures are discovered and identified, associations are made between the switches and the enclosures where they reside. This association appears in the **System Name** column on the system table view page by showing *switch_name* in *Encl. enclosure_name*. The **System Type** column displays Switch as the system type. For HP SIM to identify and manage the HP ProLiant p-Class server blades correctly, HP Insight Management Agent 5.50 or later must be installed on the blades to make associations work and event correlation function properly. Clicking an enclosure name in the **System Name** column displays a list of all discovered systems in the selected enclosure. The status for both racks and enclosures is always Unknown.
- When a server blade is identified through another system in the same rack or enclosure, associations are made between the iLO and the enclosures where they reside. This association appears in the **System Name** column on the system table view page by showing the system serial number prepended with *Server_* in *Encl. enclosure_name*. For example, *Server_C349KJP5D876* in *Encl. Encl4*. The system address, product name, and operating system are not displayed for these systems.

You can launch HP Serviceguard Manager to manage a server belonging to an HP Serviceguard cluster. To do so, ensure that:

- HP Serviceguard Manager is installed and registered with HP SIM
- The system selected is an HP-UX or Linux server that belongs to an HP Serviceguard cluster

System Type

This column displays the system type (for example, Server or Desktop). The system type Unmanaged indicates systems that have no management protocol that HP SIM can detect (for example, no *SNMP*, *WBEM*, *Desktop Management Interface (DMI)*, or *Secure Shell (SSH)*). The system type Unknown indicates systems that have some management protocol but have not matched any identification rule in HP SIM. See “System types” for more information about the different system types.



NOTE: Unmanaged systems might indicate that the credentials were not set correctly to communicate with the system. If you know that there are HP Insight Management Agents installed, verify the credentials used.

System Address

This column displays the primary IP address of the system that HP SIM uses to communicate with the system. Not all systems have an IP address, including HP Serviceguard clusters.

Product Name

This column displays the product name of the system.

Operating system name

The **OS Name** column displays the system's operating system on the system. For a Serviceguard cluster, this column displays **HP Serviceguard** if the cluster is of type HP-UX, or **HP Serviceguard for Linux** if the cluster is of type Linux. **HP Serviceguard** and **HP Serviceguard for Linux** under the **OS Name** column in the *virtual* cluster system column do not represent the actual operating system name and type. This field is used to alert you that the servers that comprise the cluster are of HP-UX or Linux type, respectively.

System table view page buttons

Three buttons at the bottom of the system table view page are available to users with *administrative rights*. These buttons are not available when using a tool and selecting an individual target system.

- **Save As Collection** When a system is highlighted, this button is used to save the selection with a new name. Changes are saved on a per-user basis. If you click **Save As Collection**, the collection is saved as a combination of the system and event collections. See “Saving collections” for more information.
- **Delete** This button is used to delete one or more systems from the *database*. Select the systems to be deleted, and then click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the operation. See “Deleting systems from the HP SIM database” for more information.



NOTE: If a virtual machine host is deleted, it can still be accessed through the Virtual Machine Management Pack console. The operations that can be performed on a virtual machine host are not affected by the fact that the HP SIM system has been deleted. The Virtual Machine Management Pack console continues to show the HP SIM status.

- **Print** This button is used to create a printer-friendly version of the list in a new window. From the table view page, select **File**→**Print** from the browser menu to print the report.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

Customizing the view

The **Customize** link is located in the upper right corner of the system table view page. Click this link to configure what columns are displayed and in what order. When you modify the columns to display on the system table view page and select **Apply to all system table views**, these columns become the default set of columns displayed for any system collection selected if the collection does not already have customized columns defined. See “Customizing the system table view page” for more information.

Related procedures

- Customizing the system table view page
- Saving collections
- Deleting systems from the HP SIM database
- Printing a system collection view

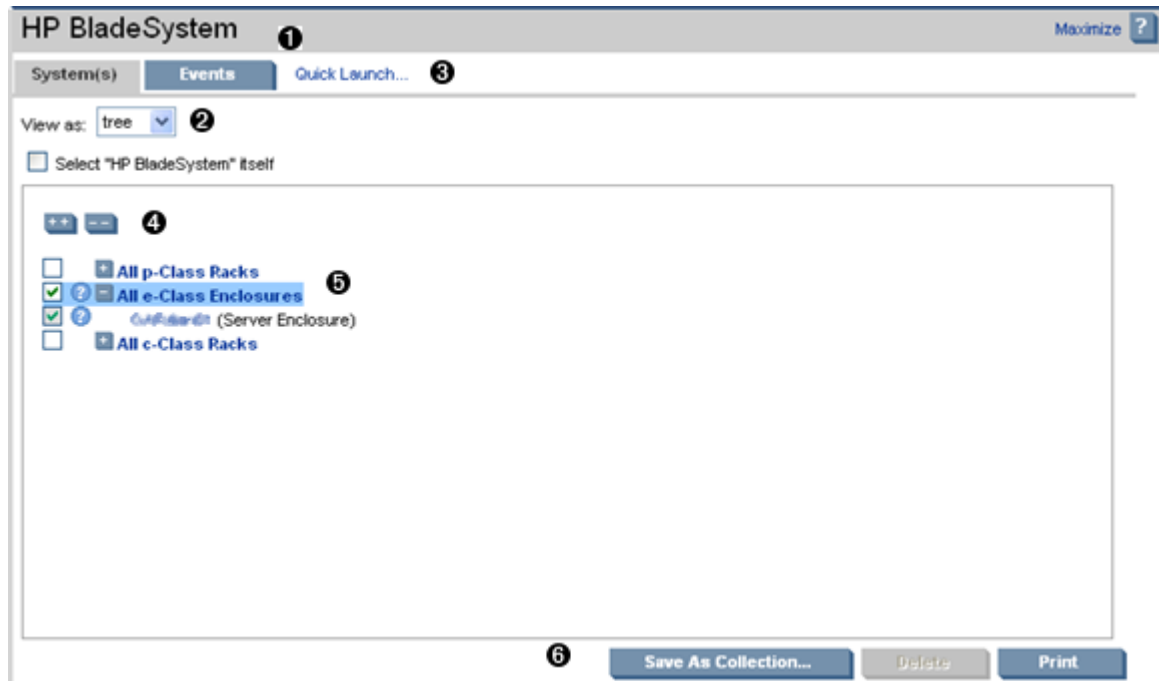
Related topics

- Monitoring systems, clusters, and events
- System table view page
- System status types
- Software status types
- Navigating the picture view page
- Contract and warranty status types

Navigating the tree view page

When a collection is selected that was created based on individual members, the tree view is displayed in the workspace. The tree view is initially collapsed. Systems might appear in multiple locations, because they can be in multiple containers. Users can view only systems that they are authorized to view. Therefore, if a user is not authorized to view a particular system in the tree, that branch is not displayed. The following sections are available on the tree view page:

1. Tabs
2. View as
3. Quick Launch
4. Expanding the tree view
5. Tree view hierarchy
6. Tree view buttons



Tabs

The system table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab "remembers" the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

View as



This dropdown list is used to select **table**, which displays the results in a table form, **icons**, which displays only the **HS** status icon and the **System Name** for each system, and **tree**, which displays the **HS** status icon and the system name for each system in a tree format. See "Navigating the icon view page" for more information about the icon view.

Quick Launch

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting

a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.


Expanding the tree view


Branch nodes can be expanded by clicking the toggling expansion icon. However, the system name is not an expansion control, but a hyperlink to a page that displays more information about that particular system. When a branch is collapsed, the icon appears as . When clicked, the branch expands to show the child systems, and the icon toggles to . Clicking the icon again collapses the branch and toggles the icon.



NOTE: The expansion state persists only for the page session. When the page is reloaded or navigated to again, a fresh tree is loaded to ensure that all newly discovered systems are added to the view.

A paging mechanism is provided in the branches. When a branch is expanded, the first 100 systems are displayed. To view additional systems, click **next...of...** Clicking this link displays either the remaining systems or the next 100 system.

At the top of each tree view there are two expansion buttons. To expand all branches of the tree, click .





To collapse all branches of the tree to first-level branches, click . If there are too many systems to load into the expand all page, a message appears, advising you that there are too many systems in the tree and the function cannot be performed.

Tree view hierarchy

The tree view displays status data for each system. The status icon is located in the left of the tree view next to the selection checkbox. If the status of the system is Unknown, no status icon appears. If the systems are containers, the status to the left of the container name is displayed as the most critical status of the systems in the container, including the container status itself. The status of the actual container is displayed to the right of the system name, along with a system type label.

Selection in the tree view

When a container can be selected independently of its contents, the selection control for the tree view cycles through four states using the following check icons:

-  First, or initial state; nothing selected.
-  Second state; both the container and the contents are selected. If the contents are not already expanded, the next level of children is expanded to show the selection.
-  Third state; all contents are recursively selected. The children are expanded (if not already) to show they are selected. Only the next level is expanded.
-  Fourth state; only the container is selected.



NOTE: If a collection is selected and the collection selects its own contents, the checkboxes are disabled.




Available drilldowns

The tree view contains hyperlinks for the system name and status icon drilldowns. When you click a system name, the **System Page** for that particular system appears. The status icons drill-down to the status URL for that system, unless the status icon is the status icon to the left of a container. Clicking the roll-up status of a branch loads a table view of all systems in that branch that match the roll-up status. Therefore, you are presented with all the systems that are contributing to the severity of the roll-up status. For example, if the

status icon to the left of the rack is Critical, and you click the icon, a table view of all systems in the rack with the status of Critical are displayed.

Selection states for collections

In the tree view, you cannot simultaneously select a collection and members of the same collection. When a collection is selected, the members are displayed and their selection boxes are disabled. The selection states for a collection are as follows:

-  The initial state; nothing is selected.
-  The collection itself is selected; the contents of the collection are disabled.
-  The members of the collection are selected; the collection itself is unselected

Additionally, a checkbox at the top of the tree enables you to select the collection that is viewed. When the checkbox is selected, all the checkboxes under the collection are cleared and disabled. When a checkbox is cleared, the checkboxes under the collection become selectable.

Tree view buttons

The following buttons at the bottom of the tree view page are available to users with *administrative rights*:

- **Save As Collection** When a system or group of systems is selected, this button is used to save the selection with a new name. Changes are saved on a per-user basis. See “Saving collections” for more information.
- **Delete** This button is used to delete one or more systems from the *database*. Select the systems to be deleted, and then click **Delete**. A dialog box appears. Click **OK** to continue with the deletion, or click **Cancel** to cancel the operation. The tree view is refreshed. See “Deleting systems from the HP SIM database” for more information.



NOTE: Only systems can be deleted from the tree view. If a collection is selected, the **Delete** button is disabled. Collections must be deleted through the **Customize Collections** page. See “Deleting system or cluster collections” for more information about deleting collections.

NOTE: If a virtual machine host is deleted, it can still be accessed through the Virtual Machine Management Pack console, and the operations that can be performed on a virtual machine host are not affected by the deletion of the HP Systems Insight Manager (HP SIM) system. The Virtual Machine Management Pack console continues to show the HP SIM status.

NOTE: If you select a collection by selecting **Select "collection name" itself**, the **Delete** button is disabled. To delete collections, go to the **Customize Collections** page. See “Deleting system or cluster collections” or “Deleting event collections” for more information.

- **Print** This button is used to create a printer-friendly version of the list in a new window. From the table view page, select **File**→**Print** from the browser menu to print the report.

Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

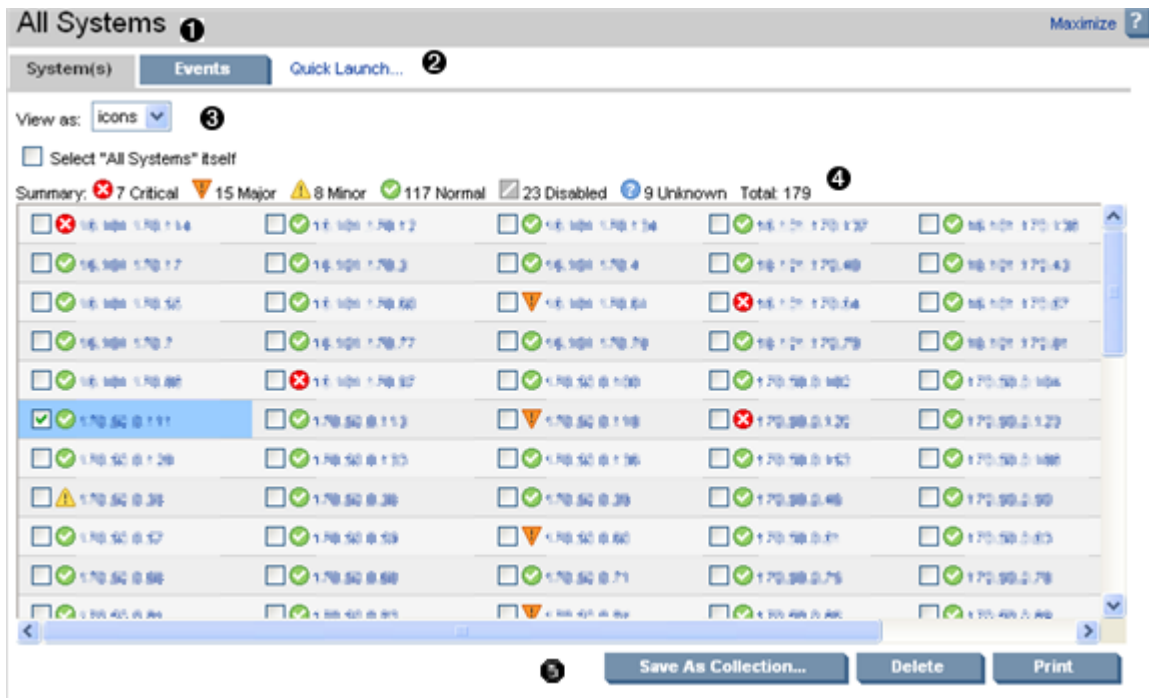
Related topics

- [Navigating the picture view page](#)
- [Navigating the system table view page](#)
- [Navigating the event table view page](#)
- [Navigating the picture view page](#)

Navigating the icon view page

The icon view lists the system name of all discovered systems, as well as the *system health status* for each system. The legend shows how many systems in the view are Critical, Major, Minor, Normal, Disabled, and Unknown. Select the checkbox next to system name to select a system. You can select more than one system, or to select an entire collection, select the checkbox, **Select "collection name" itself**. This page includes the following sections:

1. Tabs
2. Quick Launch
3. View as
4. System health status summary
5. Icon view buttons



Tabs

The icon view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab "remembers" the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

Quick Launch

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

View as

The **View as** dropdown list is used to select either **table**, which displays the results in a table form, **icons**, which displays only the **HS** status icon and the **System Name** for each system, and **tree**, which displays

the **HS** status icon and the System Name for each system in a tree format. See “Navigating the tree view page” for more detailed information on the tree view. See “Navigating the system table view page” for more information about the system table view.

System health status summary

This summary shows how many systems in the view have a status of Critical, Major, Minor, Normal, Disabled, and Unknown. See “System status types” for more information about system status types.

Icon view buttons

The following buttons at the bottom of the icon view page are available to users with *administrative rights*.

- **Save As Collection** When a system or group of systems is selected, this button is used to save the selection with a new name. Changes are saved on a per-user basis. See “Saving collections” for more information.
- **Delete** This button is used to delete one or more systems from the *database*. See “Deleting systems from the HP SIM database” for more information.



NOTE: If a virtual machine host is deleted, it can still be accessed through the Virtual Machine Management Pack console, and the operations that can be performed on a virtual machine host are not affected by the deletion of the HP Systems Insight Manager (HP SIM) system. The Virtual Machine Management Pack console continues to show the HP SIM status.

NOTE: If you select a collection by selecting **Select "collection name" itself**, the **Delete** button is disabled. See “Deleting system or cluster collections” or “Deleting event collections” for more information.

- **Print** This button is used to create a printer-friendly version of the list in a new window. From the icon view page, select **File**→**Print** from the browser menu to print the report.

Related topics

- Navigating the system table view page
- Navigating the tree view page
- Navigating the picture view page

Navigating the picture view page

The picture view page, if available, appears when a container is selected from the **System Name** column on the system table view page. The container view page that is displayed depends on the type of container selected. For example, if a *rack* is selected, the rack view page appears. The following are the types of container collection views:

- Rack view page
- Enclosure view page

By default, racks are not created. However, you can select a discovered enclosure and create a rack. See “Creating and editing racks” for more information.

Rack view page

The picture view page for racks contains a diagram of the *discovered systems* in the rack if available. The rack name appears along with a picture view, table view, or icon view of the rack. While signed-in to HP Systems Insight Manager (HP SIM), placing your cursor over a server shown in this view displays information about that particular server, including server blade name, slot number, and the rack in which the server is located. You can also click a server name to display information about the server. The **System Page** appears.

Enclosure view page

The picture view page for enclosures contains a diagram of the *discovered systems* in the enclosure if available. The enclosure name appears along with a picture view, table view, or icon view of the enclosure. While signed-in to HP SIM, placing your cursor over a server shown in this view displays information about

that particular server, including server blade name, slot number, and the enclosure in which the server is located. You can also click a server name to display information about the server. The **System Page** appears.

The following systems are displayed in the picture view for racks and enclosures:

- Servers or desktops
- Interconnect switch
- Power supply enclosure

Interconnect bays that have no server, desktop, or interconnect switch identified are displayed in the picture view for enclosures.

View as

You can change the way the picture view page appears. Click the down arrow on the **View as** dropdown list, and then select **table**, **icon**, or **picture view**. However, the picture view is only available if you have already drilled down to a rack or enclosure by clicking the rack or enclosure name on the system table view page, and *then* switching back to a table or icon view. Drilling down to a rack or enclosure restricts the systems to only those that pertain to the rack or enclosure. You can then switch between the other view types.



NOTE: The **HP BladeSystem** collection does not provide a picture view option.

Quick Launch

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Related topics

- [System table view page](#)
- [Navigating the system table view page](#)
- [About racks and enclosures](#)

Creating and editing racks

Creating a rack

When HP Systems Insight Manager (HP SIM) discovers systems, it only displays enclosures. From the picture view of the enclosure, you can add it to a rack. The racks that you created in the previous release are all available in the **All Racks** collection. You can add the enclosure to these previously created racks or you can create new racks and add enclosures to it. After you create these racks, they are listed in the **All Racks** collection. The **All p-class Racks** and **All e-Class Racks** collections are no longer available.

To create a rack:

You can create a rack only from the picture view of an enclosure. You can add the enclosure to an existing rack, or you can create a rack and add the enclosure to it.

1. To access the picture view, navigate to **All e-Class Enclosures**, **All c-Class Enclosures** or **All p-Class Enclosures** in the **System and Event Collections** panel.
2. Click an enclosure. The enclosure picture view appears.

Note: In an enclosure under the **Identification** section, if the Rack name displays **Not Available** then the enclosure is not included in any rack.

3. To add the enclosure to a new rack, click **Add Enclosure to a rack**. The **Add to rack** dropdown list appears.

Note: This option is only available if an enclosure is not associated with a rack.

- Select **Add to new rack** from the **Add to Rack** dropdown list and click **Go**. The **Edit Rack** page appears. When a new rack is created from an enclosure view, the enclosure is automatically added to the **Selected enclosures** section.

Note: The **Add to Rack** dropdown list also lists the racks that were previously created. To add an enclosure to an existing rack, select the rack name and click **Go**.

*Required field **

User defined rack name *: 42 U

Data Centre ID: Data Centre Location:

Row Number: Position in Row:

Available enclosures

Filter by

- Encl_09USE644285C (c-class)
- Encl_09USE6442859 (c-class)
- C7000_Enclaaa (c-class) in **cauvery**
- BLEnclosureG2-3 (p-class) in **cauvery**
- Encl_07EA0RMJS144 (p-class) in **cauvery**
- Encl_03EA0WJTK544 (p-class) in **cauvery**
- Enclosure** (p-class) in **cauvery**
- Encl_05TSLPR25062 (p-class)

Selected Enclosures

- To create a rack, you must add the following details:
 - Rack Name.** Enter a name for the new rack and select the rack type from the dropdown list. This is a required field.
 - Rack Height.** Enter the height of the new rack.
 - Data Centre ID.** Select the height of the rack from the dropdown list.
 - Data Centre Location** Enter the data centre location.
 - Row Number.** Enter the row number where the enclosure is located.
 - Position in Row.** Enter the position in the row where the enclosure is located.

Note: If you are adding an enclosure to an existing rack, these details are automatically populated.

- From the **Available Enclosures** dropdown list, select the filter by which you want to view the list of enclosures. You can select **All Enclosures** or **Class**. You can filter the collection by entering a class. For example, if you enter *p-Class*, then all *p-Class* enclosures are available to be added to the rack.
- Select one or more of the relevant enclosures and click the >> symbol to add them to the rack. You can click << to remove enclosures from the rack. You can also drag and drop the enclosure in the desired position within the rack.

Note: indicates enclosures which are daisy chained.

- Click **Save**. The enclosure is added to the rack and the picture of the new rack with the added enclosure appears. If an enclosure has already been added to another rack, a message appears indicating the

enclosure is already assigned to another rack. You can confirm your intention to remove the enclosure from the existing rack and it is added to the new rack. You can click **Cancel** to discard the rack and close the window.

Editing a rack


From the picture view of a rack, you can edit the rack to add or remove enclosures.

To edit a rack:

1. To access the picture view, navigate to **All Racks** and select the rack to be edited and click **Edit Rack**. The **Rack View** page appears.

Note: The rack can be edited and deleted only from the picture view.

2. To edit a rack, you can change any of the following details:
 - **Rack Name.** Enter a name for the new rack and select the rack type from the dropdown list.
 - **Rack Height.** Enter the height of the rack.
 - **Data Centre ID.** Enter the data centre ID.
 - **Data Centre Location** Enter the data centre location.
 - **Row Number.** Enter the row number where the enclosure is located.
 - **Position in Row.** Enter the position in the row where the enclosure is located.
3. From the **Available Enclosures** dropdown list, select the filter by which you want to view the list of enclosures. You can select **All Enclosures** or **Class**.
4. Select one or more of the relevant enclosures and click the >> symbol to add them to the rack. You can click << to remove enclosures from the rack.

Note:  indicates enclosures which are daisy chained.

5. Click **Save**. The enclosure is added to the rack and the picture of the new rack with the added enclosure appears. If an enclosure has already been added to another rack, a message appears indicating the enclosure is already assigned to another rack. You can confirm your intention to remove the enclosure from the existing rack and it is added to the new rack.

Related procedures

- Saving collections
- Deleting systems from the HP SIM database
- Customizing the system table view page

Related topics

- System table view page
- Navigating the system table view page

About management processors

HP Systems Insight Manager (HP SIM) uses HTTP and *SNMP* to identify management processors. Previous versions of HP SIM used only *SNMP identification* to identify management processors and obtain their status. Now, HTTP identification is performed first, followed by *SNMP identification*. If a new management processor is installed in the server, the Web Agents must be reinstalled on the server, or the management processor might not be correctly identified. If both the server and the management processor have been *discovered* and identified, an association is made. The association between the management processor and other systems is displayed in the **System Name** column on the system table view page by showing one of the following:

- "*management processor*" in server "*system*"
- "*management processor*" to "*complex*"
- "*management processor*" to server "*nPar*"

SNMP Status Polling obtains the status for the host server. HP SIM can distinguish between the following management processor products:

- Remote Insight Board PCI
- Remote Insight Board EISA
- Remote Insight Lights-Out Edition (RILOE)

The system table view page provides the following information about management processors:

- The server entry displays a **Status** icon in the **MP** column. The tool tip for the icon displays the status of the management processor. Clicking this icon launches the **Remote Insight Home** page.
- The management processor entry displays the name of the server with which the management processor is associated by showing "*management processor*" in server "*system*."
- For all remote management processor entries, the **System Type** field shows **management processor**, and the **Product Name** field shows **Remote Insight Management**.

The system table view page contains an **MP** column, which displays the status of the management processor. There are seven different status levels (Critical, Major, Minor, Normal, Warning, Disabled, and Unknown). These status-level icons are the same status-level icons used for software status. See "[Software status types](#)" for more information about each status type.

The management processor status icons launch the **Remote Insight Home** page and display in a separate browser window. On this page, you can find the following information:

- Current User
- Server Name
- Server Power Status
- Remote Insight IP Address
- Remote Insight Name
- Latest Integrated Management Log Entry
- Latest Remote Insight Event Log Entry
- Remote Insight Mouse Cable

Clicking the management processor in the **System Name** column launches the **System Page** for that management processor. See "[System tab](#)" for more information.

For a server with a Remote Insight board, the **System Page** includes the **Management Processor Information** box.

Related topics

- [System table view page](#)
- [Navigating the system table view page](#)
- [Navigating the picture view page](#)
- [System Page](#)
- [System types](#)

About racks and enclosures

HP Systems Insight Manager (HP SIM) *discovers* and *identifies server blade racks and enclosures*.

There are two specific *search criteria* for racks and enclosures:

- Rack
- Enclosure

Running searches using these criteria returns a list of *systems* contained in the selected racks or enclosures. Any other criteria, except for the two listed previously, returns the racks and enclosures themselves, not the systems in those racks and enclosures. For instance, a **system name** search for the rack **Franklin 1** would return the system **Franklin 1**, not any system *in* **Franklin 1**.

Two default collections are related to racks and enclosures and are listed under the **System Type** collection:

- All Racks
- All Enclosures

On the system table view page, racks are displayed in the following formats:

- Encl1 in Rack1
- Rack1

The **Picture View** page can be displayed by clicking a rack hyperlink on the system table view page or from the **System and Event Collections** panel.

Clicking an enclosure name in the **System Name** column on the system table view page produces a list of all discovered systems in the selected enclosure. The status for both racks and enclosures is always Unknown.

The **Picture View** page contains a diagram of the discovered systems in the enclosure and, if available, in the rack. While signed-in to HP SIM, if you place your cursor over a server shown in the view, you receive information about that particular server, including server blade name, slot number, and the enclosure in which the server is located.

Related topics

- [System table view page](#)
- [Navigating the system table view page](#)
- [Navigating the picture view page](#)

Customizing the system table view page

The **Customize** link is located in the upper right corner of the system table view page. Click this link to configure what columns are displayed and in what order. When you modify the columns to display on the system table view page and select **Apply to all system table views**, these columns become the default set of columns displayed for any system collection selected if the collection does not already have customized columns defined. See “Customizing the system table view page” for more information.

To customize the system table view page:

1. On the system table view page, click **Customize**. The **Customize Table Appearance** page appears.
2. Select the columns you want displayed in the **Available Columns** box, and then click **>>** to add the columns to the **Displayed Columns** box.
3. To remove one or more columns from the display, select the columns in the **Displayed Columns** box, and then click **<<** to move them to the **Available Columns** box.
4. To rearrange how the columns are displayed, select a column in the **Displayed Columns** box, and then click **^** or **v**.
5. To sort collection results by a particular column, select a column from the **Sort by** dropdown list.
6. Select **Ascending** or **Descending**.
7. To apply the customization to all system collections, select **Apply to all system collections**.
8. To save selections and return to the system table view page, click **OK**, or to cancel all changes and return to the system table view page, click **Cancel**.

Related procedures

- [Saving collections](#)
- [Deleting systems from the HP SIM database](#)
- [Printing a system collection view](#)

Related topics

- [System table view page](#)
- [Navigating the system table view page](#)

Deleting systems from the HP SIM database



NOTE: Deleting multiple systems from the database at one time can cause performance delays.

NOTE: The Central Management Server (CMS) cannot be deleted.

NOTE: Clusters that contain cluster members cannot be deleted. To delete a cluster with its cluster members, you must first go to the system table view page by selecting the **All Systems** collection in the **System and Event Collections** panel. Then, select the cluster along with all of its members, and then click **Delete**.



IMPORTANT: If you do not add the IP addresses of the systems to the discovery exclusion list, the systems are rediscovered and added again to the database.

1. On the system table view page, select one or more systems to delete from the HP SIM database by selecting them in the results display.
 2. Click **Delete**. A dialog box appears, stating, *Are you sure you want to delete these systems?*
 3. To delete the systems, click **OK**, or to return to the system table view page without deleting the events, click **Cancel**.
-



NOTE: Containers (for example, racks) must be empty before they can be deleted. Selecting a rack and all its contained systems work without error.

NOTE: Some systems that host management proxies (such as the WMI Mapper Proxy or an *SMI-S provider*) cannot be removed until all dependant systems are also removed.

Related procedures

- Saving collections
- Printing a system collection view
- Customizing the system table view page

Related topics

- System table view page
- Navigating the system table view page

Printing a system collection view

1. On the system table view page, click **Print**. A print window appears
2. When the report is displayed, select **File**→**Print** from the browser menu.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Related procedures









- Saving collections
- Deleting systems from the HP SIM database
- Customizing the system table view page

Related topics

- [System table view page](#)
- [Navigating the system table view page](#)

System status types

The following table describes the HP Systems Insight Manager (HP SIM), *system health status* types:

Status icon	Status type	Description
	Critical	HP SIM can no longer communicate with the system. The system was previously <i>discovered</i> but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems.
	Major	A major problem exists with this system that should be addressed immediately. For systems running HP Insight Management Agent, a component has failed. The system might no longer be properly functioning and data loss can occur. In Insight Manager (WIN32), this status was identified as <i>Failed</i> .
	Minor	A minor problem exists with this system. For systems running Insight Management Agent, a component has failed, but the system is still functioning. In Insight Manager (WIN32), this status was identified as <i>Degraded</i> .
	Warning	The system has a potential problem or is in a state that might become a problem.
	Normal	The system is operating normally. The system is accessible.
	Disabled	The system is suspended, which enables a system to be excluded from status polling, identification, data collection, and automatic event handling. On the Automatic Discovery page, if you select the Automatically discover a server blade when its iLO is identified option, new servers discovered through Integrated Lights Out (iLO) (for example, no operating system or IP address known) are shown as disabled until the system is discovered with an IP address or operating system.
	Unknown	HP SIM cannot obtain management information about the system using <i>SNMP</i> or <i>DMI</i> . Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting, or it might be an IP address that is no longer associated with a system.
	Informational	The system might be in a transitional state or a nonerror state.
	No Status	The system has not been polled by one or more of the polling tasks since the system was discovered.



NOTE: HP Insight Management Agent for Servers for Windows continues to use the terms Normal, Degraded, Failed, and Inaccessible. Minor and Major status are only associated with systems running these agents.


Related topic

▲ [System table view page](#)

WBEM operational status types

HP Systems Insight Manager (HP SIM) reports WBEM operational status for storage and server elements, such as storage switch ports and filled memory slots. The following statuses are available:

Status icon	Status type	Description
	Non-recoverable error, lost communication	<p>HP SIM can no longer communicate with the element.</p> <ul style="list-style-type: none"> Nonrecoverable indicates that the element has failed, and recovery is not possible. Lost communication indicates that the element was previously discovered but is currently unreachable.
	Predictive Failure, Error, Aborted, Supporting Entity in Error	<p>A major problem exists with this system and should be addressed immediately.</p> <ul style="list-style-type: none"> Predictive Failure indicates that the element is functioning nominally, but a failure is likely to occur in the near future. Error indicates that the element is in an error state. Aborted indicates that the element's functionality has stopped abruptly. The element's configuration might need to be updated. Supporting Entity in Error indicates that the element might be functioning normally, but an element that it depends upon is in an error state.
	Degraded, Stressed	<p>A minor problem exists with this element.</p> <ul style="list-style-type: none"> ▲ Degraded indicates that the element is not operating at optimal performance or might be reporting recoverable errors. ▲ Stressed indicates that the element is functioning but needs attention.
	OK	The element is operating normally.
	In service, Stopped	<p>The element is suspended.</p> <ul style="list-style-type: none"> In Service indicates that the element is being configured. Stopped indicates that element is stopped.
	Unknown, No contact	<p>No management information about the element could be obtained.</p> <ul style="list-style-type: none"> Unknown indicates that the element status is not available. No Contact indicates that the element exists, but HP SIM has never been able to communicate with it.







Status icon	Status type	Description
	Starting, Stopping, Dormant, Power Mode, Other	This status provides useful information about the port. No attention is required. <ul style="list-style-type: none"> Starting indicates that the element is starting. Stopping indicates that element is stopping. Dormant indicates that the element is inactive. Other indicates that additional information is available, but it does not fit into the previously listed categories.

Related topics

- System tab for a tape library
- System tab for a storage switch

Software status types

The following table describes HP Systems Insight Manager (HP SIM) system software status types:

Status icon	Status type	Description
	Major	An update that contains a critical bug fix is available for this system.
	Minor	An update that contains new hardware support or bug fixes is available for this system.
	Normal	All components on the system match the repository.
	Disabled	The system is suspended. No software status is available.
	Informational	The Central Management Server (CMS) could not reach the <i>HP Version Control Agent</i> on the system, so the status of the system is unknown.
	Unknown	The VCA cannot communicate with HP Version Control Repository Manager (VCRM).



NOTE: The Unknown status appears for server systems only under the following circumstances:

- The VCA is not installed on the managed server.
- The VCA is installed on a server, but that server does not have a trust relationship established with HP SIM.
- The operating system on the target server is not supported. Windows and Linux operating systems are supported.
- The correct version of the agent is not on the target system.
- The target server type brand is not supported (only HP or Compaq brand servers are supported).
- The target system is not licensed for monitoring by the HP Performance Management Pack (PMP). The target system must have the HP Insight Management Agent 6.20 or later installed.
- PMP reports an indeterminate status for the system.

Related topic

- ▲ [System table view page](#)

Cluster table view page

To access *Cluster* collections in the **System and Event Collections** panel, click **Systems** and then select one of the available cluster collections. *Users* with *administrative rights* can manage all shared cluster collections from the cluster collection view. Users can manage their own private collections from this page, as well as:

- **Save collections** Click **Save As Collection** from the cluster table view page.
- **Delete clusters** Click **Delete** from the cluster table view page. A confirmation box appears. To delete the cluster, click **OK**, or to cancel the deletion, click **Cancel**.



NOTE: Clusters that contain cluster members cannot be deleted. To delete a cluster with its cluster members, select the **All Systems** collection in the **System and Event Collections** panel. Then, select the cluster and all of its members, and then click **Delete**.

- **Print cluster collection view** Click **Print** to print the collection results.
- **Customize the view** Click **Customize** to customize which columns display and in what order. See “Customizing the cluster table view page” for more information.

Tabs

The cluster table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab “remembers” the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

Related procedures

- [Customizing the cluster table view page](#)
- [Deleting clusters from the database](#)
- [Printing a cluster collection view](#)
- [Saving collections](#)

Related topic

- ▲ [Cluster Monitor](#)

Navigating the Cluster Table View Page

A *cluster* collection logically groups clusters into a collection based on information in the HP Systems Insight Manager (HP SIM) *database*. For all other clusters, excluding HP Serviceguard clusters, clicking the name of the cluster in the **Cluster Name** column or cluster status icon in the **CS** column displays the **System Page** for that cluster. See “Cluster Name” and “CS” for more information. *Cluster Monitor* can be launched from the cluster table view page in the following ways:

- Click the name of a Microsoft Cluster Server (MSCS) cluster in the **Cluster Name** column
- Click the cluster status icon for a MSCS cluster in the **CS** column

From this page, you can save a subset of the collection with a new name, delete one or more clusters from the collection, customize the view, and print the cluster collection view. In a multiuser environment, only one

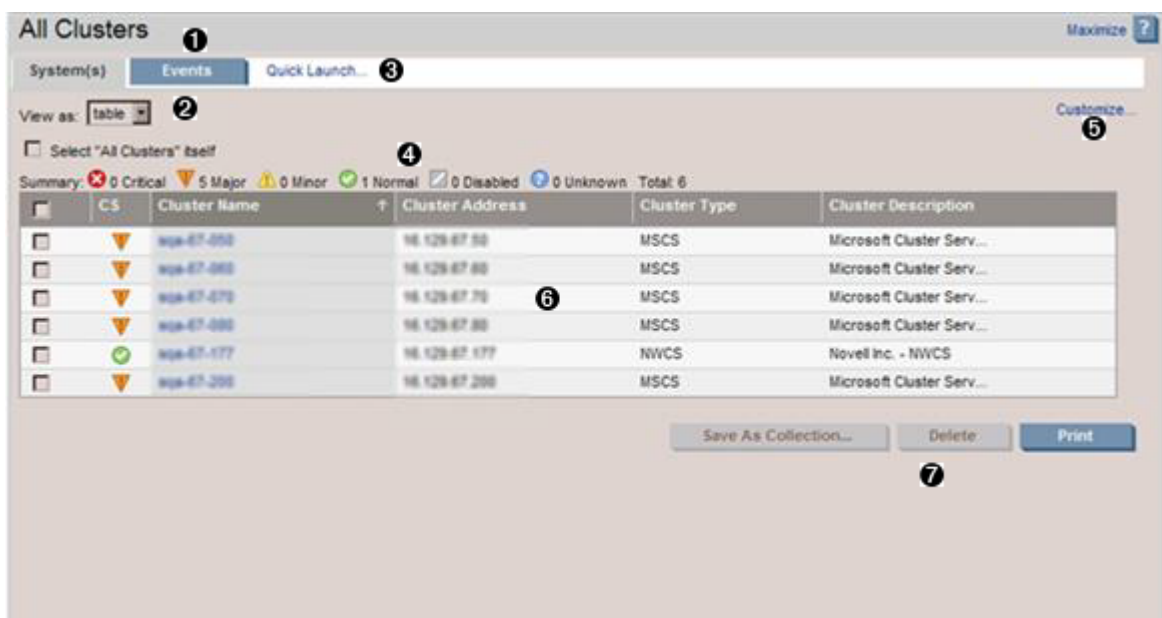
user at a time can edit a collection. If another user wants to edit the same collection, a **List Edit Warning** box appears. The user can cancel the editing request or edit the collection and save it as a new collection.



NOTE: Not all users can view all clusters. The results of the collection depend on the clusters that were assigned to the user who created the collection. Each *user* can only view the clusters that are assigned to him or her by a user with *administrative rights*. A user with administrative rights assigns managed clusters using user authorizations. See “Creating new authorizations” for more information.

The cluster table view page is divided into the following sections:

1. Tabs
2. View as
3. Quick Launch
4. Cluster status summary
5. Customizing the view
6. Cluster collection columns
7. Buttons



Tabs

The cluster table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab “remembers” the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

View as

The **View as** dropdown list is used to select either **table**, which displays all of the clusters in the collection in a tree form. See “Navigating the tree view page” for more information about navigating the tree view.

Quick Launch

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard

settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Cluster status summary

The status summary shows how many clusters in the view have a status of: Critical, Major, Minor, Normal, Disabled, and Unknown, with a total showing how many clusters are in the view.

Cluster collection columns

Sort columns by clicking the column header for ascending or descending order. Place your cursor over a column name for a brief description of the column. See “Customizing the cluster table view page” for more information about customizing columns. The following columns are displayed on the cluster view page:

- Selection
- CS
- Cluster Name
- Cluster Address
- Cluster Type
- Cluster Description

Selection

Select the checkbox in this column to select a cluster. You can select more than one cluster. This option is available in both the table view and the tree view. Select the checkbox in the column heading or select **Select "collection name" itself** to select all displayed clusters.

CS

The **CS** column (indicating cluster status) contains the cluster status icon for each cluster, a status that reflects the most severe status of all the cluster members and *Cluster Monitor Resources* (for MSCS, OpenVMS, TruClusters, and Novell Netware clusters), such as disk or CPU. This status is independent of the hardware and software status shown on the system table view page. For an HP Serviceguard cluster, cluster status is set to Unknown. To view the accurate state of a Serviceguard cluster, HP Serviceguard Manager should be used. For MSCS clusters, the status is the most critical cluster status displayed in Cluster Monitor. This status is determined by the threshold status (CPU, Disk) and the status of the cluster nodes that are retrieved by the HP Insight Management Agent (if available). For all other types of clusters, the status is determined by the most critical threshold status (CPU, Disk) and the node status of the cluster nodes retrieved by the Insight Management Agent (if available). See “System status types” for more information about the different system status types.



NOTE: To display a cluster status that includes only MSCS clusters, and show the true health of the cluster, you can edit the `globalsettings.props` file and change the `ClusterStatusWithThresholds` property to **false**. For non-MSCS clusters (OpenVMS, TruClusters, and Novell NetWare), excluding HP Serviceguard clusters, the cluster status is displayed as Unknown.

To edit the `globalsettings.props` file:

1. Open the `globalsettings.props` file located at:
 - **Windows** Typically located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`
 - **HP-UX and Linux** Located at `/etc/opt/mx/config/globalsettings.props`
2. Set the `ClusterStatusWithThresholds` property to **false**.
3. Save the file.

Cluster Name

The **Cluster Name** column contains the cluster name. When you place the cursor over the cluster name, the full system *Domain Name Service* (DNS) name is shown. If you click an MSCS cluster name, the Cluster Monitor page is displayed. See “Cluster Monitor” for more information. If the cluster selected is an HP

Serviceguard cluster, a new cluster table view page appears, showing the servers in the cluster. From this list, click a server name to access the **System Page** for that server. If the cluster is of any other type, the **System Page** for that cluster appears. See “System tab for clusters” for more information.

Cluster Address

The **Cluster Address** column contains the IP address for the cluster.



NOTE: HP Serviceguard clusters do not have an IP address. Therefore, this column is blank for this type of cluster.

Cluster Type

The **Cluster Type** column shows the cluster type. Some of the cluster types supported include:

- HP Serviceguard
- MSCS
- OpenVMS
- SCO UnixWare7 NonStop Clusters
- TruCluster Production server
- TruCluster Server

Cluster Description

The **Cluster Description** column contains a description of the cluster type. HP Serviceguard clusters have a description of **HP Serviceguard cluster**.

Buttons

The following buttons at the bottom of the page are available to users with administrative rights:

- **Save As Collection.** When clusters are selected, you can save the selection with a new name. Changes are saved on a per-user. See “Saving collections” for more information.
- **Delete.** This button is used to delete clusters from the database. Select clusters to delete from the database, and then click **Delete**. A confirmation box appears. To delete the clusters, click **OK**, or to cancel the deletion, click **Cancel**. See “Deleting clusters from the database” for more information.
- **Print.** This button is used to create a printer-friendly version of the list in a new window. From the cluster view page, select **File**→**Print** from the browser menu to print the report.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

Customizing the view

The **Customize** link is located in the upper right corner of the cluster table view page. Click this button to configure what columns are displayed and in what order. When you modify the columns to display on the cluster table view page and select **Apply to all cluster table views**, these columns become the default columns displayed for any cluster collection selected if that collection does not already have customized columns defined. See “Customizing the cluster table view page” for more information.

Related procedures

- Customizing the cluster table view page
- Deleting clusters from the database
- Saving collections
- Printing a cluster collection view

Related topics

- Cluster table view page
- Cluster Monitor
- HP Serviceguard Manager overview

Customizing the cluster table view page

When you modify the columns to display on the cluster table view page and select **Apply to all cluster table views**, these columns become the default columns displayed for any cluster collection selected if that collection does not already have customized columns defined.

1. On the cluster table view page, click **Customize**. The **Customize Table Appearance** page appears.
2. Select the columns you want displayed in the **Available Columns** box, and then click **>>** to add the columns to the **Displayed Columns** box.
3. To remove one or more columns from the display, select the columns in the **Displayed Columns** box, and then click **<<** to move them to the **Available Columns** box.
4. To rearrange how the columns are displayed, select a column in the **Displayed Columns** box, and then click **^** or **v**.
5. To sort the list by a particular column, select a column from the **Sort by** dropdown list.
6. Select **Ascending** or **Descending**.
7. If you want the customization to apply to all cluster collections, select **Apply to all cluster collections**.
8. To save selections and return to the cluster table view page, click **OK**, or to cancel all changes and return to the cluster table view page, click **Cancel**.

Related procedures

- Saving collections
- Deleting clusters from the database
- Printing a cluster collection view

Related topics

- Cluster table view page
- Navigating the Cluster Table View Page

Deleting clusters from the database

Clusters that contain cluster members defined in HP Systems Insight Manager (HP SIM) cannot be deleted. To delete a cluster with its cluster members, select the **All Systems** collection in the **System and Event Collections** panel. Then, select the cluster and all of its members, and then click **Delete**.



IMPORTANT: If you do not add the IP addresses of the deleted clusters to the discovery exclusion list, the systems will be rediscovered and added again to the database.

To delete a cluster from the database:

1. On the cluster table view page, select one or more clusters to delete from the database by highlighting them in the display.
2. Click **Delete**. A dialog box appears, stating, Are you sure you want to delete these systems?
3. To delete the clusters, click **OK**, or to return to the cluster table view page without deleting the clusters, click **Cancel**.

Related procedures

- Saving collections
- Printing a cluster collection view
- Customizing the cluster table view page

Related topics

- Cluster table view page
- Navigating the Cluster Table View Page

Printing a cluster collection view

1. From the cluster table view page, click **Print**.
2. When the report appears, select **File**→**Print** in the browser menu.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Related procedures

- Customizing the cluster table view page
- Deleting clusters from the database
- Saving collections
- Printing a cluster collection view

Related topics


- Cluster table view page
- Navigating the Cluster Table View Page

Event table view page

To access event collections, click **Events** in the **System and Event Collections** panel. *Users* with *administrative rights* can manage all shared *event* collections from the event table view page. All users can manage their own private event collections from this page, and perform the following tasks:

- **Clear events** Select one or more events to clear, and then click **Clear**.
- **Delete events** Select one or more events to delete, and then click **Delete**.
- **Assign events** Select one or more events to assign to specific users, and then click **Assign to**.
- **Add comments to events** Select one or more events to add comments to, and then click **Enter Comment**.

- **Print event collection results** Click **Print** to print the collection results.
- **Customize the view** Click **Customize** to customize which columns are displayed and in what order. See “Customizing the event table view page” for more information.

For users with *operator rights* and user rights to clear, delete, assign events, and add comments to events, you must select **Configuration Tool** from the **Show tools in category** dropdown list. Then, select **Clear Events**, **Delete Events**, **Assign Events**, and **Comment Events** as necessary, and then click  to add them to the **Toolbox contents**.

The event table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab “remembers” the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

Related procedures

- Clearing events from the collection
- Deleting events from the database
- Assigning events to users
- Entering comments on events
- Printing an event collection view

Related topics

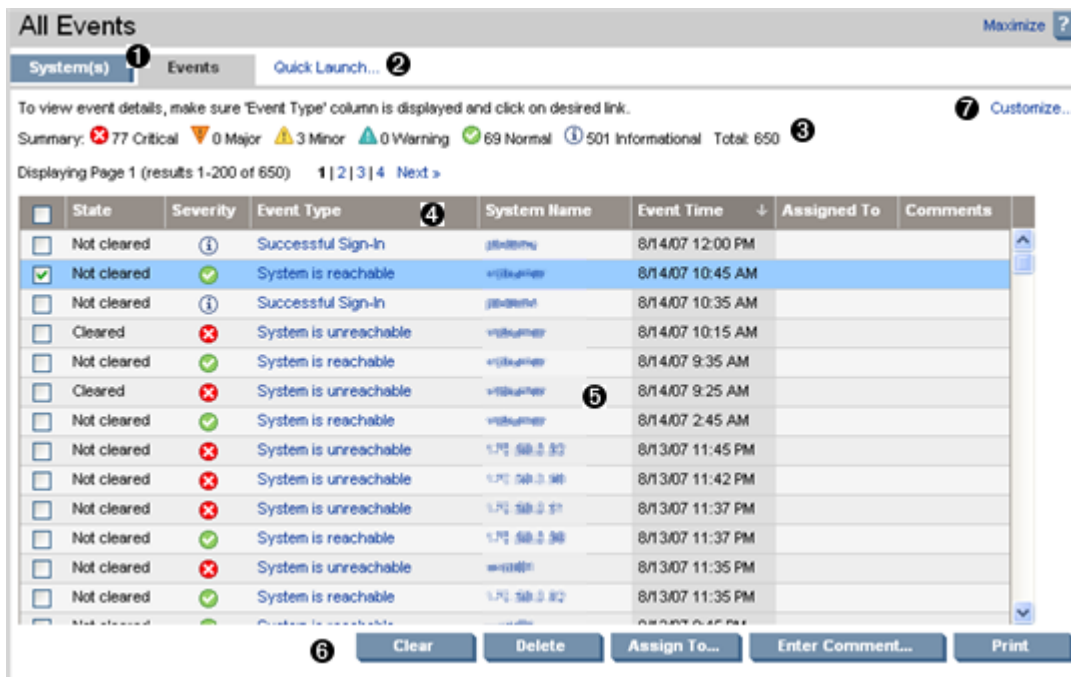
- Navigating the event table view page
- Monitoring systems, clusters, and events
- Event severity types
- Event details section

Navigating the event table view page

The event table view page is the view for an event collection and lists of *events* that meet common *criteria*.

The event table view page is divided into the following sections:

1. Tabs
2. Quick Launch
3. Event status summary
4. Event collection columns
5. Table information
6. Event management buttons
7. Customizing the view



From this page, you can clear, delete, and assign events, enter comments on the event, and view printable reports.

Tabs

The event table view page contains the following tabs:

- **System(s)** This tab lists all of the systems in the collection.
- **Events** This tab displays the events for all systems included under the **System(s)** tab. From this tab, additional filters can be applied to modify the event table display.

When switching between the **System(s)** tab and the **Events** tab, the **Events** tab "remembers" the selected events and event filter (if viewing a system collection). The **System(s)** tab remembers the selected systems, view type (table, tree, or icon), and the selected system filter (if viewing an event collection). However, the selections on each page are independent of each other.

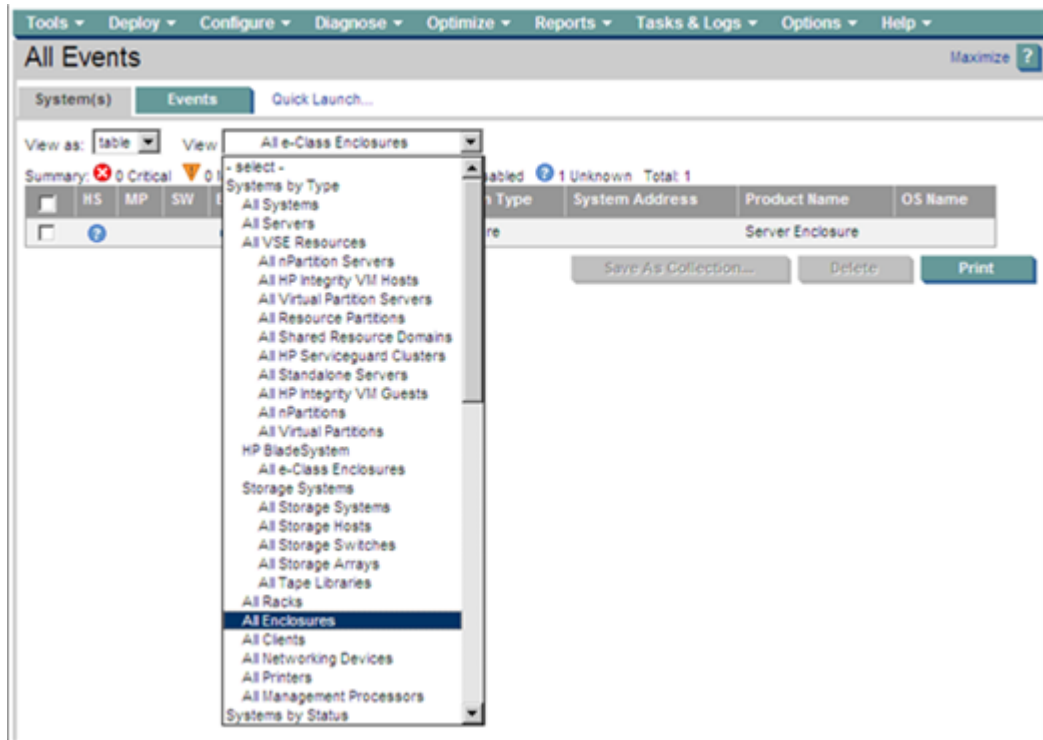
Quick Launch

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Filter criteria

Event filter criteria is available when viewing a system collection. To use an event filter:

1. From the **System and Event Collections** panel, select **All Events**. The **All Events** table view page appears.
2. Click the **System(s)** tab. The **System(s)** tab appears with a **View** dropdown list which shows the available filter criteria.
3. Click **View** to select a system collection.



Event status summary

This summary shows how many events in the view have a status of Critical, Major, Minor, Normal, and Informational. See “Event severity types” for more information about event status types.

Table information

The area includes information about the systems or events. An event collection can be displayed by clicking one of the following:

- An event collection from the **System and Event Collections** panel
- An event status icon in the **System Status** panel
- The **All Events Associated with this System** link from the **System Page**
- A private event collection
- A hyperlink in the **Uncleared Events** section on the **System Overview** page

Event collections are filtered based on authorizations. Users can only view events on *systems* for which they have the appropriate authorization. See “Users and authorizations” for more information.

When HP Storage Essentials is installed, a link in this section enables you to view the corresponding event details in HP Storage Essentials.

Event collection columns

To sort collection results by a particular column, click the column header for ascending or descending order. Place your cursor over a column name for a brief description of the column. The following columns are displayed on the event table view page:

- Selection
- State
- Severity
- Event Type
- System Name
- Event Time
- Assign To

- Comments
- System Type
- Rack Name
- Enclosure Name
- Case Status
- Case ID

Selection

Select the checkbox in this column to select an event. You can select more than one event. Select the checkbox in the column heading or select **Select "collection name" itself** to select or clear all displayed events.

State

This column displays whether the event is in the Cleared or Not Cleared state. Events start in the Not Cleared state. A Cleared state means the user is no longer interested in this event. Event states also include In Progress, which indicates that not all the data for the event has been logged. In Progress events cannot be removed or cleared. Pending state events are changed to Not Cleared when the *Central Management Server* (CMS) is restarted.

Severity

This column displays the event status icon to indicate the severity of a problem represented by the event. See "Event severity types" for more information.

Event Type

This column displays the type of an event. Some examples of event types are: *SNMP traps*, login failures, or the replicate agent settings tool. Select an event type from the list to view the **Event Details** section. The information displayed varies depending on the event. If you cannot see the entire event type in the column, place your cursor over this field, and a window appears showing the entire event type. See "Event details section" for more information about event details.

System Name

This column displays the system name on which the event occurred. Clicking a link in this column displays the **System Page** for the selected system.

When an event occurs that affects an entire *rack* or *enclosure*, it is possible for several systems in that rack or enclosure to generate a trap for that event. These container traps are filtered such that only one event is logged per rack or enclosure trap. Also, even though the source of the trap is a *server blade* or management processor, HP Systems Insight Manager (HP SIM) sets the **Event Source** and **Associated System** for the logged event to the rack or enclosure, as appropriate. See "About racks and enclosures" for more information.

Event Time

This column displays the time stamp when the *CMS* received the event, which includes the date and time. If the client is in a different time zone than the event time (CMS time), the event time is converted to the client time zone.

Assign To

To assign responsibility for an event to a user, select the event, and then click **Assign to** at the bottom of the page. The **Assign to** section appears, which enables you to select a new assignee or use an existing assignee. If you select to use an existing assignee, you can only select one user name from the list. This name does not have to be a user with privileges on the system or a name that can be used to log in to the CMS. This field is free-form text. See "Assigning events to users" for more information about assigning an event to a user.

Comments

This column displays the comments for this event or is blank if no comments have been entered. Comments are truncated in the column. Click the event type to view the entire comment if needed, or place your cursor

over a comment field to display a window that shows the entire comment to appear. See “Entering comments on events” for more information.

System Type

This column displays system types such as enclosure or rack, if the system type filter was selected for the event list display.

Rack Name

This column displays the name of the rack.



NOTE: This column is displayed when the system is a rack or enclosure and the rack or enclosure system filter is selected.

Enclosure Name

This column is displayed the name of the enclosure.



NOTE: This column is displayed when the system is a rack or enclosure and the rack or enclosure system filter is selected.

Case Status

When the HP Service Essentials Remote Support Pack and HP SIM are installed together on a Windows CMS, support case status updates are provided by the Remote Support Pack. The **Case Status** column is available when you view the **All HP Service Events** collection or select the event search criteria for service case status.

Case ID

When the Remote Support Pack and HP SIM are installed together on a Windows CMS, the support case ID is provided by the Remote Support Pack. The **Case ID** column is available when you view the **All HP Service Events** collection or select the event search criteria for service case status. Click the link in the **Event Type** column to view additional details about an event.

Event management buttons

Five buttons at the bottom of the event table view page are available to users with *administrative rights* only. These buttons might not always appear, depending on how you access the page. For example, when creating a task and selecting targets, there are no buttons displayed, only the table or system names.



NOTE: If you are unable to clear, delete, assign, or add comments to an event, see your administrator to verify that you have the appropriate authorizations. See “Users and authorizations” for more information about users and authorizations.

- **Clear** Clears one or more events from the *database*. Select the events to clear, and then click **Clear**. See “Clearing events from the collection” for more information.
- **Delete** Deletes one or more events from the database. Select the events to be deleted, and then click **Delete**. A dialog box appears. To continue with the deletion, click **OK**, or to cancel the deletion, click **Cancel**. See “Deleting events from the database” for more information.
- **Assign to** Assigns responsibility for events to a particular user. See “Assigning events to users” for more information.
- **Enter Comments** Opens an edit box to enter comments for one or more events. See “Entering comments on events” for more information.
- **Print** This button is used to create a printer-friendly version of the list in a new window. Within the window, select **File**→**Print** from the browser menu to print the report.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Buttons are disabled if you do not have appropriate rights. However, the **Print** button appears for all users.

Customizing the view

The **Customize** link is located in the upper right corner of the event table view page. Click this link to configure what columns are displayed and in what order. When you modify the columns to display on the event table view page and select **Apply to all event table views**, these columns become the default set of columns displayed for any event collection selected if the collection does not already have customized columns defined.

See “Customizing the event table view page” for more information.

Related procedures

- Customizing the event table view page
- Clearing events from the collection
- Deleting events from the database
- Assigning events to users
- Entering comments on events
- Printing an event collection view

Related topics

- Monitoring systems, clusters, and events
- Event severity types

Customizing the event table view page

When you modify what columns display on the event table view page and select **Apply to all event table views**, these columns become the default set of columns that are displayed for any cluster collection selected if the collection does not already have customized columns defined.

1. On the event table view page, click **Customize**. The **Customize Table Appearance** page is displayed.
2. Select the columns you want displayed from the **Available Columns** box, and then click **>>** to add the columns to the **Displayed Columns** box.
3. To remove one or more columns from the display, select the columns in the **Displayed Columns** box, and then click **<<** to move them to the **Available Columns** box, so they are longer displayed.
4. To rearrange how the columns display, select a column in the **Displayed Columns** box, and then click **^** or **v**.
5. To sort the collection by column, select a column from the **Sort by** dropdown list.
6. Select **Ascending** or **Descending**.
7. To apply the customization to all event collections, select **Apply to all event collections**.
8. To save selections and return to the event table view page, click **OK**, to cancel all changes and return to the event table view page or click **Cancel**.

Related procedures

- Clearing events from the collection
- Deleting events from the database

- Assigning events to users
- Entering comments on events
- Printing an event collection view

Related topics

- Event table view page
- Navigating the event table view page

Clearing events from the collection

You must have *administrative rights* to clear events.



NOTE: For users with operator and user rights to clear events, they must have the **Clear Events** tool selected in their toolbox categories. See “Editing toolboxes” for more information.

To clear an event:

1. On the event table view page, select the event that you want to clear.
2. Click **Clear**. For the events selected, the state changes from Not Cleared to Cleared in the **State** column.

Related procedures

- Customizing the event table view page
- Deleting events from the database
- Assigning events to users
- Entering comments on events
- Printing an event collection view

Related topics

- Navigating the event table view page
- Event table view page
- Event details section

Deleting events from the database

You must have *administrative rights* to delete events. However, pending events and discovered system events cannot be deleted. For users with operator and user rights to delete events, they must have the **Delete Events** tool selected in their toolbox categories. See “Editing toolboxes” for more information.

To delete an event:

1. On the event table view page, select the event you want to delete.
2. Click **Delete**. A confirmation box appears.
3. To delete the event, click **OK**, or to return to the event table view page, click **Cancel**.

Related procedures

- Customizing the event table view page
- Clearing events from the collection
- Assigning events to users
- Entering comments on events
- Printing an event collection view

Related topics

- Navigating the event table view page
- Event table view page
- Event details section

Assigning events to users

You must have *administrative rights* to assign events from shared collections. For users with operator and user rights to assign events, they must have the **Assign Events** tool selected in their toolbox categories. See “Editing toolboxes” for more information.



IMPORTANT: Assigning events to certain users, does not facilitate any tracking at all and the user is not notified of the event.



CAUTION: If selected events have previously been assigned, selecting a new assignee and clicking **OK** overrides the previous assignment.



NOTE: A maximum of 50 characters can be entered in the assignee field.

To assign an event to a user:

1. On the event table view page, select the events you want to assign to a user.
2. Click **Assign To**. The **Assign to** section appears.
3. Select **New assignee** or **Choose existing assignee**. If you select **Choose existing assignee**, click the down arrow, and then select an assignee from the dropdown list.
4. To update the *database*, click **OK**, or click **Cancel**.

Related procedures

- Clearing events from the collection
- Deleting events from the database
- Entering comments on events
- Printing an event collection view
- Customizing the event table view page

Related topics

- Navigating the event table view page
- Event table view page

Entering comments on events

Use the following procedure to add comments to *events*. You must have *administrative rights* to add comments to events.



CAUTION: If you add comments to events that already have comments, the previous comments are replaced with the new comments in the *database*.



NOTE: For users with operator and user rights to add comments to an event, they must have the **Comment Events** tool selected in their toolbox categories. See “Editing toolboxes” for more information.

NOTE: The maximum number of characters allowed for comments is 1,000.

To add comments to an event:

1. On the event table view page, select the events for which you want to enter comments.
2. Click **Enter Comments**. The **Enter Comments** section is displayed.
3. Enter the comments.
4. To update the database, click **OK**, or to return to the event table view page, click **Cancel**.



NOTE: Comments that are added to events in HP Systems Insight Manager (HP SIM) are not transferred to HP Storage Essentials.

Related procedures

- Customizing the event table view page
- Clearing events from the collection
- Deleting events from the database
- Assigning events to users
- Printing an event collection view

Related topics

- Navigating the event table view page
- Event table view page
- Event details section

Printing an event collection view

1. On the event view page, click **Print**. A printable window appears.
2. When the report is displayed, select **File**→**Print** in the browser menu.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Related procedures



- Customizing the event table view page
- Clearing events from the collection
- Deleting events from the database
- Assigning events to users
- Entering comments on events






Related topics

- Navigating the event table view page
- Event table view page
- Event details section

Event severity types

The following table lists the HP Systems Insight Manager (HP SIM) severity levels for *events*.

Status icon	Security level	Description
	Critical	Events of this type indicate a failure and signal the need for immediate attention.
	Major	Events of this type indicate an impending failure.

Status icon	Security level	Description
	Minor	Events of this type indicate a warning condition that can escalate into a serious problem.
	Normal	Events of this type indicate that this event is not a problem.
	Unknown	Events of this type indicate that this event is of unknown severity or caused by an unknown problem.
	Warning	Currently in a state that might become a problem. Note: In HP SIM 5.0, only WBEM indications map to this level.
	Informational	Events of this type require no attention and are provided as useful information.

Related topics

- [Event table view page](#)
- [Navigating the event table view page](#)

Event details section

When you click a link in the **Event Type** column on the event table view page, the **Event Details** section is displayed, providing detailed information about a particular *event*. Events are generated by *SNMP* traps, *HTTP* events, or internally generated events.



NOTE: Events can be generated from *Web-Based Enterprise Management* (WBEM) if you have subscribed to WBEM events on the managed system. See “[Subscribing to WBEM indications](#)” for more information about subscribing to WBEM events.

NOTE: Events are tracked only on *systems* that have been discovered. See [Automatic Discovery](#), see the “[Configuring automatic discovery](#)” for more information about configuring and running Automatic Discovery.

Event identification and details

The following information is provided for each HP Systems Insight Manager (HP SIM) event:

- **Event Severity** Displays the severity of the event
- **Cleared Status** Shows if the event is Cleared, Not Cleared, or Unknown
- **Event Source** Displays the system from which the event originated
- **Associated System** Displays the system that generated the event
- **Associated System Status** Shows the current status of the system that generated the event, which changes as the status of the system changes
- **Event Time** Displays the time the event was received by the *Central Management Server* (CMS)
- **Description** Explains the source or type of event, which can be an SNMP trap, a *Desktop Management Interface* (DMI) indication, or an internally generated message, such as the *discovery* of a system
- **Assignee** Displays the user to which the event has been assigned
- **Comments** Displays comments entered by a user

Depending on the event type, the following information is displayed in the **Details** box:

- **Servers in Enclosure** For *enclosure* events, this section lists all of the servers in the affected enclosure
- **Enclosures in Rack** For *rack* events, this section lists all of the enclosures in the affected rack

- **Trap Details**
 - **Date and time the event occurred**
 - **Event Description**
 - **Trap Information**
- **Discovered System Details**
- **Discovered Date**
- **Event Details**
 - **User name**
 - Name of the remote system from which the user was browsing
 - IP address of the system from which the user was browsing



NOTE: System name and IP address are not provided for the Unauthorized User Account Modified Event. It is an event internally generated by the HP SIM server.

- **Change Details**
 - **Source of current status change**
 - **Previous severity**
- **Task Details**
 - Time the *task* ran
 - User that ran the task
 - Systems on which the task was run
- **Status Change Details**
 - **Subsystem Name.** For example, memory, processor, and storage
 - **Previous Subsystem status** The status of the subsystem before the event
 - **Overall Performance status** The combined status of all the subsystems (the most critical subsystem status)
 - **Explanation**

Click **View Printable Details** to view the details in printable format. Select **File**→**Print** to print the details.

Related topics

- [Navigating the event table view page](#)
- [Event table view page](#)

Searching for systems and events

Two types of searches can be performed in HP Systems Insight Manager (HP SIM). A basic search looks for a system name or keyword, while an advanced search uses additional criteria.

To perform a basic search:

1. In the **Search** panel, enter a system name or keyword. As you type, a dropdown list appears and lists systems with names that begin with the text entered. The list includes up to 12 systems and shows an

icon for the system *health status*. If more than 12 systems are found, an ellipsis appears at the bottom of the list. Continue typing to narrow the list further.

2. Perform one of the following:
 - a. Use the mouse or the up and down arrows on your keyboard to select a system. Press **Enter** to navigate to the **System Page** of the selected system.
or
 - b. Do not select a system. Press **Enter** or click **Search**. The **Search Results** page appears and lists all matching systems.



NOTE: Press **Esc** to hide the dropdown menu.

To perform an advanced search:

1. In the **Search** panel, click **Advanced Search**.
2. Select **systems**, **events**, or **clusters**, and then select any defining criteria.
3. Click **View**. The **Search Results** page appears.

To minimize the **Search** panel, click the minimize icon in the upper right corner of the panel. To maximize the **Search** panel, click the maximize icon in the upper right corner of the panel.

Tool search

The **Tool Search** link is also available in the **Search** panel. Click this link to search for available tools in HP SIM. The only tools displayed are the tools you are authorized to use. See “Tool search” for more information about running tool searches.

Related procedures

- Performing a basic search
- Saving collections
- Performing an advanced search for systems
- Performing an advanced search for clusters
- Performing an advanced search for events

Related topics

- Basic and advanced search
- Search criteria
- System status types

Basic and advanced search

Basic search

The Search feature enables you to quickly retrieve details about a *system* using its name or common system attributes. For example, you could search for a system name or an attribute such as server, HP-UX, or storage.

The search field only allows the following characters: letters, numbers, tilde (~), dash (-), period (.), underscore (_), apostrophe ('), and space.

As you type, a dropdown list appears and lists systems with names that begin with the text entered. The list includes up to 12 systems, and shows the icon for the system *health status*. If more than 12 systems are found, an ellipsis (...) appears at the bottom of the list. Continue typing to narrow the list further. You can use the mouse or arrow keys to select a system to view, or do not select a system and press **Enter** or click **Search** to search for the indicated criteria.

If you selected a system in the dropdown list, the **System Page** for that system appears.

If you did not select a system, and you pressed **Enter** or clicked **Search**, the **Search Results** page displays a list of systems that match your criteria. Clicking a name in the list displays the **System Page** for that system. If no system in the database resembles the target system, the **Search Results** page indicates that no entries meet the criteria, and gives you the option to search again or perform an advanced search.

Advanced search

To access the **Advanced Search** page, click the **Advanced Search** link in the **Search** panel.

You can create a system, *event*, or *cluster* search by selecting **systems**, **events**, or **clusters** in the **Search for** box at the top of the **Advanced Search** page. Then you can specify the criteria to be used in the search. The result of running a search is a collection. The *criteria* selected can also be saved as a collection definition, so that search can be run again at a later date. The saved collections are stored in the **System and Event Collections** panel as **Systems** or **Events**. These collections can be saved as private or shared.

Hierarchical displays

Some search criteria require hierarchical displays. Examples of hierarchical criteria are: Operating System, Event Type, and Software/Firmware.

In these cases, the comparison selection box is replaced by a selection box containing the appropriate syntax for that particular tree level. The most complex of these cases is the Software/Firmware criteria. When Software/Firmware is selected, a series of search criteria are added below in a tree format:

- component type is
- and operating system is
- and category type is
- and name is
- and version is

In this case, as selections are made in the higher-level selection boxes, the available selections in lower-level boxes are updated.

Save as

When you click **Save As Collection**, the **Save As Collection** section displays. Enter a name for the search in the **Name** field, and then select where to save it. See “Saving collections” for more information.

View

When you click **View**, the results of the search are displayed below the search frame. This functionality enables you to preview the results of the search before saving it, or to run a search without saving it.

Related procedures

- Performing a basic search
- Saving collections
- Performing an advanced search for systems
- Performing an advanced search for clusters
- Performing an advanced search for events

Related topic

- ▲ Searching for systems and events

Performing a basic search

Perform this procedure to complete a basic system search by searching for matches in system name and common system attributes.

To perform a basic search:

1. Enter a system name or keyword in the **Search** panel.

As you type, a dropdown list displays systems with names that begin with the text entered. The list includes up to 12 systems and shows the icon for the system *health status*. If more than 12 systems are found, an ellipsis (...) appears at the bottom of the list. Continue typing to narrow the list further.

Note: Press **Esc** to hide the dropdown list.

- To view the **System Page** for a single system, select it with the mouse or select it with the up and down arrows on your keyboard, and then press **Enter**.
 - If you want to search for multiple systems or a system attribute, do not select a system in the dropdown list. Press **Enter** or click **Search**. The **Search Results** page appears and lists all matching systems.
2. To do an additional search from the **Search Results** page, enter the system name or attribute in the **Search again** field, and then select **system name** or **common system attributes** in the dropdown menu. Click **View**. The new **Search Results** appear.

Note: Common system attributes include Full DNS name, Device hostname, Serial number, Operating System Type, Operating System Version, Operating System description, Operating System name, Product model, System type, and IP address.

Note: Searching using common system attributes can be time-consuming if there are a large number of systems because the search looks at several attributes in the database multiplied by the number of discovered systems.

3. (Optional) After the search results appear, you can do one of the following:
- Save the search results. Click **Save As Collection**, enter a name for the search, and then select where to save the collection. See “Saving collections” for more information. To save the search, click **OK**, or to return to the **Search Results** page, click **Cancel**.
 - Perform a more advanced search. Click **Advanced**. The **Advanced Search** page appears. See “Basic and advanced search” for more information about the Advanced Search option.

Related procedures

- Saving collections
- Performing an advanced search for systems
- Performing an advanced search for events
- Performing an advanced search for clusters

Related topics

- Searching for systems and events
- Basic and advanced search
- Search criteria

Performing an advanced search for systems

Use the following procedure to perform an advanced search for *systems*. The following image shows the **Advanced Search** page for systems.

The screenshot shows the 'Advanced Search' interface. At the top, it says 'Advanced Search' and 'Search for matches based on selected criteria'. There is a 'Maximize ?' button in the top right. Below this, there is a 'Search for' dropdown menu with 'systems' selected. The search criteria are defined as follows:

- where system name is (any)
- and system type is Application
- and operating system name is Microsoft Windows NT Workstation (Build 2600)
- and version is (any)

At the bottom right, there are two buttons: 'View' and 'Save As Collection...'.

To perform an advanced search for systems:

1. Click **Advanced Search** in the **Search** panel.
2. Select **systems** from the **Search for** dropdown list.
3. From the first selection box (*criteria* selection), click the down arrow, and then select the search criteria.
Note: Some search criteria show no values until systems with values for that criteria have been discovered. In this case, the criteria is not displayed until values are available.
4. From the second selection box (comparison selection), click the down arrow, and then select the comparison option.
Note: Different criteria support different comparisons. The comparison options change with the criteria selected. For example, if you select **operating system** as criteria, the following possible comparisons are available: is, is not, contains, starts with, and ends with. See "Search criteria" for more information.
5. In the third selection box (value selection), select one of the available values for specific criteria or comparison combination from the dropdown list, or enter the required information in the input box.
6. To add additional criteria, click **Add**. To conduct the system search immediately, click **View**. To delete search criteria, click **Delete**. To save the search as a collection, click **Save As**. See "Basic and advanced search" for more information about **Go** and **Save as**.
Note: Criteria are reordered after clicking **View** or **Save As**. If criteria types are the same, they are placed together with "OR", if they are different, they are placed together with "AND".
7. If you clicked **View**, search results are displayed. You can choose to delete or print the results. See "Deleting system search results from a search view" for more information about deleting selections. See "Printing system search results" for information about printing search results.

Related procedures

- [Deleting system search results from a search view](#)
- [Printing system search results](#)
- [Saving collections](#)
- [Performing an advanced search for events](#)
- [Performing an advanced search for clusters](#)
- [Performing a basic search](#)

Related topics

- [Searching for systems and events](#)
- [Basic and advanced search](#)
- [Search criteria](#)

Printing system search results

1. After the **Search Results** page is displayed, click **View**. The results are displayed.
2. Click **Print**.

The results are printed.

Note: The **Print** dialog box might be hidden. If so, go to the Windows Task Bar to display the box. Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box. (see "Printing" for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Cancel printing to a file
- Print selected systems; only the entire list of systems
- Print the system search results if you close the browser immediately after issuing a print request

Related procedures

- Saving collections
- Deleting system search results from a search view

Related topic

- ▲ Performing an advanced search for systems

Deleting system search results from a search view



NOTE: Deleting multiple systems from the list can cause performance delays.

1. After the search results appear, select systems to delete from the search, and then click **Delete**. A dialog box appears, stating, *Are you sure you want to delete these systems?*
2. To delete the systems, click **OK**, or to return to the **Search Results** page without deleting the systems click **Cancel**.

Related procedures

- Performing an advanced search for systems
- Printing system search results

Related topic

- ▲ Searching for systems and events

Performing an advanced search for events

Use the following procedure to perform an advanced search for *events*. The following image shows the **Advanced Search** page for events.

The screenshot shows the 'Advanced Search' window with the following configuration:

- Search for: **events**
- where: severity **is** Major
- and: event time **<** 8/31/07 10:28 AM PDT
- Buttons: Delete, << Add, View, Save As Collection...



NOTE: You can quickly display all service events of **Any** type by selecting **Systems**→**Events**→**Shared**→**Service Events**→**All HP Service Events** from the **System and Event Collections** panel.

To perform an advanced search for events:

1. Click **Advanced Search** in the **Search** panel.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (*criteria* selection), click the down arrow, and then select the search criteria.

Note: If you selected **event type**, see “Event type criteria” for more information.

Note: Some search criteria show no values until systems with values for that criteria have been discovered. In this case, the criteria is not displayed until values are available.

4. From the second selection box (comparison selection), click the down arrow, and then select the comparison option.

Note: Different criteria support different comparisons. The comparison options change with the criteria selected. For example, if you select **operating system** as criteria, the following comparisons are available: is, is not, contains, starts with, and ends with.

5. In the third selection box (value selection), select one of the values for a specific criteria or comparison combination from the dropdown list, or enter the required information in the input box.
6. To add additional criteria, click **Add**, or to conduct the event search immediately, click **View**. To delete search criteria, click **Delete**, or to save the search as a list, click **Save as**. See “Basic and advanced search” for more information about **Go** and **Save as**.
7. If you clicked **View**, search results are displayed. You can choose to delete or print the results. See “Deleting system search results from a search view” for more information about deleting selections. See “Printing system search results” for information about printing search results.

Note: To search for new event types generated by HTTP events, select events by Event Category Selection, and then select the event type from the **and type is** list.

Related procedures

- Saving collections
- Deleting event search results
- Printing event search results

Related topics

- Searching for systems and events
- Basic and advanced search
- Search criteria

Printing event search results

1. After the **Search Results** page appears, click **View**. The results are displayed.
2. Click **Print**.

The results are printed.

Note: The **Print** dialog box might be hidden. If so, go to the Windows Task Bar to display the box.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see “Printing” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Cancel printing to a file
- Print selected events; only the entire search results
- Print the event search results if you close the browser immediately after issuing a print request

Related procedures

- Saving collections
- Deleting event search results

Related topic

- ▲ Performing an advanced search for events

Deleting event search results



NOTE: Deleting multiple events from the list can cause performance delays.

1. After the search results appear, select events to delete from the search, and then click **Delete**. A dialog box appears, stating, *Are you sure you want to delete these systems?*
2. To delete the events, click **OK**, or to return to the **Search Results** page without deleting the events click **Cancel**.

Related procedures

- Performing an advanced search for events
- Printing event search results

Related topic

- ▲ Searching for systems and events

Performing an advanced search for clusters

Use the following procedure to perform an advanced search for *clusters*. The following image shows the **Advanced Search** page for clusters.



The screenshot shows the 'Advanced Search' interface. At the top, it says 'Search for matches based on selected criteria'. Below this, there is a 'Search for' dropdown menu set to 'clusters'. Underneath, there are two criteria defined: 'where cluster type is HP Serviceguard' and 'and cluster monitor resource (any)'. Each criterion has a 'Delete' button. There is also a '<< Add' button. At the bottom right, there are 'View' and 'Save As Collection...' buttons.

To perform an advanced search for clusters:

1. Click **Advanced Search** in the **Search** panel.
2. Select **clusters** from the **Search for** dropdown list.
3. From the first selection box (*criteria* selection), click the down arrow, and then select the search criteria.
Note: Some search criteria show no values until systems with values for that criteria have been discovered. In this case, the criteria is not displayed until values are available.
4. From the second selection box (comparison selection), click the down arrow, and then select the comparison option.
Note: Different criteria support different comparisons. The comparison options change with the criteria selected.
5. In the third selection box (value selection), select one of the available values for a specific criteria or comparison combination from the dropdown list, or enter the required information in the input box.
6. To add additional criteria, click **Add**. To conduct the cluster search immediately, click **View**. To delete search criteria, click **Delete**, or to save the search as a collection, click **Save As**. See "Basic and advanced search" for more information about **Go** and **Save as**.
7. If you clicked **View**, the search results are displayed. You can choose to delete or print the results. See "Deleting system search results from a search view" for more information about deleting selections. See "Printing system search results" for information about printing search results.

Related procedures

- Saving collections
- Deleting cluster search results
- Printing cluster search results

Related topics

- Searching for systems and events
- Basic and advanced search
- Search criteria

Printing cluster search results

1. After the **Search Results** is displayed, click **View**. The results are displayed.
2. Click **Print**.

The results are printed.

Note: The **Print** dialog box might be hidden. If so, go to the Windows Task Bar to display the box.

Because the following print options are not supported in HP Systems Insight Manager (HP SIM), you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see "Printing" for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Cancel printing to a file
- Print selected clusters; only the entire search results
- Print the cluster search results if you close the browser immediately after issuing a print request

Related procedures

- Saving collections
- Deleting cluster search results

Related topic

- ▲ Performing an advanced search for clusters

Deleting cluster search results

Perform the following procedure to delete one or more *clusters* from a cluster search before saving.



NOTE: Deleting multiple clusters from a collection can cause performance delays.

NOTE: Clusters that contain cluster members cannot be deleted. To delete a cluster and its cluster members, select the **All Systems** collection in the **System and Event Collections** panel. Then, select the cluster and all of its members, and then click **Delete**.

To delete clusters from a search view:

1. After the search results appear, select clusters to delete from the search, and then click **Delete**. A dialog box appears, stating, *Are you sure you want to delete these systems?*
2. To delete the systems, click **OK**, or to return to the **Search Results** page without deleting the clusters, click **Cancel**.

Related procedures

- Performing an advanced search for clusters
- Printing cluster search results

Related topic

- ▲ Searching for systems and events

Search criteria

You can select from many *criteria* when you create a collection. Although the *task* you run is associated with one collection, one collection can include numerous conditions.

You can also exclude criteria. For example, including all systems of the type server and excluding all *systems* of a certain processor type provides a more distinct subset of the servers on the network. This filtering is accomplished by selecting **is** or **is not** comparison selections.

The more commonly used criteria include *system type*, IP address, product name, and hardware status. Less frequently used criteria include event category selection (trap categories), processor, management protocol,

and memory range. Event collections include both system criteria and event criteria. However, event criteria do not apply to system collections.

When you select multiple criteria, the system must meet all criteria for the system to be included in the collection. For example, if you select systems within a specified IP range and with more than 32 MB of RAM, the collection does not return a system in the specified IP range if the system has less than 32 MB of RAM.

Complex collections with many individual system selections or with many different selection criteria take more system resources to execute. If a task is associated with a collection, keep the collection as simple as possible to minimize the performance impacts.

System collection criteria	Finds
asset number	User-defined field listing the asset number of the system.
cluster membership	Systems that belong to a certain <i>cluster</i> .
common attributes	Systems with common attributes, including: full <i>DNS</i> name, system host name, serial number, operating system type, operating system version, operating system description, operating system name, product model, system type, and IP address.
contact	User-defined field listing the contact for system status information.
contract and warranty expires	Systems with service contracts or warranties that expire within a specified number of days. This option is available if the HP Service Essentials Remote Support Pack is installed.
directory groups	The distinguished name of a system group. Can be used to create collections used for authorizations. As comparison criteria, this can be specified without knowing the full distinguished name. With support for Dynamic Authorizations, this enables group memberships in the directory, and changes to them to be reflected and dynamically updated in HP SIM authorizations.
enclosure	Systems in an <i>enclosure</i> by a given set of enclosure names (does not include the enclosure itself).
hardware status	Systems of specified hardware status type (Critical, Disabled, Major, Minor, Normal, and Unknown).
IP address	Systems with an IP address that falls in the specified range.
location	User-defined field indicating the physical location of the system.
management protocol	Systems running one or more of the following protocols: <i>HTTP</i> , <i>WBEM</i> , <i>DMI</i> , or <i>SNMP</i>
memory range	Systems with memory in the specified range (see "Memory range criteria" for details).
network protocol	Systems running on <i>IP</i> .
organizational unit (OU)	The distinguished name of a system. Can be used to create collections used for authorizations. As comparison criteria, this can be specified without knowing the full distinguished name. With support for Dynamic Authorizations, this enables group memberships in the directory, and changes to them to be reflected and dynamically updated in HP SIM authorizations.
operating system	Systems with specific operating system, version number, or both.
processor	Systems with the specified processor type, speed, or both.
product name	Systems with the specified product names.
rack	Systems in a <i>rack</i> by a given set of rack names (does not include the rack itself).
serial number	User-defined field that displays the serial number of the system.
server role	Systems that have a certain server role set for them (see "Server role criteria" for more information).
service status	Systems that have a specified service status.
software/firmware	Systems with specific software or firmware version installed (see "Software and firmware criteria" for more information).

system name	Systems with a specific set of system names.
system setting	Systems with a specific client attribute defined. Client attributes are typically used and set by one of the HP ProLiant Essential plugins and is typically reserved for use by one of those plugins.
system subtype	Enables you to search on the product subtype field in the HP Systems Insight Manager (HP SIM) database (for example, Power Enclosure, enclosure, and VM Host)..
system type	Systems identified with the standard <i>system types</i> , including: cluster, desktop, enclosure, management processor, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and so on.
trust status	Systems that have web-enabled agents that either do or do not trust the management console.
Web Agent	Systems with specific web-servers or Web Agents installed.
windows domain	The simple domain name of a system. Can be used to create collections used for authorizations. As comparison criteria, this can be specified without knowing the full distinguished name. With support for Dynamic Authorizations, this enables group memberships in the directory, and changes to them to be reflected and dynamically updated in HP SIM authorizations.
Note: The preceding System Collection Criteria are also available as Event Collection Criteria on the Advanced Search page.	
Event collection criteria	Finds
assignee	Events that have a particular assignee assigned to them (see "Assignee criteria" for more information).
cleared state	Events with a state of Cleared, Not Cleared, or In Progress but is not displayed when the page is opened in the Automatic Event Handling UI (see "Cleared state criterion" for more information).
event category selection	Events that belong to a certain event category selection.
event time	Events that occurred at specified times or the age of events that are greater or less than a specific number of days but is not displayed when the page is opened in the Automatic Event Handling UI.
event type	Events by type grouped by categories (above), and the display is a tree of the categories with event types for each category (see "Event type criteria" for more information).
severity	Events with specified severity levels (Critical, Informational, Major, Minor, Normal, or Warning).
service case status	Status for Remote Support Pack service cases (Assigned for processing, closed, Delivered to HP, In Transit, Other, Submitted to Remote Support, Undelivered). This option is available if the Remote Support Pack is installed. See "HP Service Essentials Remote Support Pack" for more information.
Cluster collection Criteria	Finds
cluster monitor resource	Clusters with specified <i>cluster monitor resource</i> .
cluster name	Systems included in a certain cluster name.
cluster type	Clusters identified with the standard cluster types, including: MSCS clusters, TruCluster Production Server clusters, TruCluster Server clusters, OpenVMS clusters, SCO UnixWare7 NonStop clusters, and HP Serviceguard clusters.
IP address	Cluster with a specified IP address.
status type	Cluster with specific cluster status levels (Critical, Major, Minor, Normal, and Unknown).

Software and firmware criteria

Search for :

where

component type is

and operating system is

and category type is

and name is

and version is

The software/firmware criteria searches for custom support packs in the selected repository and installed software/firmware components for matches in the HP SIM database. This enables you to check software and firmware installed on the target system using the HP SIM database.



NOTE: Information retrieved from the database is displayed in the language in which it was stored. Data retrieved from the repository is displayed in the language corresponding to the browser locale.

NOTE: Searches saved with previous versions of HP SIM are still supported using the new UI. Searches on HP Support Pack are not supported and HP Support Pack software components are filtered from the tree data. HP Support Packs were removed because systems were never returned from a query containing a criteria with HP Support Packs selected. User-built custom support packs continue to be displayed in this list. However, previously saved collections containing HP Support Packs will continue to appear in the UI.

Software components with no entry for operating system are displayed under the **Other** option in the **and operating system is** selection, and software components with no entry for category are displayed under the **Other** option in the **and category type is** selection. This is sometimes the case for software/firmware criterion saved with older versions of HP SIM, since the saved operating system and category names do not match exactly with the new operating system and category names in the database.

You can search software and firmware installed on HP-UX systems. HP-UX populates data in HPUX-Product and HPUX-Bundle tables with information about software and firmware installed on managed HP-UX systems. The data retrieved from these tables are name, caption, and version of each software and firmware installed on target machines. A new entry is added to the **and operating system is** dropdown as **HP-UX Bundles and Products**. Two new categories, **Bundles** and **Products**, are added in the **and software/firmware is** dropdown list. If there is no data in one of these tables, then the category for that table does not appear. If there is no data from either of these tables, then the operating system **HP-UX Bundles and Products** does not appear.

- When comparing against a custom support, the only comparison you can use with the custom support pack is **Equal To**. In addition, HP SIM cannot determine whether a custom support pack is actually installed on a system, only whether all of the components in a custom support pack are installed on a system. A system is returned by this search only if every component in the custom support pack is on the list. It is unlikely that all of the components in a custom support pack are installed on any system, so use this criteria carefully.
- This criterion retrieves information from the SQL database table that was populated by a Software Version Status Polling task. This table is also updated when software is installed through the Update Software or Firmware HP SIM task. Therefore, if software was installed or uninstalled on systems without using HP SIM and after a Software Version Status Polling task was last run, this search might not return the correct results.

Cleared state criterion

You can run a search on the following event statuses:

- **Any.** Includes all events, whether Cleared, Not Cleared, or In Progress
- **Cleared.** Includes events that are cleared
- **Not Cleared.** Includes events that are not cleared
- **In Progress.** Includes events from tasks which are in the progress: When the event is complete, these events become Uncleared

Server role criteria

The Server Role criteria is a system or event collection search that enables you to list the servers of one or more matching roles. The server role is a user-specified value available on HP Insight Management Agent 5.4 or later. To create the criteria, select server role in the **Where** dropdown list on the **Advanced Search** page, and then select the criteria comparison option.

Assignee criteria

You can run a search on certain events that are assigned to a particular user. When you select the **assignee** collection criteria, the result is a scrollable list of users from which more than one can be selected.



NOTE: If you do not select a user, an error message is displayed, stating that there are no assignees for these events. Add assignees from the event table view page.



Event type criteria

Search for :

where is



NOTE: Only one event type criteria can be used in a given search.

When using the event type criteria, you must select comparison criteria such as **is** or **is not**. A tree view of the event types, organized by event category selection, is then displayed. Next, in the **type(s)** box, which contains the tree, select types to search against. For each event type displayed, all correlated types are also displayed. Correlated types (WBEM indications) are grouped with the matching SNMP trap into a subcategory. The event types are shown under the subcategory. You can select an entire category, click  to expand the branch and select individual categories, or click  to collapse close the branch. To add additional criteria, click **Add**. To perform the search immediately, click **View**. To save the search, click **Save As**. See "Saving collections" for more information about using **Save As**.



NOTE: While you can select a specific version of a trap (for example, Array Accelerator Bad Data, Version 1, it is better to select both versions because you might have older or newer agents on some managed systems. Selecting all versions ensures that all agent versions are included in the event collection.

The Automatic Sign-In Server Failure event type is used to indicate that a general error occurred on the server-side of authentication during automatic sign-in. This event can occur for several reasons. See “Signing in” in the **Automatically Signing In** section for more information.

- If the Service Principal Name (SPN) has not been configured on the domain, it must be registered with the HP SIM service account.
- If the SPN has been registered with more than one domain account, it must be registered for only the HP SIM service account. Delete any other SPN entries associated with other accounts.
- If browsing locally from the CMS, you must provide your credentials in the sign-in page. Automatic sign-in does not work when browsing locally.

The Automatic Sign-In No Domain Credentials event type indicates the HP SIM service is not running with a domain account. For automatic sign-in to work, use a domain account for the HP SIM service, and register the domain account with a SPN for HP SIM. See “Signing in” in the **Automatically Signing In** section for more information.

Memory range criteria

You can set the memory ranges for systems that you include in the collection. You can select multiple groups one-at-a-time from the following ranges:

- **Memory Equal To (=)** Includes systems with memory equal to a specified amount.
- **Memory Not Equal To (!=)** Includes systems with memory not equal to a specified amount.
- **Memory Less Than (<)** Includes systems with less memory than the specified amount.
- **Memory Less Than or Equal To (<=)** Includes systems with memory less than or equal to a specified amount.
- **Memory Greater Than (>)** Includes systems with more memory than the specified amount.
- **Memory Greater Than or Equal To (>=)** Includes systems with memory greater than or equal to a specified amount.
- **Memory Range Between (is between)** Includes systems with memory in the specified range.

Related topic

- ▲ [Searching for systems and events](#)

Reference

The Reference section for **Systems** and **Events** includes information about list naming conventions: all *system*-, *event*-, and *cluster*-shared collections and hidden collection names.

Related topics

- [Collection naming conventions](#)
- [Default shared collections](#)

Default shared collections

Shared system collections

All *users* can view shared collections, but only users with *administrative rights* can create, edit, or delete shared collections.

The following shared default *system* collections are based on **System Type**:

- **All Systems** Includes all *discovered* systems in the *database*.
- **All Servers** Includes all discovered servers in the database.
- **All VSE Resources** Includes all discovered *Virtual Server Environment* (VSE) resources in the database.

The following are included under **All VSE Resources**:

- **All nPartition Servers** Includes all discovered systems by type with a Complex type.
 - **All HP Integrity Virtual Machines** Includes all discovered systems by type with a Server type and HP Integrity Virtual Machine Host subtype.
 - **All Virtual Partition Servers** Includes all discovered systems by type with a Server type and HP Virtual Partition Server subtype.
 - **All Resource Partitions** Includes all discovered systems by type with a *Resource Partition* type.
 - **All Shared Resource Domains** Includes all discovered systems by type with a *Shared Resource Domain* type.
 - **All HP Serviceguard Clusters** Includes all discovered systems by type with a Cluster type and an HP Serviceguard subtype.
 - **All Standalone Servers** Includes all discovered systems by type that are HP 9000 or Integrity standalone systems.
 - **All Integrity VM Guests** Includes all discovered virtual machine guests.
 - **All nPartitions** Includes all discovered nPartitions.
 - **All Virtual Partitions** Includes all discovered virtual partitions.
- **HP BladeSystem** Includes all discovered blades in the database

The following are included under **HP BladeSystem**:

- **All p-Class Racks** Includes all p-Class racks for p-Class components including p-Class blades, switches, enclosures, and racks.
 - **All e-Class Enclosures** Includes all e-Class enclosures for Consolidated Client Infrastructure (CCI) blade PCs, e-Class blades, and enclosures.
 - **Spare Systems**
 - **Systems Needing Maintenance**
 - **All c-Class Racks** Includes all c-Class racks for c-Class components including c-Class blades, switches, c-Class enclosures, Onboard Administrator, and racks.
- **Storage Systems** Includes all discovered storage systems in the database.

The following are included under **Storage Systems**:

- **All Storage Systems** Includes all discovered storage systems in the database.
 - **All Storage Hosts** Includes all discovered storage hosts in the database.
 - **All Storage Switches** Includes all discovered storage switches in the database.
 - **All Storage Arrays** Includes all discovered storage arrays in the database.
 - **All Tape Libraries** Includes all discovered tape libraries in the database.
- **All Racks** Includes all discovered *racks* in the database.
 - **All Enclosures** Includes all discovered *enclosures* in the database.

- **All Clients** Includes all discovered clients in the database.
- **All Networking Devices** Includes all discovered networking systems in the database, which includes routers, switches, repeaters, and remote access systems.
- **All Printers** Includes all discovered printers in the database.
- **All Management Processors** Includes all discovered management processors in the database.
- **All Virtual Machine Hosts** Includes all discovered virtual machine hosts.
Note: If HP ProLiant Essentials Virtual Machine Management Pack is not installed, this collection must be manually created to support virtual machine collections.
 - **GSX and VMware Server Hosts** Includes all discovered GSX and VMware server hosts.
 - **ESX Hosts** Includes all discovered ESX hosts.
 - **Virtual Server Hosts** Includes all discovered virtual server hosts.
 - **All Virtual Machine Hosts** Includes all discovered virtual machine hosts.
- **Virtual Machines** Includes all discovered virtual machines.
Note: If HP ProLiant Essentials Virtual Machine Management Pack is not installed, this collection must be manually created to support virtual machine collections.
 - **GSX and VMware Server Virtual Machines** Includes all discovered GSX and VMware server virtual machines.
 - **ESX Virtual Machines** Includes all discovered ESX virtual machines.
 - **Virtual Server Virtual Machines** Includes all discovered virtual server virtual machines.
 - **All Virtual Machines** Includes all discovered virtual machines.
- **All Virtual Machine Farms** Includes all discovered virtual machine farms.
Note: If HP ProLiant Essentials Virtual Machine Management Pack is not installed, this collection must be manually created to support virtual machine collections.

The following collections are based on **System by Status**:

- **Critical Systems** Includes all systems in the database with Critical status.
- **Major Systems** Includes all systems in the database with Major status.
- **Minor Systems** Includes all systems in the database with Minor status.
- **Normal Systems** Includes all systems in the database with a Normal status.
- **Disabled Systems** Includes all systems in the database with a Disabled status.

The following collections are based on **Systems by Operating System**:

- **HP-UX** Includes all systems in the database that have an operating system equal to HP-UX.
- **Microsoft Windows Server 2003** Includes all systems in the database that have an operating system equal to Windows Server 2003.
- **Microsoft Windows 2000** Includes all systems in the database that have an operating system equal to Windows 2000.
- **Microsoft Windows NT** Includes all systems in the database that have an operating system equal to Windows NT.
- **Novell NetWare** Includes all systems in the database that have an operating system equal to NetWare.
- **SCO UNIX** Includes all systems in the database that have an operating system equal to SCO UNIX.

- **Microsoft Windows XP** Includes all systems in the database that have an operating system equal to Windows XP.
- **Microsoft Windows 95, 98, ME** Includes all systems in the database that have an operating system equal to Windows 95, 98, or ME.
- **HP Tru64 Unix** Includes all systems in the database that have an operating system equal to HP True64 UNIX.
- **HP OpenVMS** Includes all systems in the database that have an operating system equal to OpenVMS.
- **Red Hat Linux** Includes all systems in the database that have an operating system equal to Red Hat Linux.
- **SuSE Linux** Includes all systems in the database that have an operating system equal to SuSE Linux.
- **Linux** Includes all systems in the database that have an operating system equal to Linux.
- **HP NonStop Server** Includes all systems in the database that have an operating system equal to NonStop Server.
- **Undeployed** Includes all systems in the database that have an operating system equal to undeployed.
- **Microsoft Windows Vista** Includes all systems in the database that have an operating system equal to Microsoft Windows Vista.

The following collections are based on **Clusters by Type**:

- **All Clusters** Includes all cluster in the database.
- **MSCS Clusters** Includes all MSCS clusters in the database.
- **OpenVMS Clusters** Includes all OpenVMS clusters in the database.
- **HP TruClusters** Includes all HP TruClusters in the database.
- **HP Serviceguard** Includes all HP Serviceguard clusters in the database.

The following default collections are based on **Clusters by Status**:

- **Critical Clusters** Includes all clusters in the database with a Critical status.
- **Major Clusters** Includes all clusters in the database with a Major status.
- **Minor Clusters** Includes all clusters in the database with a Minor status.
- **Normal Clusters** Includes all clusters in the database with a Normal status.
- **Unknown Clusters** Includes all clusters in the database with an Unknown status.

The following are **System Function** collections:

- **Data Collection List** Includes all discovered systems and is used to perform data collection.
- **Status Polling List** Includes all discovered systems and their current status.
- **Server Status Polling List** Includes all discovered servers, clusters, management processors, and their current statuses.
- **Non Server Status Polling List** Includes all discovered non servers and their current statuses.

The following collection is added if HP Storage Essentials installed:

Storage Essentials Managed Includes all storage systems that are managed by HP Storage Essentials.

The following collection is added if the HP Service Essentials Remote Support Pack and HP SIM are installed together on a Windows CMS:

Remote Support Eligible Lists systems the Remote Support Pack supports if you choose to enable them for support and are entitled to support. If a system is enabled without proper entitlement, events are submitted

to the Remote Support software, but they are not monitored and do not trigger a response. See the Remote Support Pack documentation for instructions on enabling or disabling remote monitoring for your systems.

Shared event collections

All users can view shared event collections, but only users with administrative rights can create, edit, or delete shared collections.

The following shared event collections are based on **Event by Severity**:

- **All Events** Includes all *events* that have occurred on systems for which the events are logged in the database.
- **Important Events** Includes all Critical and Major events in the database, regardless of the state of events.
- **Important Uncleared Events** Includes all uncleared Critical, Major, and In Progress events.
- **Informational Events** Includes all Informational events in the database, regardless of the state of events.

The following are **Sign-in Event** collections:

- **All Sign-in and Sign-out Events** Users with administrative rights and users with the correct authorizations on the Central Management Server (CMS) can view sign-in and sign-out events. However, only users with administrative rights can see the details of these events.
- **All Failed Sign-in Events** Users with administrative rights and users with the correct authorizations on the CMS can view failed sign-in events. However, only the users with administrative rights can see the details of these events.

The following are **Service Event** collections:

- ▲ **All HP Service Events** Includes all service events in the database where the event type is HP Service Events.

Note: A service event indicates that a service action is required, such as hardware maintenance. You can open the service event to review the recommended actions and call status, if applicable.

Note: Service events can be obtained from the Remote Support Pack and Open Service Event Manager (OSEM). See <http://h18023.www1.hp.com/support/svctools/>, the documentation for the Remote Support Pack, and the OSEM documentation for information about *How to change the HP SIM Host Name* to configure these tools to send service events to HP SIM. A service contract might be required to receive these events.

The following are **Events by Time** collections

- ▲ **All Virtual Machine Management Events** Includes all virtual machine management events in the database.

The following collection is added if HP Storage Essentials installed:

Storage Essentials Includes all HP Storage Essentials events.

Related procedures

- Customizing system or cluster collections
- Customizing event collections

Related topics

- Navigating the System and Event Collections panel
- System table view page
- Event table view page
- Cluster table view page
- System types

- Service notification events
- Changes to HP SIM storage functionality when HP Storage Essentials is installed

Collection naming conventions

Use the following guidelines for naming **Systems** or **Events**:

- All collection names must be unique, except for private collections.
- The terms **Systems**, **Events**, and all shared collections are reserved names in HP Systems Insight Manager (HP SIM). Do not use them as collection names.
- Multiple spaces in collection names are collapsed to a single space. For example, a collection named

My Collection, is saved as **My Collection**

- Do not use the following symbols in collection names: < > " & ' _ + | % \ / and ;.
- After saving the collection, the name appears under the **System and Event Collections** panel. All collection names must be unique.
- Private collection names cannot match the name of any **Systems** or shared collection but can match the name of a second user's private collection.
- If you create a private collection and get a duplicate name error, you might find that the name exists in another user's private collection.

Related topics

- [Monitoring systems, clusters, and events](#)
- [Event table view page](#)
- [System table view page](#)
- [Cluster table view page](#)
- [Reference](#)

10 Storage integration

HP Systems Insight Manager (HP SIM) discovers *SNMP* and *SMI-S* storage devices.

- For information about using storage devices with HP SIM, see “Storage integration using SNMP” and “Storage integration using SMI-S”.
- For information about the configuration steps for discovering storage devices, see “Discovering storage using SNMP” and “About storage discovery using SNMP” for SNMP devices and “Configuring HP SIM with storage systems” for SMI-S devices.

Related topics

- Viewing storage systems
- Viewing storage system reports
- Viewing storage array capacity
- Changes to HP SIM storage functionality when HP Storage Essentials is installed
- Using HP SIM with SNMP storage solutions

Storage integration using SMI-S

About storage systems

Storage systems are SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters). HP Systems Insight Manager (HP SIM) uses *WBEM SMI-S providers* to discover and collect data from storage systems. See <http://www.hp.com/go/hpsim/providers> to view the latest information about HP SIM device support and for information about obtaining and installing SMI-S providers.

The default *collection* **Storage Systems** is listed under **Systems by Type** in the tree in the **System and Event Collections** panel. The following collections are available under **Storage Systems**:

- **All Storage Systems.** This category includes all devices that were discovered through an *SMI-S provider*.
- **All Storage Hosts.** A storage host is a server, desktop, or workstation that is connected by a host bus adapter (HBA) to a storage area network (SAN). Storage hosts are also included in the **All Servers** and **All Systems** collections.
- **All Storage Switches.** A storage switch is a Fibre Channel switch that is connected to a SAN. Storage switches are also included in the **All Systems** and **All Network Devices** collections.
- **All Storage Arrays.** A storage array is a disk array that uses a Fibre Channel controller to connect to a SAN. Storage arrays are also included in the **All Systems** collection.
- **All Tape Libraries.** A tape library is a tape drive that is connected to SAN. Tape libraries are also included in the **All Systems** collection.

Related procedures

- Configuring HP SIM with storage systems
- Viewing storage system reports
- Viewing storage systems
- Viewing storage array capacity

Related topics

- ▲ Changes to HP SIM storage functionality when HP Storage Essentials is installed

Introduction to SMI-S for HP Systems Insight Manager

The Storage Management Initiative Specification (SMI-S) is a Storage Networking Industry Association (SNIA) standard that enables interoperable management for storage networks and storage devices. HP Systems Insight Manager (HP SIM) uses this standard to discover and manage the storage systems it supports.

About SMI-S

SMI-S replaces multiple disparate managed object models, protocols, and transports with a single object-oriented model for each type of component in a storage network. The specification was created by SNIA to standardize storage management solutions. SMI-S enables management applications (such as HP SIM) to support storage devices from multiple vendors quickly and reliably because they are no longer proprietary. SMI-S detects and manages storage elements by type, not by vendor.

Key components

The key SMI-S components are:

- Common Information Model (CIM)
- Web-based Enterprise Management (WBEM)
- Service Location Protocol (SLP)

CIM

CIM, the data model for WBEM, provides a common definition of management information for systems, networks, applications and services, and allows vendor extensions. SMI-S is the interpretation of CIM for storage. It provides a consistent definition and structure of data, using object-oriented techniques. The standard language used to define elements of CIM is Managed Object Format (MOF). Unified Modeling Language (UML) is used to create a graphical representation (using boxes and lines) of objects and relationships.

WBEM

WBEM is a set of management and internet standard technologies developed to unify the management of enterprise computing environments. WBEM includes the following specifications:

- xmlCIM: Defines XML elements, conforming to Document Type Definition (DTD), which can be used to represent CIM classes and instances
- CIM Operations over HTTP: Defines a mapping of CIM operations onto HTTP; used as a transport mechanism

SLP

SLP enables computers and other devices to find services in a local area network without prior configuration. SLP has been designed to scale from small, unmanaged networks to large enterprise networks.

Profiles

SMI-S is organized around profiles, which describe objects relevant for a class of storage subsystem. SMI-S includes profiles for arrays, Fibre Channel host bus adapters (HBAs), Fibre Channel switches, and tape libraries. Other storage devices (for example, NAS heads) are expected to be added in the future. Profiles are registered with the CIM server and advertised to clients using SLP. HP SIM determines which profiles it intends to manage, and then uses the CIM model to discover the actual configurations and capabilities.

SMI-S implementation

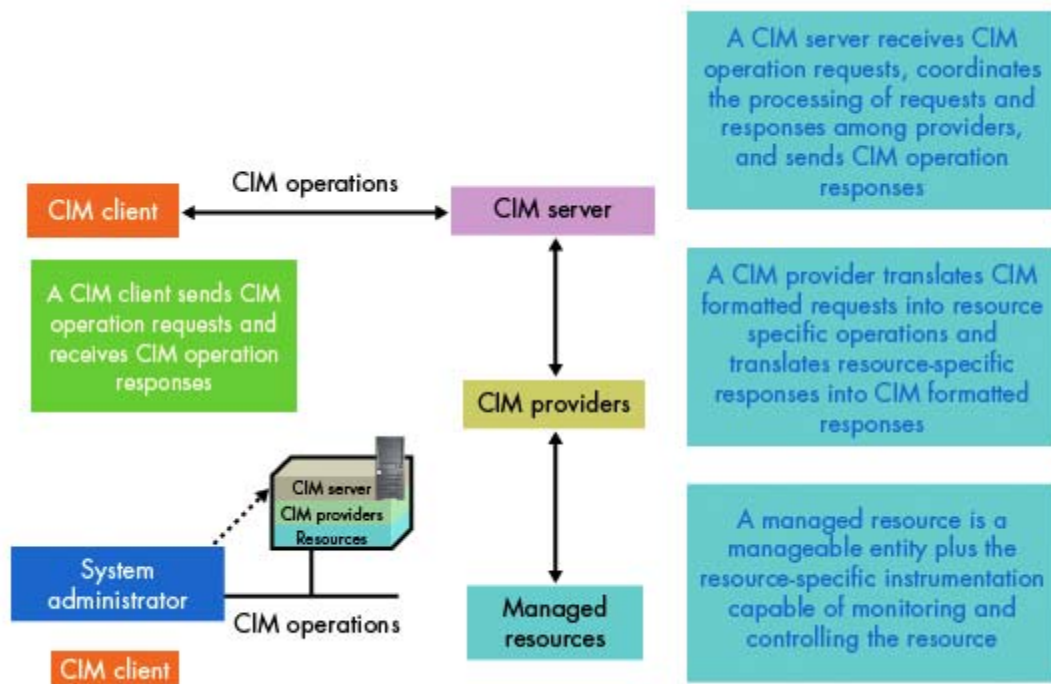
SMI-S is implemented with the following components:

- CIM server (called a CIM Object Manager or CIMOM), which listens for WBEM requests (CIM operations over HTTP) from a CIM client, and responds.
- CIM provider, which communicates to a particular type of managed resource (for example, HP MSA arrays), and provides the CIMOM with information about them. In theory, providers for multiple types of devices (for example, HP MSA arrays and Brocade switches) can be plugged into the same CIMOM. However, in practice, all storage vendors provide the CIMOM and a single provider together, and they do not co-exist well with solutions from other vendors.

These components may be provided in several different ways:

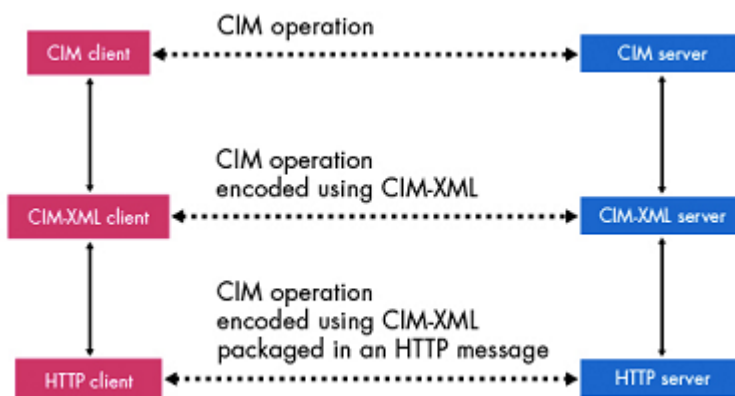
- Embedded agent: The hardware device has an embedded SMI-S agent. No other installation of software is required to enable management of the device.
- SMI solution: The hardware or software ships with an agent that is installed on a host. The agent needs to connect to the device and obtain unique identifying information. This is the method used by all HP storage devices and most SAN devices.

Clients, servers, and providers



The system administrator uses the CIM client to communicate with the CIM server. The CIM server communicates with CIM providers, which manage resources.

WBEM communication



Communication between a CIM client and a CIM server (CIMOM) occurs on three different levels as defined in the CIM/WBEM specification, and as shown in the figure above.

Related topics

- Storage integration
- Viewing storage systems
- Viewing storage system reports
- Viewing storage array capacity
- Changes to HP SIM storage functionality when HP Storage Essentials is installed
- Using HP SIM with SNMP storage solutions

Configuring HP SIM with storage systems

Configuring HP Systems Insight Manager with storage systems

For optimal interaction between HP SIM and *storage systems*, complete the following procedures.

Configure HP SIM to discover storage systems

HP Systems Insight Manager (HP SIM) *discovers* and *identifies storage systems*.

To discover and collect data from a storage system:

1. Verify that the storage system has an installed and configured *SMI-S provider*. See **HP Systems Insight Manager Storage management and SMI-S providers** at <http://h18013.www1.hp.com/products/servers/management/hpsim/smi-s-providers.html> and the HP SIM user guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about obtaining and installing SMI-S providers.
2. Enter the user name and password for the *SMI CIMOM* in the **Default WBEM settings** section on the “Setting global protocols” page.
3. Add each SMI CIMOM IP address to the **System Automatic Discovery** task, or create a new discovery task. See “Editing a discovery task” and “Creating a new discovery task” for instructions.

Your storage systems will be discovered after the next automatic discovery task. If you want to discover your storage systems immediately, run the discovery task. See “Running a discovery task” for instructions.

Subscribe to WBEM indication events

If a storage system's *SMI-S provider* supports WBEM indication events and you want to view WBEM indication events on the Event View page, you must subscribe to WBEM events for the storage system. See “Subscribing to WBEM indications” for instructions.

Related procedures

- Setting global protocols
- Subscribing to WBEM indications
- Editing a discovery task
- Running a discovery task
- Creating a new discovery task
- Viewing storage systems
- Viewing storage system reports

Related topic

- ▲ Storage integration using SMI-S

Viewing storage systems

HP Systems Insight Manager (HP SIM) enables you to view *storage system* information for collections and individual storage systems.

Viewing storage system collections

To view a storage system *collection*:

1. In the System and Event Collections panel, expand **Systems, Shared, Systems by Type, and Storage Systems**.
2. Select one of the following:
 - **All Storage Systems**
 - **All Storage Hosts**
 - **All Storage Switches**
 - **All Storage Arrays**
 - **All Tape Libraries**

The system table view page for that collection appears. See “Navigating the system table view page” for more information.

Viewing individual storage systems

To view an individual storage system:

1. In the System and Event Collections panel, expand **Systems, Shared, Systems by Type, and Storage Systems**.
2. Expand the storage system collection that contains the system you want to view.
3. Click the name of the storage system you want to view.

The **System Page** for that system appears. See “System Page” for more information.

Related procedures

- [Configuring HP SIM with storage systems](#)
- [Viewing storage system reports](#)
- [Viewing storage array capacity](#)

Related topics

- [Navigating the System and Event Collections panel](#)
- [Storage integration using SMI-S](#)

Viewing storage system reports

HP Systems Insight Manager (HP SIM) provides predefined and customized *storage system* reports.

If HP Storage Essentials is installed, no data is displayed in HP SIM storage system reports. This information displays because HP SIM data collection from SMI-S devices is disabled to avoid duplicate data collection from both HP SIM and HP Storage Essentials. For information about storage system reporting with HP Storage Essentials, see your HP Storage Essentials documentation.

See “Reporting views” for specific details about the fields that are displayed in storage system reports.

Existing storage system reports

The following predefined reports are available:

- **Storage Device Capacity—All Storage Arrays** lists capacity usage details for all storage arrays.
- **Storage Device Controllers—All Storage Arrays** lists the status, port count, and number of ports utilized for each storage array controller.
- **Storage Device Inventory—All Storage Arrays** lists vendor, status, and port information for each storage array.
- **Storage Device Inventory—All Storage Switches** lists vendor, status, and port information for each storage switch.
- **Storage HBAs—All Storage Hosts** lists vendor, status, and port information for each host bus adapter (HBA) that is installed on a storage host.
- **Storage Logical Units—All Storage Arrays** lists LUN information and status for all LUNs on all storage arrays.
- **Storage Ports—All Storage Arrays** lists port information for all storage arrays.

- **Storage Ports—All Storage Hosts** lists port information for all storage host HBAs.
- **Storage Ports—All Storage Switches** lists port information for all storage switches.
- **Changer Devices—All Tape Libraries** lists the name, firmware version, and status for all tape libraries.
- **Media Access Devices—All Tape Libraries** lists the name, firmware version, and status for all tape libraries.



NOTE: See “System reporting” for instructions on viewing existing reports.

Custom reports

See “Adding a report” for instructions on creating custom reports.

Related procedures

- System reporting
- Adding a report

Related topics

- Reporting
- Storage integration using SMI-S
- Printing reports
- Reference information
- Reporting views


Viewing storage array capacity

HP Systems Insight Manager (HP SIM) enables you to view capacity details for storage arrays.

Viewing storage capacity for all arrays

To view storage capacity for all arrays, run the **Storage Device Capacity-All Storage Arrays** report. See “System reporting” for instructions.

Viewing storage capacity for a single array

1. In the **System and Event Collections** panel, expand **Systems, Shared, Systems by Type, Storage Systems**, and **All Storage Arrays**.
2. Select a storage array.
3. Click the  icon next to **Capacity Information**.

Related procedures

- Viewing storage system reports
- Viewing storage systems

Related topics

- Storage integration using SMI-S
- System tab for a storage array

Changes to HP SIM storage functionality when HP Storage Essentials is installed

If HP Storage Essentials is installed, the following changes occur within HP Systems Insight Manager (HP SIM):

- HP Storage Essentials items are added to the **Tools, Deploy, Optimize, Reports, Tasks & Logs**, and **Options** menus. See your HP Storage Essentials documentation for details about these menu items.
- A shared collection called **Storage Essentials Systems** is added to the **Systems & Events** panel.
- The following collections are included under **Storage Essentials Systems: SE Cluster Nodes, All SE Systems, SE Hosts, SE Switches, SE Storage Arrays**, and **SE Tape Libraries**.

- If a storage system is managed by HP Storage Essentials, storage-specific details do not appear in its **System** tab, and an **SE System Properties** link appears in the **HP Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage system.
- For storage hosts, HP Storage Essentials adds the **System Application Discovery Settings** link to the **Tools & Links Page**. Use this link to access the preferences for HP Storage Essentials system application discovery.
- No data is displayed in HP Systems Insight Manager (HP SIM) storage system reports. This is because HP SIM data collection from SMI-S devices is disabled to avoid duplicate data collection from both HP SIM and HP Storage Essentials. For information about storage system reporting with HP Storage Essentials, see your HP Storage Essentials documentation.
- The storage tables in HP SIM's Data Collection reports are not populated with data because HP SIM's SMI-S data collection is disabled.
- Storage systems that are managed by HP Storage Essentials show a subtype of **Storage Essentials Managed**, and do not show the **SMI** subtype.
- HP SIM determines device *health status* by polling the SMI-S providers of storage systems. If HP Storage Essentials discovered a storage array, storage switch, or tape library by a method other than SMI-S, HP SIM lists the device's status as **Unknown**.
- System properties that are edited in HP SIM are not transferred to HP Storage Essentials.
- The Suspend or Resume Monitoring command has no effect on HP Storage Essentials systems.
- HP Storage Essentials events are handled as follows:
 - HP Storage Essentials events are available in the **Events** tab of the **System Page** for all storage systems.
 - A collection called **Storage Essentials** is added to the list of shared collections under **Events** in the **System and Event Collections** panel.
 - When an event is cleared in HP SIM, it is also cleared in HP Storage Essentials.
 - Deleting an event in HP SIM causes the same event to be deleted in HP Storage Essentials.
 - When an event is cleared in HP Storage Essentials, it is also cleared in HP SIM.
 - Deleting an event in HP Storage Essentials does not cause the event to be deleted in HP SIM.
 - Comments that are added to events in HP SIM are not transferred to HP Storage Essentials.
 - A link in the **Event Details** section enables you to view the corresponding event details in HP Storage Essentials.
- The **Automatic** tab on the **Discovery** page shows the status of the HP Storage Essentials discovery process and provides a link to the HP Storage Essentials discovery log.
- The **General Settings for All Discoveries** section in the **Automatic** tab on the **Discovery** page includes a link to the HP Storage Essentials global application settings configuration page.
- When HP Storage Essentials is installed, a Toolbox for Storage Essentials tools is added to the **Toolboxes** tab of the **Users and Authorizations** page.
- The **Users and Authorizations** tabs are updated with instructions and links for managing user security when HP SIM and HP Storage Essentials are used together.
- If HP SE detects a device manager URL for a system, the URL is added to the HP SIM Tools & Links page in the System Web Application Pages section.
- If HP SIM and HP SE are installed on the same computer, you cannot delete the HP SE management station from HP SIM.
- The HP SIM First Time Wizard and the **Discovery** page are updated with information about HP SE licensing.



NOTE: For additional information about HP Storage Essentials, see your HP Storage Essentials documentation.

Related topics

- [Storage integration using SMI-S](#)
- [HP Storage Essentials overview](#)

Storage integration using SNMP

Overview

Storage devices can be broken down into real-time access and backup systems. Real-time access systems can be subdivided into internal disks, redundant disks (RAID), tape libraries, storage area networks (SAN), and network attached storage (NAS).

Most data centers have combinations of these systems including:

- **Small Business** Almost entirely internal disk drives
- **Medium Business** Varying combination of internal disks and RAID systems
- **Large Business** Varying combination of internal disks, RAID, and some SAN or NAS
- **Enterprise Business** Mostly large SAN or NAS, and some RAID and internal disks might be present

HP Systems Insight Manager (HP SIM) can retrieve the information for the internal disk drives for systems being monitored. This does not mean that HP SIM actively manages and configures each of the systems previously indicated.

HP SIM can:

- Discover and identify storage systems that are directly attached to a server
- Discover and identify storage systems that are on the network, including tape libraries
- Discover and identify HP StorageWorks Command View storage device manager systems
- Receive storage system events and associate them with the system that generated the event (through Command View) running on a system, or from a tape library management card
- Context launch appropriate management application from the context of the event or the context of the system running the Command View that generated the event

Storage events

With HP SIM, administrators can monitor inventory and, configure and manage hardware resources and the system software that affects the systems.

HP SIM, provides the administrator with a complete overview of the hardware status. Storage events provide notification that a problem exists that could affect the availability of storage resources, which can affect system and application availability. HP SIM receives detailed event messages through WBEM events or SNMP traps. These events identify the system and the affected disk and provide an error number for looking up details and a description of the problem. The event details also contain links to the Command View server that generated the event. HP SIM associates a disk or RAID subsystem with the controller managing these drives for internal storage.

Storage inventory details

HP SIM inventory retrieves and stores the following information from internal disk drives:

- Disk
 - Total number of disk slots
 - Number of used slots
 - Slot ID

- The type of disk in slot
- Disk manufacturer
- Disk model
- Disk part number
- Disk characteristics
- Firmware version
- Controller ID that is managing this disk
- Controller details
 - Total number of controllers
 - Controller type
 - Controller manufacturer
 - Model number
 - Part number
 - Slot ID that this card is installed in
 - Firmware version
 - Controller characteristics
- RAID details
 - RAID type
 - RAID configuration
- SAN and NAS
 - Network addresses
 - Manufacturer
 - Model
- IS and MNHA
 - Part number
 - Total number of disks
 - Disk details
 - Servers being serviced by this system

Related procedures

- [Discovering storage using SNMP](#)
- [Using HP SIM with SNMP storage solutions](#)

Related topics

- [System Page](#)
- [About storage discovery using SNMP](#)
- [System Page](#)

About storage discovery using SNMP

Discovery and identification

HP Systems Insight Manager (HP SIM) discovers the storage systems that are on the LAN and Command View storage device managers running on managed systems or devices. For internal disks, the HP SIM inventory component can identify all of the drives installed, the disk manufacturer, models, disk types, firmware revision, the internal location of the drive in the system, and the details of the controllers by which the systems are managed. For RAID drives, the RAID type (1 to 5) and manufacturer is discovered in addition

to the details gathered for the internal drives. For SAN systems, HP SIM discovers the Command View servers that manage the devices on the SAN.

HP SIM displays storage systems as follows:

- **Internal drives** These systems must appear in the **Properties** pages and the inventory database as components of their respective systems.
- **Tape libraries** These devices are identified and included in the **All Systems**, **All Storage Systems**, and **All Tape Libraries** collections.
- **SAN** The Command View systems for these devices are identified and available from the **Tools & Links** tab of the **System Page** for the systems serving the Command View systems.



NOTE: HP SIM discovers SAN and NAS management applications and provides user access to system information when those applications are started.

Related procedures

- [Discovering storage using SNMP](#)
- [Using HP SIM with SNMP storage solutions](#)

Related topic

- ▲ [System Page](#)

Discovering storage using SNMP

The HP Systems Insight Manager (HP SIM) discovery process for systems running Command View includes the following:



NOTE: To access the links to Command View, select **Tools**→**System Information**→**System Page**→**Links**.

- CV XP on port 80 (http)
- CV VA/SDM on port 4096 (http)
- CV TL on port 4095 (http)
- Discovery of Command View EVA is encapsulated within the discovery of the HP StorageWorks Storage Management Appliance on ports 2301 or 2381

HP SIM must be permitted to access the web server.

To configure Command View and SDM:

1. Verify that the HP SIM CMS is within a secure IP range in the Command View server configuration.
 - **Host based** CMS IP address included in `.../sanmgr/hostagent/config/access.dat`.
 - **Storage Area Manager management server (if applicable)** CMS station IP address included in `/sanmgr/managementserver/config/authorizedClients.dat`.
2. Run discovery to discover or re-identify the Command View systems. See “Discovery and identification” for more information regarding running discovery.
3. When discovery is complete, you can group systems in HP SIM and launch Command View from the **System Page**. See “System Page” for more information regarding the **System Page**.

To load the EVA MIB, enter `mxmib -a cpqhsv110v3.cfg`.

Note: Loading the MIB could take several minutes to complete. See “Managing MIBs” for more information about MIBs.

Related procedure

- ▲ Using HP SIM with SNMP storage solutions

Related topics

- System Page
- About storage discovery using SNMP
- Discovery and identification

Using HP SIM with SNMP storage solutions

Viewing a storage event

There are two ways to view a storage event:

- Select **Tools**→**System Information**→**System Page**.
- Click the system name in the **System Name** column on the system table view page.

Creating a storage by type group

You can create a search for systems of type, such as ESL or MSL, for tape libraries, or create a search for Web Agents of type for each type of Command View system.

- **HP StorageWorks Command View SDM** Search for Web Agent == HP StorageWorks Command View SDM.
- **HP StorageWorks Command View XP** Search for Web Agent == HP StorageWorks Command View XP.
- **HP StorageWorks Command View ESL** Search for Web Agent == HP StorageWorks Command View ESL.
- **HP StorageWorks Tape Libraries** Search for system type == storage device.
- **HP StorageWorks Management Appliance** Search for Web Agent == Management module hp_OpenView_Storage_Management_Appliance or Web Agent == Management Module OpenSANManager.

Event collection and launch

To receive events, the Command View software must be configured to send SNMP events to the HP Systems Insight Manager (HP SIM) CMS.

For Command View SDM:

To configure the SNMP trap destination on Windows NT 4.0 on the Command View server:

1. Select **Start**→**Settings**→**Control Panel**→**Network**→**Services**→**SNMP Service**.
The **SNMP Service Properties** dialog box appears.
2. Click **Traps**.
3. Enter a community name, such as `public`.
4. Click **Add**.
5. At the bottom of the dialog box, click **Add**.
The **SNMP Service Configuration** dialog box appears.
6. Enter the host name or IP address of the enterprise management station, and then click **Add**.
The SNMP trap destination is added.
7. Click **OK** to save the changes and close the dialog box.

To configure the SNMP trap destination on Windows 2000:

1. Select **Start**→**Settings**→**Control Panel**→**Network**→**Services**→**SNMP Service**.
The **SNMP Service Properties** dialog box appears.
2. Click **Traps**.
3. Enter a community name, such as **public**.
4. Click **Add to list**.
5. At the bottom of the dialog box, click **Add**.
The **SNMP Service Configuration** dialog box appears.
6. Enter the host name or IP address of the enterprise management station, and then click **Add**.
The SNMP trap destination is added.
7. Click **OK** to save the changes and close the dialog box.

To configure the SNMP trap destination on HP-UX:

1. Using a text editor, open the following file:
`/etc/snmpd.conf`
2. Insert the following information at the end of the `snmpd.conf` file:
`trap-dest: X.X.X.X`
Replace the `X.X.X.X` with the IP address of the enterprise management station.
3. Save and close the `snmpd.conf` file.
4. Stop the SNMP daemon by entering the following at a shell command prompt:
`ps -ef | grep snmpd`
`kill -9 PID`
Replace `PID` with the process ID returned by the previous command.
5. Restart the SNMP daemon by entering the following at a shell command prompt:
`snmpd`

To load the HSV MIB on the CMS for EVA:

1. On a Windows operating system, go to a command prompt. Navigate to `\Program Files\HP\System Insight manager\mibs` directory. See “Registering a MIB” for more information regarding MIBs.
2. Run `mxmib -a cpqhsv110v3.cfg`.

Related procedures

- [Discovering storage using SNMP](#)
- [Configuring SNMP traps](#)

Related topic

- ▲ [System Page](#)

11 Managing with tasks

HP Systems Insight Manager (HP SIM) enables you to manage *systems* and *events* by scheduling and executing tasks. Tasks are actions performed using an HP SIM *tool*. Task instances are an executed single instance of a *task*.

Users can:

- Create a variation of a task
- Schedule a task
- Modify a task you created
- Delete a task
- Stop an executing task
- Track task status

Task information is available by selecting one of the following:

- **Tasks & Logs**→**View All Scheduled Tasks**
- **Tasks & Logs**→**View Task Results**



NOTE: HP SIM provides system-delivered (default) tasks. These tasks can be disabled or have their schedules modified but they cannot be removed or reassigned to another user. HP SIM requires these tasks to provide a complete picture of the systems being monitored.

For more information about user privileges and configuration rights, see “Users and authorizations”.

Related procedures

- Creating a task
- Scheduling a task
- Running a scheduled task
- Stopping a task
- Deleting task results
- Printing reports
- Editing a scheduled task
- Deleting a scheduled task
- Viewing task results

Related topics

- About default system functions
- Navigating the All Scheduled Tasks page
- Applying a time filter
- Task status types

About default system functions

Polling tasks track *the health status* of systems in associated collections. Hardware status polling must occur periodically to determine when systems go offline or when hardware degrades. You can customize polling tasks for specific systems to run at scheduled times. You can also create polling tasks with different collections to meet your needs.

You can configure polling tasks to take place based on the receipt of an event. Event polling tasks are associated with event collections. For example, you might set up a hardware status polling task for when traps are received from a system.

When a polling task is set up to run as the result of a change in an event collection, the polling task is applied to all systems generating events that match the given collection.



NOTE: HP does not recommend scheduling a polling task based on periodic event collection. The task would run on the set of systems for each event in the associated collection.

NOTE: If you remove a hardware status polling task, systems continue to be discovered, but the status on them is not updated. If you remove the Daily System Identification task, you would no longer detect changes in management on systems.

The following default tasks are available on the **View All Scheduled Tasks** page:

- Biweekly Data Collection
- Daily Device Identification
- Delete Events Older Than 90 Days
- Hardware Status Polling for Non Servers
- Hardware Status Polling for Servers
- Hardware Status Polling for Systems No Longer Disabled
- Initial Data Collection
- Initial Hardware Status Polling
- Software Version Status Polling
- Software Version Status Polling for Systems no Longer Disabled

Biweekly Data Collection

Use this task to collect data. This task runs on all systems in the **Data Collection List** collection. The default schedule sets the task to run every other Saturday at noon.

Daily Device Identification

Use this task to gather information about systems such as networking systems. By default, this task runs once a day. The information is identified and stored in the database.

- Single Login and Secure Task Execution (STE) support on a managed system
- Type of management protocol on the system (HTTP, SNMP, DMI, and WBEM)
- Type and subtype of system (server, storage, switch, router, and so on)
- Product name of the system
- Operating system name and version
- Web Agents running on the system
- Web-based software running on the system (for example, printer management software)
- System associations with management processors (for example, a system and its Remove Insight board)
- Storage proxies and related storage systems
- Wake-on-LAN information

Delete Events Older Than 90 Days

This task deletes events older than 90 days and can be used to help maintain HP SIM by limiting the total number of events. By default, this task is disabled. To enable the task:

On the **All Scheduled Tasks** page and click **Enable**.

For more information about scheduling tasks, see “Creating a task”.

In some installations there might be high volumes of events. If so, consider using this task and event collections as a model and create an event collection for events older than 30 days (for example), and then create a task to delete events older than 30 days.

Hardware Status Polling for Non Servers

This task collects status information through management protocols (SNMP, WBEM, and so on) for systems that are not Server, Cluster, or Management Processor type. By default, this task polls every 10 minutes and at start-up.



NOTE: If you discover more than 500 systems, HP suggests you change the interval to something greater than 10 minutes (for example, 15 minutes for every 1000 systems).

Hardware Status Polling for Servers

This task collects status information for SNMP, DMI, or WBEM systems that are Server, Cluster, or Management Processor types. By default, this task polls every 5 minutes and at start-up.



NOTE: If you discover more than 500 systems, HP suggests you change the interval to something greater than 5 minutes (for example, 10 minutes for every 1,000 systems).

Hardware Status Polling for Systems No Longer Disabled

This task runs when a system goes from a disabled state to an enabled state. You could use this task to get the latest status after a planned maintenance window on a system that was set to disabled.

Initial Data Collection

This task collects *static* information from a number of systems that have WBEM, DMI, or SNMP running (for example, serial numbers and model numbers). For more information about the type of data collected, see “Reference information”.

Initial Hardware Status Polling

This task runs hardware status polling on systems that are newly discovered. Therefore, you do not need to wait for the periodic tasks to run before the system has a valid status.

Software Version Status Polling

This task determines software version update status and is set to run every seven days by default at midnight. You can edit this task or manually run it at any time.

For more information about the type of data collected, see “Software status polling”.

Software Version Status Polling for Systems no Longer Disabled

This task runs the software version tool when a system changes from a disabled state to an enabled state so that the status of the software loaded on the system is kept current in HP SIM.

For more information about the type of data collected, see “Software status polling”.

Related procedures

- [Creating a task](#)
- [Running a scheduled task](#)
- [Editing a scheduled task](#)
- [Printing reports](#)
- [Running a scheduled task](#)
- [Editing a scheduled task](#)

Related topic

- ▲ [Navigating the All Scheduled Tasks page](#)

Bypassing target verification

Set task wizard settings to bypass the **Verify target systems** page when running a tool.

To configure task wizard settings:

1. Select **Options**→**Task Wizard Settings**. The **Task Wizard Settings** page appears.
2. Select **Bypass target verification page when all targets are valid**.
3. If the target verification page includes the options to run now or schedule, select **Run Now** or **Schedule**. If you select **Run Now** when a tool is selected, the tool runs immediately. If you select **Schedule** when a tool is selected, the **Schedule Task** page appears. For more information about scheduling a task, see “Scheduling a task”.

Note: This option is only relevant for tools that do not require user input beyond the targets selected for the tool, such as **Ping** and **System Page**. If the selected tool cannot be scheduled, the **Run Now** option is used for the tool.

4. Click **OK**. A dialog box appears stating that the settings have been saved.

Related procedures

- Creating a task
- Running a scheduled task
- Viewing task results
- Deleting task results
- Printing reports
- Editing a scheduled task

Related topics

- Applying a time filter
- Managing with tasks

Creating a task

Create a *task* to execute a *tool* on specific *systems* or *events*.



NOTE: If you have selected target systems and do not want to verify the systems, you can modify task wizard settings by selecting **Options**→**Task Wizard Settings** and selecting **Bypass target verification page when all targets are valid**. For more information, see “Bypassing target verification”.

To create a task:

1. Select a tool from the HP SIM menu. The **Select Target Systems** page usually appears; however, if targets are selected before selecting a tool, the **Verify Target Systems** page appears.

The **OS** column displays the first 40 characters of the operating system name, with an ellipse at the end of the name if it is more than 40 characters long. Place your cursor over the name to see the entire operating system name.

2. Add multiple or single targets:
 1. To add targets, you can choose one of two radio buttons above the drop-down selection box, either the **Collection** option or the **Search** option which is used to indicate the method of target selection or click **Cancel** which will result in no additions.

Note: You are not allowed to select individual events for Targets or Filters, so the ability to search will not be available when those selections are made. The two radio buttons will not be present in these cases.

2. Choosing the **Collection** option will allow you to select targets from the drop-down selection box.
3. If you choose the **Search** option, the drop-down selection box and **View Contents** button will be replaced with the **Quick Search** user interface. Type a **Device Name** into the **Text Field** and then click **Search**.

Note: If there are **Device Names** that match the characters typed in the **Text Field**, a dynamic list is displayed with those matches.

4. If you select one of the **Device Names** displayed in the dynamic list, a **System Table** containing the selected system will be displayed below the **Quick Search** user interface. Items displayed in

the **Search Results** table will be selected (checked) by default and the **Apply** button will be enabled as long as there is at least one item from the **Search Results** table selected. Only items that are selected will be added when you click **Apply**.

Note: The maximum number of **Device Names** displayed is six.

5. If you click **Search**, a **Basic Search** using common attributes will be performed using the characters typed into the **Text Field**. The results will be displayed in the **Search Results** table below the **Quick Search** user interface.

While the search user interface remains open, the **Task Wizard** will retain a reference to the **Query** object created to perform the **Dynamic Query** generation used when performing searches. Each new search term will be added to this **Query** object and a new **Dynamic Query** will be generated. The **Task Wizard** will release its reference to the search **Query** when you close the search user interface or by clicking **Cancel** or **Apply**.

Note: A barbershop pole will be seen while **Basic Search** results are loading.

Once you choose the system to add, the **Select <item> itself** checkbox is checked by default and the **Apply** button and **View Contents** button are enabled. You can choose to click **Apply** or **View Contents**.

Note: If you choose to change the selected item in the drop-down selection box, the **Select <item> itself** text will be updated to reflect the change.

Note: If the **Select <item> itself** checkbox is unchecked, the **Apply** button will become disabled.

Selecting **View Contents** will display the **Table View** or **Tree View** of the selected item and the **Apply** button will become disabled.

Note: When **View Contents** is selected, the **Target Selection Page** displays a barbershop pole and the message *"Please wait while the data is loading"* while the **Table View** or **Tree View** is loading.

Once you select items from the displayed **Table View** or **Tree View**, the **Apply** button becomes enabled.

Note: If the **Select <item> itself** checkbox is checked while a **Tree View** is displayed, the **Tree View** will be closed and the **Apply** button will become enabled. If you uncheck the **Select <item> itself** checkbox, the **Tree View** will not be redisplayed. You must click **View Contents** in order to have the **Tree View** displayed again.

3. Click **Apply**. The targets appear in the **Verify Target Systems** page.

Note: If selected targets are not compatible with the tool, the **Tool Launch OK?** column provides a brief explanation of the problem.

To remove a target, select **Remove Targets**.

A sub-window will open below the row of buttons that displays a smaller table with the Targets currently chosen on the **Target Selection Page**. The "remove" table will not display more than ten rows of items.

- a. Select the checkboxes for the items you wish to remove from your current list of chosen Targets.
- b. Click **Apply**. This will close the sub-window and redraw the **Target Selection Page** with the updated list of targets.

Note: The **Apply** button will become enabled when there is at least one item selected from the **Remove Targets** table.

- c. Select **Cancel** if you choose not to remove any of the target selections. If you select **Cancel**, the sub-window closes and no items are removed.

Note: If the tool targets systems, any **Filter** selected is a single **Event Collection**. If the tool targets events, the **Target** selected is a single **Event Collection**. When these cases arise, a table will not be displayed. The item will be displayed as a static text or a hyperlink following the same logic when displaying the selected item in a table.

4. To filter target selections, complete the following.
 - a. Click **Add Event Filter**.
 - b. From the **Add filters by selecting from** dropdown box, select an event filter. If you do not select an event filter, an error message appears.
 - c. Click **Apply** to apply the filter to the target systems (or, click **Cancel** to cancel adding a filter). The **Filtered by** table appears below the list of selected target systems.

Note: If the target selections are events instead of systems, the button changes to **Add System Filter** and you can select from different system collections. Unlike event filters, you can select multiple system filters.
5. To modify an event filter, click **Modify Event Filter**.

Note: If the filters are systems, you will see an **Add System Filters** and **Remove Filters** buttons. If there is only one event filter, the **Remove Filters** button will simply remove the single event filter. If you have more than one event filters, the **Remove Filters** button will open a sub-pane that you may select the event filters to remove.

 - a. From the **Add filters by selecting from** dropdown box., select an event filter. If you do not select an event filter, an error message appears.
 - b. Click **Apply** to change the event filter and apply the filter to the target systems, or click **Cancel** to cancel editing the filter.

Note: If the target selections are events instead of systems, the button does not change to **Modify System Filter** you will have the option to select either the **Add System Filters** or **Remove Filters**. It is possible to have one or more system and event combination collections already selected. If there are combination collections selected, they will provide filtering.
6. To remove a filter, select the filter(s) from the sub-pane that you wish to remove and click **Remove Filters**.
7. Click **Next** and specify tool parameters. If the tool does not require parameters, **Next** is replaced with **Schedule** and **Run Now**. The **Schedule** option is only present if the tool can be scheduled.
8. Select one of the following options:
 - Click **Previous** to return to the previous screen.
 - Click **Schedule** to schedule when the task should run. For more information about scheduling options, see "Scheduling a task".
 - Click **Run Now** to run the task immediately.



NOTE: If multiple users are accessing a task simultaneously, the changes made by the last user who edited the task are saved. For example, if User1 and User2 sign-in to HP SIM with *administrative rights* and User1 is editing a task while User2 is deleting the task, when User1 tries to save the edited task a message appears indicating that the task does not represent an object in the system and User1 cannot save the edited task.

Command line interface

Use the `mxexec` command to execute tools immediately, or the `mxtask` command to schedule tasks for later. Perform this task from the *command line interface* (CLI). For assistance with this command, see the HP-UX or Linux manpage by entering `man mxexec` at the command line or see the Windows command line help. For information about how to access a manpage, see "Using command line interface commands".

Related procedure

- ▲ Bypassing target verification

Related topics

- Managing with tasks
- Navigating the All Scheduled Tasks page

Applying a time filter

Use time filters to decide when a task should or should not run by applying them to a *task*. Time filters can be created, copied, edited, and deleted.

Time filters can be created by any user and are accessible to all users.

1. Select a *tool* from the tool menu, follow the steps to get to the **Schedule** button, and then click it. For more information, see “Creating a task” and “Scheduling a task”.
2. To apply a time filter to a task, select the **Use Time Filter** checkbox.
3. Below the **Schedule Task** section, click **Manage Filters** and choose from the following options:
 - **New.** The new time filter has the default name **New Time Filter X**, where X is a number making the time filter name unique. Click **OK** or **Apply** to save the new time filter, or click **Cancel** to cancel the new time filter changes.
 - **Edit.** Time filters created by users can be edited. A time filter cannot be renamed, so if a time filter must be renamed, copy the time filter and give the copy a new name. Changes made to a time filter are saved after clicking **OK** or **Apply**. If the time filter to be edited is in use by one or more tasks, a message appears, stating *Editing the time filter could have undesirable effects in the tasks currently using the time filter. To eliminate this problem, copy the time filter and give the copy a new name.*
 - **Copy.** Time filters can be copied by any user. The copied time filter name appears with a number appended to it (to make the name unique). To save changes made to the time filter, click **OK** or **Apply**.
 - **Delete.** A user can delete a time filter that is created by another user. Select the time filter to be deleted, and then click **Delete**. If the time filter being deleted is in use by one or more tasks, a message appears, stating *The time filter cannot be deleted at this time because it is in use by one or more tasks.*

Time filters are created and viewed in the time zone of the user creating the time filter. For example, if the default time filter of business hours (8 a.m. to 5 p.m.) is used and the filter is viewed in the same time zone as the CMS, it will display from 8 a.m. to 5 p.m. If the CMS is in Eastern Standard Time (EST) and a user accesses it in Pacific Standard Time (PST), the time filter appears as 5 a.m. to 2 p.m. instead. Time filters created at installation use the time zone of the CMS.

Note: If you want to schedule a task to run once a month on the 31st of the month and the month only has 30 days, the task will run on the 1st day of the following month.

Related topics

- [Managing with tasks](#)
- [Scheduling a task](#)

Scheduling a task

The options presented for scheduling a *task* vary depending on the tool you use and the target *systems* you select. Scheduling a task requires a unique name for the task. Not all tools can be scheduled.

To schedule a task:

1. Select a tool from the menus. For more information, see “Creating a task”.
2. In the **Task name** field, enter a unique name for the task.
3. Under the **When would you like this task to run?** section, select one of the following options:
 - **Periodically** Select from intervals of minutes, hours, days, weeks, or months. With periodic scheduling, you can configure the task to run until a certain date and time or to execute only a set number of times. Periodic scheduling allows time filters to be applied. These filters specify the hours of the day when a scheduled task can operate. For more information about time filters, see “Applying a time filter”.

Note: If you want to schedule a task to run once a month on the 31st of the month and the month only has 30 days, the task will run on the 1st day of the following month.

 - **Once** Specify the date and time the task is to run.

- **When new systems or events are added to the collection** This option is only available if you select a **Collection of Systems or Events** as your target. The task runs only when new systems or events meet the collection criteria. You can also apply a time filter to this type of scheduling. For more information about time filters, see “Applying a time filter”.
 - **When systems or events are removed from the collection** This option is almost identical to the previous option, except that the task only runs when systems contained in the **Collection of Systems or Events** no longer meets the collection criteria. A time filter can be applied to this type of scheduling. For more information about time filters, see “Applying a time filter”.
 - **Not Scheduled** This option specifies that the task runs only when manually executed by a user with appropriate privileges. This task never runs automatically. Tasks can be manually run from the **All Scheduled Tasks** page or the *command line interface* (CLI).
4. Under **In addition**, select from the following options:
 - **Run when the central management server is started** Select this option if you want the task to run every time the *Central Management Server* (CMS) is started.
 - **Run now** Select this option to run the task immediately after it is saved.
 - **Disable this task** Select this option to temporarily disable the task. This task is shown as Disabled on the **All Scheduled Tasks** page.
 5. After you select a scheduling option, refine the schedule in the **Refine schedule** section. The available options vary depending on the scheduling option selected in step 3.
 6. Click **Done**, and the **All Scheduled Tasks** page appears, or click **Previous** to return to the previous page. For more information about the **All Scheduled Tasks** page, see “Navigating the All Scheduled Tasks page”.

Viewing all scheduled tasks

To view all scheduled tasks, select **Tasks & Logs**→**View All Scheduled Tasks**.

The list of tasks that a user can see is based on the user's privileges. All users are allowed to edit, delete, and view the tasks they have created. With *administrative rights*, the user is allowed to edit, delete, and view tasks other users have created.

Related procedures

- Running a scheduled task
- Viewing task results
- Deleting task results
- Printing reports
- Editing a scheduled task

Related topics

- Applying a time filter
- Managing with tasks

Running a scheduled task

Run a *task* to initiate a task instance. Running a scheduled task executes a specific *tool* on specific systems or *for specific events*.

To run a scheduled task:

1. From the tool menus, select **Tasks & Logs**→**View All Scheduled Tasks**. The **All Scheduled Tasks** are displayed in the workspace.
2. Select a task from the list, and then click **Run Now**.

Note: If an instance of the task is running, the **Run Now** button is disabled.

Command-line interface

Use the `mxexec` command to execute tools immediately; use the `mxtask` command to schedule tasks for later. Perform these tasks from the CLI. For assistance with these commands, see the HP-UX or Linux manpage for the command by entering `man mxexec` at the command line or see the Windows command line help. For more information about how to access the manpage, see “Using command line interface commands”.

Related procedures

- Editing a scheduled task
- Deleting a scheduled task
- Printing reports
- Viewing task results
- Stopping a task

Related topics

- Managing with tasks
- Navigating the All Scheduled Tasks page

Editing a scheduled task

Edit a scheduled *task* to:

- Change the *tool* parameters
- Set the time
- Re-enable a task that has been disabled
- Modify target *systems*

To edit a scheduled task:

1. Select **Tasks & Logs**→**View All Scheduled Tasks**. The **All Scheduled Tasks** page appears.
2. From the **All Scheduled Tasks** page, select the task to be edited.
3. Click **Edit**.

The previously configured task information appears. Follow the same steps as if you are creating the task. For more information, see “Creating a task”.

Because the task has a schedule associated with it, you must visit the **Schedule Task Page**. The **Run Now** button is not present (as it is when a task is being created). *Users* with *administrative rights* can change the owner of the task.

If the new owner does not have access rights to the tool or to selected targets, an error message appears when the user attempts to edit or save the task.

4. After you edit the task, click **Done**, or to run the task immediately, select the **Run Now** checkbox on the **Schedule Task** page before clicking **Done**.

This task is saved and displayed on the **All Schedule Task Page**.

Related procedures

- Running a scheduled task
- Deleting a scheduled task
- Printing reports
- Viewing task results
- Stopping a task

Related topics

- Managing with tasks
- Navigating the All Scheduled Tasks page

Deleting a scheduled task

Deleting a *task* removes the task and its associated task instances from the **All Scheduled Tasks** page and the *system*.



CAUTION: If you delete a task, the task is permanently deleted from the *database* and cannot be restored.



NOTE: You cannot delete system delivered (default) tasks.

To delete a scheduled task:

1. Select **Tasks & Logs**→**View All Scheduled Tasks**.
2. Select a task from the **All Scheduled Tasks** list.
3. Click **Delete**.

Note: If an instance of the task is running, a message appears stating that you must stop the running task instance before the task can be deleted.

Related topics

- [Navigating the All Scheduled Tasks page](#)
- [Scheduling a task](#)

Viewing task results

Task results appear on the **Task Results** page. Information, similar to the following appears on the page:

- Task start and stop time
- The *tool* used by the *task*
- The command the task executes

To view task results:

1. From the menu, select **Tasks & Logs**→**View Task Results**.
2. Select a task.
3. To stop or delete a task instance, select a task instance from the **View Task Results** page.
4. Click **Stop** or **Delete**.

The **Task Results** page displays a list of task instances created by all tasks.

Viewing task instance results

From the **Task Results** page, select a task instance by selecting a row from the Task Instances list.

The **Task Instance** section displays the following information:

- **Status** This field displays the status of the task.
- **ID** This field displays the task job ID number.
- **Task Name** This field displays the name of the task that was executed.
- **Tool** This field displays the name of the tool that was used.
- **Owner** This field displays the user name that currently owns the task.
- **Command** This field displays the command used to run the task.
- **Summary Status** This field displays the summary status and indicates the status of some tasks. For more information, see “[Task status types](#)”.
- **Target** This field displays the name of the target collection or individual systems where the task executed. If you run a custom tool or a *multiple-system aware* (MSA) tool, this field displays the *Central Management Server* (CMS) system name. With MSA commands, the command resides on the CMS and runs from the CMS for a remote system or list of systems. Therefore, the target for this type of command always shows as the CMS.

- **Executed As** This field displays the user context where the tools were executed from.
- **Start Time** This field displays the time when the task was started.
- **End Time** This field displays the time when the task was completed or cancelled.
- **Duration** This field displays the amount of time it took to run the task.



NOTE: The list of task instances is based on user privileges and access levels. Users with *administrative rights* can view all task instances known to the system.

Viewing target details



NOTE: This section is displayed for *single-system aware* (SSA) tools only.

Target details include the following:

- **Target Name** This field displays the name of the target.
- **Status** This field displays the status of the target.
- **Exit Code** This field represents the success or failure of an executable program. Typically, if the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed.
- **The Stdout tab** This tab displays the output text information.
- **The Stderr tab** This tab displays information if the executable experienced an error.
- **Files Copied tab** This tab displays what files are in the process of being copied or have been copied to the target system. This tab is not present for tools that do not perform any file copies to their target systems.

To view target details:

1. From the **Task Instance Results** section, select a target system from the table below the **Summary Status**.

A window appears.

2. View the target details.

Related procedures

- [Running a scheduled task](#)
- [Deleting a scheduled task](#)
- [Printing reports](#)
- [Editing a scheduled task](#)
- [Stopping a task](#)

Related topics

- [Managing with tasks](#)
- [Navigating the All Scheduled Tasks page](#)

Printing reports

Reports can be printed for the selected target *system* or all target systems associated with the task instance. For task instances that do not have multiple target systems, the report is created without asking whether you want to view the report for the selected target system or all target systems.

To print a report:

1. From the menu, select **Tasks & Logs**→**View Tasks Results**.
2. Click **View Printable Report**.

A **Print Report Question** appears, asking to generate a report containing the selected target system or all target systems associated with the task instance.

3. Select the report to print.
4. Click **OK** to print the report.

Related procedures

- Running a scheduled task
- Deleting a scheduled task
- Editing a scheduled task
- Viewing task results
- Stopping a task

Related topics

- Managing with tasks
- Navigating the All Scheduled Tasks page

Stopping a task

Perform this procedure to stop a task instance from running.

To stop a task instance:

1. From the menu, select **Tasks & Logs**→**View Task Results**, and then select a task instance from the **Task Results** list.
2. Click **Stop**. If the task instance is in a terminal state, **Stop** is disabled. If the *task* can be stopped, a dialog appears, asking if you want to cancel or kill the selected task instance. If the *tool* does not signify that the task can be stopped, the dialog box asks you to confirm the cancellation of the task instance. Stopping a task attempts to interrupt In Progress commands. Canceling stops pending systems from starting and enables Running or In Progress commands to complete.

Related procedures

- Running a scheduled task
- Editing a scheduled task
- Deleting a scheduled task
- Printing reports
- Viewing task results

Related topics

- Scheduling a task
- Task results list
- Navigating the All Scheduled Tasks page

Deleting task results

Perform this procedure to delete *task* instances from the **Task Results** page.



NOTE: When a user is deleted from HP SIM, tasks that belong to that user are deleted.

To delete an instance:

1. Select **Tasks & Logs**→**View Task Results** and then select a *task* from the table.
2. Click **Delete**. The task instance is deleted from the *database*.

Note: If the task instance is running, a message appears, stating that you must stop the running task instance before it can be deleted.

Command line interface

Use the `mxtask` command to execute tools immediately and to schedule tasks for later time. Perform this task from the *command line interface* (CLI). For assistance with this command, see the HP-UX or Linux manpage by entering `man mxtask` at the command line or see the Windows command line help. For information about accessing the manpage, see “Using command line interface commands”.

Related procedures






- Creating a task
- Stopping a task

Related topic




- ▲ Managing with tasks

Task status types

HP SIM reports the following summary status for *tasks*:

-  **Failed**. The task instance or task target instance failed and needs immediate attention.
-  **Killed**. The task instance or task target instance stopped.
-  **Canceled**. The task instance or task target instance was canceled before the task was complete.
-  **Complete**. The task instance or task target instance is complete.
-  **Running**. The task instance or task target instance is running without a problem.

The following status types are for the task target instance:

-  **Copying**. The task target instance is copying without a problem.
-  **Pending**. The task target instance is not complete or is pending.
-  **Skipped**. The task target instance includes a system that is not supported or the system was in a disabled state.



NOTE: If the task instance status of Skipped, the task results (job status) shown in the **Task Results** table is Complete.

NOTE: When a tool does not support a system (for example, running a Windows tool on a Linux system), the task status is **Skipped** and the tool is not run on that system. The task can be created against collections even if some systems might not match the tool filter. When the task runs, the tool filtering is applied at that point. This differs from selecting a handful of systems and receiving the verify target selections screen with errors like `system is not a Linux OS`. Skipped also appears if a system is disabled and a polling tool (for example, Status polling or Data Collection) is run on it.

Related topic

- ▲ Managing with tasks

Task results list

This list displays the list of task instances known to the *system*. Each *task* instance listed displays:

- Its unique job ID
- Task name
- Owner, status, and duration
- Start and end time

The list provides status information for scheduled tasks that have run and for runnable tasks (tasks that do not have a schedule). The list enables you to stop, delete, and view task instance results.

To see task information:

1. From the menu, select **Tasks & Logs**→**View Task Results**.
2. Click the task row and then select one of the following options:
 - **Stop**. Click **Stop** to stop a running task instance. For more information, see “Stopping a task”.
 - **Delete**. Select a task instance, and then click **Delete**. For more information, see “Deleting task results”.

Note: If a task instance is running, a message appears informing you to stop the task instance before attempting to delete it.
3. View the results of a task instance below the **Task Results** list.

The **Task Instance Results** section displays the following information:

- **Status**. This field displays the status of the task. For more information about the different status types, see “Task status types”.
- **ID**. This field displays the task job ID number.
- **Task Name**. This field displays the name of the task that was executed.
- **Tool**. This field displays the name of the tool that was used.
- **Owner**. This field displays the user name that owns the task.
- **Command**. This field displays the command used to run the task.
- **Target**. This field displays the name of the target collection or systems that the task executed on. If you run a custom command tool or a multiple-system aware (MSA) tool, this field displays the Central Management Server (CMS) system name. With custom command and MSA tools, the executables reside on the CMS and are run from the CMS to the remote system. Therefore, the Target for these types of commands are always shown as the CMS.

The remaining tool types (single-system aware (SSA), Automation, and so on) have the actual targets the tool ran on listed in the Target field. This value could be a single system, multiple systems (comma-separated), or the name of the collection selected for the task. If the Target is a collection or multiple systems, the Target value becomes a hyperlink. Click the hyperlink to display the contents of the collection or the complete list of systems if the Target field displays a partial comma-separated list of the target systems.

- **Executed As**. This field displays the user context where the tools were executed.
- **Start time**. This field displays the time the task started.
- **End time**. This field displays the time the task ended.
- **Duration**. This field displays the time that the task took to run.

The list of task instances is based on user privileges and access levels. Users with *administrative rights* can view all task instances known to the system.

Related topics

- [Creating a task](#)
- [Managing with tasks](#)

Navigating the All Scheduled Tasks page

The **All Scheduled Tasks** page displays the tasks scheduled to run at periodic times or based on *event* criteria. A scheduled *task* can also have a schedule of **not scheduled**, which means that the task is listed but only runs when manually executed by a *user*.

To see task information, select **Tasks & Logs**→**View All Scheduled Tasks**, and then select a task by clicking the task row. See:

- “Run now”
- “Enable/Disable”
- “Edit”

- “Delete”
- “View task results”



NOTE: If multiple users are accessing a task simultaneously, the changes made by the last user who edited the task are saved. For example, if User1 and User2 sign-in to HP SIM with *administrative rights* and User1 is editing a task while User2 is deleting the task, when User1 tries to save the edited task a message appears indicating that the task does not represent an object in the system and User1 cannot save the edited task.

User privileges

The list of tasks that a user can see is based on the user's privileges. All users can edit, delete, and view the tasks they have created. With administrative rights, a user can edit, delete, and view tasks other users have created.

Run now

Run a task to initiate a task instance. (Running a task executes a tool on specific systems or events. For more information, see “Running a scheduled task”.

Edit

1. Select **View All Scheduled Tasks**.
2. Select a task, and click **Edit**.

The previously configured task information appears.

3. Edit the task, and then click **Done**.

For more information, see “Editing a scheduled task”.

Delete

Deleting a task:

- Removes the task from the **All Scheduled Tasks** page and the system.
- Deletes associated task instances.

To delete a task:

1. Select **View All Scheduled Tasks**.
2. Select a task, and click **Delete**.

For more information, see “Deleting a scheduled task”.

Enable/Disable

If the selected task is currently enabled, this button will read **Disable** and clicking it will disable the task. If the selected task is currently disabled, this button will read **Enable** and clicking it will enable the task.

View task results

When you view task results, you see information similar to the following:

- The tasks schedule
- The tool used by the task
- The command the task executes
- A list of task instances created by the task
- Summary status, the target systems list, and target details

For more information, see “Viewing task results”.

Related topics

- [Managing with tasks](#)
- [Task status types](#)

12 Tools that extend management

HP Systems Insight Manager (HP SIM) provides you with the following powerful management *tools*:

- **Cluster Monitor** Use to monitor and manage multi-system Microsoft Cluster Service (MSCS) *clusters*
- **Command Line Tools** Use as part of a *Distributed Task Facility* (DTF). Available in HP SIM to run on *single-system aware* (SSA) systems
- **Custom Tools** Use to create and manage custom tools that run on the Central Management Server (CMS) and on target systems. These tools can reference environment variables set by the tool to access system or event information
- **Device Ping** Use to ping one or more systems
- **Disk Thresholds** Use to define the Normal, Minor, and Major ranges for disk utilization on monitored nodes and to set and remove disk thresholds
- **DMI Access** Used to set the HP SIM CMS as the event target on selected HP-UX systems where *Desktop Management Interface* (DMI) is installed
- **HP Server Migration Pack - Universal Edition (SMP Universal)** Use to extend the functionality of the HP ProLiant Essentials Virtual Machine Management Pack (Virtual Machine Management Pack) to provide integrated physical-to-virtual (P2V), virtual-to-virtual (V2V), and virtual-to-physical (V2P) migrations
- **Initial ProLiant Support Pack Install** Use to install software on managed systems
- **Licensing** Use to manage license *keys* from HP SIM, including key distribution, reconciliation, and reporting across Windows platforms
- **Management processor tools** Use after management processors are discovered to manage the following: system power, system locator, new user, modify user, delete user, LAN access, Lightweight Directory Access Protocol (LDAP) settings, Integrated Lights-Out (iLO) control, firmware update, and deploying Secure Shell (SSH) public keys
- **Management Information Base (MIB) tools** Use to compile, edit, register, unregister, and view MIBs.
- **OpenSSH Install** Use from the CMS to install the OpenSSH service onto target Windows systems. Then, run the `mxagentconfig` command to complete the configuration.
- **HP Performance Management Pack (PMP)** Use to watch and analyze in real-time the performance of a monitored server in real-time and to view recorded data sessions from the PMP repository
- **Process Resource Manager (PRM) tools** Use to provide system resources where the business needs them.
- **Property Pages** Provide to users so they can view the **Property** pages on a *Web-Based Enterprise Management* (WBEM) system. Also use to access WBEM properties, such as those that help describe the target system on the network, help determine the status of the system, and that provide an inventory of the target system.
- **Replicate Agent Settings** Use to enable HP SIM to retrieve and edit Web *Agent* configuration settings from a source system and distribute that configuration remotely to target systems through Web Agents.
- **Serviceguard Clusters** Use to provide a mechanism to view cluster information by running HP Serviceguard Manager.
- **SNMP Access** Use to set the HP SIM CMS as the trap target on selected HP-UX systems.
- **System Management Homepage** Use to view the status of management software and utilities on the system.
- **System Page** Use to view information related to a specific system, including general information of the system, system status, and URLs that are related to the system.

- **Version Control** Use to facilitate Software Update and tasks related to it. Uses HP Insight Management Agent, including HP Version Control Repository Manager HP Version Control Agent and other agents.
- **Webmin** Use as a web-based interface for system administration for UNIX and Linux . Using HP SIM, you can set up user accounts, Apache, Domain Name Service (DNS), file sharing, and so on.

Related procedures

- Creating a new remote tool
- Creating a new CMS tool
- Creating a new web page tool
- Removing and restoring custom tools
- Managing custom tools
- Editing a remote tool
- Editing a CMS tool
- Editing a web page tool
- Deleting a custom tool
- Viewing tool definition files
- Setting disk thresholds
- Collecting license information
- Managing licenses
- Adding licenses from a file
- Adding licenses individually
- Viewing licensed systems
- Deleting management processor users
- Deploying SSH public keys to management processors
- Editing management processor users
- Upgrading management processor firmware
- Executing internal control actions through management processors
- Configuring LAN access on management processors
- Configuring LDAP settings on management processors
- Creating new users on management processors
- Controlling the system locator LED through management processors
- Controlling system power options through management processors
- Compiling a MIB
- Editing a MIB
- Registering a MIB
- Unregistering a MIB
- Viewing a MIB
- Property Pages
- Initial ProLiant Support Pack Install
- Deploying OpenSSH to multiple systems using RDP
- Installing OpenSSH
- Creating a Replicate Agent Settings task
- Discovering storage using SNMP
- Using HP SIM with SNMP storage solutions

- Installing RPM
- Querying RPM
- Uninstalling RPM
- Verifying RPM
- Accessing the System Management Homepage
- Editing system properties for a single system
- Suspending or resuming system monitoring for a single system
- Installing Software and Firmware
- Accessing the Version Control Agent
- Accessing the Version Control Repository Manager

Related topics

- Command line tools
- Custom tools
- Cluster Monitor
- Device ping
- Disk thresholds
- Configuring DMI access
- Storage integration using SNMP
- License manager
- Management processor tools
- Managing MIBs
- Partner applications
- PMP tools
- HP Process Resource Manager overview
- Replicate Agent Settings - Reference
- RPM Package Manager
- HP Serviceguard Manager overview
- Server Migration Pack
- Configuring SNMP access
- System Management Homepage
- System Page
- Version Control
- Webmin overview

Quick Launch menu

The **Quick Launch** menu is a place for a short list of frequently used tools. Customizing the **Quick Launch** menu enables you to select which tools are displayed in the menu. Tools only appear in the **Quick Launch** menu if all the selected targets are valid for that tool. Customizations are on a per-user basis. The **Quick Launch** menu is available from the following pages in HP Systems Insight Manager (HP SIM):

- All views (table, tree, icon, or picture) of all collections
- **Search Results** page
- **System Page**

To customize the **Quick Launch** menu:

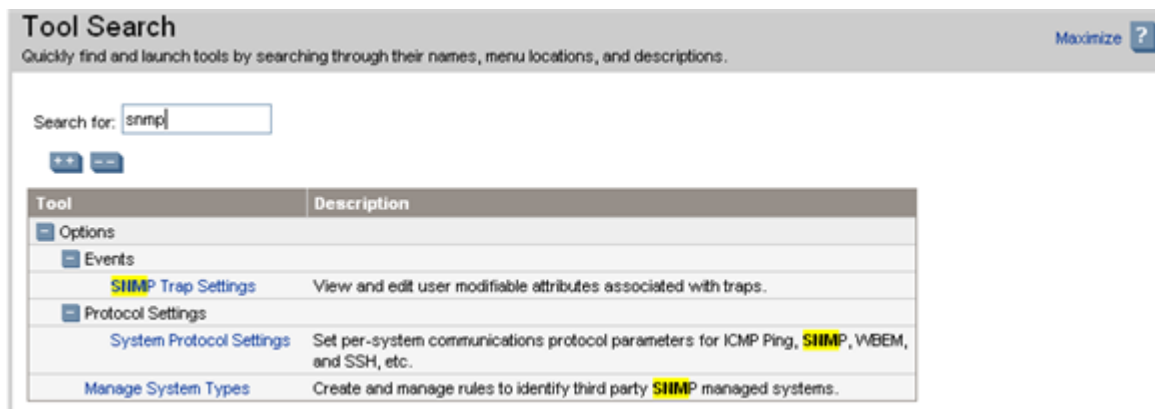
1. Click **Customize** in the **Quick Launch** menu. The **Customize Quick Launch** page appears.
2. Select a menu category from the **Available tools from** dropdown list. All available tools from that menu are listed.
3. Select tools to add to the **Selected tools** list and click **>>**.
To remove tools from the **Selected tools** list, highlight the tools to remove and click **<<**.
Click **↓** or **↑** to arrange tools in the list.
4. (Optional) Select **Show original menu structure (and order) in the Quick Launch menu**. This displays the tools' menu paths in the **Quick Launch** menu.
5. Click **OK** to save changes, or click **Restore Defaults** to restore system defaults.

Related topics

- Navigating the system table view page
- Navigating the picture view page
- Navigating the icon view page
- Navigating the tree view page
- Navigating the event table view page

Tool search

The tool search feature provides a quick way to find a tool by entering text (often less than a single word) that is used to search and filter, textually, based on tool names, tool locations in the HP Systems Insight Manager (HP SIM) cascading menu structure, and tool descriptions.



- The tool search feature searches, matches, and highlights as you type in information.
- The tree structure of the menu is represented exactly. If no filter text is supplied, the entire menu is rendered in a tree format for browsing.
- All searches are case insensitive.
- Tools are hyperlinked and can be launched from the tree.
- Tool names, menu paths, and descriptions are searched. If you are not authorized for a tool, it is not included in the search.
- In the image above for a search on **SNMP**, there are matching tools that include SNMP not in their names, but in their descriptions. By reading the short description, you learn not only how SNMP applies to the tool, but you get a quick overview of the tool.


Related procedure

- ▲ Searching for tools

Searching for tools

To perform a tool search

1. Click **Tool Search** in the **Search** panel. The **Tool Search** page appears.

2. The HP Systems Insight Manager (HP SIM) menu structure is displayed on the main page. You can either click the  icon to expand the tree or enter text in the **Search for** box.
3. After you locate the tool you are searching for, click the tool link to be taken to the appropriate tool page.

Related topic

- ▲ [Tool search](#)

Cluster Monitor

Use Cluster Monitor to monitor Microsoft Cluster Server (MSCS) clusters.

To use Cluster Monitor:

1. Access the **Cluster Monitor** page by using one of the following methods:
 - Method 1:
 1. Select **Tools**→**System Information**→**Cluster Monitor**.
Note: If no MSCS clusters are discovered, **Cluster Monitor** is not listed in the menu.
 2. Select a target MSCS cluster, and then click **Run Now**. See “Creating a task” for more information about selecting a target cluster.
or
 - Method 2:
 1. Locate a cluster by expanding **Systems** under the **System and Event Collections** panel and selecting a cluster collection.
The appropriate cluster collection table appears in the workspace.
Note: Only MSCS clusters you are authorized to access appear on the cluster table view page.
 2. Choose one of the following:
 - In the **Cluster Name** column, click the name of the MSCS cluster.
 - In the **CS** column on the cluster table view page, click the MSCS cluster status icon.The **Cluster Monitor** page appears for that cluster.
2. Select from the following tabs available on the **Cluster Monitor** page. Every tab includes a **Problem Info** section that provides details about problems reported on the tab. For example, on the **Cluster** tab, this section includes status information if the cluster has a status of anything other than Normal.
Each tab also includes a **Last Update** field that displays the last time the information on the tab was updated.
 - **Cluster** Use to view cluster information such as the cluster status, name, IP address, and quorum.
 - **Nodes** Use to view node information such as the node status, name, and IP address.
 - **Network** Use to view network information such as the network status, name, mask, state, role, and description.
 - **Resources** Use to view MSCS Resource information for the cluster, including the status, name, IP address, state, group, owner node, type, and drive of the resources.

Related topics

- [Cluster Monitor Cluster tab](#)
- [Cluster Monitor Nodes tab](#)
- [Cluster Monitor Network tab](#)
- [Cluster Monitor Resources tab](#)

Configuring cluster resource settings

Configure the cluster resource settings to customize *Cluster Resources* for your environment.



NOTE: When using the keyboard to input an alphanumeric character to highlight an option with the arrow keys in any dropdown list in the Cluster Monitor, press the **Enter** key to select the item.

To configure cluster resource settings:

1. Select **Options**→**Cluster Monitor**→**Cluster Resource Settings**. The **Cluster Monitor - Cluster Resource Settings** page appears.
2. Select **ALL (MSCS)** from the **Cluster Type** list to configure MSCS clusters.
3. Select **MSCS** from the **Resource** list.
4. Select **Polling** and set the polling rate.
Note: HP recommends setting the polling rate to no less than five minutes.
5. Click **OK** to save the changes.

Related procedures

- ▲ [Configuring node resource settings](#)

Related topics

- [Cluster table view page](#)
- [Cluster Monitor](#)

Configuring node resource settings

Configure the node resource settings to customize *Cluster Monitor* for your environment.

To configure node resource settings:

1. Select **Options**→**Cluster Monitor**→**Node Resource Settings**. The **Cluster Monitor - Node Resource Settings** page appears.
2. Select the cluster from the **Cluster** list at the top of the page. Select **All** to configure a *resource* the same for all *clusters*. To set polling values for CPU utilization or disk capacity, the cluster choice must be set to **All**.
3. Select the node from the **Node** list. Select **All** to configure a resource the same for all nodes in the selected cluster. As in the case of clusters in step 1, some resource attributes can only be set once for all nodes and so require you to select all clusters and nodes. See the individual attribute descriptions for a particular resource.
4. Select the resource from the **Resource** list to display buttons for the resource configurable parameters.
5. Specify the appropriate resource options.

Note: HP recommends settings the polling rate to no less than 5 minutes.

Note: If you select **All** from the **Cluster** list and select **CPU** or **Disk** from the **Resource** list, you can set polling or threshold values. If you select **Polling**, set the value, then select **Thresholds**, set the values, and then select **Polling** again. The new polling values are still displayed. No matter when you click **OK** after setting the polling or thresholds values, these values are saved and not reset to the original value, which is the same when setting thresholds.

6. Click **OK** to save the changes.

Related procedures

- ▲ [Configuring cluster resource settings](#)

Related topics

- [Cluster table view page](#)
- [Cluster Monitor](#)

Cluster Monitor Cluster tab

The Cluster Monitor **Cluster** tab displays the following information for MSCS clusters:

- **Status** Displays the cluster status. Cluster statuses include Critical, Major, Minor, Normal, and Unknown. See “System status types” for more information about status types.
- **Name** The cluster name or alias.
- **IP Address** The IP address of the cluster alias.
- **Quorum** Resource that maintains essential cluster data and guarantees that all nodes have access to the most recent database changes.

You can sort the information located on the **Cluster** tab by clicking a column heading. This feature sorts the information by that column in ascending or descending order.

The **Problem Info** section displays detailed information on any cluster status other than Normal.

Related topics

- Cluster Monitor
- Cluster Monitor Nodes tab
- Cluster Monitor Network tab
- Cluster Monitor Resources tab
- System status types

Cluster Monitor Nodes tab

The Cluster Monitor **Node** tab displays the following information for MSCS clusters:

- **Status** Displays the node status. Node statuses include Critical, Major, Minor, Normal, Failed, and Unknown. See “System status types” for more information about node status types.
- **Name** The node name.
- **IP Address** The IP address of the node.

You can sort the information located on the **Nodes** tab by clicking a column heading. This sorts the information by that column in ascending or descending order.

The **Problem Info** section displays detailed information on any node status other than Normal.

Related topics

- Cluster Monitor
- Cluster Monitor Cluster tab
- Cluster Monitor Network tab
- Cluster Monitor Resources tab
- System status types

Cluster Monitor Network tab

The Cluster Monitor **Network** tab displays the following information for MSCS clusters:

- **Status** Displays the network status. Network statuses include Critical, Major, Minor, Normal, Disabled, and Unknown. See “System status types” for more information about network status types.
- **Name** Server cluster object that carries internal communication between nodes and provides client access to cluster resources.
- **Mask** The subnet mask associated with the network within the cluster.
- **State** The state of the network: Normal (the network state is online or available), Degraded (the network is partitioned), Failed (the network state is offline), and Other (the network state indicates that

an error has occurred and the exact state of the network could not be determined or the network state is unavailable).

- **Role** Role the network name plays in the cluster: network name for the cluster, network name for computer systems in the cluster, or network name for groups in the cluster.
- **Description** Description of the network.

You can sort the information located on the **Network** tab by clicking a column heading. This sorts the information by that column in ascending or descending order.

The **Problem Info** section displays detailed information on any network status other than Normal.

Related topics

- Cluster Monitor
- Cluster Monitor Cluster tab
- Cluster Monitor Nodes tab
- Cluster Monitor Resources tab
- System status types

Cluster Monitor Resources tab

The Cluster Monitor **Resources** tab displays the following information for MSCS clusters:

- **Status** Displays the resource status. Resource statuses include Critical, Major, Monitor, Normal, and Unknown. See “System status types” for more information about network status types.
- **Name** Physical or logical entity that is capable of being owned by a node, brought online and taken offline, moved between nodes, and managed as a server cluster object.
- **IP** The IP address of the cluster.
- **State** State of the resource: Normal (the resource state is online), Degraded (the resource state is Unavailable, Offline, Online, Pending, or Offline Pending), Failed (the resource state is failed), and Other (unable to determine the resource condition).
- **Group** Collection of resources managed as a single server cluster object.
Note: A group must have a network name and an IP address associated with it for you to access group resources. A group can be owned by any node in the cluster and can be moved by users with *administrative rights* for load balancing and other administrative purposes. When a failure takes place, the entire group fails over, prompting the cluster software to transfer all group resources and data to a different node in the cluster. The resources and data in a transferred (failed-over) group are still accessible under the same network name and IP address, even after they have been moved to a different node.
- **OwnerNode** Node on which a resource resides.
- **Type** Server cluster object used to categorize and manage resources that have similar characteristics.
- **Drive** Disk or drive on which the resource resides.

The **Last update** field displays the date and time of the last update of the information included on the tab. The **Problem Info** section includes detailed information on any resource problems reported.

The **Problem Info** section displays detailed information on any resource status other than Normal.

Related topics

- Cluster Monitor
- Cluster Monitor Cluster tab
- Cluster Monitor Nodes tab
- Cluster Monitor Resources tab
- System status types

MSCS status

Monitoring MSCS status

HP Systems Insight Manager (HP SIM) monitors Microsoft Clustering Service (MSCS) status on each monitored Windows *cluster* and displays it as a cluster attribute in the *Cluster Monitor*. It is a contributor to the cluster status shown in the **CS** column on the cluster table view page. Cluster Monitor polls the cluster on a set interval to retrieve the status value.

See “Cluster Monitor polling rate” for information about MSCS Resource Settings.

To access the **Cluster Monitor - Cluster Resource Settings** page, click **Options**→**Cluster Monitor**→**Cluster Resource Settings**.



NOTE: Only *users* with *administrative rights* can change the polling values.

Related topics

- Cluster Monitor
- Cluster resources supported by HP SIM

Cluster resources supported by HP SIM

HP Systems Insight Manager (HP SIM) supports several Cluster Monitor resources:

- Disk
- CPU

Disk and CPU resources monitor the Disk capacity and CPU utilization, respectively. You can set minor and major thresholds for individual nodes in a cluster. When those thresholds are reached, *Cluster Monitor* creates an HP SIM event. The *event* triggers associated e-mail and paging notification as configured in the HP SIM options.

- System

The System resource monitors the system health of the cluster member.

Cluster Monitor states



NOTE: The cluster condition is Other when all nodes of a cluster are down.

The following table explains the condition categories for each list.

List	Normal	Degraded	Failed	Other
Node	The node status is an active cluster member.	The node status is down, trying to reform or rejoin a cluster, is operating as an active member of a cluster but cannot host any resources or resource groups, or is up but cluster activity is paused.	The node status is down or trying to form or rejoin a cluster.	The node status is Unavailable or could not be determined.
Network	The network state is Online or Available.	The network state is Partitioned.	The network state is Offline.	The network state indicates that an error has occurred, and the exact state of the network could not be determined, or the network state is unavailable.
Resources	The resource state is Online.	The resource state is Unavailable, Offline, Online Pending, or Offline Pending.	The resource state is Failed.	The resource state is Unknown.



NOTE: For additional information about the Microsoft Cluster Service, see Microsoft's documentation.

Related topic

- ▲ [Cluster Monitor](#)

Cluster Monitor resources and associated settings



NOTE: Although Cluster Monitor is used for MSCS clusters only, the CPU and Disk thresholding functionality for Cluster Monitor works for any cluster in which the cluster nodes are running HP Insight Management Agents.

This version of HP Systems Insight Manager (HP SIM) includes these node-level *cluster monitor* resources and associated settings:

- CPU (see “Cluster Monitor polling rate” or “Cluster Monitor resource thresholds”)
 - Disk (see “Cluster Monitor polling rate” or “Cluster Monitor resource thresholds” for clusters)
 - System (see “Cluster Monitor polling rate” for nodes)
-



NOTE: See “Cluster resources supported by HP SIM” for information about the CPU utilization data.

Related procedures

- [Customizing system or cluster collections](#)
- [Performing an advanced search for clusters](#)

Related topics

- [Cluster Monitor](#)
- [Searching for systems and events](#)
- [Cluster resources supported by HP SIM](#)
- [Cluster table view page](#)
- [Navigating the System and Event Collections panel](#)

Cluster Monitor polling rate



NOTE: You can specify only one polling rate (interval) for all nodes in all *clusters*. You cannot specify different rates for different nodes, so the polling fields display on the configuration page only when you select **All** in both the **Cluster** and **Node** dropdown lists.

CPU polling rate

The CPU polling rate determines how often Cluster Monitor checks CPU utilization as reported by the appropriate HP Insight Management Agent on monitored nodes.

Adjust the CPU polling rate by configuring the Cluster Monitor node resource settings. See “Configuring node resource settings” for more information.

Disk polling rate

The Disk polling rate determines how often Cluster Monitor checks the free disk space as reported by the appropriate HP Insight Management Agent on monitored nodes.

Adjust the polling rate by configuring the Cluster Monitor node resource settings. See “Configuring node resource settings” for more information.

MSCS status polling rate

The polling rate you enter determines how often Cluster Monitor checks the MSCS status of monitored clusters.

Adjust the status polling rate by configuring the Cluster Monitor's cluster resource settings. See “[Configuring cluster resource settings](#)” for more information.

System status polling rate

The system polling rate determines how often Cluster Monitor checks node status as reported by the appropriate HP Insight Management Agent running on the nodes.

System is a node-level attribute. You can adjust the polling rate by configuring Cluster Monitor node resource settings. The polling rate is a global attribute of the resource, so you can specify only one polling interval for all nodes in all clusters. The polling fields display on the configuration page only when you select **All** in both the **Cluster** and **Node** dropdown lists.

Related procedures

- [Configuring cluster resource settings](#)
- [Configuring node resource settings](#)

Related topic

- ▲ [Cluster Monitor](#)

Cluster Monitor resource thresholds

Cluster resources use *thresholds* to trigger HP Systems Insight Manager (HP SIM) events. The Disk resource sets thresholds for disk capacity, and the CPU resource sets thresholds for CPU utilization.

Disk capacity thresholds

The Disk resource collects disk capacity data. To access the **Cluster Monitor - Node Resource Settings** page where the thresholds are set, select **Options**→**Cluster Monitor**→**Node Resource Settings**.

The threshold values you enter in the **Settings for the Selected Resource** section define the Normal, Minor, and Major ranges for disk utilization on monitored nodes.

For each disk, there are four thresholds in pairs. The Minor and Major thresholds are each associated with a corresponding reset threshold. Utilization enters the Major range when it equals or exceeds the Major threshold value and remains in the Major range until it falls to or below the Major reset value. The Minor and Major reset thresholds behave similarly.

You can specify different thresholds for each disk in each node of a cluster.

See “[Configuring node resource settings](#)” for more information about setting disk thresholds.

CPU utilization thresholds

The CPU resource collects utilization data for the CPUs in a particular cluster. To access the **Cluster Monitor - Node Resource Settings** page where the thresholds are set, select **Options**→**Cluster Monitor**→**Node Resource Settings**.

The threshold values you enter in the **Settings for the Selected Resource** section define the Normal, Minor, and Major ranges for CPU utilization on the selected node.

For each CPU, there are four thresholds in pairs. The Minor and Major thresholds are each associated with a corresponding reset threshold. Utilization enters the Major range when it equals or exceeds the Major threshold value and remains in the Major range until it falls to or below the Major reset value. The Minor and Major reset thresholds behave similarly.

You can specify different thresholds for each CPU in each node of a cluster.

See “[Configuring cluster resource settings](#)” for more information about CPU thresholds.

Related topic

- ▲ [Cluster Monitor](#)

Command line tools

Use the *command line interface* (CLI) *tools* to execute basic UNIX and Windows commands remotely on one or more *systems*.



NOTE: For additional information about the individual commands, see the associated manpage on an HP-UX and Linux system or the Windows command line help where the command tool is installed.

NOTE: Command line tools provided by HP-UX and Linux, such as the `ls` and `df` commands, are run as root by default. For security reasons, you might want them to run as a specific user to avoid permitting unintended capabilities to a user.

To launch a command line tool:

1. Choose one of the following:
 - Select **Tools**→**Command Line Tools**→**UNIX/Linux** for Linux or UNIX command line tools.
 - Select **Tools**→**Command Line Tools**→**Windows** for Windows command line tools.
2. Select the command line tool that you want to run, and follow the steps to launch the tool. See “Creating a task” for assistance with the steps.
3. Click **Run Now** to launch the tool.

Command line interface

Use the `mexec` command to launch these command tools on one or more systems from the command line interface. For assistance with this command, see the associated manpage. See “Using command line interface commands” for information about accessing the manpage.

Related topics

- Using command line interface commands
- Managing with tasks
- Viewing task results

Configuring or repairing agents

Overview

Managed systems must be able to communicate status to the HP Systems Insight Manager (HP SIM) Central Management Server (CMS) in order for commands to be launched to the managed systems. To configure the managed *systems* to communicate with the CMS, common configurations and trust relationships must be configured. The *Configure or Repair Agents* feature enables you to configure or repair agents in Windows, Linux, and HP-UX.

The *Configure or Repair Agents* tool enables you to repair *Simple Network Management Protocol* settings and trust relationships that exist between *HP Systems Insight Manager* and target systems if you have 7.2 agents or later installed. If you have 7.1 agents or earlier installed, you can update Web Agent passwords on target systems.

The *Configure or Repair Agents* feature adds the security and trap community strings and trust settings to the target systems, but it does not replace existing settings. To replace the existing settings on target systems, use the *Replicate Agent Settings* feature in HP Systems Insight Manager.

You can use *Configure or Repair Agents* tool to send test SNMP traps from Windows systems with HP Insight Management Agents and send test *Web-Based Enterprise Management* indications from Windows and HP-UX systems with HP WBEM provider installed.

You can also configure WBEM certificates for HP-UX systems and WBEM/WMI users for Windows systems with HP Insight Management WBEM Providers for Windows Server 2003/2008.

The *Configure or Repair Agents* feature on a Windows CMS, also enables you to install various agents and providers on a ProLiant or Itanium-based system with Windows operating system. It can install:

- HP Insight Management WBEM Providers for Windows Server 2003/2008
- OpenSSH
- HP Version Control Agent (VCA) for Windows
- HP Insight Management Agents for Windows

Related procedures

- Windows CMS
- HP-UX and Linux CMS
- Setting up managed systems

Windows CMS

Configuring managed systems from a Windows Central Management Server

To run *Configure or Repair Agents* remotely against a system, you must have authorization to run the Configure or Repair Agents tool. You must have administrator privileges for Windows systems on the target systems to configure or repair the agent settings. You must have root privileges for HP-UX and Linux systems.

To run Configure or Repair Agents remotely against HP-UX and Linux target, you must have SSH installed on them.

To configure agents remotely:

1. Select **Configure**→**Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.

Note: The **Step 1: Verify Target Systems** page appears if the targets are selected before selecting a tool.

2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Note: If you plan to **Configure secure shell (SSH) access** on a Windows target system, the account specified must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group if applicable.

Configure or Repair Agents

Target: pbdemo Maximize ?

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:

Password:

Password (Verify):

Domain:

[< Previous](#) [Next >](#)

4. From the **Step 2: Enter credentials** page:
 - a. In the **User name** field, enter the system administrator name.
 - b. In the **Password** field, enter the system administrator's password for the user name previously entered.

- c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain if you are using a domain account.
- Note:** The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

5. Click **Next**. The **Step 3: Install Providers and Agents (Optional)** page appears.



6. You can install Insight Management Agents or providers, either *Web-Based Enterprise Management* or *Simple Network Management Protocol*, on managed systems so HP SIM can collect inventory and status information from these systems and receive event notifications from the systems. Installation is supported only on ProLiant or Itanium-based servers with Windows operating system.

From the **Step 3: Install Providers and Agents (Optional)** page:

- a. Select **Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** to install *WBEM* or *WMI* providers on Windows managed systems.
- b. Select **Install SNMP Agent (HP Insight Management Agents) for Windows** to install the *SNMP* agent on Windows managed systems. This Insight Management Agent allows network monitoring and control.
- c. Select **Install Open SSH** to install *OpenSSH* on Windows managed systems. See “Installing OpenSSH” for more information.
- d. Select **Install the Version Control Agent (VCA)** to install the *HP Version Control Agent*, (VCA) on Windows managed systems. The VCA enables you to view the HP software installed on a system and when updates for the software are available in the repository. See “About the Version Control Agent” for more information.

HP SIM determines the type of agent/provider to install based on the system type, subtype, and operating system description of the system.

Table 12-1 Version Support Matrix for components used for install.

Supported systems	HP WBEM Provider	HP ProLiant Agent	Open SSH	Version Control Agent
Unknown	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (64 bit)	7.90 (64 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating systems (2000)	Not supported	7.60 (32 bit)	3.71	2.1.8

Supported systems	HP WBEM Provider	HP ProLiant Agent	Open SSH	Version Control Agent
Itanium-based systems with Windows operating system (2003)	Not supported	5.1.10	3.71	2.1.7.770

System Management Homepage version 2.1.7 is also installed, if necessary, with these agents.



NOTE: If you wish to install a 64 bit agent or provider, make sure the target system is identified as a 64 bit system in HP SIM.

If your system is not correctly identified, go to **System Page** → **Edit System Properties**. Select the correct system type, subtype and enter the operating system description manually.

Edit System Properties

blade31
Go back to blade31

System Information

Identification

Preferred system name: [Restore default name](#)

Prevent the Discovery process from changing this system name

Serial number:

Product Description

System type:

System subtype 1:

System subtype 2:

System subtype 3:

System subtype 4:

System subtype 5:

System subtype 6:

System subtype 7:

System subtype 8:

Product model:

Hardware description:

Operating system description:

Example: Installing Insight Management Agents on a ProLiant Windows 64 bit system:

1. Select system **Type**: server.
2. Select system **subtype 1**: ProLiant
3. Enter operating system description as Microsoft Windows Server 2003, x64 Enterprise Edition Service Pack 1 or the correct operating system description of your system.

If you want to configure the agents after installing, select the force reboot option. This allows the newly installed component to be completely initialized before configuring it.

Note: Installation with reboot typically takes about 8 minutes to complete.

7. Click **Next**. The **Step 4: Configure or Repair Agents** page appears.

Configure WBEM / WMI [Learn More..](#)

Create subscription to WBEM events

Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM event lists.

Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system. *This will deploy a WBEM certificate to the managed system. This option is only valid for HP-UX systems.*

Configure a non-administrative account for HP SIM to access WMI data [Learn More..](#)

This option applies only to Windows Systems with HP WBEM Provider installed.
 Administrative accounts can be used without further configuration. If non-administrative access to a managed system is desired, an existing domain account or one local to the managed system can be used by HP SIM to access WMI information over the network.

Enter the credentials for HP SIM to use to access the managed system:

User name:

Password:

Password (Verify):

Domain:

Configure SNMP [Learn More..](#)

Set read community string:

Set traps to refer to this instance of HP Systems Insight Manager. *Note: A ReadWrite string will be created automatically on Windows systems.*

Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM event lists.

Configure secure shell (SSH) access authentication [Learn More..](#)

Host based authentication *Note: All users from this instance of HP SIM will be authenticated on the managed system.*

User based authentication for user: *Each user has to be authenticated on the managed system*

Set Trust relationship to "Trust by Certificate" [Learn More..](#)

This enables HP SIM users to connect to the System Management Homepage, Onboard Administrators, Integrated Lights-Out (version 2 and later), and VCA using the HP SIM certificate for authentication.

Configure Version Control Agent(VCA) [Learn More..](#)

This option applies only to Windows Systems.
 The Version Control Repository Manager (VCRM) contains a repository that stores the software and firmware components used to support Windows and Linux platforms. The VCA can be configured to point to the VCRM, enabling easy version comparison and software updates.

Select the system where the VCRM is installed:

Enter the credentials for the VCA to use to access the VCRM:

User name:

Password:

Password (Verify):

Domain:

Set administrator password for Insight Management Agents version 7.1 or earlier [Learn More..](#)

This option applies only to ProLiant Systems

Password:

Password (Verify):

[< Previous](#) [Schedule](#) [Run Now](#)

8. The **Step 4: Configure or Repair Agents** page enables you to select options to configure the target system.

The following options are available:

- **Configure WBEM / WMI.** This section enables you to configure the target Linux, Windows or HP-UX system to send WBEM indications or events to HP Systems Insight Manager.

For this section, the following must be considered:

- **Create subscription to WBEM events, so that WBEM events will be sent to the CMS.**
- **Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system.**

Note: The indication will appear as an **Informational Event** in the **Event List** of HP SIM. If you do not receive test WBEM indications in the **Event List**, see "Troubleshooting".

Note: This is supported only on HP-UX and Windows managed systems with WBEM provider installed.

- **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system.** This option deploys a WBEM certificate to the managed system and is only valid for HP-UX systems.
- **Configure a non-administrative account for HP SIM to access WMI data.** This option is applicable to Windows systems with HP WBEM providers. The configuration of the managed system will be updated to allow the specified user to access WMI information over the network. This user will be used by HP SIM to read inventory and configuration information from the

system, and will be configured as the WBEM user in the System Protocol Settings. This configuration step is not necessary if HP SIM is configured with a user with administration rights. This user is not created by HP SIM; it should already exist as either a domain user or one local to the managed system.

The user will be added to the "DCOM Users" group on the managed system and will be given read-only access to WMI information, plus read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system and need not have logon rights. A special purpose domain account is recommended, and should be created by the domain administrator.

To enter the credentials for HP SIM to use to access the managed systems:

1. In the **User name** field, enter a user name.
2. In the **Password** field, enter the password for the user's name previously entered.
3. In the **Password (Verify)** field, reenter the password exactly as it was entered in the **Password** field.
4. In the **Domain** field, enter the Windows domain if the target belongs to a domain.

If configuring a non-administrative user is successful, then these credentials are saved as the System Protocol settings for WBEM access in HP SIM.

- **Configure SNMP.** This section enables you to configure *SNMP* settings.

For this section, the following must be considered:

- a. Select **Set read community string** to specify a community string. By default, HP SIM's first community string, that is not public, appears in the field. If no community string exists in HP SIM, you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you need not set this option. HP-UX enables read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over 30 characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP SIM over the network. Linux and HP-UX systems do not require a **Read Write** community string; hence the **Read Write** community is added on Windows systems only.

- b. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This setting enables the target systems to send *SNMP traps* to this instance of HP SIM.

- c. Select **Send a sample SNMP trap to this instance of the HP SIM to test that events appear in HP SIM event lists** to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

Note: A test trap can only be sent from a Windows managed system with HP Insight Management Agent installed. If you attempt to run this task on a Linux or HP-UX managed system, a message displays indicating the operation is not supported.

Note: The trap will appear as a Generic Trap from the system. This event will appear as an **Informational Event** in the **Event List** of HP SIM.

- **Configure secure shell (SSH) access.** Select this option to configure SSH access on managed systems. If this option is selected, you must select one of the following options:
 - **Host based authentication for SSH.**

Note: For this option to work, the user name and password provided in step 2 must be an administrative level account. For Linux or HP-UX targets, it must be the "root" account and password.
 - **Each user has to be authenticated on the managed system**

Note: If you do not want all users that have login access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** as done in step three or by selecting the tool under **Deploy**→**Deploy Drivers**→**Firmware and Agents**→**Install Open SSH**.
- **Set Trust relationship to "Trust by Certificate".** Select this option to configure systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP SIM system certificate to the target system's trusted certificate directory. This option enables HP SIM users to connect to the System Management Homepage using the certificate for authentication. See "Trusted certificates" for more information.

Note: If you experience problems later setting the trust status on a Linux managed system, see "Troubleshooting" under **Certificate Problems** for assistance.

You can configure Single Sign-On (SSO) to management processors for Onboard Administrators and for Integrated Lights-Out 2 (iLO2). To configure SSO, select **Set Trust Relationship**. After SSO is configured, you are not continually prompted to supply the login credentials for the management processor.

Note: For systems with Management HTTP Server 4.x and earlier, Configure or Repair Agents adds the Administrator password in the Management HTTP Server store and modifies the SNMP settings but cannot change trust relationship information because Management HTTP Server 4.x and earlier did not deploy trust relationships.
- **Configure Version Control Agent (VCA).** Select this option to configure the VCA to point to the HP Version Control Repository Manager (VCRM), where the repository of software and firmware is located, enabling version comparison and software updates. This option is available only for Windows systems. This section can be accessed in the **Configuration** section of all CMS systems including Windows, Linux and HP-UX.

To configure VCA:

 1. In the **Select the system where the VCRM is installed** field, select the server where the VCRM is installed from the dropdown list.
 2. In the **User Name** field, enter the user name to access the VCRM. This user cannot be the default "Administrator" user. It has to be an user with administrative privileges.
 3. In the **Password** field, enter the password to access the VCRM.
 4. In the **Confirm Password** field, reenter the password for the VCRM just as you entered it in the **Password** field.
- **Set administrator password for Insight Management Agents version 7.1 or earlier.** Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Do not set this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you need not set this option.

If this option is selected, you must complete the following steps:

- a. In the **Password** field, enter the new administrator password.
 - b. In the **Confirm Password** field, reenter the new administrator password exactly as you entered it previously.
9. Click **Run Now**. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The log results indicate whether the repair attempt was successful.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed and for some to fail.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout tab.** This tab displays the output text information.
- **The stderr tab.** This tab displays information if the executable experienced an error.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

- a. Click **View Printable Report**.
An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.
 - b. Select which report to display.
 - c. Click **OK** to display the report, or click **Cancel** to return to the **View Task Results** page.
10. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents tool can be configured to run automatically on a schedule, or you can run it manually. Only one instance of Configure or Repair Agents tool can run at a time.

Related Topics

Related topics

- ▲ [Configuring or repairing agents](#)

HP-UX and Linux CMS

Configuring managed systems from a HP-UX and Linux Central Management Server

To run *Configure or Repair Agents* remotely against a system, you must have authorization to run the Configure or Repair Agents tool. You must have administrator privileges for Windows systems on the target systems to configure or repair the agent settings. You must have root privileges for Linux and HP-UX systems.

To run Configure or Repair Agents remotely against a system, you must have SSH installed on Windows, HP-UX, and Linux target systems.

To configure agents remotely:

1. Select **Configure**→**Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.
Note: The **Step 1: Verify Target Systems** page appears if the targets are selected before selecting a tool.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:	<input type="text"/>
Password:	<input type="password"/>
Password (Verify):	<input type="password"/>
Domain:	<input type="text"/>

[< Previous](#)[Next >](#)

4. From the **Step 2: Enter credentials** page:
 - a. In the **User name** field, enter the system administrator name.
 - b. In the **Password** field, enter the system administrator's password for the user name previously entered.
 - c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

5. Click **Next**. The **Step 3: Configure or Repair Agents** page appears.

Configure WBEM and SNMP settings, SSH authentication mode, Version Control Agent settings, trust relationships, and for Insight Management Agents version 7.1 or earlier, the administrator password.

Configure WBEM / WMI [Learn More..](#)

- Create subscription to WBEM events
- Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM event lists.
- Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system. *This will deploy a WBEM certificate to the managed system. This option is only valid for HP-UX systems.*
- Configure a non-administrative account for HP SIM to access WMI data [Learn More..](#)

This option applies only to Windows Systems with HP WBEM Provider installed.

Administrative accounts can be used without further configuration. If non-administrative access to a managed system is desired, an existing domain account or one local to the managed system can be used by HP SIM to access WMI information over the network.

Enter the credentials for HP SIM to use to access the managed system:

User name:

Password:

Password (Verify):

Domain:

Configure SNMP [Learn More..](#)

- Set read community string:
- Set traps to refer to this instance of HP Systems Insight Manager. *Note: A ReadWrite string will be created automatically on Windows systems.*
- Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM event lists..

Configure secure shell (SSH) access authentication [Learn More..](#)

- Host based authentication *Note: All users from this instance of HP SIM will be authenticated on the managed system.*
- User based authentication for user: *Each user has to be authenticated on the managed system*

Set Trust relationship to "Trust by Certificate" [Learn More..](#)

This enables HP SIM users to connect to the System Management Homepage, Onboard Administrators, Integrated Lights-Out (version 2 and later), and VCA using the HP SIM certificate for authentication.

Configure Version Control Agent(VCA) [Learn More..](#)

This option applies only to Windows Systems.

The Version Control Repository Manager (VCRM) contains a repository that stores the software and firmware components used to support Windows and Linux platforms. The VCA can be configured to point to the VCRM, enabling easy version comparison and software updates.

Select the system where the VCRM is installed:

Enter the credentials for the VCA to use to access the VCRM:

User name:

Password:

Password (Verify):

Domain:

Set administrator password for Insight Management Agents version 7.1 or earlier [Learn More..](#)

This option applies only to ProLiant Systems

Password:

Password (Verify):

[< Previous](#) [Schedule](#) [Run Now](#)

6. The **Step 3: Configure or Repair Agents** page enables you to select options to configure the target system.

The following options are available:

- **Configure WBEM / WMI.** This section enables you to configure the target Linux, Windows or HP-UX system to send WBEM indications or events to HP Systems Insight Manager.

For this section, the following must be considered:

- **Create subscription to WBEM events, so that WBEM events will be sent to the CMS.**
- **Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM in the Event list or All Event User Interface for the selected system.**

Note: The indication will appear as an **Informational Event** in the **Event List** of HP SIM. If you do not receive test WBEM indications in the **Event List**, see "Troubleshooting".

Note: This is supported only on HP-UX and Windows managed systems with WBEM provider installed.

- **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system.** This option deploys a WBEM certificate to the managed system and is only valid for HP-UX systems.
- **Configure a non-administrative account for HP SIM to access WMI data.** This option is applicable to Windows systems with HP WBEM providers. The configuration of the managed system will be updated to allow the specified user to access WMI information over the network. This user will be used by HP SIM to read inventory and configuration information from the

system, and will be configured as the WBEM user in the System Protocol Settings. This configuration step is not necessary if HP SIM is configured with a user with administration rights. This user is not created by HP SIM; it should already exist as either a domain user or one local to the managed system.

The user will be added to the "DCOM Users" group on the managed system and will be given read-only access to WMI information, plus read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system and need not have logon rights. A special purpose domain account is recommended, and should be created by the domain administrator.

To enter the credentials for HP SIM to use to access the managed systems:

1. In the **User name** field, enter a user name.
2. In the **Password** field, enter the password for the user's name previously entered.
3. In the **Password (Verify)** field, reenter the password exactly as it was entered in the **Password** field.
4. In the **Domain** field, enter the Windows domain if the target belongs to a domain.

If configuring a non-administrative user is successful, then these credentials are saved as the System Protocol settings for WBEM access in HP SIM.

- **Configure SNMP.** This section enables you to configure *SNMP* settings.

For this section, the following must be considered:

- a. Select **Set read community string** to specify a community string. By default, HP SIM's first community string, that is not public, appears in the field. If no community string exists in HP SIM, you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you need not set this option. HP-UX enables read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over 30 characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP SIM over the network. Linux and HP-UX systems do not require a **Read Write** community string; hence the **Read Write** community is added on Windows systems only.

- b. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This setting enables the target systems to send *SNMP traps* to this instance of HP SIM.

- c. Select **Send a sample SNMP trap to this instance of the HP SIM to test that events appear in HP SIM event lists** to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

Note: A test trap can only be sent from a Windows managed system with HP Insight Management Agent installed. If you attempt to run this task on a Linux or HP-UX managed system, a message displays indicating the operation is not supported.

Note: The trap will appear as a Generic Trap from the system. This event will appear as an **Informational Event** in the **Event List** of HP SIM.

- **Configure secure shell (SSH) access.** Select this option to configure SSH access on managed systems. If this option is selected, you must select one of the following options:
 - **Host based authentication for SSH.**

Note: For this option to work, the user name and password provided in step 2 must be an administrative level account. For Linux or HP-UX targets, it must be the "root" account and password.
 - **Each user has to be authenticated on the managed system**

Note: If you do not want all users that have login access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** as done in step three or by selecting the tool under **Deploy**→**Deploy Drivers**→**Firmware and Agents**→**Install Open SSH**.
- **Set Trust relationship to "Trust by Certificate".** Select this option to configure systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP SIM system certificate to the target system's trusted certificate directory. This option enables HP SIM users to connect to the System Management Homepage using the certificate for authentication. See "Trusted certificates" for more information.

Note: If you experience problems later setting the trust status on a Linux managed system, see "Troubleshooting" under **Certificate Problems** for assistance.

You can configure Single Sign-On (SSO) to management processors for Onboard Administrators and for Integrated Lights-Out 2 (iLO2). To configure SSO, select **Set Trust Relationship**. After SSO is configured, you are not continually prompted to supply the login credentials for the management processor.

Note: For systems with Management HTTP Server 4.x and earlier, Configure or Repair Agents adds the Administrator password in the Management HTTP Server store and modifies the SNMP settings but cannot change trust relationship information because Management HTTP Server 4.x and earlier did not deploy trust relationships.
- **Configure Version Control Agent (VCA).** Select this option to configure the VCA to point to the HP Version Control Repository Manager (VCRM), where the repository of software and firmware is located, enabling version comparison and software updates. This option is available only for Windows systems. This section can be accessed in the **Configuration** section of all CMS systems including Windows, Linux and HP-UX.

To configure VCA:

 1. In the **Select the system where the VCRM is installed** field, select the server where the VCRM is installed from the dropdown list.
 2. In the **User Name** field, enter the user name to access the VCRM. This user cannot be the default "Administrator" user. It has to be an user with administrative privileges.
 3. In the **Password** field, enter the password to access the VCRM.
 4. In the **Confirm Password** field, reenter the password for the VCRM just as you entered it in the **Password** field.
- **Set administrator password for Insight Management Agents version 7.1 or earlier.** Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Do not set this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you need not set this option.

If this option is selected, you must complete the following steps:

- a. In the **Password** field, enter the new administrator password.
 - b. In the **Confirm Password** field, reenter the new administrator password exactly as you entered it previously.
7. Click **Run Now**. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The log results indicate whether the repair attempt was successful.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed and for some to fail.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout tab.** This tab displays the output text information.
- **The stderr tab.** This tab displays information if the executable experienced an error.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

- a. Click **View Printable Report**.
An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.
 - b. Select which report to display.
 - c. Click **OK** to display the report, or click **Cancel** to return to the **View Task Results** page.
8. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents tool can be configured to run automatically on a schedule, or you can run it manually. Only one instance of Configure or Repair Agents tool can run at a time.

Related Topics

Related topics

- ▲ [Configuring or repairing agents](#)

Learn More - Installing the WBEM/WMI Provider for Windows

- **Web-Based Enterprise Management (WBEM)** An Industry initiative to provide management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM client applications. For HP-UX, WBEM is included in the operating system install. For Linux Itanium Processor Family (IPF), if WBEM is not installed, it must be manually installed. Go to the HP Software Depot (<http://www.software.hp.com/>) to download. The WBEM download from the openPegasus website does not include the hardware specific data for HP SIM to manage Linux x86 systems.



NOTE: *Windows Management Instrumentation* (WMI) is the implementation of WBEM from Microsoft. See *WMI* for more information.

NOTE: The WBEM providers cannot be installed on HP-UX or Linux systems.

NOTE: A Common Information Model Object Manager (CIMOM) acts as the interface for communication between WBEM providers and management applications such as HP Systems Insight Manager.

The CMS must have the correct credentials to authenticate to WBEM and WMI. There are two ways to authenticate client certificates:

- Basic authentication to WBEM Services or WMI using user name and password.
- Using the CMS certificate to authenticate is available only for HP-UX WBEM Services 02.05.00, which supports client certificate authentication. Use the Configure or Repair Agents **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system** option to deploy a WBEM certificate to the managed system and is only valid for HP-UX systems.
- **WMI** An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled.

The WMI Mapper Proxy is a configuration setting for WMI. The WMI Mapper receives client CIM/XML WBEM requests and converts the requests to *Windows Management Instrumentation* (WMI) requests. The WMI results are converted to CIM/XML format and returned to the Central Management Server (CMS). The *discovery* and *Identification* task uses the proxies in the WMI Mapper Proxy list to discover whether a *system* is a WMI-enabled system. If the system is WMI-enabled, then the identification information for that system based on that specific proxy is returned.

The WMI Mapper makes it possible to retrieve WMI instrumented data on a Windows machine through WBEM requests. The Windows version of HP SIM installs this WMI Mapper locally so that it can make WMI requests across the network to the systems without the need to install the WMI Mapper on the managed Windows systems.

The WMI Mapper is included in a Typical install of the HP SIM on a Windows CMS (optional in a Custom install) . For HP-UX and Linux-based systems, the WMI Mapper is not available.

Related topics

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols

Related topics

- Global protocols
- Configuring or repairing agents

Learn More - Installing the SNMP Provider for Windows

One of the management protocols supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.

To obtain SNMP:

For Windows systems, if SNMP itself is not installed during the operating system installation, you can install it from the Windows CD using **Add Remove Windows Component** feature.

To install the HP Insight SNMP agents for ProLiant systems running on Linux x86 operating system, go to <http://www.software.hp.com/> and select the ProLiant Support Pack 7.90.



NOTE: The HP Insight SNMP agents cannot be installed on HP-UX systems.

To install the SNMP provider from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install SNMP Agents (HP ProLiant Insight Management Agents) for Windows**.

To configure the read community string on the CMS, select **Options**→**Protocol Settings**→**System Protocol Settings** from the HP SIM menu. To configure the read community string for multiple systems, select **Options**→**Protocol Settings**→**Global Protocol Settings** and set the read community string.

Related topics

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols

Related topics

- Global protocols
- Configuring or repairing agents

Learn More - Installing OpenSSH from CRA

- **Secure Shell (SSH)** SSH is used to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

You can download SSH from the HP Software Depot (<http://www.software.hp.com/>).

- **OpenSSH** A set of network connectivity tools providing encrypted communication sessions over a computer network using SSH. It was created as an open source alternative to the proprietary SSH software suite offered by SSH Communications Security.

You can download OpenSSH from the HP Software Depot (<http://www.software.hp.com/>).

Related procedures

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols
- Deploying OpenSSH to multiple systems using RDP
- Installing OpenSSH

Related topics

- Global protocols
- Configuring or repairing agents

Learn More - Installing the Version Control Agent

In HP Systems Insight Manager (HP SIM), the software status indicates both the availability of software updates and how critical they are. If HP Version Control Agent (VCA) is installed on the system, clicking the software status icon for that system displays HP Version Control Agent Software Inventory page.

To update managed servers with the most current software, HP SIM provides software update capabilities that use the *HP Version Control Agent (VCA)* and *HP Version Control Repository Manager (VCRM)*.

For Windows operating systems, you must install the *HP Insight Management Agent 5.40* or later to obtain any inventory data. For Linux operating systems, you must install *HP Server Management Application and Agents (hpsm RPM) 7.00* or later to obtain any inventory data. HP recommends installing the current version that is in the same *HP ProLiant and Integrity Support Pack* as the VCA.



NOTE: If the Insight Management Agents are not installed, *software inventory* cannot be collected by the VCA. However, the VCA can still be used to install software.

HP Version Control Agent

The *HP Version Control Agent* (VCA) is an *HP Insight Management Agent* that is installed on a system to enable you to view the HP software and firmware that is installed on that system. The VCA can be configured to point to a *repository* being managed by the *HP Version Control Repository Manager* (VCRM), enabling easy version comparison and software updates from the repository to the system on which the VCA is installed.

The VCA provides *version control* and system update capabilities for a single HP system. The VCA determines system software status by comparing each *component* installed on the local system with the set of individual components or a specified ProLiant or Integrity Support Pack listed in the VCRM. While browsing to the VCA, you can update individual components or an entire ProLiant or Integrity Support Pack by clicking the install icon located next to the system software status icon.

HP Version Control Repository Manager

The *HP Version Control Repository Manager* (VCRM) is an HP Insight Management Agent that manages a directory of HP software and firmware components. The VCRM can be used without the *HP Version Control Agent* (VCA) to provide a listing of available software and firmware to load on the local machine. The VCRM is part of the HP Foundation Pack.

The VCRM is designed to be used in a one-to-many configuration with a VCA installed on each managed HP system to manage installed HP software and firmware. In conjunction with HP Systems Insight Manager (HP SIM), the VCRM, and VCAs provide enterprise-wide management of HP software and firmware on HP ProLiant and Integrity systems. Alone, the VCRM can be used to catalog and manage a repository of ProLiant and Integrity Support Packs and individual software and firmware from HP for HP ProLiant and Integrity systems.



NOTE: Although it is possible to install an *HP ProLiant and Integrity Support Pack* or *component* to the local machine using the VCRM, you cannot install the software on remote servers unless the VCA has been installed on the remote server and the install is initiated using the VCA.

Related topics

- [Version Control](#)
- [About the Version Control Agent](#)
- [About the Version Control Repository Manager](#)

Related procedures

- [Setting protocols and credentials for a system or groups of systems](#)
- [Setting protocols for a single system](#)
- [Setting global protocols](#)

Related topics

- [Global protocols](#)
- [Configuring or repairing agents](#)

Learn More - Configuring WBEM/WMI

Configuring *Web-Based Enterprise Management* (WBEM) enables you to configure the target Linux, Windows, or HP-UX system to send WBEM indications or events to HP Systems Insight Manager (HP SIM).

You can add and remove subscriptions to WBEM indication events through the GUI. You can also add and remove subscriptions to WBEM indication events from the *command line interface* (CLI). If you do not subscribe to WBEM indication events for a system that supports them, any WBEM events that occur will not appear on the event table view page.

Related topic

- ▲ [WBEM indications](#)

Learn More - Configuring a non-administrative account for HP SIM to access WMI data

Configure a non-administrative account for HP SIM to access WMI data. This option is applicable to Windows systems with HP WBEM providers. The configuration of the managed system will be updated to allow the specified user to access WMI information over the network. This user will be used by HP SIM to read inventory and configuration information from the system, and will be configured as the WBEM user in the System Protocol Settings. This configuration step is not necessary if HP SIM is configured with a user with administration rights. This user is not created by HP SIM; it should already exist as either a domain user or one local to the managed system.

The user will be added to the "DCOM Users" group on the managed system and will be given read-only access to WMI information, plus read-write permissions to the HPQ name space. This user does not need to be an administrator of the managed system and need not have logon rights. A special purpose domain account is recommended, and should be created by the domain administrator.

Related topics

- [Windows CMS](#)
- [HP-UX and Linux CMS](#)

Learn More - Configuring SNMP

Select **Set read community string** to specify a community string. By default, HP SIM's first community string, that is not public, appears in the field. If no community string exists in HP SIM, you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you need not set this option. HP-UX enables read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed systems do not always enable SNMP communication between themselves and a remote host. This setting is modified to enable the instance of the HP SIM system to communicate using SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over 30 characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP SIM over the network. Linux and HP-UX systems do not require a **Read Write** community string; hence the **Read Write** community is added on Windows systems only.

Select **Send a sample SNMP trap to this instance of the HP SIM to test that events appear in HP SIM event lists** to verify that SNMP events appear in the HP SIM events list.

To successfully send a test trap, you must configure target systems to send a trap to this instance.

Note: A test trap can only be sent from a Windows managed system with HP Insight Management Agent installed. If you attempt to run this task on a Linux or HP-UX managed system, a message displays indicating the operation is not supported.

Related topics

- [Windows CMS](#)
- [HP-UX and Linux CMS](#)

Learn More - Configuring SSH

If you select **Configure secure shell (SSH) access**, you must select one of the following:

- **Host based authentication for SSH.**

Note: For this option to work, the user name and password provided in step 2 must be an administrative level account. For Linux or HP-UX targets, it must be the "root" account and password.

- **Each user has to be authenticated on the managed system**

Note: If you do not want all users that have login access to HP SIM to run the tool and you would like to control which users need to have access, this option is more secure.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** as done in step three or by selecting the tool under **Deploy**→**Deploy Drivers**→**Firmware and Agents**→**Install Open SSH**.

Related topics

- [Global protocols](#)
- [Configuring or repairing agents](#)

Learn More - Configuring VCA

Configure Version Control Agent (VCA). Select this option to configure the VCA to point to the HP Version Control Repository Manager (VCRM), where the repository of software and firmware is located, enabling version comparison and software updates. This option is available only for Windows systems. This section can be accessed in the **Configuration** section of all CMS systems including Windows, Linux and HP-UX.

Related topics

- [Version Control](#)
- [About the Version Control Agent](#)
- [Configuring or repairing agents](#)

Learn More - Setting the administrator password for Insight Management Agents

Set administrator password for Insight Management Agents version 7.1 or earlier. Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Do not set this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you need not set this option.

Related topic

- ▲ [Configuring or repairing agents](#)

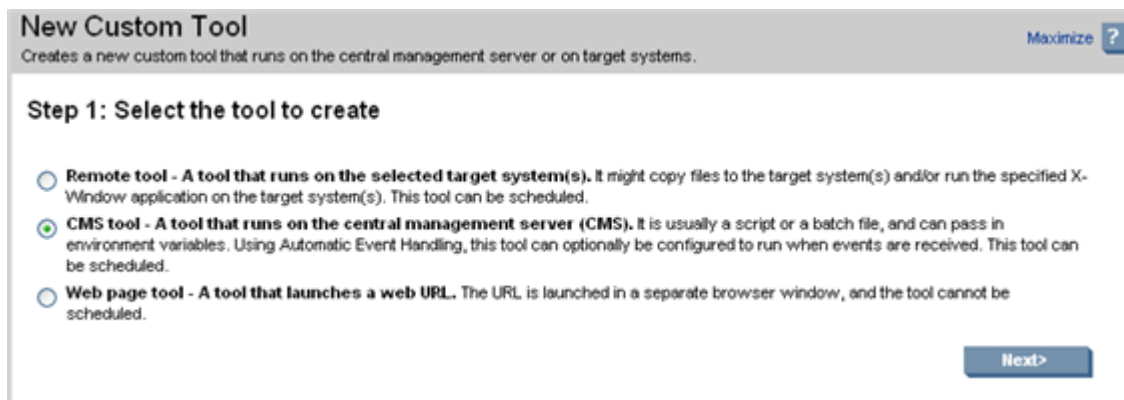
Custom tools

Custom tools are executed on the *Central Management Server (CMS)* and on target systems. They are intended to be scripts, batch files, or executables that can reference environment variables set by the tool in order to access system or event information. For example, creating a custom tool to launch Notepad.

Single-system aware (SSA), *multiple-system aware* (MSA), and *Web-launch aware* (WLA) tools can be created and launched. You can create the following types of custom tools:

- **Remote tool** A tool that runs on selected target systems. It might copy files to the target systems or run specific X-Window applications on the target systems. This tool can be scheduled.
- **CMS tool** A tool that runs on the CMS. It is usually a script or batch file and can pass in environment variables. Using Automatic Event Handling, this tool can optionally be configured to run when events are received. This tool can be scheduled.
- **Web page tool** A tool that launches a web URL. The URL is launched in a separate browser window on the Central Management Server. This tool cannot be scheduled.

Remote tools require the use of environment variables which are parameters passed to the launched application to make it perform as expected. See “[Environment variables for custom tools](#)” for more information. The launch command string includes system variables and user-defined variables for your application. For example, you could pass an environment variable that runs a script to check on the status of your mail server.



DOS environment variables are supported in the custom tool parameters and work as parameters on the **New Custom Tool** page or the **Manage Custom Tools** page. However, they must be surrounded by double percent (%) signs. For example, to pass in the *NOTICELABEL* environment variable as a parameter, it should be entered as `%%NOTICELABEL%%` on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single percent (%) sign should precede and succeed the environment variable name. See “[Custom tools reference](#)” for a list of other substitutable variables.

Custom tools that you create are displayed under the **Tools**→**Custom Tools** menu option.

You have multiple scheduling options. See “[Scheduling a task](#)” for more information about scheduling options.



IMPORTANT: The application must be able to execute in the security context provided to HP Systems Insight Manager (HP SIM) (the default is LocalSystem).

- **New Custom Tools** Select **Tools**→**Custom Tools**→**New Custom Tool**. The **New Custom Tool** page appears.
- **Manage Custom Tools** Select **Tools**→**Custom Tools**→**Manage Custom Tools**. The **Manage Custom Tools** page appears.

Use custom tools that run on target SSA systems create a temporary `.XML` tool definition file under `/var/tmp`, then load the tool with the `mxtool -af filename`. You only enter data in required fields.



WARNING! If you define a custom tool to run as root, any user authorized to run the tool might gain full access to the managed system, depending on how you define the command, and what its capabilities are.

Otherwise, the tool runs as the HP Systems Insight Manager (HP SIM) user and that user's SSH public key must be configured on the managed system using the `mxagentconfig` command.

Menu placement

A string in the form *base/submenu/subsubmenu* can be used to place custom tools in specific menu locations.

Menu level	Example
<i>top-level-menu</i>	Tools
<i>top-level-menu/first-level-cascade</i>	Tools Custom Tools
<i>top-level-menu/first-level-cascade/second-level-cascade</i>	Tools Custom Tools <i>My Tools</i>

To place a tool under **Tools**→**Custom Tools**, the **Menu placement** field should have an entry like **Tools|CustomTools**.

By default, if the **Menu placement** field is left blank, the tools are placed under **Tools**→**Custom Tools**.

Related procedures

- Creating a new remote tool
- Creating a new CMS tool
- Creating a new web page tool
- Managing custom tools

Related topic

- ▲ Environment variables for custom tools

Creating a new remote tool

Create a remote tool that runs on selected target systems. This tool might copy files to the target systems or run a specified X-Window application on target systems. This tool can be scheduled.

New Custom Tool Maximize ?

Creates a new custom tool that runs on the central management server or on target systems.

Step 2: Describe how the new custom tool will work.

Tool Type: Remote tool

A custom tool that runs a command on each selected target will be created. SSH must be installed and configured on each target in order for the tool to run.

Required field *.

Tool Parameters:

Name of the tool, e.g. My Custom Tool *

Description, e.g. This is My Custom Tool:

Help comment, e.g. To use this tool, type...:

Menu placement: ([Help on menu placement](#))

The user account on the target system that will be used to run this tool:

Logged-in user

Special user ("root" for Unix and Linux systems, "Administrator" for Windows systems) †

Specific user †

SSH must be configured to allow access for this user; see [Configure/Repair Agent Settings](#) or `mxagentconfig`.

†SECURITY WARNING: If the tool runs as "root" or "Administrator" on the target system, any user who runs this tool may be able to gain full access to that system. Carefully select options and parameters to appropriately limit this tool.

The maximum number of targets the tool can select when creating the task (if "None" is selected, the target selection page will not be displayed.):

None

One

Unlimited

Copy files to the target systems

Source path of the file on the central management server (must be a fully qualified path): *

Destination path for the file on the target system (must be a fully qualified path): *

Command with parameters: ([Help on substitutable parameters](#)) *

Command output format: *

To create a custom remote tool:

1. Select **Tools**→**Custom Tools**→**New Custom Tool**. The **New Custom Tool** page appears.
2. Select **Remote tool**.
3. Click **Next**. The **Describe how the new custom tool will work** page appears with the tool type and description displayed.
4. Under **Tool Parameters**, enter the following information:
 - a. In the **Name** field, enter the command name. Custom tool names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Subsequent characters can be letters, digits, spaces, or any of the following: "-", ".", "(", ")", or "_".
 - b. In the **Description** field, enter the necessary information for the application.
 - c. In the **Help comments** field, enter any comments for the application.
 - d. In the **Menu placement** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:

`c:\custom code\romflash.bat`

5. Specify the user account on the target system that will be used for the tool. Select one of the following options:
 - **Logged-in user** Execution of the tool will be whatever user is logged in.
 - **Special user ("root" for UNIX and Linux systems, "Administrator" for Windows systems)** Execution of the tool will substitute Administrator for targets running Windows and root targets with targets running Linux and HP-UX. The tool will not run on targets with an unknown operating system.
 - **Specific user** Execution of the tool will be under the specified user account.
6. Specify the maximum number of targets the tool can select when creating the task. Select from the following:
 - **None** If none is selected, the target selection page is not displayed.
 - **One** If one is selected, the execution of the tool will be on only one target system.
 - **Unlimited** If unlimited is selected, the tool can be executed multiple target systems.
7. Select **Copy files to the target systems**.
 - a. (Optional) Click **Delete** to delete a specified file.
 - b. (Optional) Click **Add** to add additional files.
8. Enter the **Command with parameters** field.

Note: The UI supports only nine parameters. If you enter more than nine parameters, the last parameter is displayed as **Zero(0)** on the **Task Results** page.
9. Under **Command output format**, select from the following:
 - Standard output
 - X-Window
10. To prompt the user for input at the time they choose this tool to be run or scheduled, enter up to 10 labels that can be used to ask for input. You can use the substitution parameters %1, %2, through %10 in your command line to access the values they enter.
 - a. (Optional) Select **Required (user must enter data)** to require the user to enter data.
 - b. (Optional) Select **Private (masks the data with *)** to mask the user input.
11. Select if the tool can be scheduled.
12. Click **OK** to add the new tool to the **Custom Tools** menu and access the **Manage Custom Tools** page, or click **Previous** to return to the previous page to select another type of custom tool.



NOTE: New custom tool tools are located under **Tools**→**Custom Tools**.

Related procedures

- [Creating a new CMS tool](#)
- [Creating a new web page tool](#)
- [Managing custom tools](#)

Related topic

- ▲ [Custom tools](#)

Creating a new CMS tool

A CMS tool usually runs on the Central Management Server (CMS) and is usually a script or batch file that can pass environment variables. Using automatic event handling, this tool can optionally be configured to run when specific events are received. This tool can be scheduled and is selected by default when accessing the **New Custom Tool** page. See “Events” for more information about automatic event handling. See “Environment variables for custom tools” for more information about the environment variables that can be passed. In previous releases of HP Systems Insight Manager (HP SIM), CMS tools were called custom tools.

New Custom Tool Maximize ?

Creates a new custom tool that runs on the central management server or on target systems.

Step 2: Describe how the new custom tool will work.

Tool Type: CMS tool

A custom tool that launches an application or a script on the central management server (CMS) will be created.

Required field *.

Tool Parameters:

Name of the tool, e.g. My Custom Tool *

Description, e.g. This is My Custom Tool:

Help comment, e.g. To use this tool, type...:

Menu placement: ([Help on menu placement](#))

The user account on the target system that will be used to run this tool:

Logged-in user

Special user ("root" for Unix and Linux systems, "Administrator" for Windows systems) †

Specific user †

SSH must be configured to allow access for this user; see [Configure/Repair Agent Settings](#) or `mxcagentconfig`.

†SECURITY WARNING: If the tool runs as "root" or "Administrator" on the target system, any user who runs this tool may be able to gain full access to that system. Carefully select options and parameters to appropriately limit this tool.

The maximum number of targets the tool can select when creating the task (If "None" is selected, the target selection page will not be displayed.):

None

One

Unlimited

Command with parameters: ([Help on substitutable parameters](#)) *

Environment variables (Optional): In addition to the standard environment variables available from HP SIM ([More information](#)), you can also create your own environment variables to pass to this tool.

Name Value

Tool can be scheduled

To create a custom Central Management Server tool:

1. Select **Tools**→**Custom Tools**→**New Custom Tool**. The **New Custom Tool** page appears.
2. Select **CMS tool**.
3. Click **Next**. The **Describe how the new custom tool will work** page appears with the tool type and description displayed.
4. Under **Tool Parameters**, enter the following information:
 - a. In the **Name** field, enter the command name. Custom tool names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Subsequent characters can be letters, digits, spaces, or any of the following: "-", ".", "(", ")", or "_".
 - b. In the **Description** field, enter the necessary information for the application.
 - c. In the **Help comments** field, enter any comments for the application.
 - d. In the **Menu placement** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:

```
c:\custom code\romflash.bat
```

5. Specify the user account on the target system that will be used for the tool. Select one of the following options:
 - Logged-in user
 - Special user ("root" for UNIX and Linux systems, and "Administrator" for Windows systems)
 - Specific user
6. Enter the **Command with parameters** field.
7. (Optional) Enter the **Environment variables** for the tool. See "Environment variables for custom tools" for a list of variables available from HP Systems Insight Manager (HP SIM).
 - (Optional) Click **Delete** to delete a specified variable.
 - (Optional) Click **Add** to add additional variables.

DOS environment variables are supported in the custom tool parameters and work as parameters on the **New Custom Tool** page or the **Manage Custom Tools** page. However, they must be surrounded by double percent (%) signs. For example, to pass in the *NOTICELABEL* environment variable as a parameter, it should be entered as *%%NOTICELABEL%%* on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single percent (%) sign should precede and succeed the environment variable name. See "Custom tools reference" for a list of other substitutable variables.
8. Select **Tool can be scheduled** if the tool can be scheduled.
9. Click **OK** to add the new tool to the **Custom Tools** menu and access the **Manage Custom Tools** page, or click **Previous** to return to the previous page to select another type of custom tool.



NOTE: New custom tool tools are located under **Tools**→**Custom Tools**.

Related procedure

- ▲ [Editing a CMS tool](#)

Related topics

- [Custom tools](#)
- [Managing custom tools](#)

Creating a new web page tool

Use this tool to create a tool that integrates a Web application or website. All tools are automatically launched into a separate browser window. For example, to add a path to the HP website, add the URL: <http://hp.com>. To add a link to the site on a selected system, add a URL such as: <https://%n:2381>. The target system is substituted for the %n when the tool is launched. The resulting command launches the System Management Homepage on the target system. This tool creates a temporary XML tool definition file under `/var/tmp` then loads it with the command `mxtool -af filename`. You only need to enter data into the required fields.

This tool is available on Linux and HP-UX systems only.

1. Select **Tools**→**Custom Tools**→**New Custom Tool**. The **New Custom Tool** page appears.
2. Select **Web page tool**.
3. Click **Next**. The **Describe how the new custom tool will work** page appears with the tool type and description displayed.
4. Under **Tool Parameters**, enter the following information:
 - a. In the **Name** field, enter the command name. Custom tool names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Subsequent characters can be letters, digits, spaces, or any of the following: "-", ".", "(", ")", or "_".
 - b. In the **Description** field, enter the necessary information for the application.
 - c. In the **Help comments** field, enter any comments for the application.
 - d. In the **Menu placement** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:


```
c:\custom code\romflash.bat
```
5. Specify the user account on the target system that will be used for the tool. Select one of the following options:
 - Logged-in user
 - Special user ("root" for UNIX and Linux systems, and "Administrator" for Windows systems)
 - Specific user
6. Specify the maximum number of targets the tool can select when creating the task. Select from the following:
 - None
If none is selected, the target selection page is not displayed.
 - One
 - Unlimited
7. Enter the **URL to the site or application to launch**.
8. Enter the format of how target systems are passed to the URL.
9. Click **OK** to add the new tool to the **Custom Tools** menu and access the **Manage Custom Tools** page, or click **Previous** to return to the previous page to select another type of custom tool.



NOTE: New custom tool tools are located under **Tools**→**Custom Tools**.

Related procedures

- [Creating a new remote tool](#)
- [Creating a new CMS tool](#)

Related topics

- [Custom tools](#)
- [Managing custom tools](#)

Managing custom tools

The **Manage Custom Tools** page displays all the custom tools created through the **New Custom Tool** feature. The **Manage Custom Tools** page displays a table listing all custom tools and information on each tool. The table includes:

- Selection column
- Name
- Description
- Command

- Run as user
- Automatic Event Handling

The following options are available for managing custom tools:

- “New”
- “Edit”
- “View tool definition”
- “Run Now/Schedule”
- “Delete”

New

This option enables you to create a new custom tool and opens the **Select the tool to create** page.

Edit

This option enables you to edit an existing custom tool. To edit a tool, select the tool, and then click **Edit**. The **Edit Custom Tool Details** section appears. All fields can be edited and environment variables can be added and deleted.

View tool definition

This option displays the XML code for the tool and is not enabled if more than one tool is selected.

Run Now/Schedule

This option runs the tool immediately. If the tool can be scheduled, the schedule a task page is displayed. You can schedule when and how often the tool runs.

See “Scheduling a task” or “Running a scheduled task” for more information.

Delete

This option deletes selected tools. Deleting a tool removes it from the **Manage Custom Tools** page and from the system.



NOTE: If a tool being deleted is dependent on a task, an alert displays with the list of tasks associated with the tool.

Related procedures

- Editing a remote tool
- Editing a CMS tool
- Editing a web page tool

Related topic

- ▲ Custom tools

Editing a remote tool

All fields are optional:

1. Select **Tools**→**Custom Tools**→**Manage Custom Tools**. The **Manage Custom Tools** page appears.
2. Select the tool to edit, and then click **Edit**. The **Describe how the new custom tool will work** page appears with the tool type and description displayed.
3. Under **Tool Parameters**, enter the following information:
 - a. In the **Name** field, enter the command name. Custom tool names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Subsequent characters can be letters, digits, spaces, or any of the following: “-”, “.”, “(”, “)” or “_”.
 - b. In the **Description** field, enter the necessary information for the application.

- c. In the **Help comments** field, enter any comments for the application.
 - d. In the **Menu placement** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:

```
c:\custom code\romflash.bat
```
4. Specify the user account on the target system that will be used for the tool. Select one of the following options:
 - **Logged-in user** Execution of the tool will be whatever user is logged in.
 - **Special user ("root" for UNIX and Linux systems, "Administrator" for Windows systems)** Execution of the tool will substitute Administrator for targets running Windows and root targets with targets running Linux and HP-UX. The tool will not run on targets with an unknown operating system.
 - **Specific user** Execution of the tool will be under the specified user account.
5. Specify the maximum number of targets the tool can select when creating the task. Select from the following:
 - **None** If none is selected, the target selection page is not displayed.
 - **One** If one is selected, the execution of the tool will be on only one target system.
 - **Unlimited** If unlimited is selected, the tool can be executed multiple target systems.
6. Select **Copy files to the target systems**.
 - a. (Optional) Click **Delete** to delete a specified file.
 - b. (Optional) Click **Add** to add additional files.
7. Enter the **Command with parameters** field.

Note: The UI supports only nine parameters. If you enter more than nine parameters, the last parameter is displayed as **Zero(0)** on the **Task Results** page.
8. Under **Command output format**, select from the following:
 - Standard output
 - X-Window
9. To prompt the user for input at the time they choose this tool to be run or scheduled, enter up to 10 labels that can be used to ask for input. You can use the substitution parameters %1, %2, through %10 in your command line to access the values they enter.
 - a. (Optional) Select **Required (user must enter data)** to require the user to enter data.
 - b. (Optional) Select **Private (masks the data with *)** to mask the user input.
10. Select if the tool can be scheduled.
11. Click **OK** to add the new tool to the **Custom Tools** menu and access the **Manage Custom Tools** page, or click **Previous** to return to the previous page to select another type of custom tool.



NOTE: New custom tool tools are located under **Tools**→**Custom Tools**.

Related procedures

- Editing a remote tool
- Deleting a custom tool
- Viewing tool definition files

Related topics

- Custom tools
- Managing custom tools

Editing a CMS tool

All fields are optional.

1. Select **Tools**→**Custom Tools**→**Manage Custom Tools**. The **Manage Custom Tools** page appears.
2. Select the tool you want to edit, and then click **Edit**. The **Describe how the new custom tool will work** page appears with the tool type and description displayed.
3. Under **Tool Parameters**, enter the following information:
 - a. In the **Name** field, enter the command name. Custom tool names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Subsequent characters can be letters, digits, spaces, or any of the following: "-", ".", "(", ")", or "_".
 - b. In the **Description** field, enter the necessary information for the application.
 - c. In the **Help comments** field, enter any comments for the application.
 - d. In the **Menu placement** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:


```
c:\custom code\romflash.bat
```
4. Specify the user account on the target system that will be used for the tool. Select one of the following options:
 - Logged-in user
 - Special user ("root" for UNIX and Linux systems, and "Administrator" for Windows systems)
 - Specific user
5. Enter the **Command with parameters** field.
6. (Optional) Enter the **Environment variables** for the tool. See "Environment variables for custom tools" for a list of variables available from HP Systems Insight Manager (HP SIM).
 - (Optional) Click **Delete** to delete a specified variable.
 - (Optional) Click **Add** to add additional variables.

DOS environment variables are supported in the custom tool parameters and work as parameters on the **New Custom Tool** page or the **Manage Custom Tools** page. However, they must be surrounded by double percent (%) signs. For example, to pass in the *NOTICELABEL* environment variable as a parameter, it should be entered as *%%NOTICELABEL%%* on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single percent (%) sign should precede and succeed the environment variable name. See "Custom tools reference" for a list of other substitutable variables.
7. Select **Tool can be scheduled** if the tool can be scheduled.
8. Click **OK** to add the new tool to the **Custom Tools** menu and access the **Manage Custom Tools** page, or click **Previous** to return to the previous page to select another type of custom tool.



NOTE: New custom tool tools are located under **Tools**→**Custom Tools**.

Related procedures

- [Creating a new CMS tool](#)
- [Deleting a custom tool](#)
- [Viewing tool definition files](#)

Related topics

- [Custom tools](#)
- [Managing custom tools](#)

Editing a web page tool

All fields are optional.

1. Select **Tools**→**Custom Tools**→**Manage Custom Tools**. The **Manage Custom Tools** page appears.
2. Select the tool to edit, and then click **Edit**. The **Describe how the new custom tool will work** page appears with the tool type and description displayed.
3. Under **Tool Parameters**, enter the following information:

- a. In the **Name** field, enter the command name. Custom tool names must be at least one character in length, and no more than 255 characters in length. The first character of the name must be alphabetic. Subsequent characters can be letters, digits, spaces, or any of the following: "-", ".", "(", ")", or "_".
 - b. In the **Description** field, enter the necessary information for the application.
 - c. In the **Help comments** field, enter any comments for the application.
 - d. In the **Menu placement** field, enter the full path (from the root of the HP SIM console) and the file name of the application. For example:


```
c:\custom code\romflash.bat
```
4. Specify the user account on the target system that will be used for the tool. Select one of the following options:
 - Logged-in user
 - Special user ("root" for UNIX and Linux systems, and "Administrator" for Windows systems)
 - Specific user
 5. Specify the maximum number of targets the tool can select when creating the task. Select from the following:
 - None

If none is selected, the target selection page is not displayed.
 - One
 - Unlimited
 6. Enter the **URL to the site or application to launch**.
 7. Click **OK** to add the new tool to the **Custom Tools** menu and access the **Manage Custom Tools** page, or click **Previous** to return to the previous page to select another type of custom tool.
 8. Enter the format of how target systems are passed to the URL.



NOTE: New custom tool tools are located under **Tools**→**Custom Tools**.

Related procedures

- Creating a new web page tool
- Deleting a custom tool
- Viewing tool definition files

Related topics

- Custom tools
- Managing custom tools

Deleting a custom tool

Deleting a custom tool removes it from the **Manage Custom Tools** page, from the **Custom Tools** menu, and from the system. If a tool being deleted is dependent on a task, an alert is displayed with the list of tasks associated with the command.

To delete a custom tool:

1. Select **Tools**→**Custom Tools**→**Manage Custom Tools**. The **Manage Custom Tools** page appears.
2. Select a tool to delete, and then click **Delete**. A confirmation box is displayed.
3. Click **OK** to delete the tool or click **Cancel** to cancel the deletion process.

Related topics

- Custom tools
- Managing custom tools

Viewing tool definition files

You can view the XML code, which are tool definition files, below the table of custom tools by clicking **View Tool Definition** from the **Manage Custom Tools**.

To display the tool definition files:

1. Select **Tools**→**Custom Tools**→**Manage Custom Tools**. The **Manage Custom Tools** page appears.
2. Select a tool, and then click **View Tool Definition**. The XML code appears.

Related topics

- [Custom tools](#)
- [Managing custom tools](#)

Removing and restoring custom tools

Removing a tool

The Remove a Tool tool, removes another tool from the menu for all users in HP Systems Insight Manager (HP SIM). The tool name must match the name in the tool definition file.



CAUTION: This tool can remove any tool, including tools supplied by HP.

To remove a tool from HP SIM:

1. Select **Options**→**Remove a Tool**. The **Remove a Tool** page appears.
2. Under **Parameters**, add information using the standard tool parameters. **Tool name** is the only required field.
3. Click **Run Now** to run the task immediately, or click **Schedule** to schedule when the task runs. See “Scheduling a task” for more information about scheduling a task.

To remove tools using the command line, enter

```
mxtool -r -t badtool
```

where *badtool* is the name of the tool you want to delete. See [mxtool\(1M\)](#) for more information.

Restoring a tool

To restore a tool using the command line, enter:

```
mxtool -a -f /home/user1/defs/mytooldef
```

where */home/user1/defs/* is the folder of the user restoring the tool and *mytooldef* is the tool to be restored. See [mxtool\(1M\)](#) for more information.

Related topics

- [Custom tools](#)
- [Custom tools reference](#)

Environment variables for custom tools



NOTE: If your user-defined variables have the same names as the HP Systems Insight Manager (HP SIM) environment variables, the HP SIM environment variables override the user-defined variables.

DOS environment variables are supported in the custom tool parameters and work as parameters on the **New Custom Tool** page or the **Manage Custom Tools** page. However, they must be surrounded by double percent (%) signs. For example, to pass in the *NOTICELABEL* environment variable as a parameter, it should be entered as *%%NOTICELABEL%%* on the parameter line. The environment variables can also be accessed from a batch file or script file. To use them in a batch file or a script file, only a single percent (%) sign should precede and succeed the environment variable name. See “Custom tools reference” for a list of other substitutable variables.

NOTICELABEL. Type of notice; a small string that contains discovered system, other HP SIM server-level notices, or the type of trap that caused the notice

NOTICESTATE. Internal value used by HP SIM, indicating whether the notice is cleared

NOTICEPLAINTEXT. Plain text description of the notice that contains detailed information about the notice (In Progress, Cleared, or Not Cleared)

NOTICERAWDATA. The raw data from the notice is passed as a string; this is a small pipe (|) delimited set of variables and might be useful for some simple parsing rules

NOTICESEVERITYSTR. Verbose description of the notice severity that can be one of Critical, Informational, Major, Minor, Unknown, Warning, and Normal

NOTICESEVERITY. Integer value of the *NOTICESEVERITYSTR* that can be one of:

- 0, Unknown
- 1, Normal
- 2, Warning
- 3, Minor
- 4, Major
- 5, Critical
- 100, Informational

NOTICEQUERYNAME. Displays the collection name based on how the notice was generated; this value can say one of the following:

- This system or event meets the following search criteria: +QueryName;
- This system or event now meets the following search criteria: +QueryName;
- This system or event no longer meets the following search criteria: +QueryName;

DEVICENAME. Name of the *system* that caused the notice

DEVICEIPADDRESSCOUNT. Number of IP addresses that are mapped to this system

DEVICEIPADDRESS%d. Based on the count, %d is an integer that shows the actual IP address, for example:

```
IF, DEVICEIPADDRESSCOUNT = 2
```

```
Then, DEVICEIPADDRESS0 = 111.111.111.111
```

```
DEVICEIPADDRESS1 = 222.222.222.222
```

DEVICEMACADDRESSCOUNT. Number of MAC addresses collected for the system (a *Data Collection Task* must be run before this information is available)

DEVICEMACADDRESS%d. Based on the MAC address count, %d is an integer that references the actual MAC address environment variable, for example:

```
IF, DEVICEMACADDRESSCOUNT = 2
```

```
Then, DEVICEMACADDRESS0=00:80:5F:7F:B0:81
```

```
DEVICEMACADDRESS1=00:80:C7:29:EF:B6
```

GENERICTRAPID. Set to the SNMP Generic Trap ID of the trap received if this is an event-based list and originated from an *SNMP trap*

SPECIFICTRAPID. Set to the SNMP Specific Trap ID of the trap received if this is an event-based list and originated from an SNMP trap

Path. Has the Path environment variable value from the context in which the service is running

SystemRoot. Has the SystemRoot environment variable value from the context in which the service is running

Windir. Has the Windir environment variable value from the context in which the service is running

COMPUTERNAME. Has the COMPUTERNAME environment variable value from the context in which the service is running

MPIP. This environment variable returns the IP address of the associated management processor

MPNAME. This environment variable returns the name of the associated management processor

RELATEDDEVICECOUNT. This environment variable returns the count of how many associated systems are there

RELATEDDEVICENAME%d. This environment variable returns the name of the associated system where %d is the iteration number, for example:

```
IF, RELATEDDEVICECOUNT = 2
Then, RELATEDDEVICENAME0=DeviceName0
RELATEDDEVICENAME1=DeviceName1
```

RELATEDDEVICEIP%d. This environment variable returns the IP address of the associated system where %d is the iteration number, for example:

```
IF, RELATEDDEVICECOUNT = 2
Then, RELATEDDEVICEIP0=111.111.111.111
RELATEDDEVICEIP1=222.222.222.222
```

RELATIONSHIP%d. This environment variable returns the relationship string with the associated device and %d is the iteration number

```
IF, RELATEDDEVICECOUNT = 2
Then, RELATIONSHIP0=ServerToEnclosure
RELATIONSHIP1=VMGuestToVMHost
```

Related procedure

- ▲ Creating a new CMS tool

Related topics

- Custom tools
- Managing custom tools

Examples of using parameter strings in custom tools

The URL strings for Web aware tools and command line tools must be provided as absolute URLs beginning with `http://` or `https://`. For example,

```
https://%n:1188/kcweb/ https://%l:2381/
```

Web-launch aware tools and command line tools that always run on the *Central Management Server* (CMS) must be relative URLs beginning with `/`. For example,

```
/propertypages/Identify.jsp?device=%n
```

Multiple selections can be substituted into the URL. A selection index is used during the substitution process to keep track of the *current* selection. The selection index is initially set to one, and the first selection of the list of selected target systems remains current until a `%z` parameter is encountered in the URL (an exception to this exists in the repeat block, discussed later), at which time the next selection becomes current, the selection index is incremented by one, and so on. For example,

```
http://server/app/doiit.jsp?name=%n%z&addr=%a
```

where the *doiit.jsp* page is invoked with the network name of the first selected system assigned to the *name* parameter and the IP address of the second selected target assigned to the *addr* parameter.

Any number of selected targets can be substituted by using the repeat block construct, `%(... %)`. Anything inside the repeat block delimiters is repeated until the selection list is exhausted, starting with what is then the current selection and selection index. For example,

```
https://%{deploy.server%}/deploy/deployimage.jsp? device1=%n%z%(&device%i=%n%z%)
```



NOTE: The use of the `%i` parameter. The current selection index (1, 2, 3, and so on) is substituted for this parameter during the substitution process.

NOTE: If the end of the repetition clause is reached and no `%z` parameter has been encountered, then the selection index and current election are automatically incremented to avoid an infinite loop during the substitution phase.

If we have two selected target systems in the above example, the expanded URL string would look like:

```
https://deploy.hp.com:280/deploy/deployimage.jsp?
device1=nodea.hp.com&device2=nodeb.hp.com
```

If we have only 1 selected target system in the above example, the expanded URL string would look like:

```
https://deploy.hp.com:280/deploy/deployimage.jsp? device1=nodea.hp.com
```

Because there is no current selection when we get to the repeat block, the entire repeat block is suppressed during the substitution process.

Related procedures

- Creating a new remote tool
- Creating a new CMS tool
- Creating a new web page tool
- Removing and restoring custom tools

Related topics

- Command line tools
- Managing custom tools

Custom tools reference

Tool types

There are six basic types of HP Systems Insight Manager (HP SIM) tools, *single-system aware* (SSA) tools, *multiple-system aware* (MSA) tools, *Web-launch aware* (WLA) tools, automation tools, message driven bean tools, and application launch.

SSA tools are executed on a target system and are only aware of the target system environment. When executing an SSA tool, therefore, the *Distributed Task Facility* (DTF) sends the tool information to each HP SIM agent to execute the tool. An example of an SSA tool would be a tool that wraps a common UNIX command, such as `ls`, `cat`, or `cp`.

MSA tools are executed on a central system, sometimes the *Central Management Server* (CMS), and know how to handle a list of target systems. An example of an MSA tool would be a tool that wraps the functionality of Ignite-UX on HP-UX systems.

WLA tools are generally executed in a browser and are specified by a universal resource location (URL).

Automation and message driven bean tools are executed on the CMS and perform some action, such as discovery on the target systems.



IMPORTANT: These two tools are internal HP tools and are not for general use.

Custom tools are executed on the CMS. One instance of the tool is started for each target system.

Parameterized strings

To create tools properly, the tool developer must understand how URLs and command lines are formed. Using parameterized strings, tool developers can greatly enhance the options available in creating tool definition files (TDEFs).

Parameterized strings are strings that contain replacement fields, similar to the format strings used in the popular `printf()` function in the standard C library. These fields can be replaced by values entered by the user at runtime (as defined by the tool parameters attribute), by some standard task properties supplied by the Task Controller, values related to the selected target systems or system groups, or by property values retrieved from a global tool properties file. This allows a very specific URL or command line to be generated.

Parameterized strings substitution table

The following parameters provide substitution of global attribute values:

Parameter	Description
%t	Task ID for the task being executed

Parameter	Description
%u	Name of the user running this tool
%e	Name of the user to execute this tool as
%s	Management server host name of the core CMS running the tool
%#	(where # is a positive integer) Substitute the value input by the user for the parameter referenced by the number (#) provided, as a list index position (one-based... %1, %2, %3, and so on)
%y	Simple Object Access Protocol (SOAP) logon token, for use with SOAP single sign-on web applications

The following parameters provide substitution of the current selected target:

Parameter	Description
%f	The name of the target system (or system group, if the %x toggle was in the string).
%n	Network name (host name, IP address, or system name in that order).
%a	Network address (IP address).
%l	Link name in format specified by System Link Configuration setting (name, IP address, or full DNS name).
%p	IP address of WBEM proxy, if any, for this target, in the form <ip address>:<port#></port#></ip>.
%g	Database GUID of the target system (or system group, if the %x toggle was in the string).
%b	System type of the target system.
%c	System sub-type of the target system
%r% (rt[.attribute]%)	Substitutes the related system that has the relationship type as specified in the parameter "rt." If the [.attribute] is specified, then one of the named system attributes would be returned for the related system. In addition, the common attributes such as Network name (.a) also work. For example, to get the server's management processor's IP address, use %r{MgmtProcToServer.a%}. To get the contact use %r{MgmtProcToServer.Contact%}. If the related systems attribute is omitted then for each system, the network name and IP address is returned. The network name and IP address are returned in the form "network name ip address". If more than one system is returned, they are comma-delimited. Note that the relationship type "MgmtProcToServer" can be used to return related system information for all management processor relationship types.
%(attribute%)	The value of the named attribute of the target system.

The following parameters provide repetition to support multiple selected target systems:

Parameter	Description
%(... %)	Repeated pattern (only repeats if a current selection exists). If a current target selection does not exist, the text between the delimiters is removed on expansion. This enables the text to be optional and dependent upon the target selection list.
%i	Selection index (one-based).
%z	Do not substitute anything, but increment the selection index to the next integer and the referenced target system to the next target in the selected target list.
%< ... %>	Encrypted text (encrypt after all other parameters have been substituted).
%%	Enables you to retain a % in the command/URL after substitution.

Tool filtering

Tool filtering is a facility enabling the tool writer to control whether the tool should be executed on a selected system. Most tools are platform dependent in that their successful execution depends on commands that are provided on some platforms but not on others. For example, the `bdf` tool depends on the `bdf` command, which is provided on HP-UX platforms, but is not available under that name on Linux platforms. A tool should only be visible in the **Tools** menu when there is at least one discovered system that passes the filter requirements. A discovered system must pass the filter requirements and is executed only if all the filter requirements are passed. To do this, the tool specifies in a system filter expression the system attributes that must be possessed by all systems it can run on.



NOTE: If a tool cannot be launched for selected systems, an error message is displayed with information about why the tool cannot be launched.

The system attributes required for a tool to run are specified by system filter expressions having the form:

```
<node-filter name="attribute-name" operator="eq"
  value="attribute-value" />
  or
<node-filter name="attribute-name" operator="ge"
  value="attribute-value" />
  or
<node-filter name="attribute-name" operator="lt"
  value="attribute-value" />
  or
<node-filter name="attribute-name" operator="ct"
  value="attribute-value" />
  or
<node-filter name="attribute-name" operator="neq"
  value="attribute-value" />
  or
<node-filter name="attribute-name" operator="nct"
  value="attribute-value" />
```

The `eq` operator specifies that the system on which the tool can run must have exactly the attribute value specified. It applies to any attribute name allowed in a system filter expression. The `ge` operator specifies that a system on which the tool can run on must have at least the attribute value specified. The `lt` and `ge` operators can only be used with revision attributes, specifically *OSRevision* in the *OS type* filter and all of the attributes of the *Protocol type* filter. The value of these attributes can be numeric or can be character strings. The `ct` operator specifies that a system on which the tool can run on must have an attribute that contains the value specified. The `neq` operator specifies that a system on which the tool can run on must not have the exact attribute value specified. It applies to any attribute name allowed in a system filter expression. The `nct` operator specifies that a system on which the tool can run on must have the attribute that does not contain the value specified. For systems, the numeric valued attributes the filter expression can specify include the *OSRevision* and *Protocol Support* attributes, whose values are version numbers. The values permitted for version numbers and how they are compared is described in the **Version Numbers** in the following section. The attribute-name is one of the values listed in the tables in the following section, or a protocol name from the *ProtocolSupport* attribute of a system. The attribute-value is one of the possible system attribute values for attribute-name.

Attribute values are based on the Distributed Management Task Force (DMTF) Common Information Model (CIM). Usually these values are defined during the system identification process, which uses WBEM and SNMP to determine system attributes. For this release, valid *OSName* values are HP-UX and Linux. For an *OSName* value of HP-UX, the *OSRevision* attribute values have the leading alphabetic field removed (for example B.11.11 is stored as 11.11).

A system filter expression is used as part of an include filter expression. There are three types of include filter expressions. Each type allows a different category of attribute names on which to be filtered.

Category	Filter type	Attribute names allowed
Operating System	os	OSName, OSVendor, OS Revision
Hardware	hardware	DeviceType, DeviceSubType, Model
Protocol Support	protocol	Any protocol name, except HTTP
Other	other	Can be any predefined system attribute or any custom-system attribute.

An include filter includes one or more system filter expressions using the attributes names allowed for it. For example, an `os` filter could consist of:

```
<include-filter type="os">
  <node-filter name="OSName"
operator="eq" value="LINUX" />
  <node-filter name="OSVendor"
operator="eq" value="RedHat" />
  <node-filter name="OSRevision"
operator="ge" value="7.2" />
</include-filter>
```

The include filter need not include all attributes allowed. If more than one attribute is included, the conditions are logically AND'd together. An attribute cannot appear in an include filter more than once, except that an attribute having a version number value can appear twice if one operator is `lt` and the other operator is `ge`. For example:

```
<include-filter type="protocol">
  <node-filter name="WBEM"
operator="lt" value="2.6" />
  <node-filter name="WBEM"
operator="ge" value="2.4" />
</include-filter>
```

This would specify that the tool should be shown for any collection of systems supporting the WBEM protocol version 2.4 or higher, but less than 2.6.

If a tool contains more than one include filter of different types, the conditions of the filters are logically AND'd together. A tool with both operating system and hardware dependencies could use the filter:

```
<include-filter type="os">
  <node-filter name="OSName"
operator="eq" value="LINUX" />
</include-filter>
<include-filter type="hardware">
  <node-filter name="DeviceSubType"
operator="eq" value="HPVectra" />
```



```
</include-filter>
```

If a tool contains more than one include filter of the same type, the conditions of the filters are logically OR'd together. A tool available on two different operating systems could specify:

```
<include-filter type="os">
  <node-filter name="OSName"
    operator="eq" value="LINUX" />
</include-filter>
<include-filter type="os">
  <node-filter name="OSName"
    operator="eq" value="HPUX" />
</include-filter>
```

This tool could be launched on any collection of systems using Linux or HP-UX.

Tool filtering depends on the attributes being filtered having a value defined on the systems selected. For the *os* filter type, if any attribute being filtered on is not defined for a system, the system is assumed to have the value required by the filter. Thus, a system with none of the *os* attributes specified by a tool filter are assumed capable of running the tool. For the *hardware* filter type, the above statement is true in the case of the *Model* attribute. But for the *DeviceType* and *DeviceSubType* attributes, the tool filter will apply only for known values on the selected systems. The *protocol* filter type requires that the protocol must exist on the system before the operators can be applied. This means that the *neg* and *not* operators also depend on the system to have that protocol. The other filter also works like the *protocol* filter such that the attribute being filtered upon must exist on the system before the operators can be applied. If a tool uses the other *and/or* *protocol* filters, then at least one system must contain the filterable attributes for the tool to be displayed in the GUI.

Version numbers

The *OSRevision* and *Protocol Support* system attributes have values that are interpreted as version numbers if possible. A version number is a series of non-negative decimal numbers separated by period (.) characters. When comparing version numbers, the following rules are used:

- The leftmost numbers in the series are most significant, so 1.0 is greater than 0.1.
- Leading zeroes on the numbers are disregarded, so 003 is equal to 3.
- Two adjacent period characters are interpreted as if they delimited the number zero, so 1.0.3 is equal to 1..3
- A beginning period character is interpreted as if preceded by a zero, so .9 is equal to 0.9.
- Trailing zero numbers are disregarded, so 1.0.0 is equal to 1.

Other requirements

SSA command tools must contain an execute statement (*execStmnt*) or a file copy statement (*copyStmnt*), or both. If only the execute statement is specified, no files are copied before executing the command. If only a file copy statement is specified, after the files are copied, no command is executed. If they are both specified, the files are copied first and then the command is executed.

MSA command tools must specify a command and the system on which the command will execute.

Tool names must be at least one character, and no more than 256 characters in length. The first character of the name must be alphabetic. Characters after the first can be letters, digits, spaces, or any of the characters - . () or _.

Web-launch aware tools must specify a main URL.

When specifying file copy pairs, the destination file paths for each file copy pair within a single TDEF must be unique. Specifying the same destination file path for multiple source file paths results in a file parsing error.

An error occurs when running a tool that copies a file if the file does not exist or is unreadable. The source file path is not checked at the time the tool is created or modified, but the path must exist at the time the tool is executed.

When the *log* element is set to true, standard out and standard error output from the execution of the tool is logged in the Central Management Server (CMS) log file `/var/opt/mx/logs/mx.log`. When it is set to false, only summary task log information, such as start and end times and task status is logged.

Document type definition

The Document Type Definition (DTD) file defines the constraints for an XML file. These constraints include the valid element tags, attributes, and the cardinality of elements in an XML file. The tool DTD file is named `toollist.dtd` and is included in the following paragraph. Note that because of manpage formatting, the DTD contents might not appear the same as in the file.

```
<?xml version="1.0" encoding="UTF-8" ?>

<!-- The tool-list element can contain zero or more of
      ssa-command-tool elements, msa-command-tool elements,
      web-launch-tool elements, automation-tool elements, mdbean-tool
      elements, or app-launch-tool elements.-->

<!ELEMENT tool-list ( ssa-command-tool |
                      msa-command-tool |
                      web-launch-tool |
                      automation-tool |
                      app-launch-tool )* >

<!-- The ssa-command-tool element specifies a single-system aware
      tool. The ssa-command-tool element can optionally specify a
      category element, a description element, a comment element, an
      owner element, a default-target element, an execute-as-user
      element, a job-display-handler element, a toolbox-enabled
      element, zero or more toolbox elements, zero or more
      include-filter elements, or zero or more env-variable elements.
      (NOTE: The role-enabled and role elements are deprecated
      elements and should not be used with this product. These
      are provided for backward compatibility with previous
      products. The toolbox-enabled element and the toolbox
      element should be used in their stead.)
      If more than one of these elements are specified, the element
      must appear in the order as listed in this definition. The
      ssa-command-tool element must contain an ssa-block element. The
      ssa-block element must appear after the previously described
      optional elements, if any of the optional elements are
      specified. Following the ssa-block element, one can specify zero
      or more attribute elements.-->

<!ELEMENT ssa-command-tool (category?, description?, comment?,
                             owner?, default-target?, execute-as-user?,
                             job-display-handler?,
                             toolbox-enabled?, toolbox*,
                             role-enabled?, role*,
                             include-filter*, env-variable*,
                             ssa-block, attribute* ) >
```

```
<!-- In addition to the previously described elements, the
      ssa-command-tool element specifies the following attributes. The
      name attribute specifies the tool name and must be specified in
      the ssa-command-tool element. The visible attribute specifies
      whether the tool is visible for running. By default tools are
      visible. The max-targets attribute specifies the maximum number
      of targets against which a tool can run. The revision attribute
      allows a tool author to specify a revision for the tool. Note
      that this is for information aboutly. The job-log attribute
      specifies whether the results of the command will be kept in this
      system's job log. This attribute applies only to tools when they
      are run as scheduled tasks, not when they are run as "run now"
      tasks. When job-log="true" the job and target status for the tool
      will be kept for a relatively lengthy system-defined period in
      the database after the job completes. When job-log="false" only
      the last completed copy of the job and target status for the task
      will be kept in the cache for a much shorter period of time, and
      will not be written to the database. Job logging is enabled by
      default. The schedulable attribute specifies whether the tool can
      be run as a schedulable task. When scheduled="false" the tool can
      only run as a "run now" task. Tools are scheduled by default.
      The GUID attribute specifies a globally unique identifier (GUID)
      for the tool. Because the system generates a GUID for a tool
      during the add operation, this field should only be specified
      during a modify operation. The accepts-targets attribute specifies
      whether the tool accepts targets for execution. The
      accepts-targets attribute is true by default. -->
```

```
<!ATTLIST ssa-command-tool name      CDATA      #REQUIRED
      visible      (true | false) "true"
      max-targets  NMTOKEN #IMPLIED
      revision     CDATA      #IMPLIED
      job-log      (true | false) "true"
      schedulable (true | false) "true"
      guid         NMTOKEN #IMPLIED
      accepts-targets (true|false) "true" >
```

```
<!-- The ssa-block specifies the elements specific to a single-system
      aware tool. The ssa-block can specify a command or copy-block or
      both. Only one command should be specified but up to 16 multiple
      copy-blocks can be specified. After the command and/or
      copy-blocks, one can specify the parameters for the command
      and/or copy-block. -->
```

```
<!ELEMENT ssa-block (( command | copy-block )+, parameter*) >
```

```
<!-- The copy-block specifies a source file path and a destination
      file path for a copy operation. -->
```

```
<!ELEMENT copy-block ( source, destination )+ >
```

```
<!-- The source element specifies the source file path for a copy
      operation. -->
```

```
<!ELEMENT source (#PCDATA) >
```

```
<!-- The destination element specifies the destination file path for a
      copy operation. -->
```

```

<!ELEMENT destination (#PCDATA) >

<!-- The msa-command-tool element specifies a multiple-system aware
      tool. The msa-command-tool element can optionally specify a
      category element, a description element, a comment element, an
      owner element, a default-target element, an execute-as-user
      element, a job-display-handler element, a toolbox-enabled
      element, zero or more toolbox elements, zero or more
      include-filter elements, or zero or more env-variable elements.
      (NOTE: The role-enabled and role elements are deprecated
      elements and should not be used with this product. These
      are provided for backward compatibility with previous
      products. The toolbox-enabled element and the toolbox
      element should be used in their stead.)
      If more than one of these elements are specified, the element
      must appear in the order as listed in this definition. The
      msa-command-tool element must contain an msa-block element. The
      msa-block element must appear after the previously described
      optional elements, if any of the optional elements are
      specified. Following the msa-block element, one can specify zero
      or more attribute elements.-->

<!ELEMENT msa-command-tool (category?, description?, comment?, owner?,
      default-target?, execute-as-user?,
      job-display-handler?,
      toolbox-enabled?, toolbox*,
      role-enabled?, role*,
      include-filter*, env-variable*,
      msa-block, attribute* ) >

<!-- In addition to the previously described elements, the
      msa-command-tool element specifies the following attributes. The
      name attribute specifies the tool name and must be specified in
      the msa-command-tool element. The visible attribute specifies
      whether the tool is visible for running. By default tools are
      visible. The max-targets attribute specifies the maximum number
      of targets against which a tool can run. The revision attribute
      allows a tool author to specify a revision for the tool. Note
      that this is for information aboutly. The job-log attribute
      specifies whether the results of the command will be kept in this
      systems job log. When job-log="true" the job and target status
      for the tool will be kept for a relatively lengthy system-defined
      period in the database after the job completes. When
      job-log="false" only the last completed copy of the job and
      target status for the tool will be kept in the cache for a much
      shorter period of time, and will not be written to the database.
      Job logging is enabled by default. The schedulable attribute
      specifies whether the tool can be run as a scheduled task. When
      schedulable="false" the tool can only run as a "run now" task.
      Tools are schedulable by default. The guid attribute specifies a
      globally unique identifier (GUID) for the tool. Because the
      system generates a GUID for a tool during the add operation, this
      field should only be specified during a modify operation. The
      accepts-targets attribute specifies whether the tool
      accepts targets for execution. The accepts-targets attribute is
      true by default. -->

<!ATTLIST msa-command-tool name          CDATA      #REQUIRED

```

```

    visible      (true | false) "true"
    max-targets  NMTOKEN #IMPLIED
    revision     CDATA    #IMPLIED
    job-log      (true | false) "true"
    schedulable (true | false) "true"
    guid         NMTOKEN #IMPLIED
    accepts-targets (true|false) "true" >

<!-- The msa-block specifies the elements specific to a
multiple-system aware (MSA) tool. The msa-block can specify an
MSA command, the parameters for the command and an execution system
on which the command executes. -->

<!ELEMENT msa-block ( command, parameter*, execution-system ) >

<!-- The command element specifies the command for an SSA or an MSA
tool. If the command accepts parameters, it must be specified as
a parameterized string. -->

<!ELEMENT command ( #PCDATA ) >

<!-- The command element can have two attributes. The command-type
attribute specifies whether the command is an x-window, stdout,
restart, launch, or an unknown command type. The default command
type is stdout. The log attribute specifies whether the results
of the command will be output to this system's audit log. When
log="true" the stdout and stderr results of the command will be
output to the system's audit log. Command output is not logged
by default. -->

<!ATTLIST command command-type (x-window |
stdout      |
restart     |
launch      |
unknown) "stdout"
log (true | false) "false" >

<!-- The execution-system element specifies the system on which an MSA
tool will execute. -->

<!ELEMENT execution-system ( #PCDATA ) >

<!-- The web-launch-tool element specifies a web launch tool. The
web-launch-tool element can optionally specify a category
element, a description element, a comment element, an owner
element, a default-target element, an execute-as-user element, a
job-display-handler element, a toolbox-enabled element, zero or
more toolbox elements, zero or more include-filter elements, or
zero or more env-variable elements.
(NOTE: The role-enabled and role elements are deprecated
elements and should not be used with this product. These
are provided for backward compatibility with previous
products. The toolbox-enabled element and the toolbox
element should be used in their stead.)
If more than one of these elements are specified, the element
must appear in the order as listed in this definition. The
web-launch-tool element must contain a web-block element. The
web-block element must appear after the previously described
optional elements, if any of the optional elements are

```

specified. Following the web-block element, one can specify zero or more attribute elements.-->

```
<!ELEMENT web-launch-tool (category?, description?, comment?, owner?,
  default-target?, execute-as-user?,
  job-display-handler?,
  toolbox-enabled?, toolbox*,
  role-enabled?, role*,
  include-filter*, web-block, attribute* ) >
```

```
<!-- In addition to the previously described elements, the
  web-launch-tool element specifies the following attributes. The
  name attribute specifies the tool name and must be specified in
  the web-launch-tool element. The visible attribute specifies
  whether the tool is visible for running. By default tools are
  visible. The max-targets attribute specifies the maximum number
  of targets against which a tool can run. The revision attribute
  allows a tool author to specified a revision for the tool. Note
  that this is for information aboutly. The job-log attribute
  specifies whether the results of the command will be kept in this
  systems job log. When job-log="true" the job and target status
  for the tool will be kept for a relatively lengthy system-defined
  period in the database after the job completes. When
  job-log="false" only the last completed copy of the job and
  target status for the tool will be kept in the cache for a much
  shorter period of time, and will not be written to the database.
  Job logging is enabled by default. The schedulable attribute
  specifies whether the tool can be run as a scheduled task. When
  schedulable="false" the tool can only run as a "run now" task.
  Tools are schedulable by default. The guid attribute specifies a
  globally unique identifier (GUID) for the tool. Because the
  system generates a GUID for a tool during the add operation, this
  field should only be specified during a modify operation. -->
```

```
<!ATTLIST web-launch-tool name      CDATA #REQUIRED
  visible      (true | false) "true"
  max-targets  NMTOKEN #IMPLIED
  revision     NMTOKEN #IMPLIED
  job-log      (true | false) "true"
  schedulable  (true | false) "true"
  guid         NMTOKEN #IMPLIED >
```

```
<!-- The web-block specifies the elements specific to a web launch
  tool. The web-block must specify a main-url element. Optionally,
  the web-block can specify a side-url element, a status-url
  element, and a current-url element. Additionally, the web-block
  can specify the parameters for the URLs. Finally, the web-block
  can optionally specify a target format to describe how targets
  are passed to a Web-launch aware tool. -->
```

```
<!ELEMENT web-block (main-url, (side-url?, status-url?, current-url?),
  parameter*, target-format? ) >
```

```
<!-- In addition to the above elements, the web-block element has one
  attribute. The accepts-targets attribute specifies whether the
  web launch tool accepts targets for execution. The
  accepts-targets attribute is true by default. -->
```

```
<!ATTLIST web-block accepts-targets (true|false) "true">
```

```

<!-- The main-url specifies the URL to launch the tool. If the URL
      accepts parameters, the URL must be specified as a parameterized
      string. -->

<!ELEMENT main-url ( #PCDATA ) >

<!-- The status-url specifies a URL at which one might find the status
      of this web launch tool during execution. -->

<!ELEMENT status-url ( #PCDATA ) >

<!-- The current-url specifies the current URL. -->

<!ELEMENT current-url ( #PCDATA ) >

<!-- The side-url specifies a set-aside URL. -->

<!ELEMENT side-url ( #PCDATA ) >

<!-- The target-format defines the format of targets in a web launch
      tool and is specified as a parameterized string.-->

<!ELEMENT target-format ( #PCDATA ) >

<!-- The mdbean tool performs an action on the &cms2; which
      involves accessing the target nodes. The mdbean-tool element
      may optionally specify a category element, a menu-category
      element, a description element, a comment element, an owner
      element, a default-target element, an execute-as-user element, a
      job-display-handler element, a default-parameter element, a
      role-enabled element, zero or more role elements, zero or more
      include-filter elements, or zero or more env-variable elements.
      If more than one of these elements are specified, the element
      must appear in the order as listed in this definition. The
      mdbean-tool element must contain an mdbean-block element.
      The mdbean-block element must appear after the previously
      described optional elements, if any of the optional elements are
      specified. Following the mdbean-block element, one may
      specify zero or more attribute elements. -->

<!ELEMENT mdbean-tool (category?, description?, comment?, owner?,
default-target?, execute-as-user?, job-display-handler?, toolbox-
enabled?, toolbox*, role-enabled?, role*, include-filter*, mdbean-block,
attribute*)>

<!-- In addition to the previously described elements, the
      mdbean-tool element specifies the following attributes. The
      name attribute specifies the tool name and must be specified in
      the mdbean-tool element. The visible attribute specifies
      whether the tool is visible for running. By default tools are
      visible. The max-targets attribute specifies the maximum number
      of targets against which a tool may run. The revision attribute
      allows a tool author to specify a revision for the tool. Note
      that this is for information aboutly. The job-log attribute
      specifies whether the results of the command will be kept in this
      systems job log. When job-log="true" the job and target status
      for the tool will be kept for a relatively lengthy system-defined
      period in the database after the job completes. When

```

job-log="false" only the last completed copy of the job and target status for the tool will be kept in the cache for a much shorter period of time, and will not be written to the database. Job logging is enabled by default. The schedulable attribute specifies whether the tool can be run as a scheduled task. When schedulable="false" the tool can only run as a "run now" task. Tools are schedulable by default. The guid attribute specifies a globally unique identifier (GUID) for the tool. Because the system generates a GUID for a tool during the add operation, this field should only be specified during a modify operation. The accepts-targets attribute specifies whether the tool accepts targets for execution. The accepts-targets attribute is true by default.-->

```
<!ATTLIST mdbean-tool
  name CDATA #REQUIRED
  visible (true | false) "true"
  max-targets NMTOKEN #IMPLIED
  revision CDATA #IMPLIED
  job-log (true | false) "true"
  schedulable (true | false) "true"
  guid NMTOKEN #IMPLIED
  accepts-targets (true | false) "true">
```

```
<!-- The mdbean-block specifies the elements specific to an
  mdbean tool. The mdbean-block must specify a
  bean-name and jms-queue-name. -->
```

```
<!ELEMENT mdbean-block (bean-name, jms-queue-name)>
```

```
<!-- The bean-name is the internal string representation of the bean
  name -->
```

```
<!ELEMENT bean-name (#PCDATA)>
```

```
<!-- The jms-queue-name is the internal string representation of the bean's
  queue name -->
```

```
<!ELEMENT jms-queue-name (#PCDATA)>
```

```
<!-- The automation tool performs an action on the &cms2; which
  involves accessing the target systems. The automation-tool element
  can optionally specify a category element, a menu-category
  element, a description element, a comment element, an owner
  element, a default-target element, an execute-as-user element, a
  job-display-handler element, a default-parameter element, a
  role-enabled element, zero or more role elements, zero or more
  include-filter elements, or zero or more env-variable elements.
  If more than one of these elements are specified, the element
  must appear in the order as listed in this definition. The
  automation-tool element must contain an automation-block element.
  The automation-block element must appear after the previously
  described optional elements, if any of the optional elements are
  specified. Following the automation-block element, one can
  specify zero or more attribute elements. -->
```

```
<!ELEMENT automation-tool (category?, description?, comment?, owner?,
  default-target?, execute-as-user?,
  job-display-handler?,
```



```
toolbox-enabled?, toolbox*,
role-enabled?, role*,
include-filter*, automation-block,
attribute* ) >
```

```
<!-- In addition to the previously described elements, the
automation-tool element specifies the following attributes. The
name attribute specifies the tool name and must be specified in
the automation-tool element. The visible attribute specifies
whether the tool is visible for running. By default tools are
visible. The max-targets attribute specifies the maximum number
of targets against which a tool can run. The revision attribute
allows a tool author to specify a revision for the tool. Note
that this is for information aboutly. The job-log attribute
specifies whether the results of the command will be kept in this
systems job log. When job-log="true" the job and target status
for the tool will be kept for a relatively lengthy system-defined
period in the database after the job completes. When
job-log="false" only the last completed copy of the job and
target status for the tool will be kept in the cache for a much
shorter period of time, and will not be written to the database.
Job logging is enabled by default. The schedulable attribute
specifies whether the tool can be run as a scheduled task. When
schedulable="false" the tool can only run as a "run now" task.
Tools are schedulable by default. The guid attribute specifies a
globally unique identifier (GUID) for the tool. Because the
system generates a GUID for a tool during the add operation, this
field should only be specified during a modify operation. The
accepts-targets attribute specifies whether the tool
accepts targets for execution. The accepts-targets attribute is
true by default. -->
```

```
<!ATTLIST automation-tool name CDATA #REQUIRED
visible (true | false) "true"
max-targets NMTOKEN #IMPLIED
revision CDATA #IMPLIED
job-log (true | false) "true"
schedulable (true | false) "true"
guid NMTOKEN #IMPLIED
accepts-targets (true|false) "true" >
```

```
<!-- The automation-block specifies the elements specific to an
automation tool. The automation-block must specify a
message-id. -->
```

```
<!ELEMENT automation-block (message-id) >
```

```
<!-- The message-id is the internal string representation of the message
sent by the Automation engine to cause the tool to run. -->
```

```
<!ELEMENT message-id ( #PCDATA ) >
```

```
<!-- The app-launch-tool element specifies an application launch
tool. The app-launch-tool element can optionally specify a
category element, a menu-category element, a description element,
a comment element, an owner element, a default-target element, a
execute-as-user element, a job-display-handler element, a
default-parameter element, a role-enabled element, zero or more
role elements, zero or more include-filter elements, or zero or
```

more env-variable elements. If more than one of these elements are specified, the element must appear in the order as listed in this definition. The app-launch-tool element must contain an app-launch-block element. The app-launch-block element must appear after the previously described optional elements, if any of the optional elements are specified. Following the app-launch-block element, one can specify zero or more attribute elements. -->

```
<!ELEMENT app-launch-tool (category?, description?, comment?, owner?,
    default-target?, execute-as-user?,
    job-display-handler?,
    role-enabled?, role*,
    toolbox-enabled?, toolbox*,
    include-filter*, env-variable*,
    app-launch-block, attribute* ) >
```

```
<!-- In addition to the previously described elements, the
    app-launch-tool element specifies the following attributes. The
    name attribute specifies the tool name and must be specified in
    the app-launch-tool element. The visible attribute specifies
    whether the tool is visible for running. By default tools are
    visible. The max-targets attribute specifies the maximum number
    of targets against which a tool can run. The revision attribute
    allows a tool author to specify a revision for the tool. Note
    that this is for information aboutly. The job-log attribute
    specifies whether the results of the command will be kept in this
    systems job log. When job-log="true" the job and target status
    the tool will be kept for a relatively lengthy system-defined
    period in the database after the job completes. When
    job-log="false" only the last completed copy of the job and
    target status for the tool will be kept in the cache for a much
    shorter period of time, and will not be written to the database.
    Job logging is enabled by default. The schedulable attribute
    specifies whether the tool can be run as a scheduled task. When
    schedulable="false" the tool can only run as a "run now" task.
    Tools are schedulable by default. The guid attribute specifies a
    globally unique identifier (GUID) for the tool. Because the
    system generates a GUID for a tool during the add operation, this
    field should only be specified during a modify operation. The
    accepts-targets attribute specifies whether the tool
    accepts targets for execution. The accepts-targets attribute is
    true by default. -->
```

```
<!ATTLIST app-launch-tool  name          CDATA      #REQUIRED
    visible      (true | false) "true"
    max-targets  NMTOKEN #IMPLIED
    revision     CDATA      #IMPLIED
    job-log      (true | false) "true"
    schedulable (true | false) "true"
    guid         NMTOKEN #IMPLIED
    accepts-targets (true|false) "true" >
```

```
<!-- The app-launch-block specifies the elements specific to an
    application launch tool. The app-launch-block specifies a
    required command element. -->
```

```
<!ELEMENT app-launch-block (command, app-parameters?) >
```

```

<!-- In addition to the previously described elements, the
      app-launch-block element specifies the following attribute. The
      alert-driven attribute specifies whether the alert list or the
      system list is used to determine the target systems to run the tool
      on. -->

<!ATTLIST app-launch-block alert-driven (true | false) "false" >

<!-- The app-parameters element is an application parameters
      definition string whose value is a string -->

<!ELEMENT app-parameters ( #PCDATA ) >

<!-- The env-variable element is an environment variable definition
      string whose value is a string -->

<!ELEMENT env-variable ( #PCDATA ) >

<!-- In addition to the previously described elements, the
      env-variable element specifies the following attribute. The
      name attribute specifies the name of the environment variable.-->

<!ATTLIST env-variable name CDATA #REQUIRED >

<!-- The owner element specifies the tool owner. When the owner field
      is specified, the tool is only associated with the All Tools toolbox.
      When the owner field is not specified, tool is enabled in all
      of its associated toolboxes. When a limited-rights user adds or
      modifies a tool, the owner field contains the name of the
      limited-rights user. Only a full-rights user can add or modify a
      tool without the owner specified. -->

<!ELEMENT owner ( #PCDATA ) >

<!-- The comment field specifies additional information about the
      tool. It is usually more verbose than the description. -->

<!ELEMENT comment ( #PCDATA ) >

<!-- The parameter element specifies the first to the tenth parameter
      of a tool. -->

<!ELEMENT parameter EMPTY >

<!-- The parameter element has three attributes. The index attributes
      specifies which argument in a parameterized string this parameter
      substitutes. Parameters can be indexed from 1 to 10 with a
      default index of 1. Tools cannot contain parameters with
      duplicate indexes. If more than one parameter in a tool
      definition contains the same index, only the first parameter added
      to the tool with the duplicate index remains in the tool. The
      prompt attribute provides information about the parameter that
      can be displayed in a GUI for assistance. The required attribute
      specifies whether this parameter must be specified when the tool
      is executed. By default, parameters are not required. The private
      attribute specifies whether this parameter is encoded and stored
      securely. By default, parameters are not private. -->

<!ATTLIST parameter index (1|2|3|4|5|6|7|8|9|10) "1"

```

```

    prompt CDATA #REQUIRED
    required (true|false) "false"
    private (true|false) "false" >

<!-- The toolbox-enabled element specifies whether the toolboxes
    associated with a tool are enabled. -->

<!ELEMENT toolbox-enabled EMPTY >

<!-- The toolbox-enabled element has one attribute. The value
    attribute specifies whether the tool within the toolboxes is enabled.
    This allows a full-rights user to explicitly disable the tools in
    a toolbox though the tool is always enabled in the All Tools
    toolbox. By default, the tool is enabled in all the toolboxes that
    it is in. If a tool is disabled within a toolbox, it cannot be
    executed. -->

<!ATTLIST toolbox-enabled value (true|false) "true">

<!-- The role-enabled element specifies whether the roles associated
    with a tool are enabled. This is an obsolete element. The
    toolbox-enabled element should be used instead.-->

<!ELEMENT role-enabled EMPTY >

<!-- See description of toolbox-enabled element attributes. -->

<!ATTLIST role-enabled value (true|false) "true">

<!-- The default-target element specifies a target on which the tool
    can run if no targets are specified at run time. One can specify
    a system, &cms2; to run on the &cms2; by default, or ALL to run on all
    authorized systems by default. -->

<!ELEMENT default-target ( #PCDATA ) >

<!-- The category element specifies the category with which to
    associate the tool. By default, tools are associated with the
    "Local Tools" category. -->

<!ELEMENT category ( #PCDATA ) >

<!-- The description element specifies a simple description of the
    tool. To specify more verbose information such as how to run the
    tool, use the comment element. -->

<!ELEMENT description ( #PCDATA ) >

<!-- For SSA and MSA command tools, the execute-as-user element
    specifies the user name that the tool runs as or under whose
    account the tool runs on the target systems. For Web-launch
    tools the execute-as-user is passed to the URL for its use. -->

<!ELEMENT execute-as-user ( #PCDATA ) >

<!-- The job display handler element specifies the fully-qualified
    name of a class implementing the JobDisplayHandler interface,
    used to display the results of a job created by running this
    tool. -->

```

```

<!ELEMENT job-display-handler ( #PCDATA ) >

<!-- The toolbox element specifies a toolbox to associate with the
      tool. To run a tool the user must be authorized with one of the
      specified toolboxes. -->

<!ELEMENT toolbox EMPTY >

<!-- The toolbox element has one attribute to specify the toolbox
      name. -->

<!ATTLIST toolbox toolbox-name CDATA #REQUIRED >

<!-- The role element specifies a role to associate with the tool. To
      run a tool the user must be authorized with one of the specified
      roles. This element is obsolete. The toolbox element should be
      used instead. -->

<!ELEMENT role EMPTY >

<!-- See the toolbox element attribute description. -->

<!ATTLIST role role-name CDATA #REQUIRED >

<!-- The include-filter element specifies system attributes against
      which to filter a tool for execution. A specified include-filter
      element must contain one or more system-filter elements. When
      filtering a tool each include-filter block is OR'd together to
      get the final filter result. Each system-filter element within an
      include-filter block is AND'd together. -->

<!ELEMENT include-filter (system-filter)+ >

<!-- The include-filter elements has one attribute. The type attribute
      specifies the type of include filter to execute. Four types are
      currently recognized. Three of them are os (operating system),
      hardware, protocol filtering. The fourth type is called other which
      will allow all other system attributes to be filtered upon.-->

<!ATTLIST include-filter type (os | hardware | protocol | other) "os" >

<!-- The system-filter element is an empty element that contains
      attributes used to specify the system attributes against which to
      filter a tool for execution. -->

<!ELEMENT system-filter EMPTY >

<!-- The system-filter element is specified with three attributes. The
      name attribute specifies the system attribute name to filter
      against. The operator attribute specifies whether to filter
      against an equal value, a less than value, a greater than or
      equal value, a contains value, a not equals value or a not
      contains value. The operator name is case-insensitive. The
      value attribute specifies the value of the system attribute to
      filter against. -->

<!ATTLIST node-filter name CDATA #REQUIRED
      operator (EQ | GE | LT | CT | NEQ | NCT |

```

```

eq | ge | lt | ct | neq | nct |
Eq | Ge | Lt | Ct | Neq | Nct |
eQ | gE | lT | cT | nEQ | nCT ) "EQ"
value CDATA #REQUIRED >

```

```

<!-- The attribute element specifies the name value pairs that
      comprise client attributes. The client attribute name is
      specified using the name attribute and the client attribute value
      is specified as the PCDATA of the element. -->

```

```

<!ELEMENT attribute ( #PCDATA ) >

```

```

<!ATTLIST attribute name CDATA #REQUIRED >

```

Related procedures

- Removing and restoring custom tools
- Editing a CMS tool
- Editing a remote tool
- Editing a web page tool

Related topic

- ▲ Command line tools

Configuring DMI access

The **Configure→DMI Access** tool enables you to set the HP Systems Insight Manager (HP SIM) *Central Management Server* (CMS) as the event target on selected HP-UX systems where DMI has been installed. This adds the HP SIM CMS server name to `/var/dmi/dmiMachines` on each selected system.

Related procedure

- ▲ Configuring SNMP access

Configuring SNMP access

The **Configure→SNMP Access** tool enables you to set the HP Systems Insight Manager (HP SIM) *Central Management Server* (CMS) as the trap target on selected HP-UX systems. This adds the HP SIM CMS server name to `/etc/SnmpAgent.d/snmpd.conf` on each selected system.

To configure SNMP to send traps to the CMS:

1. Add the full host name or IP address of the CMS as a *trapdest* in the file `/etc/SnmpAgent.d/snmpd.conf`:

```
trap-dest: hostname_or_ip_address
```
2. Stop the SNMP Master agent and all subagents with the command:

```
/sbin/init.d/SnmpMaster stop
```
3. Restart the SNMP Master agent and all subagents with the command:

```
/usr/sbin/snmpd
```

Related procedure

- ▲ [Configuring DMI access](#)

Device ping

Use the Ping tool to ping an individual system or multiple systems. To ping systems, select **Diagnose**→**Ping**. The **Ping** window appears. Select the target systems and click **Run Now** to run the task. See “Creating a task” for more information.

If a system does not resolve to an *IP* address, the request cannot be performed. For systems with multiple IP addresses, the result of each IP address occupies one row in the result page. The status on the upper-right corner displays: *Pinging selected systems*. After all the systems on the list have been pinged, the status displays: *Ping completed* with a time stamp of the completion time.

The ping results are displayed in a separate window. You might receive the following replies:

- *Replied*. The request has been executed successfully, and the pinged system has responded.
- *Request timed out*. The request has been executed, but the pinged system failed to respond.
- *System has no IP address*. There is no IP address associated with the system. Unable to perform ping.
- *No system is selected*. No system is selected.

If the ping is successful, there is no retry. You can only retry when the ping fails. The ping results have no effect on the system status on the **Task Results** or system view pages.

Disk thresholds

Setting disk thresholds

Setting disk *thresholds* is a *task* you can perform in HP Systems Insight Manager (HP SIM). Use this task to set a disk threshold for *systems* in an associated list. This threshold is set on all disk volumes on the target system.

To set disk thresholds, select **Configure**→**Disk Thresholds**→**Set Disk Thresholds**. The **Set Disk Thresholds** window appears. To select target systems, see “Creating a task”, and to specify the disk thresholds settings, see “Setting disk thresholds” for more information.

Follow these guidelines for setting thresholds:

- When you save the thresholds, disabled thresholds are deleted. A **Critical Disk Percent Usage Threshold** can never go higher than 99% or lower than a warning threshold plus 3%. Therefore, if the warning threshold is 85%, the valid range for the critical threshold is 88% to 99%.
- A **Reset Critical Disk Percent Usage Threshold** must drop below the reset value before the threshold is rearmed. This setting prevents the threshold from being sent multiple times if the variable fluctuates near the threshold value.
- The **Warning Disk Percent Usage Threshold** should be less than the critical threshold. A warning threshold must drop below the reset value before the warning threshold is rearmed. This setting prevents the threshold from being sent multiple times if the variable fluctuates near the threshold value. The minimum difference between the value and the reset value must be greater than or equal to 2%.
- When you save the thresholds, disabled thresholds are deleted. A **Reset Warning Disk Percent Usage Threshold** can never be higher than the critical threshold minus 3%. For example, if the critical threshold is 95%, the valid range for the warning threshold is 6% to 92%.
- The **Agent Polling Interval** value is the polling interval in seconds that determines how often the agents check if the current values exceed the threshold. A common value is 120 seconds.

Removing disk thresholds

Removing disk thresholds is another task that you can perform in HP SIM. Use this task to remove disk thresholds from systems in an associated list. This task only removes disk thresholds that were set by HP SIM or by browsing directly to the HP Insight Management Agent. Any thresholds set by Insight Manager (WIN32), including disk thresholds, are not removed by this task.

To remove disk thresholds, select **Configure**→**Disk Thresholds**→**Remove All Disk Thresholds**. The **Remove All Disk Thresholds** window appears. To select target systems, see “Creating a task” for more information. After the target systems are selected, click **Schedule** to schedule when to run the task, or click **Run Now** to run the task immediately. The **All Scheduled Tasks** page appears.

Related procedures

- Setting disk thresholds
- Scheduling a task

Setting disk thresholds

You can create a *systems* list to use with this *task*, specifying system characteristics, or use existing system lists. Specify the disk *thresholds* to be set on supported systems.

To set disk thresholds:

1. Select **Configure**→**Disk Thresholds**→**Set Disk Thresholds**. The **Set Disk Thresholds** page appears.
2. Select target systems, and then click **Next**. See “Creating a task” for more information.
3. In the **Specify the disk thresholds to be set on supported systems** section, enter the following information:
 - Critical disk percent usage threshold (percent)
 - Reset critical disk percent usage threshold at (percent)
 - Warning disk usage threshold (percent)
 - Reset warning disk usage threshold at (percent)
 - Agent polling interval (seconds)See “Disk thresholds” for guidelines on setting these parameters.
4. Click **Previous** to return to the previous page. Click **Schedule** to schedule when the task runs, or click **Run Now** to run the task immediately. The **Task Results** page appears. See “Scheduling a task” for more information about scheduling the task.

Related procedures

- Creating a task
- Scheduling a task

Related topic

- ▲ [Disk thresholds](#)

Creating a task to delete disk thresholds on a monthly basis

The following example describes the necessary steps to set up a task that removes all disk thresholds on a monthly basis from the HP Systems Insight Manager (HP SIM) database.

Creating the task

1. Select **Configure**→**Disk Thresholds**→**Remove All Disk Thresholds**. The **Remove All Disk Thresholds** page appears.
2. Select **All Servers** from the **Add targets by selecting** dropdown list.
3. Select the **Select "All Servers" itself** checkbox.
4. Click **Apply**.
5. Click **Schedule**.
6. In the **Task name** field, enter a name for the task, such as **Delete Disk Thresholds Monthly**.
7. Under **When would you like this task to run?** section, select **Periodically**.
8. In the **Refine schedule** section, select every month and select a day for the task to run.
9. Click **Done**.

Related procedures

- Setting disk thresholds
- Creating a task
- Scheduling a task
- Running a scheduled task

Related topic

- ▲ Disk thresholds

License manager

License Manager enables you to view and manage product licenses within the HP Systems Insight Manager (HP SIM) user interface. This release supports only ProLiant Essentials licensing.



NOTE: To run License Manager, you must have *administrative rights* on the *Central Management Server* (CMS) (to set, select **Options**→**Security**→**Users and Authorizations**→**User**) and the **All Tools** toolbox (to set, select **Options**→**Security**→**Users and Authorizations**→**Authorizations**).

See “Users and user groups” and “Toolboxes” for more information.

Licenses can be viewed and assigned to specified target *systems* known to HP SIM. For some products, the licenses are actually sent to the specified system and in the License Manager database, while for other products, the licensing information is updated in the License Manager database only. The installed licenses can be viewed by product name. New licenses can be added individually or added in bulk from a file.

License Manager includes license information for management processors such as Integrated Lights-Out (iLO) systems. You can manage all aspects of iLO2 licensing using the License Manager menu Graphical User Interface (GUI) including deploying license keys to iLO and collecting licensing information from iLO. Not all servers can communicate with iLO at this time.

License Manager's **Manage Licenses**, **Assign Licenses**, **Un-Assign Licenses**, and **Collect License Info** features operate directly on the License Manager database. Some products manage licenses locally on the target system in the Windows registry. In these cases, license information is collected directly from those targets using DCOM and placed in the License Manager database. **Collect License Info** will also collect licensing information directly from the selected target system if the target is an iLO using SSH. When using **Collect License Info**, License Manager will understand the correct mechanism to use to collect licensing information automatically.

Apart from early versions of HP Performance Management Pack (PMP) plug-in, all license information for HP SIM plug-ins is maintained by License Manager in the HP SIM database. For some products, the license is stored in a licensing structure in the Windows registry on the licensed system. License Manager employs Microsoft's remote registry Application Programming Interfaces (API) over the Microsoft Distributed COM (DCOM) protocol to assign licenses to and collect license information from, those remote systems. License information is duplicated in the HP SIM database, but the licenses are managed directly on those systems by the product and must be periodically collected to keep this information current. Authentication credentials for the specified systems are needed only in those situations in which licenses are sent to the specified system. If WBEM authentication credentials have been provided for a specific target, these credentials are used. See “Setting protocols and credentials for a system or groups of systems” for more information. If specific credentials have not been provided, each set of *Web-Based Enterprise Services* (WBEM) credentials provided as global credentials are used in turn. See “Setting global protocols” for more information. If no credentials are provided, the connection is attempted using the default credentials of the HP SIM server. The remote registry service must be started and run on candidate target systems for key collection or assignment.

Communication with iLO uses the HP SIM provided SSH channel. You will need to provide the SSH username and password for each individual iLO. If the user name and password are common to a group of iLO's, the username and password can be defined for the group.

License Manager does not permanently bind (or apply) a product license to a system. Users can assign and un-assign licenses as needed.



NOTE: Currently, the ability to un-assign licenses, for iLO or iLO for Integrity, is not supported.

Once a product executes a licensed operation on a system, the license is bound (locked) to that system. License Manager can no longer move a license that has been applied or locked. Assigning a license to a system is a way for the user to ensure that a particular type of license (permanent versus trial) will be automatically consumed by the product when it is run on that system. For remote systems, licenses are deployed to those systems but not applied or locked. Running the product on a target system locks or applies the license. Assigning and deploying are not the same as binding. For a remote system, a deployed license remains on the system, but is not consumed until the associated product is used. If multiple keys and corresponding licenses are deployed to a target, only the required numbers of licenses are consumed. The remaining licenses are unused.

Generally, when a license is applied as part of the product operation, the license is bound (locked) and can no longer be unassigned and used elsewhere. A license deployed to a remote target cannot be recalled.

License Manager can be used to review license usage for all classes of systems, including plug-ins, remotely managed systems, and management processors. Some products permit you to view the license usage and status *only* using the License Manager GUI. Specific license management must be done using the tools provided by those products.



NOTE: License input using a v0 key will fail to work. However, it is rare that you will encounter a v0 key license. All v1 key licenses work. Both v0 and v1 keys can be collected but only v1 keys can be deployed.

To access License Manager, select **Deploy**→**License Manager**. The following information is displayed for each licensed product:

- **Product.** The name of the product.
- **Licenses Used.** The number of licenses in use.
- **Licenses (Select 'Manage Licenses' for detail).** The total number of licenses in the License Manager database for the product.

Related procedures

- [Collecting license information](#)
- [Managing licenses](#)
- [Assigning and unassigning licenses](#)
- [Viewing licensed systems](#)
- [Adding licenses individually](#)
- [Adding licenses from a file](#)

Related topics

- [System license information reporting](#)
- [About licenses](#)
- [Licensing with ProLiant Essentials applications](#)

About licenses

License Manager displays licenses by product. If a license authorizes multiple products, the number of seats permitted by the license is applied in full to each authorized product. For example, a license authorizing five seats and two products authorize five seats for each product.

Eight types of licenses are available:

- **Flexible Quantity.** This license offers full, unlimited functionality for an unlimited time and for a specific number of seats purchased, up to 50,000 seats.
- **Activation Key Agreement.** This license offers full, unlimited functionality for an unlimited time. This license represents an expected upper limit on the number of seats, up to 50,000 seats.

- **Subscription.** This license is a time limited full functionality license. This key can indicate unlimited use for a specified period of time or a limited number of seats for that same period of time. The basic time unit encoded in the key is one month. HP SIM considers one month equal 30 days.
- **Demo (seats and time).** This license offers full, unlimited functionality for a limited time and a specific number of seats. The license determines the number of days the key enables the product to function. The days begin counting from the day of first use. The key can permit more than one instance of the product to run. Demo keys can authorize up to 255 seats for up to 255 days.
- **Demo.** This license offers full, unlimited functionality for a limited time. The license determines the number of days the key allows the product to function. The days begin counting from the day of first use. The key can permit more than one instance of the product to run. Demo keys can authorize use for up to 65,535 days.
- **Beta.** This license offers full, unlimited functionality for a limited time. The license determines the number of days the key enables the product to function. The days begin counting from the day the key was created. The key can permit more than one instance of the product to run. Demo keys can authorize use for up to 65,535 days.
- **Free Flexible Quantity.** Some ProLiant Essentials products ship with some free, permanent licenses. This key type is the embodiment of those free licenses. The number of licenses provided by this key depends on the product. Keys of this type cannot be entered by the user into the License Manager database. The product alone can insert these keys into the database.
- **Evaluation.** This license offers full, unlimited functionality and is distributed only in special circumstances.

License types reported by Integrated Lights-Out (iLO) products include:

- **Intrinsic.** This license offers full, unlimited functionality and represents a single-use key for the product. This license type is specific to management processors.
- **Individual.** This license offers full, unlimited functionality and represents a single-use key for the product. This license type is specific to management processors.

Some products now provide licenses to enable other products. The license keys generated by these products cannot be manually added by the user.

Related procedures

- Collecting license information
- Managing licenses
- Assigning and unassigning licenses
- Adding licenses individually
- Adding licenses from a file
- Viewing licensed systems

Related topics

- License manager
- System license information reporting
- About licenses
- Licensing with ProLiant Essentials applications

Collecting license information

Collect License Info collects license details that now include Site license and Maintenance license from the selected targets. If the licenses are stored directly on the selected system (see the specific product information for details), the *Central Management Server* (CMS) and the selected machine must be running a variant of the Microsoft Windows operating system.

The License manager core has the means to establish and maintain a secure communication channel with iLO2 through two options provided by HP SIM, SSL and SSH. Both of these meet the requirements for a secure channel. If the target systems are iLO's, the iLO must support SSH and you must provide the required credentials. An SSH based solution uses Command Line Protocol (CLP). All iLO2 firmware releases include

support for SSH/CLP. SSH/CLP support is included in v1.70 or later of the iLO firmware . All iLO's can be updated to this version or later.



NOTE: iLO2 support is only for ProLiant iLO's and not for Integrity MP or Integrity iLO's.



NOTE: All current SSH connections to the intended target must be closed because iLO only supports two (2) simultaneous connections at one time. It is recommended that no connections exist.



NOTE: Automatic collection of iLO licenses is no longer supported.

Many products (mostly HP Systems Insight Manager (HP SIM) plug-ins) save their license information in the License Manager database only. License information for these products is already available for viewing and manipulation, and does not need to be collected with the **Collect License Info** feature. For these products, there are no restrictions on the operating system of the CMS or selected system. Licensing information for all product licenses recorded on remote systems is collected.



NOTE: For Linux and HP-UX CMS, you can only collect iLO and iLO2 keys. License information will not be collected and stored as part of HP SIM Discovery and Identification for iLO and iLO2 targets. You are provided with functionality to deploy and collect a PE license key to or from a selected iLO or iLO2 target. All operations of License Manager can be accomplished on iLO with firmware v1.70 and later. License keys for iLO2, older than 18 months, can only be collected but not deployed from HP SIM.

The **Collect License Info** functionality is disabled when you select a product with licensing information that is managed and maintained exclusively by HP SIM and all licensing information is stored on the CMS. **Collect License Info** is enabled to collect licenses for products where the license resides on the remote target. If that target is not a management processor, a windows only based communication protocol is used. iLO information requires SSH support to be included on HP SIM but has no operating system restrictions on the CMS or target.



NOTE: You are no longer provided support or upgrade options by default. After July 9, 2007, all license keys are included in a one year of 24 x 7 Software Technical Support and Update service. The License manager will keep you informed as to which license keys are "support and update enabled" and which license keys will require the purchase of future updates and upgrades.

1. Select **Deploy**→**License Manager**.
2. Click **Collect License Info**. The **Select Target Systems** section appears.
3. Select target systems, and then click **Apply**. See "Creating a task" for more information. The **Verify target systems** section appears. The following information is available:
 - **Name**. The name of the target system.
 - **OS**. The operating system on the target system.
 - **Type**. The system type. See "System types" for more information.
 - **Tool launch OK?** If any selected targets are not compatible with the tool, this column provides a brief explanation of the problem. To remove a target, select the target's checkbox and click **Remove Targets**.
4. Add or remove target systems by clicking **Add Targets** or **Remove Targets**, and then click **Next**. The **License Collection Results** window appears and shows the collection status for each target. There might be a delay in collecting data from some targets. You can continue with other HP SIM activities during the collection process. The results window shows the following information:
 - **System Name**. The names of the systems on which the task was executed.
 - **Key**. The license keys received from the target systems. Each key retrieved from a system is listed on a separate line. Some products have more than one license key. License details are contained within the key, and each key might enable more than one product.

- **Product.** The name of the product associated with the use of this key.
- **Response Status.** The status of the request for license data for the selected system. If the task was successful, the following message appears: Licensing information collected successfully.

When the target is an iLO, SSH is used. When the credentials for a target are not known to HP SIM, the results table includes a URL to launch to permit you to enter those credentials immediately. If ignored, licenses will not be collected from this target. These credentials can be preconfigured in groups if the group shares a common user name and password.



NOTE: When a collected license is different from one recorded in the LM database for this iLO 2, the existing license record will be discarded and replaced with the new license just collected.



NOTE: The **Collect License Info** button is disabled until the current task finishes.

Related procedures

- [Managing licenses](#)
- [Assigning and unassigning licenses](#)
- [Viewing licensed systems](#)
- [Adding licenses individually](#)
- [Adding licenses from a file](#)

Related topics

- [License manager](#)
- [System license information reporting](#)
- [About licenses](#)
- [Licensing with ProLiant Essentials applications](#)

Viewing licensed systems

HP Systems Insight Manager (HP SIM) enables you to view a list of systems licensed for the selected product. Although a target may be licensed to use a product, the product license may not appear in the Graphical User Interface (GUI) or Report. Products may optionally elect to not display all or some of their specific licensing details.

1. Select **Deploy**→**License Manager**.
2. In the **Product License Information** section, select a product.
3. Click **Licensed Systems**. The list of systems licensed for the selected product appears. You can click a column header to sort the list based on the entries in that column. The following information is displayed:
 - **System.** The system licensed for the selected product.
 - **Serial Number.** The serial number can be any number the licensing products chooses to identify systems. Check product information for specific details.
 - **Licenses used.**
 - **Days permitted.** The total number of days authorized for use by this license (time-specific licenses only).
 - **Days remaining.** The number of days before the license expires for the corresponding system. For BETA licenses, this is the number of days from the date the license was issued. For subscription licenses, it is the number of days since the license was first used on any target. For all others, it is the number of days from when the license was first used on the selected target. All uses of this license after the first use have the same number of days remaining as the target first licensed.
 - **License Category.**

- **License Source.** The source of the corresponding license. This can be:
 - **Purchased.** The license was purchased directly as part of a license agreement.
 - **Free Trial.** The license was supplied free of charge.
- **Status.** The status of the use of this license on the named system.
- **Updates and Upgrades**
 - Reports level of service associated with this license.
- **Technical Support**
 - Reports level of service associated with this license.

Related procedures

- Collecting license information
- Managing licenses
- Configuring automatic discovery
- Assigning and unassigning licenses
- Adding licenses individually
- Adding licenses from a file

Related topics

- License manager
- System license information reporting
- About licenses
- Licensing with ProLiant Essentials applications

Managing licenses

The Manage Licenses feature enables you to manage licenses for the product selected in the **Product License Information** table. Licenses can originate from direct *user* input, license information collected using **Collect License Info**.

From the **License Manager** page, select a product, and then click **Manage Licenses**. The License Manager window is updated with information about the available licenses for the selected product, including:

- **License Category.** The type of license. All permanent, paid licenses are displayed as a single category, even though you might have purchased several separate licenses. License Manager does not consider the purchase date.
- **Licenses Available.** The total number of licenses that are available to assign to *systems*.
- **Licenses Assigned.** The total number of licenses of the selected type that are assigned to systems.
- **Licenses Used.** The total number of licenses that have been used by systems. A license is not used until the product has been used on a system. This total includes previously used licenses that have expired.
- **Days permitted.** The total number of days authorized for use by this license (time specific licenses only). For BETA licenses, this is the number of days from the date the license was issued. For subscription licenses, it is the number of days since the license was first used on any target. For all others, it is the number of days from when the license was first used on the selected target. All uses of this license after the first use has the same number of days remaining as the target first licensed.
- **Days remaining.** The number of days before the license expires. Some licenses will show Days remaining as the same as Days permitted as the time to expire is determined when the license is applied to a target and only relates to that target. Others will show an equal or lesser number as the time to expire is based on the first application of the license or based on when the licenses was issued for these types of license. With a BETA license, the Days remaining will always be less than the Days permitted even if the license has not been used on any target.

- **License Source.** The source of the corresponding license. This can be:
 - **Purchased.** The license was purchased directly as part of a license agreement.
 - **Free Trial.** The license was supplied free of charge.
- **Status.** The status of the use of this license on the named system.
Status messages include:
 - `OK.` The license is valid and in compliance.
 - `Key not in use.` The license is valid but not used.
 - `License is fully subscribed.` The license key is in full use on this system and consequently, if used elsewhere as well, might be over-subscribed in total.
 - `License is over subscribed.` The license key is over used on this system.
 - `License trial period has expired.` The time limit on a timelimited key has been exceeded.
 - `License time period has expired.` The time limit on a timelimited key has been exceeded.
 - `License subscription period has expired.` The subscription key has expired.
 - `Wrong host equipment.` The serial number of the target on which this key was found does not agree with the serial number contained within the key information retrieved from this machine.
- **Updates and Upgrades**
 - Reports level of service associated with this license
- **Technical Support**
 - Reports level of service associated with this license

Manage Licenses shows only the license categories that can be used. License categories with all licenses consumed are not listed in this table. Adding the number of licenses in all categories in the **Manage Licenses** table might result in a total less than the number shown in the **Licenses** column of the **Product License Information** table.

In the **Manage Licenses** table, the total number of **Licenses Assigned** plus **Licenses Used** might exceed the number of licenses shown in the **Product License Information** table. This happens when the license category is oversubscribed. Systems with assigned licenses from this category might fail to be automatically licensed when used with the corresponding product. This can occur when a category of license is assigned to a collection of systems, and then later, the same category is applied to a different set of systems such that the total exceeds the number of licenses in that category. Un-Assign the licenses assigned to these systems. Assigned licenses are not bound or locked to systems, and licenses are used on a first-applied basis.

To manage licenses, select a license category, and then click one of the following buttons:

- **Add Licenses** Enter an individual license key. See [“Adding licenses individually”](#) for more information.
- **Adding Licenses from File** Enter license keys from a specially formatted key file. See [“Adding licenses from a file”](#) for more information.
- **Assign Licenses** Assign available licenses to systems. See [“Assigning and unassigning licenses”](#) for more information.
- **Un-Assign Licenses** Un-Assign licenses from systems. See [“Assigning and unassigning licenses”](#) for more information.

Related procedures

- [Collecting license information](#)
- [Assigning and unassigning licenses](#)
- [Viewing licensed systems](#)
- [Adding licenses individually](#)
- [Adding licenses from a file](#)

Related topics

- License manager
- System license information reporting
- About licenses
- Licensing with ProLiant Essentials applications

Adding licenses individually

HP Systems Insight Manager (HP SIM) enables you to add individual license *keys* to the License Manager database.



NOTE: There are types of valid license keys that you might not enter directly. These include the Free Flexible Quantity License (FFQL) type key and keys generated through normal operation of certain products.

iLO product license keys may now be added into the database as they can be deployed directly to iLO's.

To add a single key:

1. Select **Deploy**→**License Manager**.
2. Select either the product that corresponds to the license you want to add or **Add New Product**, and then click **Manage Licenses**. The **Manage Licenses** section appears.
3. Click **Add Licenses**. The **Add Licenses** section appears.
4. Enter one of the following:
 - The key string by typing it into the five fields as individual characters (five per field). The cursor automatically advances to the next field when the current field is full as you enter the key code starting from the left-most box.
 - The key by pasting the entire key into one of the five input fields, for example, if you received a key as text in an e-mail:
 1. Select the complete key string, and press **Ctrl + C** to copy it.
 2. Position the cursor in any of the five fields forming the input box, and press **Ctrl + V** or right-click your mouse to paste the license key. You can also right-click to paste. If the Add License function was selected after you copied the key, press **Ctrl + V** to paste the key. The license key displays with five characters in each field.



NOTE: When pasting in the complete key, the key can be in the normal format of five groups of five characters, with each separated by a hyphen (-), for example, 12345-67890-54321-09876-12345. There are no spaces between the characters and the hyphens.

5. Click **Open** to display the license details, including the product name, license version, type, and purchase date, and the maximum number of days the license can be used.
6. Click **Add Licenses Now** to add the new licenses to the database. If the licenses are added successfully, they are listed in the **Product License Information** section. An error message appears if the key is invalid, and that license information is not added to the database.



NOTE: You cannot add Integrated Lights-Out (iLO) keys with this procedure. The iLO keys must be added directly as described in the iLO documentation.

Related procedures

- Collecting license information
- Managing licenses
- Assigning and unassigning licenses
- Viewing licensed systems
- Adding licenses from a file

Related topics

- License manager
- System license information reporting
- About licenses
- Licensing with ProLiant Essentials applications

Adding licenses from a file

HP Systems Insight Manager (HP SIM) enables you to add *keys* to the License Manager database by importing an XML file.

iLO product license keys may now be added into the database as they can be deployed directly to iLO's.



NOTE: There are types of valid keys that you might not enter directly. These include the Free Flexible Quantity License (FFQL) type keys and keys generated through normal operation of certain products.

License keys are defined in an *XML* file with a *.key* extension. You can create these files if needed. The format is as follows. The keylist, key, and keystack values are required.

```
<?xml version="1.0" encoding="UTF-8"?>
<KEYLIST>
<KEY>
  <KEYSTRING>A2345-1B345-12C45-123D5-123E5</KEYSTRING>
</KEY>
<KEY>
  <KEYSTRING>987RK-AB456-EW123-3489K-XQ555</KEYSTRING>
  <PURCHASER>XYZ Company</PURCHASER>
  <DATE>29 July 2006</DATE>
  <PRODUCTNAME>Productname</PRODUCTNAME>
  <PRODUCTVERSION>1.1</PRODUCTVERSION>
  <DISP>1<DISP>
</KEY>
</KEYLIST>
```

The PURCHASER, DATE, PRODUCTNAME, PRODUCTVERSION and DISP fields are optional and are not needed if the only purpose is to load multiple keys. If a key file is provided, the content should be left as is. A minimal file would have a structure similar to the following, with at least one KEY tag:

```
<?xml version="1.0" encoding="UTF-8"?>
<KEYLIST>
<KEY>
<KEYSTRING>A2345-1B345-12C45-123D5-123E5</KEYSTRING>
</KEY>
<KEY>
<KEYSTRING>987RK-AB456-EW123-3489K-XQ555</KEYSTRING>
</KEY>
</KEYLIST>
```

To add one or more keys to the database from a specially formatted key file:

1. Select **Deploy**→**License Manager**.
2. Select **Add New Product**, and then click **Manage Licenses**. The **Manage Licenses** section appears.
3. Click **Add Licenses from File**. The **Add Licenses from a File** section appears at the bottom of the page.
4. Enter one of the following:
 - Enter the full path and file name in the **Specify a file name and path** field,
 - click **Browse**.
 - a. The **Choose file** dialog box appears.
 - b. Navigate to the file that contains the licenses to be added.
 - c. When a file has been located, click **Open**.
5. When the full path and file name display in the **Specify a file name and path** field, click **Open** to open the file. The contents of the license key file are displayed.
6. Click **Add Now** to add the keys to the database.
7. HP SIM notifies you when each key in the file was added. Click **OK**. If a key is invalid, an error for that key is reported and that key is not added to the database.

Related procedures

- [Collecting license information](#)
- [Managing licenses](#)
- [Assigning and unassigning licenses](#)
- [Viewing licensed systems](#)
- [Adding licenses individually](#)

Related topics

- [License manager](#)
- [System license information reporting](#)
- [About licenses](#)
- [Licensing with ProLiant Essentials applications](#)

Assigning and unassigning licenses

HP Systems Insight Manager (HP SIM) enables you to assign and un-assign product licenses for plugins, and to assign licenses to remote target systems when licenses are managed remotely. For plugins, when assigning licenses, note the following for non-iLO 2 targets:

- When a license is assigned to a system, it is not bound or consumed until the product operates on that system.
- A system can be licensed with a demo key just once. If the license expires, the only option to continue to use the system with that product is to purchase a license. A system licensed by a demo key can be relicensed at any time with a paid license.
- An assigned license can be unassigned from one system and assigned to another system, as long as the product enabled by the license has not consumed the license. When a product has been used on a system, the license is bound (locked) to that system permanently. Licenses delivered directly to the actual target system cannot be unassigned. There is no penalty for having these licenses remain on those systems because they are consumed on an as-needed basis. The remaining licenses can be used elsewhere.

Some products will limit the use of the License Manager Graphical User Interface (GUI). The reason for this is that target filtering and possibly other factors must be considered and these are not known to the HP SIM License Manager. Consequently, **Manage Licenses** may be selected, however **Assign/Un-assign** may be disabled.

For iLO 2 targets:

- When a license is assigned to an iLO 2, a license record is created and stored in the License Manager database.
- If the selected iLO 2 is already licensed, you cannot replace that license with a new license from License Manager. You must first delete the existing license at the iLO 2 console and then insert the new license (directly or using License Manger).
- An assigned license cannot be un-assigned from one iLO 2 and assigned to another iLO 2. Licenses delivered directly to the actual target system cannot be un-assigned as the behavior of the product operating with that license is outside the scope of License Manager.

When assigning licenses to iLO targets, the SSH credentials for each target must be known. When deploying licenses to remote servers, the access credentials must be known. See “Setting global protocols” for more information.

Assigning a license

1. Select **Deploy**→**License Manager**.
2. Select a product, and then click **Manage Licenses**. The **Licenses Currently Available** is displayed.
3. Select the **License Category** you want to assign, and then click **Assign Licenses**. The **Assign Licenses** section appears.
4. Select target systems, and then click **Apply**. See “Creating a task” for more information. The **Verify target systems** section appears.
5. Add or remove target systems by clicking the **Add Targets** or **Remove Targets** buttons.
6. Click **Next**.

For products where licensing information is managed by HP SIM, the **Assigning Licenses** page appears. This page lists the selected system's name, licensing status, operating system, system type and IP address. Select one or more systems from this list and click **Assign License Now**. The page refreshes and shows the updated license status. Select additional systems to make more assignments, or reselect License Manager to refresh the page. To remove an assigned license, reselect Manage Licenses, the license category, and then select **Un-Assign Licenses**.

For products that require the license to be delivered to the actual target, the **License Assignment Results** table appears in a separate window and reports the status of the assignment process for each target. There might be a delay in sending license data to some targets. You can continue with other HP SIM activities during the license assignment process. The results window shows the following information:

- **System Name**. The names of the systems on which the task was executed.
- **Key**. The license keys sent to the target systems. Each key is listed on a separate line. License details are contained within the key, and each key might enable more than one product.
- **Product**. The name of the product associated with the use of this key.
- **Response Status**. The status of the request to send license data to the selected system. If the task was successful, the following message appears: `License assignment successful`.

Unassigning a license

1. Select **Deploy**→**License Manager**.
2. Select a product, and then click **Manage Licenses**. The **Licenses Currently Available** is displayed.
3. Select the **License Category** you want to unassign. If there are licenses assigned using this category, the **Un-assign Licenses** button is available. Click **Un-assign Licenses**. The **Un-assign Licenses** section appears.

Licenses delivered directly to the actual target system cannot be unassigned. There is no penalty for having licenses remain on those systems. The Un-Assign Licenses function is disabled in this case.

4. Select the systems to remove license assignments from by selecting the checkboxes next to the name of each system.
5. Click **Un-assign Licenses Now**. The **Un-Assign Licenses** table is refreshed and shows the updated status.



NOTE: Licenses deployed to remote systems such as an iLO 2 cannot be un-assigned.

Related procedures

- Collecting license information
- Managing licenses
- Viewing licensed systems
- Adding licenses individually
- Adding licenses from a file

Related topics

- License manager
- System license information reporting
- About licenses
- Licensing with ProLiant Essentials applications

System license information reporting

The System License Information Reporting feature provides a quick and efficient way to track ProLiant Essentials License Information, including licenses used on Integrated Lights-Out (iLO) systems.

System license information reporting

The **System License Information** report provides a summary of the details and distribution of licenses.

- **System Name**
- **System Serial Number**
 - The serial number can be any number the licensing products chooses to identify systems. (Check product information for specific details).
- **Product Name**
- **Product Version**
- **Licenses Used**
- **License Source.** The source of the corresponding license. This can be:
 - **Purchased.** The license was purchased directly as part of a license agreement.
 - **Free Trial.** The license was supplied free of charge.
- **License Type**
 - **Permanent**
 - The license does not expire.
 - **Subscription, Demo (seats and Time), Demo (time), BETA.**
 - The license expires after a specified period of time.
- **Days permitted.**
 - The total number of days authorized for use by this license (time-specific licenses only).
- **Expiration Date.**
 - The number of days before the license expires for the corresponding system. For BETA licenses, this is the number of days from the date the license was issued. For subscription licenses, it is the number of days since the license was first used on any target. For all others, it is the number of

days from when the license was first used on the selected target. All uses of this license after the first use have the same number of days remaining as the target first licensed.

- **Staus**
 - The staus of the use of this license on the named system.
 - Status messages include:
 - **OK.** The license is valid and in compliance.
 - **Key not in use.** The license is valid but not used.
 - **License is fully subscribed.** The license key is in full use on this system and consequently, if used elsewhere as well, might be over-subscribed in total.
 - **License is over subscribed.** The license key os over used on this system.
 - **License trial period has expired.** The time limit on a time limited key has been exceeded.
 - **License time period has expired.** The time limit on a time limited key has been exceeded.
 - **License subscription period has expired.** The subscription key has expired.
 - **Wrong host equipment.** The serial number of the target on which this key was found does not agree with the serial number contained within the key information retrieved from this machine.
- **Updates and Upgrades.**
 - Reports level of service associated with this license
- **Technical Support.**
 - Reports level of service associated with this license

In this release, unlike previous releases, iLO licensing information must be manually collected using **Collect License Info** from each target of interest. The appropriate SSH credentials must be supplied for each iLO2 selected.

Although a target may be licensed to use a product, the product license may not appear in the GUI or Report. Products may optionally elect to not display all or some of their specific licensing details.

See "Reporting views" for specific field information.

Related procedures

- [System reporting](#)
- [Collecting license information](#)
- [Managing licenses](#)

Related topics

- [Reporting](#)
- [Reporting views](#)
- [System reporting](#)

Licensing with ProLiant Essentials applications

The **License unlicensed systems (optional)** page appears when some of the targets selected are not licensed to use this product. Only those targets that are not licensed or licensed with a demo key are displayed.

This page is not directly accessible from the menus. It occurs in a sequence of one or more pages specific to a particular product. The same page is shared by all products using this page, so the page format and operation is the same for all products.

Four buttons are available from this page:

Previous Click **Previous** to return to a previous page.

Add Key If you have additional licenses available which are not yet known to HP Systems Insight Manager (HP SIM), you can add these keys. If you have a key string, click **Add Key**, and enter the key in the **Specify**

a **key string** field and click **OK**. Only license keys applicable to this product are accepted and added. To add other product keys, use License Manager, Manage Keys (**Deploy**→**License Manager**).

Apply License If there are licenses available for use, select the unlicensed targets you want to license and click **Apply License**. Clicking **Apply License** is final because it consumes (locks) the license for the selected target, and the license cannot be un-assigned. Targets licensed with some type of time-limited key are also shown. These can be selected but can only be relicensed using a PAID key. After all targets are licensed, this page is not displayed again (in this sequence). If there are targets that are still not licensed or licensed with a demo key, this page redisplaying showing the original list of unlicensed targets, indicating which target systems are now licensed and which are not. Selecting to license a target that has been licensed using a demo key relicenses the target with a permanent key, if a key is available. If there are insufficient licenses remaining at the time of the relicense, the demo license remains in force. When licensing, the full licenses (including those included with the product) are used first. If there are systems which remain unlicensed after all these licenses are consumed, any demo key not used to capacity is used if the product permits it. Finally, as other users might be attempting to license other targets for use with the product at the same time, it is possible to select a number of targets equal to the available licenses and yet fail to license some of those targets. A message advises when this has occurred.

Next If you do not want to license any of these unlicensed targets or at any time after licensing some of those targets, you can continue directly by clicking **Next**, provided at least one of the selected targets is licensed. If no selected targets are licensed, the **Next** button is displayed.

Upon successful completion, the number of licenses available should increase by the number of licenses enabled by the key. Those additional licenses are now available for use.



NOTE: When some or all of the selected targets are licensed using a demo key, those targets appear in the not licensed table with the status **Licensed using a demo key**. You can select any of these targets and relicense with a full key at this time. Demo and evaluation keys are not accepted to relicense a system with such a key.

Related topics

- [License manager](#)
- [About licenses](#)

Management processor tools

HP's Management Processor enables remote server management over the web regardless of the system state. In the unlikely event that the operating system is not running, Management Processor can be accessed to power cycle the server, view event and status logs, enable console redirection, and more.

New menu items are displayed in HP Systems Insight Manager (HP SIM) after management processors are discovered.

- **System Power** This tool enables you to control the power options on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems. To access, select **Tools**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**System Power**.
- **System Locator** This tool enables you to control the locator LED on one or more HP Integrity and HP 9000 iLO systems. To access, select **Tools**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**System Locator**.
- **New User** This tool enables you to add a new user account to one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**New User**.
- **Modify User** This tool enables you to modify an existing user account on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Modify User**.
- **Delete User** This tool enables you to remove an existing user account from one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Delete User**.

- **LAN Access** This tool enables you to modify LAN access settings on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**LAN Access**.
- **LDAP Settings** This tool enables you to configure the LDAP service on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**LDAP Settings**.
- **iLO Control** This tool enables you to execute internal control actions on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**iLO Control**.
- **Firmware Upgrade** This tool enables you to initiate a firmware upgrade through FTP on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Firmware Upgrade**.
- **Deploy SSH Public Key** This tool enables you to deploy the HP Systems Insight Manager (HP SIM) SSH public key on one or more HP Integrity and HP 9000 iLO systems. To access, select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Deploy SSH Public Key**.

Related procedures

- [Creating new users on management processors](#)
- [Editing management processor users](#)
- [Deleting management processor users](#)
- [Configuring LAN access on management processors](#)
- [Configuring LDAP settings on management processors](#)
- [Executing internal control actions through management processors](#)
- [Upgrading management processor firmware](#)
- [Deploying SSH public keys to management processors](#)

Controlling system power options through management processors

This tool enables you to control the power of one or more servers through the associated HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To set the system power control:

1. Select **Tools**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**System Power**. The **System Power** page appears.
2. Select target systems, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Select an action** page appears.
3. Under **System power control**, select one of the following:
 - Power cycle
 - Power on
 - Power off
 - Graceful shutdown (except HP 9000)
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **System Power** page. See “Scheduling a task” for more information about scheduling a task.

Related procedure

- ▲ [Controlling the system locator LED through management processors](#)

Controlling the system locator LED through management processors

This tool enables you to control the locator LED on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To control the system locator:

1. Select **Tools**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**System Locator**. The **System Locator** page appears.
2. Select target systems, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Select an action** page appears.
3. Under **System locator/Unit Identification LED**, select one of the following:
 - On
 - Off
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **System Power** page. See “Scheduling a task” for more information about scheduling a task.

Related procedure

- ▲ Controlling system power options through management processors

Creating new users on management processors

This tool enables you to add a new user account to one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To create a new user:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**New User**. The **New User** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Select an action** page appears.
3. Under **Enter properties for a new user account**, enter:
 - **Login id** (Mandatory) This is the name that must be used when logging into iLO. The maximum length for a Login Id is 25 characters.
 - **Password** (Mandatory) The password must be provided when logging into iLO. The password must be a minimum of 6 characters with a maximum of 24 characters.
 - **Password (Verify)** (Mandatory) The password must be provided a second time for verification.
 - **User name** (Mandatory) This name appears in the iLO user list. It is not necessarily the same as the login name. The maximum allowed length is 25 characters.
4. Under **Access Rights**, select the one or more access rights for the user. Usually, a new user is granted the Console Access right.
 - **Console access**
 - **Power access**
 - **Management processor configuration**
 - **User administration**
5. Click **Run Now** to run the task immediately. Click **Previous** to return to the previous **New User** page.

Related procedure

- ▲ Controlling the system locator LED through management processors

Editing management processor users

This tool enables you to modify an existing user account on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To modify a user:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Modify User**. The **Modify User** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Enter properties to modify an existing user account** page appears.
3. Under **Enter the login name of the user account you wish to modify**, enter the **Login id** to be modified.
4. Under **Select the properties you wish to modify for this user account**, select the attribute to modify and enter the appropriate information. Select from:
 - **Password** If you select to change the password, verify the password in the **Password (Verify)** field.
 - **User name** Select this field to modify the user name. This is not necessarily the same as the login name. The maximum allowed length is 25 characters.
 - **Access rights** If you select to modify the access rights, select from **Console access**, **Power access**, **Management processor configuration**, and **User administration**. To remove all access rights for an account, select the **Access rights** checkbox and leave the **Console access**, **Power access**, **Management processor configuration**, and **User administration** checkboxes cleared.
5. Click **Run Now** to run the task immediately. Click **Previous** to return to the previous **Modify User** page.

Related procedures

- [Creating new users on management processors](#)
- [Deleting management processor users](#)

Deleting management processor users

This tool enables you to remove an existing user account from one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To delete a user:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Delete User**. The **Delete User** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Enter properties to delete an existing user account** page appears.
3. Enter the **Login id** to be deleted.
4. Click **Run Now** to run the task immediately. Click **Previous** to return to the previous **Delete User** page.



NOTE: HP Systems Insight Manager (HP SIM) uses the Admin account to execute Management Processor tools. If this account is removed from the iLOs, the tools cannot access the iLOs on those systems, unless tool execution is reconfigured.

To configure HP SIM tool execution on a different iLO account:

1. Select a user account that is to be used to run tools on iLOs. This user account must be present on all managed iLOs and must have all rights on the iLOs.
2. Navigate to the tools directory on the Central Management Server (CMS) and edit `MpTools.xml`.
3. Find each `<execute-as-user>` line in the XML file and change *Admin* to the user account specified in step 1.
4. Run `mxtool -m -f MpTools.xml -x force`.
5. On the CMS, run `mxagentconfig` or the Deploy SSH Public Key tool to copy the authentication keys for this user account to each managed iLO. See “Deploying SSH public keys to management processors” for more information about deploying the SSH public key.

Related procedures

- [Creating new users on management processors](#)
- [Editing management processor users](#)

Configuring LAN access on management processors

This tool enables you to modify LAN access settings on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To modify LAN access:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**LAN Access**. The **LAN Access** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Enter LAN access settings** page appears.
3. Under **Select the settings you wish to configure and choose their values**, select from:
 - **Telnet access** Select to **Enable** or **Disable** Telnet access. This does not affect the IP configuration or the ability of the management processor to perform upgrades over the LAN.
 - **Web SSL** Select to **Enable** or **Disable** Web SSL.
 - **Web console port** If you select this option, you must enter a valid port number. Valid port numbers are 23 and 2000 through 2400.
 - **IPMI over LAN access** Select to **Enable** or **Disable** IPMI over LAN access.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **LAN access** page. See “Scheduling a task” for information about scheduling a task.

Configuring LDAP settings on management processors

This tool enables you to configure the LDAP service on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To configure the LDAP service:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**LDAP Settings**. The **LDAP Settings** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Enter LDAP directory settings** page appears.
3. Under **Select the settings you wish to configure and choose their values**, select from the following:
 - **Local user accounts** Select to **Enable** or **Disable** access to local iLO user accounts. If local user accounts are enabled, a user can log in to iLO using locally stored user credentials. If local user accounts are disabled, user access is limited to valid directory credentials only.
 - **Directory authentication** Select to **Enable** or **Disable** to activate or deactivate directory support on the selected iLOs. If directory authentication is enabled and configured properly, users can log in to iLO using directory credentials. If this is disabled, user credentials are not validated using the directory.
 - **Directory server IP address** Enter the IP address of the directory server.
 - **Directory server LDAP port** Enter the LDAP for secure LDAP service on the server. The default value for this port is 636.
 - **Distinguished name** Specifies where this iLO instance is listed in the directory tree. For example: *cn=MP Server.ou=Management Devices.o=hp*
 - **User search context 1** User name contexts that are applied to the login name entered to access iLO.

- **User search context 2** User name contexts that are applied to the login name entered to access iLO.
 - **User search context 3** User name contexts that are applied to the login name entered to access iLO.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **LDAP Settings** page. See “Scheduling a task” for more information about scheduling a task.

Executing internal control actions through management processors

This tool enables you to execute internal control actions on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems.

To execute internal control actions:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**iLO Control**. The **iLO Control** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Select one or more actions** page appears.
3. Select one or both of the options listed:
 - **Clear event logs** This option clears the system event logs.
 - **Reset management processor** This option executes a reset of the iLO.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **iLO Control** page. See “Scheduling a task” for more information about scheduling a task.

Upgrading management processor firmware

This tool enables you to initiate a firmware upgrade through FTP on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems. The upgrade is performed simultaneously on all selected iLOs.

To initiate a firmware upgrade:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Firmware Upgrade**. The **Firmware Upgrade** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Specify firmware upgrade parameters** page appears.
3. Enter the following information:
 - **Source IP** You must enter the IP address of the ftp server.
 - **File path** The path to the directory (on the ftp server) in which the upgrade files reside.
 - **Login ID** The login ID used to log in to the ftp server.
 - **Password** The password to the ftp server.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs or click **Previous** to return to the previous **Firmware Upgrade** page. See “Scheduling a task” for more information about scheduling a task.

Deploying SSH public keys to management processors

This tool enables you to deploy the HP Systems Insight Manager (HP SIM) SSH public key on one or more HP Integrity and HP 9000 Integrated Lights Out (iLO) systems. Before executing this tool, SSH must be enabled on the target iLO and SSH keys must have been generated on the iLO. This tool must be executed once after initial installation or after the Central Management Server (CMS) public key has changed. It is a prerequisite to executing any of the Management Processor tools.

This tool must be run from an account that has administrative privileges on the HP SIM CMS.

To deploy the HP SIM SSH public key:

1. Select **Configure**→**Management Processor**→**HP Integrity and HP 9000 iLO**→**Deploy SSH Public Key**. The **Deploy SSH Public Key** page appears.
2. Select target management processors, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Enter login credentials** page appears.
3. Enter credentials for the administrator account on the target iLOs.
 - **User name** This is an administrative account on the managed iLO. Usually it is the Admin account.
 - **Password** This is the administrative account password on the managed iLOs.
 - **Password (Verify)** Verify the password.
4. Click **Run Now** to run the task immediately. Click **Schedule** to schedule when the task runs, or click **Previous** to return to the previous **Deploy SSH Public Key** page. See “Scheduling a task” for more information about scheduling a task.

Cycling on the power on an HP ProLiant iLO

This tool enables you to cycle the power on a single HP ProLiant Integrated Lights Out (iLO) system.

To cycle the power:

1. Select **Tools**→**Management Processor**→**HP ProLiant iLO**→**Power Cycle**. The **Power Cycle** page appears.
2. Select target system, and click **Next**. See “Creating a task” for information about selecting a target. The **Step 2: Task confirmation** page appears.
3. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **Power Cycle** page. See “Scheduling a task” for more information about scheduling a task.

Powering on a system managed by an HP ProLiant iLO

This tool enables you to power on a system managed by an HP ProLiant Integrated Lights Out (iLO) system.

To power on a system:

1. Select **Tools**→**Management Processor**→**HP ProLiant iLO**→**Power On**. The **Power On** page appears.
2. Select target system, and then click **Next**. See “Creating a task” for information about selecting a target. The **Step 2: Task confirmation** page appears.
3. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **Power On** page. See “Scheduling a task” for more information about scheduling a task.

Related procedure

- ▲ Powering off a system managed by an HP ProLiant iLO

Powering off a system managed by an HP ProLiant iLO

This tool enables you to power off a system managed by an HP ProLiant Integrated Lights Out (iLO) system.

To power off a system:

1. Select **Tools**→**Management Processor**→**HP ProLiant iLO**→**Power Off**. The **Power Off** page appears.
2. Select target system, and then click **Next**. See “Creating a task” for information about selecting a target. The **Step 2: Task confirmation** page appears.
3. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **Power Off** page. See “Scheduling a task” for more information about scheduling a task.

Related procedure

- ▲ Powering on a system managed by an HP ProLiant iLO

Turning on the UID for a system managed by an HP ProLiant iLO

This tool enables you to turn on the Unit Identification Light (UID) on an HP ProLiant Integrated Lights Out (iLO) system.

To turn off the UID:

1. Select **Tools**→**Management Processor**→**HP ProLiant iLO**→**Turn On Unit Identification Light**. The **Turn On Unit Identification Light** page appears.
2. Select target system, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Task confirmation** page appears.
3. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **Turn On Unit Identification Light** page. See “Scheduling a task” for more information about scheduling a task.

Related procedure

- ▲ Turning off the UID for a system managed by an HP ProLiant iLO

Turning off the UID for a system managed by an HP ProLiant iLO

This tool enables you to turn of the Unit Identification Light (UID) on an HP ProLiant Integrated Lights Out (iLO) system.

To turn off the UID:

1. Select **Tools**→**Management Processor**→**HP ProLiant iLO**→**Turn Off Unit Identification Light**. The **Turn Off Unit Identification Light** page appears.
2. Select target system, and then click **Next**. See “Creating a task” for information about selecting targets. The **Step 2: Task confirmation** page appears.
3. Click **Run Now** to run the task immediately. Click **Schedule** to schedule the task to run at another time, or click **Previous** to return to the previous **Turn Off Unit Identification Light** page. See “Scheduling a task” for more information about scheduling a task.

Related procedure

- ▲ Turning on the UID for a system managed by an HP ProLiant iLO

Managing Communications

The **Manage Communications** feature enables you to troubleshoot communication problems between the Central Management Server (CMS) and targeted systems. For each failed communication function, troubleshooting information is available. You can reconfigure certain communication settings, launch agents, and push certificates to target systems. This feature is available from the **Configure**→**Manage Communications** menu and includes the following information:

- Communication status
- Manage Communications table columns
- Manage Communications main page buttons

Manage Communications Maximize ?

Targets: **All Servers**

To maximize the manageability of each system, HP SIM can configure communication protocols, passwords, agents.

Placing the cursor over a status icon will show when the data was last updated. To get more recent status, select the system(s) and click the "Update" button. The update process may take several minutes.

Summary: ✖ 0 Critical ▽ 11 Major ▲ 4 Minor ✔ 23 Normal 23 Disabled ? 0 Unknown Total: 61

<input type="checkbox"/>	System Name	Identification	Events	Run Tools	Version Control	System Type	OS Name
<input type="checkbox"/>	1.8.1021.1.78.05	✔	✖	✖	▽	Server	Microsoft Windows Serv...
<input type="checkbox"/>	1.8.1021.1.78.01	✔	✖	✖	▽	Server	Linux - VMware ESX Ser...
<input type="checkbox"/>	1.8.1021.1.78.02	✖	✖	✖	?	Server	HP-UX
<input type="checkbox"/>	1.8.1021.1.78.09	✔	✖	✖	▽	Server	Linux - VMware ESX Ser...
<input type="checkbox"/>	1.8.1021.1.78.7	✖	✖	✖	?	Server	HP-UX
<input type="checkbox"/>	1.8.1021.1.78.77	✖	✖	✖	?	Server	
<input type="checkbox"/>	1.8.1021.1.78.78	✔	✖	✖	▽	Server	LINUX
<input type="checkbox"/>	1.8.1021.1.78.05	✖	✖	✖	?	Server	
<input type="checkbox"/>	1.78.50.0.1.36	✔	✖	✖	▽	Server	LINUX
<input type="checkbox"/>	1.78.50.0.33 #-E1621-81401	✔	✖	✖	▽	Server	Linux - Red Hat Enterp...
<input type="checkbox"/>	1.78.50.0.41	✔	✖	✖	▽	Server	Microsoft Windows Serv...
<input type="checkbox"/>	6440-380Ag5-w2k3	✔	✖	✖	▽	Server	Microsoft Windows Serv...
<input type="checkbox"/>	6417-4895C	✖	✖	✖	▽	Server	Microsoft Windows Serv...
<input type="checkbox"/>	6440Ag5	✔	✖	✖	▽	Server	Microsoft Windows Serv...

Communication status

The communication status between the CMS and the targeted systems appear in the table. Placing your mouse over a status icon displays available information explaining the status. If you click the status icon, the **Advise and Repair** section appears with the corresponding tab open. For example, if you click a status icon in the **Run Tools** column, the **Run Tools** tab is open in the **Advise and Repair** section instead of the default **Identification** tab.

Manage Communications table columns

Columns display the status of an operation between the CMS and the targeted systems. See:

- Selection
- System Name
- Identification
- Events
- Run Tools
- Version Control
- System Type
- OS Name



NOTE: Systems that do not have an IP address (enclosures, racks, clusters, complex, and storage devices) have no status displayed.

Selection

Select the checkbox in this column to select a system. You can select more than one system. Select the checkbox in the column heading to select or deselect all displayed systems.

System Name

This column contains the actual system name of all discovered systems. Systems can be shown as a single system or as a system in a container. When you place the cursor over the system name, the full system

Domain Name Service (DNS) name is displayed, which helps differentiate between two or more systems that share the same system name. If you click the system name link, the **System Page** is displayed. See “System Page” for more information. If you click a system that is a container (rack or enclosure), the picture view for that object is displayed. See “Navigating the picture view page” for more information. See “About racks and enclosures” for more information about racks and enclosures.

The **System Name** column displays systems along with their associations.

Identification

The **Identification** column includes status information on the state of an identification process. Identification attempts to determine what the system type is, what management protocol a system supports, using credentials from the **Global Protocol Settings** page, and attempts to determine the operating system and version loaded, along with other basic attributes about the system. Finally, it determines if the system is associated with another system. The status in this column is a roll-up of the status of all available protocols. The statuses are analyzed based on the status itself, the system type, the system operating system, and instrumentation options. There are no status icons for systems that cannot have a status, such as, complexes, enclosures, and racks. The identification status is updated each time an identification task runs.

Events

The **Events** column indicates if the CMS can receive events from the target systems. This status considers the setting of SNMP traps and WBEM indications.



NOTE: For HP-UX, if sending a package to test if the CMS name or IP address exists on the managed systems does not work, then testing sending trap destinations is not supported.

NOTE: The informational icon is displayed if the **Daily Check Event Configuration** task has not run or if the system does not support events.

Run Tools

The **Run Tools** column indicates if the CMS can run tools locally on target systems. For example, System Management Homepage (SMH). Communication issues in this column usually relate to security and trust relationships. See “Setting up trust relationships” for more information about setting up trust relationships.

Version Control

The **Version Control** column indicates the availability of the software and firmware inventory data for target systems. The status is collected and stored during data collection.

System Type

This column displays the system type, for example, Server or Desktop. The Unmanaged system type indicates systems that have no management protocol that HP SIM can detect, for example, no *Simple Network Management Protocol*, *Web-Based Enterprise Management (WBEM)*, *Desktop Management Interface (DMI)*, or Secure Shell (SSH). The Unknown system type indicates that none of the built-in or System Type Manager (STM)-based tasks could identify the system. However, some management protocol was detected on the system. See “System types” for more information about system types. See “Managing system types” for more information about STM tasks.

OS Name

The operating system of the target systems.

Manage Communications main page buttons

- Advise and Repair
- Quick Repair
- Update
- Print


Advise and Repair

This button displays the **Advise and Repair** section and includes a tabbed interface with a tab for each functional column (**Identification**, **Events**, **Run Tools**, and **Version Control**). Each tab displays the diagnostic results and includes troubleshooting tips and advice for fixing communication problems. See “[Advising and repairing managed system settings](#)” for more detailed information.

Quick Repair

This button launches the **Configure and Repair Agents** tool. Configure or Repair Agents enables you to quickly and optimally configure systems for manageability. See “[Repairing managed system settings](#)” for more detailed information.

Update

This button runs to get an updated communication status. During the update process, the status icon first changes to the  icon. As data becomes available, the correct status icon is displayed.

Print

This button is used to create a printer friendly version of the list in a new window. Within the window, select **File**→**Print** from the browser menu to print the report. See “[Printing Manage Communications table](#)” for more detailed information.

Related procedures

Related procedure

- [Advising and repairing managed system settings](#)
- [Updating communication statuses](#)
- [Repairing managed system settings](#)
- [Printing Manage Communications table](#)

Advising and repairing managed system settings

The Advise and Repair tool diagnoses many problems with managed system communication and displays the results of the diagnosis as well as advice for resolving the problem. This tool is very helpful when you are trying to troubleshoot communication problems between the *Central Management Server (CMS)* and managed systems.

To run the Advise and Repair tool on selected systems:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. For more information, see “[Creating a task](#)”.
3. Click **Run Now**. The System List appears.
4. Select the systems to be repaired.
5. Click **Advise and Repair**. The **Advise and Repair** section appears below the System List.
6. The following tabs display.
 - **Identification**. This tab displays detailed system identification errors and recommendations for resolving the problems. For more detailed information, see “[Identification tab](#)” .
 - **Events**. This tab displays detailed error messages and recommendations for generating and receiving events. For more detailed information, see “[Events tab](#)”.
 - **Run Tools**. This tab displays any problems that a Central Management Server(CMS) has for executing a tool on a managed system. For more detailed information, see “[Run Tools tab](#)”.
 - **Version Control**. This tab displays error messages that appear when the CMS attempts to run the version control tool. See “[Version Control tab](#)” for more detailed information.

Related procedures

- [Repairing managed system settings](#)
- [Events tab](#)
- [Identification tab](#)

- Run Tools tab
- Version Control tab
- Updating communication statuses
- Printing Manage Communications table
- Windows CMS
- HP-UX and Linux CMS

Related topic

- ▲ Managing Communications

Identification tab

The Advise and Repair **Identification** tab is launched by default when you click **Advise and Repair** from the **Manage Communications** page. It can also be launched when you click a status icon in the **Identification** column in the table on the **Manage Communications** page.

This tab displays detailed identification errors and recommendations for fixing the errors. Identification communication status and errors are generated based on the system type, the operating system that the managed system is running, the availability of management protocols on the managed systems, and if the protocol has a higher weight than other protocols. Each **Causes and Recommendations** section can be expanded for each error.

Accessing the **Identification** tab:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Advise and Repair**. The **Advise and Repair** section appears.
4. Click the **Identification** tab.

Related procedures

- Events tab
- Run Tools tab
- Version Control tab
- Repairing managed system settings

Related topics

- Repairing managed system settings
- Managing Communications

Events tab

The **Events** tab includes detailed error messages and recommendations for generating and receiving events. The event error codes are captured and stored during data collection, identification, and status polling. For HP Systems Insight Manager (HP SIM) to receive events from managed systems, either a WBEM subscription must be created, or the Central Management Server (CMS) IP address must be in the SNMP trap destination list on the managed system. Each **Causes and Recommendations** section can be expanded for each error.

Accessing the **Events** tab:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Advise and Repair**. The **Advise and Repair** section appears.
4. Click the **Events** tab.

Related procedures

- Managing Communications
- Identification tab

- Run Tools tab
- Version Control tab
- Repairing managed system settings

Related topics

- Repairing managed system settings
- Managing Communications

Run Tools tab

The **Run Tools** tab includes detailed error messages and recommendations for problems that a Central Management Server (CMS) has for executing a tool on a target system. These problems are often issues related to security and trust. Each **Causes and Recommendations** section can be expanded for each error.

Accessing the **Run Tools** tab:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Advise and Repair**. The **Advise and Repair** section appears.
4. Click the **Run Tools** tab.

Related procedures

- Managing Communications
- Identification tab
- Events tab
- Version Control tab
- Repairing managed system settings

Related topics

- Repairing managed system settings
- Managing Communications

Version Control tab

The **Version Control** tab includes detailed error messages and recommendations for problems that a Central Management Server (CMS) has when trying to collect software and firmware inventory from managed systems. Each **Causes and Recommendations** section can be expanded for each error.

Accessing the **Run Tools** tab:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click the **Version Control** tab.

Related procedures

- Managing Communications
- Identification tab
- Events tab
- Run Tools tab
- Repairing managed system settings

Related topics

- Repairing managed system settings
- Managing Communications

Repairing managed system settings

The Quick Repair tool enables you to repair communication problems with managed systems by launching the Configure or Repair Agents tool. Managed systems must be able to communicate status to the HP Systems Insight Manager (HP SIM) Central Management Server (CMS) in order for commands to be launched to the managed systems. To configure the managed *systems* to communicate with the CMS, common configurations and trust relationships must be configured. The *Configure or Repair Agents* feature enables you to configure or repair agents in Windows, Linux, and HP-UX.

This tool is very helpful when you want to repair communication problems between the *Central Management Server* (CMS) and managed systems.

To repair communication problems on selected systems:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Run Now**. The System List appears.
4. Select the systems to be repaired from the list.
5. Click **Quick Repair**. The **Step 2: Enter Credentials** section appears below the System List.
6. From the **Step 2: Enter credentials** page:
 - a. In the **User name** field, enter the system administrator name.
 - b. In the **Password** field, enter the system administrator's password for the user name previously entered.
 - c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

7. Click **Next**. The **Step 3: Install Providers and Agents (Optional)** page appears.

Step 3: Install Providers and Agents (Optional)

If agents or providers are already installed, skip this step and proceed to the configuration step.

By installing agents or providers on the managed systems, HP SIM will be able to collect inventory and status information from the systems. It will also enable HP SIM to receive event notifications from the system(s). In most cases, you will want to install either WBEM / WMI providers or SNMP agents, but not necessarily both.
This option applies only to ProLiant or Itanium-based Systems with Windows Operating Systems

- Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** [Learn More...](#)
- Install SNMP Agent (HP Insight Management Agents) for Windows** [Learn More...](#)
- Install Open SSH** SSH is used for running tools remotely on managed systems. [Learn More...](#)
- Install the Version Control Agent for Windows (VCA)** The VCA, in conjunction with the HP ProLiant Version Control Repository Manager, enables management of the HP ProLiant software and firmware on the managed systems. [Learn More...](#)

For selected installs:

- Force downgrade, or reinstall the same version
- Reboot system(s) if necessary after installation

Click “Next” to configure the providers and agents

< Previous Next >

8. You can install Insight Management Agents or providers, either *Web-Based Enterprise Management* or *Simple Network Management Protocol*, on managed systems so HP SIM can collect inventory and status information from these systems and receive event notifications from the systems. Installation is supported only on ProLiant or Itanium-based servers with Windows operating system.

From the **Step 3: Install Providers and Agents (Optional)** page:

- a. Select **Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** to install *WBEM* or *WMI* providers on Windows managed systems.
- b. Select **Install SNMP Agent (HP Insight Management Agents) for Windows** to install the *SNMP* agent on Windows managed systems. This Insight Management Agent allows network monitoring and control.

- c. Select **Install Open SSH** to install *OpenSSH* on Windows managed systems. See “Installing OpenSSH” for more information.
- d. Select **Install the Version Control Agent (VCA)** to install the *HP Version Control Agent*; (VCA) on Windows managed systems. The VCA enables you to view the HP software installed on a system and when updates for the software are available in the repository. See “About the Version Control Agent” for more information.

HP SIM determines the type of agent/provider to install based on the system type, subtype, and operating system description of the system.

Table 12-2 Version Support Matrix for components used for install.

Supported systems	HP WBEM Provider	HP ProLiant Agent	Open SSH	Version Control Agent
Unknown	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (32 bit)	7.90 (32 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating system (2003, 2008)	2.1 (64 bit)	7.90 (64 bit)	3.71	2.1.8
ProLiant systems with 32 bit Windows operating systems (2000)	Not supported	7.60 (32 bit)	3.71	2.1.8
Itanium-based systems with Windows operating system (2003)	Not supported	5.1.10	3.71	2.1.7.770

System Management Homepage version 2.1.7 is also installed, if necessary, with these agents.



NOTE: If you wish to install a 64 bit agent or provider, make sure the target system is identified as a 64 bit system in HP SIM.

If your system is not correctly identified, go to **System Page** → **Edit System Properties**. Select the correct system type, subtype and enter the operating system description manually.

Edit System Properties

blade31
Go back to blade31

System Information

Identification

Preferred system name: [Restore default name](#)

Prevent the Discovery process from changing this system name

Serial number:

Product Description

System type:

System subtype 1:

System subtype 2:

System subtype 3:

System subtype 4:

System subtype 5:

System subtype 6:

System subtype 7:

System subtype 8:

Product model:

Hardware description:

Operating system description:

Example: Installing Insight Management Agents on a ProLiant Windows 64 bit system:

1. Select system **Type**: server.
2. Select system **subtype 1**: ProLiant
3. Enter operating system description as Microsoft Windows Server 2003, x64 Enterprise Edition Service Pack 1 or the correct operating system description of your system.

If you want to configure the agents after installing, select the force reboot option. This allows the newly installed component to be completely initialized before configuring it.

Note: Installation with reboot typically takes about 8 minutes to complete.

9.

10. Click **Run Now**. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The log results indicate whether the repair attempt was successful.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed. This exit code does not indicate that all configuration attempts were successful. It is possible for some to succeed and for some to fail.
- **Target Name.** This field displays the name/IP address of the target.
- **The stdout tab.** This tab displays the output text information.
- **The stderr tab.** This tab displays information if the executable experienced an error.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

a. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.

b. Select which report to display.

c. Click **OK** to display the report, or click **Cancel** to return to the **View Task Results** page.

11. If the Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Related procedure

▲ Repairing managed system settings


Related topics

- Advising and repairing managed system settings
- Updating communication statuses
- Printing Manage Communications table
- Windows CMS

Related topic

▲ Managing Communications

Updating communication statuses

Selecting **Update** runs tools on the selected systems, including identification and software status polling, and runs tests for SSH, trust status, and *Web-Based Enterprise Management* (WBEM) indications. As the tests complete, the status in the Manage Communications table updates. During the update process, the status icon first changes to the  icon. As data becomes available, the correct status icon is displayed.

Perform this procedure to accomplish these results.

To update the communication status between the CMS and target systems:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Update**.

Related procedures

Related procedure

- Repairing managed system settings
- Printing Manage Communications table

Related topic

- ▲ Managing Communications

Printing Manage Communications table

To display and print the manage communications table:

1. Select **Configure**→**Manage Communications**. The **Select Target Systems** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Print**.
4. When the table is displayed, select **File**→**Print** from the browser menu.

Because certain print options are not supported in HP SIM, you cannot perform the following tasks:

- Change the **Orientation** to **Landscape** in the **Print** dialog box (see **Printing Problems** in “Troubleshooting” for a workaround to this issue)
- Cancel printing after the print job has been executed; however, you can access the operating system's print queue and cancel the print job
- Print to a file
- Print specific selections; you can print the entire list only
- Print the table view page if you close the browser immediately after issuing a print request

Related procedures

- Repairing managed system settings
- Repairing managed system settings
- Updating communication statuses

Related topic

- ▲ Managing Communications

Firewall

A firewall might be preventing HP Systems Insight Manager (HP SIM) from communicating with the managed system. If a firewall is installed on the managed system, or lies between the HP SIM Central Management Server (CMS) and the managed system, then it must be configured to allow management communication. The CMS must be able to make requests to and receive responses from the managed system, and the managed system must be able to send alerts to the Central Management Server.

Ports used by HP SIM which might need to be configured in a firewall

The following inbound ports must be open on each managed system:

Description	Port	Protocol
Ping Discovery (ICMP)**	ICMP	ICMP
Ping Discovery (TCP)**	TCP 80	HTTP
SSH port++	TCP 22	SSH
SNMP Agent	UDP 161	SNMP
HP SMH Web Server*	TCP 2301	HTTP

Description	Port	Protocol
HP SMH Secure Web Server*	TCP 2381	HTTPS
WBEM/WMI Mapper Secure Port+	TCP 5989	HTTPS

The following outbound ports must be open to allow communication between a managed system and the Central Management Server. Not all firewalls on managed systems block outbound requests.

Description	Port	Protocol
SNMP Trap	UDP 162	SNMP
WBEM/WMI Mapper Secure Port+	TCP 50004	HTTPS

* If the system is not being managed from HP SIM, only ports 2301 and 2381 must be configured to enable browser access to System Management Homepage.

** Usage is configurable in HP SIM and Internet Control Message Protocol (ICMP) echo is used by default.

+ Only open port 5989 and 50004 on a Windows system if the WMI mapper is installed.

++ Only open port 22 if OpenSSH is installed.

See the *Understanding HP SIM 5.0 security* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

Configuring the firewall

Configuring the firewall on a Windows system

The following steps describe how to configure the Microsoft Windows firewall on a managed server. If a firewall from a different vendor is used, then you must follow the instructions from your vendor, open the inbound, and possibly the outbound, ports from the table above, and enable remote administrative access through the firewall.

1. Select **Start**→**Settings Control Panel**.
2. Double-click **Windows Firewall** to configure the firewall settings.
3. Select **Exceptions**.
4. Click **Add Port** and add the ports from the inbound table above.
 - a. In the **Name** field, enter the protocol.
 - b. In the **Port number** field, enter the port number.
 - c. Click **OK** to save your settings and close the **Add a Port** dialog box.
5. Enable file and print sharing.
 - a. Select **File and Print sharing**.
 - b. Click **OK**.
6. Click **OK** to save your settings and close the **Windows Firewall** dialog box.
7. Enable Remote Administration Exception:
 - a. In the **Control Panel**, open the **Group Policy** editor.
 - b. Select **Computer Configuration**→**Administrative Templates**→**Network**→**Network Connections**→**Windows Firewall**→**Domain Profile**→**Enable the Windows Firewall: Allow Remote Administration Exception**.

Configuring the firewall on an HP-UX system

The HP-UX IPFilter firewall is included with HP-UX 11iv2 and might need to be installed on earlier versions of HP-UX. To configure the firewall, a firewall rule-set must be added to the `/etc/ipt/ipf/ipf.conf` file and the openings for the ports in the table above must be added. See the [ipf\(5\)](#) manpage for details on the file format. See the [ipf\(8\)](#) manpage for instructions on enabling the firewall.

Alternatively, HP-UX Bastille can be used to create and enable the firewall configuration. Simply add the ipf-formatted firewall port-openings from the table above to the `/etc/opt/sec_mgmt/bastille/ipf.customrules` file and use the HP-UX Bastille wizard. See the [bastille\(1\)](#) manpage for more information.

Configuring the firewall on a Linux system

Firewalls are configurable various ways depending on the version of Linux installed.

Red Hat Enterprise Linux 3 and 4

The following list displays an example for iptables firewall rules for Red Hat Enterprise Linux 3 and 4 in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

The following list displays the new value for iptables firewall rules for Red Hat Enterprise Linux 3 that allows access to SMH in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```



```
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2301 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2381 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

SuSE Linux Enterprise Server

SuSE Linux Enterprise Server 8 and 9 firewalls are configured using the YAST2 utility.

1. Using the YAST2 utility, select **Security & Users**→**Firewall**. The **Firewall Configuration (Step 1 of 4): Basic Settings** window appears.
2. Click **Next**. The **Firewall Configuration (Step 2 of 4): Services** window appears.
3. In the **Additional Services** field, enter 2301:2381 and click **Next**. The **Firewall Configuration (Step 3 of 4): Features** window appears.
4. Click **Next**. The **Firewall Configuration (Step 4 of 4): Logging Options** window appears.
5. Click **Next**. A dialog box displays asking you to confirm your intention to save settings and active firewall.
6. Click **Continue**. The firewall is configured and your settings are saved.

Installing and configuring protocols

The following management protocols are used by HP Systems Insight Manager (HP SIM):

- **Web-Based Enterprise Management (WBEM)** An Industry initiative to provide management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM client applications.

For HP-UX, WBEM is included in the operating system install. For Linux Itanium Processor Family (IPF), WBEM must be manually installed. Go to the HP Software Depot (<http://www.software.hp.com/>) to download. The WBEM download from the openPegasus website does not include the hardware specific data for HP SIM to manage Linux x86 systems.



NOTE: *Windows Management Instrumentation (WMI)* is the implementation of WBEM from Microsoft. See *WMI* for more information.

To install the HP Insight Management WBEM Provider, which is an HP extension of WBEM providers for managing ProLiant systems running Windows 2003, from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install WBEM/WMI Provider (HP Insight Management WBEM Provider) for Windows** .



NOTE: The WBEM providers cannot be installed on HP-UX or Linux systems.

NOTE: A Common Information Model Object Manager (CIMOM) acts as the interface for communication between WBEM providers and management applications such as HP SIM.

The CMS must have the correct credentials to authenticate to WBEM and WMI. There are two ways to authenticate HP SIM to a client:

- Basic authentication to WBEM Services or WMI using user name and password.
- Using the CMS certificate to authenticate is available only for HP-UX WBEM Services 02.05.00, which supports client certificate authentication. Use the Configure or Repair Agents **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the**

system option to deploy a WBEM certificate to the managed system and is only valid for HP-UX systems.

- **WMI** An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled.

The WMI Mapper Proxy is a configuration setting for WMI. The WMI Mapper receives client CIM/XML WBEM requests and converts the requests to *Windows Management Instrumentation* (WMI) requests. The WMI results are converted to CIM/XML format and returned to the Central Management Server (CMS). The *discovery* and *Identification* task uses the proxies in the WMI Mapper Proxy list to discover whether a *system* is a WMI-enabled system. If the system is WMI-enabled, then the identification information for that system based on that specific proxy is returned.

The WMI Mapper makes it possible to retrieve WMI instrumented data on a Windows machine through WBEM requests. The Windows version of HP SIM installs this WMI Mapper locally so that it can make WMI requests across the network to the systems without the need to install the WMI Mapper on the managed Windows systems.

The WMI Mapper is included in a Typical install of HP SIM on a Windows CMS (optional in a Custom install) . For HP-UX and Linux-based CMS's, the WMI Mapper is not available.

- **Simple Network Management Protocol (SNMP)** One of the management protocols supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.

For Windows systems, if SNMP itself is not installed during the operating system installation, you can install it from the Windows CD using **Add Remove Windows Component** feature.

For Linux systems, SNMP itself is part of the initial installation of the Linux operating system. If it was not installed during the initial operating system installation, you must install the SNMP .rpm file manually from the operating systemCD.

For HP-UX systems, SNMP itself is part of the operating system installation.

HP Insight SMMP agents are HP specific SNMP agents used to better manage ProLiant systems. To install HP Insight SNMP agents for Windows systems, select **Configure**→**Configure or Repair Agents, Install Providers and Agents**→**Install SNMP agents (HP ProLiant Insight Management Agents) for Windows**.

To install the SNMP provider from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install SNMP Agents (HP ProLiant Insight Management Agents) for Windows**.

To install the HP Insight SNMP agents for ProLiant systems running on Linux x86 operating system, go to <http://www.software.hp.com/> and select the ProLiant Support Pack 7.90.



NOTE: The HP Insight SNMP agents cannot be installed on HP-UX systems.

For HP SIM to manage target systems using SNMP protocol, verify on the target system that the SNMP service allows a remote connection from the CMS. If there are different read community sets on the target system, ensure that the read community string is configured in CMS SNMP protocol. The read community string can be set on the target through Replicate Agent Settings, by selecting **Configure**→**Configure or Repair Agents**, in step 4. See “Windows CMS” for additional information.

To configure the read community string on the CMS for one or more systems, select **Options**→**Protocol Settings**→**System Protocol Settings** from the HP SIM menu. Or select **Options**→**Protocol Settings**→**Global Protocol Settings**, and set the read community string for multiple systems.

To configure the read community string on the CMS, select **Options**→**Protocol Settings**→**System Protocol Settings** from the HP SIM menu. To configure the read community string for multiple systems, select **Options**→**Protocol Settings**→**Global Protocol Settings** and set the read community string.

- **Desktop Management Interface (DMI)** An industry-standard protocol, primarily used in client management, established by the Desktop Management Task Force (DMTF). DMI provides an efficient

means of reporting client system problems. DMI-compliant computers can send status information to a central management system over a network.

For HP-UX and Linux-based systems, you can download DMI from the HP Software Depot (<http://www.software.hp.com/>).

- **OpenSSH** A set of network connectivity tools providing encrypted communication sessions over a computer network using SSH. It was created as an open source alternative to the proprietary SSH software suite offered by SSH Communications Security.

You can download OpenSSH from the HP Software Depot (<http://www.software.hp.com/>).

To install OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**. To configure OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**→**Configure secure shell (SSH) access**.



NOTE: OpenSSH can also be installed from the HP SIM menu by selecting **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install OpenSSH**.

- **Secure Shell (SSH)** SSH is used to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

You can download SSH from the HP Software Depot (<http://www.software.hp.com/>).

To install the SSH provider from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**. To configure OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**→**Configure secure shell (SSH) access**.

Related procedures

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols
- Adding a WMI Mapper Proxy
- Deploying OpenSSH to multiple systems using RDP
- Installing OpenSSH
- Creating an OpenSSH task through the CLI
- Configuring DMI access
- Configuring SNMP access

Related topics

- Global protocols
- WMI Mapper Proxy
- Configuring or repairing agents

Trusted certificates

Trusted *certificates* provide the highest level of security. Users with *administrative rights* can import certificates from other systems into the HP Systems Insight Manager (HP SIM) Trusted System Certificates List.

The purpose of the Trusted System Certificates List in HP SIM is to maintain a list of certificates in the HP SIM *keystore*. Certificates include the HP SIM system certificate and the certificates of *managed systems* that are trusted by the HP SIM system. These imported certificates are placed in the keystore and are displayed in the Trusted System Certificates List.

There are two options for accepting managed system certificates; **Always Accept** and **Require. Always Accept** is the default option, but is vulnerable to man-in-the-middle attacks. With this option selected, as you browse to each managed system, their certificate is added to the HP SIM Trusted System Certificate List. If

you select **Require**, you must set up the trust by manually installing the system's certificate into the HP SIM Trusted System Certificate List. This option is the most secure.



NOTE: The HP SIM certificate must also be installed on the managed system. See "Exporting a server certificate" for more information about exporting the HP SIM server certificate.

Importing trusted certificates

If you have selected **Require** on the **Trusted System Certificates** page, you must import certificates that represent the *managed systems* you want to trust to the Trusted Certificates List. You can import the *certificate* of the system itself on a per-system basis. You can also import the signing certificate of the *Certificate Authority (CA)* or intermediate CA used to sign and issue certificates for groups of systems, which simplifies the maintenance of this list.

1. Select **Options**→**Security**→**Certificates**→**Trusted Certificates**, and then click **Import**. The **Import Trusted System Certificate** section appears.
2. Next to the **Certificate filename** field, click **Browse**.
The **Choose file** dialog box appears.
3. Navigate to the location of the certificate to be imported, and then select the file name. Click **Open**.
The certificate is imported.

For *Single Login* and *Secure Task Execution (STE)* to function properly, the *managed system* must be running a supported agent and be configured to trust the HP SIM server. The trust mode is configured from the System Management Homepage (SMH). The following trust modes are available:

Trust By Certificate. The **Trust by Certificate** mode sets the **System Management Homepage** to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of a digital signature and certificates. This mode provides the highest level of security because it verifies the digital signature before allowing access. HP recommends this option.



NOTE: If you do not want to enable any remote configuration changes by HP SIM, leave **Trust by Certificate** selected, and leave the list of trusted systems empty.

Trust By Name. The **Trust By Name** mode sets the **System Management Homepage** to accept certain configuration changes only from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure, and prevents nonmalicious access. For example, you might use this option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server name submitted, not the digital signature.

Trust All. The **Trust All** mode sets the **System Management Homepage** to accept configuration changes from any system. For example, you could use the **Trust All** option if you have a secure network, and everyone in the network is trusted.



NOTE: For **Trust By Certificate**, the certificate from the HP SIM system can be installed during the initial support pack deployment. See "Initial ProLiant Support Pack Install" for more information.

Related topics

- Requiring trusted certificates
- Importing trusted certificates
- Setting up trust relationships
- Exporting trusted certificates

Setting trust relationships

Configuration of the managed system

For *Single Login* and *Secure Task Execution* (STE) to function properly, the *managed system* must be running a supported agent and be configured to trust the HP SIM server. The trust mode is configured from the System Management Homepage (SMH). The following trust modes are available:

Trust By Certificate. The **Trust by Certificate** mode sets the **System Management Homepage** to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of a digital signature and certificates. This mode provides the highest level of security because it verifies the digital signature before allowing access. HP recommends this option.



NOTE: If you do not want to enable any remote configuration changes by HP SIM, leave **Trust by Certificate** selected, and leave the list of trusted systems empty.

Trust By Name. The **Trust By Name** mode sets the **System Management Homepage** to accept certain configuration changes only from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure, and prevents nonmalicious access. For example, you might use this option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server name submitted, not the digital signature.

Trust All. The **Trust All** mode sets the **System Management Homepage** to accept configuration changes from any system. For example, you could use the **Trust All** option if you have a secure network, and everyone in the network is trusted.



NOTE: For **Trust By Certificate**, the certificate from the HP SIM system can be installed during the initial support pack deployment. See “Initial ProLiant Support Pack Install” for more information.

Importing the HP SIM certificate over the network

If you prefer importing the HP SIM certificate from a file, see [Importing the HP SIM certificate from a file](#) for more information.

1. From a web browser, navigate to the managed server using the address:
https://managed-server:2381. The **System Management Homepage** appears.
2. Log in to the **System Management Homepage**.
3. On the **Settings** tab, select **System Management Homepage**→**Security**.
4. Click **Trust Mode**. The **Trust Mode** page appears.
5. To require trusted certificates, select **Trust by Certificate**.
6. To save the trust mode, click **Save Configuration**, or to cancel all changes, click **Reset Values**.
7. Click the browser **Back** button to return to the **Trust Mode** page.
8. To access the Trusted Management server certificate, click **Trusted Certificate**.
9. In the text box next to **Add Certificate From Server**, enter the name of the HP SIM server that contains the certificate to be added.
10. Click **Add Certificate From Server**. The certificate information is presented for verification before it is added to the list.

Note: Because this is a nonsecure request over HTTP, a malicious party could intercept the request and substitute an untrusted certificate in response to the request. A more secure method for obtaining the HP SIM certificate is described in the “[Importing the HP SIM certificate from a file](#)” section.

11. Verify the certificate information. , If you want to add it to the Trusted Certificate List, click **Add Certificate to Trust List**.

Note: If you are setting up a trusted certificate on a cluster, see “[Cluster](#)” for more information.

Related topics

- ▲ [Setting up trust relationships](#)

Configuring WMI Mapper proxy

You can configure *Web-Based Enterprise Management* (WBEM) certificates for HP-UX systems and WBEM/*Windows Management Instrumentation* (WMI) users for Windows systems with HP Insight Management WBEM Providers for Windows Server 2003/2008.

From a Windows Central Management Server (CMS), you can install HP Insight Management WBEM Providers for Windows Server 2003/2008 x64 Editions including:

- OpenSSH
- HP Version Control Agent (VCA) for Windows
- HP Insight Management Agents for Windows to Windows Managed systems

Any system that has a HP Insight Management WBEM Providers for Windows Server 2003/2008 x64 Editions WBEM providers profile identified have data collected through this provider taking precedence over WMI/*Simple Network Management Protocol* (SNMP) collection.

By installing HP Insight Management WBEM Providers for Windows Server 2003/2008 x64 Editions, more data about ProLiant systems is provided than what you would otherwise receive, including:

- Memory
- CPU
- IO (PCI)
- Firmware
- Management Processors
- Network
- Power Supplies
- Cooling
- Small Computer System Interface (SCSI) Host Bus Adapter (HBA)s
- Smart Array HBAs
- Serial Attached SCSI (SAS) Controllers
- Sensors

To install the HP Insight Management WBEM Provider, which is an HP extension of WBEM providers for managing ProLiant systems running Windows 2003, from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install WBEM/WMI Provider (HP Insight Management WBEM Provider) for Windows** .

To retrieve the most recent version of the HP Insight Management Agent for Windows ProLiant systems, go to the HP Software Depot (<http://www.software.hp.com/>), and enter **HP SIM Insight Management Agents for Windows** in the **Search** box.

Related topic

- ▲ [WMI Mapper Proxy](#)

SNMP

Simple Network Management Protocol

SNMP is one of the management protocols supported by HP Systems Insight Manager. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.

Installing the SNMP agent

For Windows systems, if SNMP itself is not installed during the operating system installation, you can install it from the Windows CD using **Add Remove Windows Component** feature.

For Linux systems, SNMP itself is part of the initial installation of the Linux operating system. If it was not installed during the initial operating system installation, you must install the SNMP .rpm file manually from the operating system CD.

For HP-UX systems, SNMP itself is part of the operating system installation.

HP Insight SMMP agents are HP specific SNMP agents used to better manage ProLiant systems. To install HP Insight SNMP agents for Windows systems, select **Configure**→**Configure or Repair Agents, Install Providers and Agents**→**Install SNMP agents (HP ProLiant Insight Management Agents) for Windows**.

To install the SNMP provider from the **Manage Communications** page, select **Quick Repair**→**Install Providers and Agents**→**Install SNMP Agents (HP ProLiant Insight Management Agents) for Windows**.

To install the HP Insight SNMP agents for ProLiant systems running on Linux x86 operating system, go to <http://www.software.hp.com/> and select the ProLiant Support Pack 7.90.



NOTE:

The HP Insight SNMP agents cannot be installed on HP-UX systems.

For HP SIM to manage target systems using SNMP protocol, verify on the target system that the SNMP service allows a remote connection from the CMS. If there are different read community sets on the target system, ensure that the read community string is configured in CMS SNMP protocol. The read community string can be set on the target through Replicate Agent Settings, by selecting **Configure**→**Configure or Repair Agents**, in step 4. See “Windows CMS” for additional information.

To configure the read community string on the CMS for one or more systems, select **Options**→**Protocol Settings**→**System Protocol Settings** from the HP SIM menu. Or select **Options**→**Protocol Settings**→**Global Protocol Settings**, and set the read community string for multiple systems.

Configuring SNMP to send test traps

You can send test traps from the Configure or Repair Agents pages to verify that automatic event handling is configured properly.

1. Select **Configure**→**Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.
Note: The **Step 1: Verify Target Systems** page appears if the targets are selected before selecting a tool.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Note: If you plan to **Configure secure shell (SSH) access** on a Windows target system, the account specified must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group if applicable.

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:	<input type="text"/>
Password:	<input type="password"/>
Password (Verify):	<input type="password"/>
Domain:	<input type="text"/>

[< Previous](#)[Next >](#)

4. From the **Step 2: Enter credentials** page:
 - a. In the **User name** field, enter the system administrator name.
 - b. In the **Password** field, enter the system administrator's password for the user name previously entered.
 - c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.
5. Click **Next**. The **Step 3: Install Providers and Agents (Optional)** page appears.

Step 3: Install Providers and Agents (Optional)

If agents or providers are already installed, skip this step and proceed to the configuration step.

By installing agents or providers on the managed systems, HP SIM will be able to collect inventory and status information from the systems. It will also enable HP SIM to receive event notifications from the system(s). In most cases, you will want to install either WBEM / WMI providers or SNMP agents, but not necessarily both. This option applies only to ProLiant or Itanium-based Systems with Windows Operating Systems.

- Install WBEM / WMI Provider (HP Insight Management WBEM Provider) for Windows** [Learn More..](#)
- Install SNMP Agent (HP Insight Management Agents) for Windows** [Learn More..](#)
- Install Open SSH** SSH is used for running tools remotely on managed systems. [Learn More..](#)
- Install the Version Control Agent for Windows (VCA)** The VCA, in conjunction with the HP ProLiant Version Control Repository Manager, enables management of the HP ProLiant software and firmware on the managed systems. [Learn More..](#)

For selected installs:

- Force downgrade, or reinstall the same version
- Reboot system(s) if necessary after installation

Click "Next" to configure the providers and agents

[< Previous](#)[Next >](#)

6. Click **Next**. The **Step 4: Configure or Repair Agents** page appears.

Configure WBEM / WMI [Learn More..](#)

Create subscription to WBEM events

Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM event lists.

Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system. *This will deploy a WBEM certificate to the managed system. This option is only valid for HP-UX systems.*

Configure a non-administrative account for HP SIM to access WMI data [Learn More..](#)

This option applies only to Windows Systems with HP WBEM Provider installed.
Administrative accounts can be used without further configuration. If non-administrative access to a managed system is desired, an existing domain account or one local to the managed system can be used by HP SIM to access WMI information over the network.

Enter the credentials for HP SIM to use to access the managed system:

User name:

Password:

Password (Verify):

Domain:

Configure SNMP [Learn More..](#)

Set read community string:

Set traps to refer to this instance of HP Systems Insight Manager *Note: A ReadWrite string will be created automatically on Windows systems.*

Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM event lists.

Configure secure shell (SSH) access authentication [Learn More..](#)

Host based authentication *Note: All users from this instance of HP SIM will be authenticated on the managed system.*

User based authentication for user: *Each user has to be authenticated on the managed system*

Set Trust relationship to "Trust by Certificate" [Learn More..](#)

This enables HP SIM users to connect to the System Management Homepage, Onboard Administrators, Integrated Lights-Out (version 2 and later), and VCA using the HP SIM certificate for authentication.

Configure Version Control Agent(VCA) [Learn More..](#)

This option applies only to Windows Systems.
The Version Control Repository Manager (VCRM) contains a repository that stores the software and firmware components used to support Windows and Linux platforms. The VCA can be configured to point to the VCRM, enabling easy version comparison and software updates.

Select the system where the VCRM is installed:

Enter the credentials for the VCA to use to access the VCRM:

User name:

Password:

Password (Verify):

Domain:

Set administrator password for Insight Management Agents version 7.1 or earlier [Learn More..](#)

This option applies only to ProLiant Systems

Password:

Password (Verify):

[< Previous](#) [Schedule](#) [Run Now](#)

7. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This setting enables the target systems to send *SNMP traps* to this instance of HP SIM.
8. Click **Run Now**. The **Task Results** page appears.

Note: On the **Manage Communication** page advice text might indicate that the CMS might not be on the SNMP trap destination list even if the above steps were taken. For HP SIM to check the trap destination list on the target system, a trust relationship with the managed system must be properly configured. See "Setting trust relationships" for more information.

Web-Based Enterprise Management

For HP-UX, WBEM is included in the operating system install. For Linux Itanium Processor Family (IPF), if WBEM is not installed, it must be manually installed. Go to the HP Software Depot (<http://www.software.hp.com>) to download. The WBEM download from the openPegasus website does not include the hardware specific data for HP SIM to manage Linux x86 systems.



NOTE: *Windows Management Instrumentation* (WMI) is the implementation of WBEM from Microsoft. See [WMI](#) for more information.

NOTE: A Common Information Model Object Manager (CIMOM) acts as the interface for communication between WBEM providers and management applications such as HP Systems Insight Manager.

The CMS must have the correct credentials to authenticate to WBEM and WMI. There are two ways to authenticate client certificates:

- Basic authentication to WBEM Services or WMI using user name and password.
- Using the CMS certificate to authenticate is available only for HP-UX WBEM Services 02.05.00, which supports client certificate authentication. Use the Configure or Repair Agents **Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system** option to deploy a WBEM certificate to the managed system and is only valid for HP-UX systems.

Subscribing to WBEM indications

You can subscribe to WBEM indications through the the Configure or Repair Agents pages or through the **Options** menu.

Subscribing to WBEM indications through the Configure or Repair Agents pages

1. Select **Configure**→**Configure or Repair Agents**. The **Step 1: Select Target Systems** page appears.
Note: The **Step 1: Verify Target Systems** page appears if the targets are selected before selecting a tool.
2. Select target systems. See “*Creating a task*” for more information.
3. Click **Next**. The **Step 2: Enter credentials** page appears. The credentials specified on this page are for a privileged account on the target system.

Note: If you plan to **Configure secure shell (SSH) access** on a Windows target system, the account specified must be a member of the local Administrators group. For Windows targets using a domain account, the account is automatically added to this group if applicable.

Configure or Repair Agents

Target: pbdemo Maximize ?

Step 2: Enter credentials

This tool allows you to configure or repair certain SNMP and secure shell (SSH) settings, trust relationships, and WBEM event subscriptions that exist between HP Systems Insight Manager and its target systems. Additionally, for target systems which only contain version 7.1 agents or earlier, this tool allows you to configure the passwords for their web-based management applications.

Enter credentials for a privileged account on the target system(s). If the 'Configure secure shell (SSH) access' is to be selected for a Windows target system, then this account must be a direct member of the local 'Administrators' group. For Windows targets using a domain account, the account will automatically be added to this group if needed.

User name:

Password:

Password (Verify):

Domain:

[< Previous](#) [Next >](#)

4. From the **Step 2: Enter credentials** page:

- a. In the **User name** field, enter the system administrator name.
- b. In the **Password** field, enter the system administrator's password for the user name previously entered.
- c. In the **Password (Verify)** field, reenter the system administrator's password exactly as it was entered in the **Password** field.
- d. In the **Domain** field, enter the Windows domain if you are using a domain account.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** credentials. Credentials entered here are not saved by HP SIM except to run a scheduled task later.

5. Click **Next**. The **Step 3: Install Providers and Agents (Optional)** page appears.

Step 3: Install Providers and Agents (Optional)

If agents or providers are already installed, skip this step and proceed to the configuration step.

By installing agents or providers on the managed systems, HP SIM will be able to collect inventory and status information from the systems. It will also enable HP SIM to receive event notifications from the system(s). In most cases, you will want to install either WBEEM /VMI providers or SNMP agents, but not necessarily both.
 This option applies only to ProLiant or Itanium-based Systems with Windows Operating Systems

- Install WBEEM /VMI Provider (HP Insight Management WBEEM Provider) for Windows** [Learn More..](#)
- Install SNMP Agent (HP Insight Management Agents) for Windows** [Learn More..](#)
- Install Open SSH** SSH is used for running tools remotely on managed systems. [Learn More..](#)
- Install the Version Control Agent for Windows (VCA)** The VCA, in conjunction with the HP ProLiant Version Control Repository Manager, enables management of the HP ProLiant software and firmware on the managed systems. [Learn More..](#)

For selected installs:

- Force downgrade, or reinstall the same version
- Reboot system(s) if necessary after installation

Click "Next" to configure the providers and agents

< Previous
Next >

6. Click **Next**. The **Step 4: Configure or Repair Agents** page appears.

Configure WBEM and SNMP settings, SSH authentication mode, Version Control Agent settings, trust relationships, and for Insight Management Agents version 7.1 or earlier, the administrator password.

Configure WBEM / WMI [Learn More..](#)

Create subscription to WBEM events

Send a sample WBEM / WMI indication to this instance of HP SIM to test that events appear in HP SIM event lists.

Use an HP SIM WBEM certificate (good for 10 years) rather than username/password to manage the system. *This will deploy a WBEM certificate to the managed system. This option is only valid for HP-UX systems.*

Configure a non-administrative account for HP SIM to access WMI data [Learn More..](#)

This option applies only to Windows Systems with HP WBEM Provider installed.
Administrative accounts can be used without further configuration. If non-administrative access to a managed system is desired, an existing domain account or one local to the managed system can be used by HP SIM to access WMI information over the network.

Enter the credentials for HP SIM to use to access the managed system:

User name:

Password:

Password (Verify):

Domain:

Configure SNMP [Learn More..](#)

Set read community string:

Set traps to refer to this instance of HP Systems Insight Manager. *Note: A ReadWrite string will be created automatically on Windows systems.*

Send a sample SNMP trap to this instance of HP SIM to test that events appear in HP SIM event lists..

Configure secure shell (SSH) access authentication [Learn More..](#)

Host based authentication *Note: All users from this instance of HP SIM will be authenticated on the managed system.*

User based authentication for user: *Each user has to be authenticated on the managed system*

Set Trust relationship to "Trust by Certificate" [Learn More..](#)

This enables HP SIM users to connect to the System Management Homepage, Onboard Administrators, Integrated Lights-Out (version 2 and later), and VCA using the HP SIM certificate for authentication.

Configure Version Control Agent(VCA) [Learn More..](#)

This option applies only to Windows Systems.
The Version Control Repository Manager (VCRM) contains a repository that stores the software and firmware components used to support Windows and Linux platforms. The VCA can be configured to point to the VCRM, enabling easy version comparison and software updates.

Select the system where the VCRM is installed:

Enter the credentials for the VCA to use to access the VCRM:

User name:

Password:

Password (Verify):

Domain:

Set administrator password for Insight Management Agents version 7.1 or earlier [Learn More..](#)

This option applies only to ProLiant Systems

Password:

Password (Verify):

[< Previous](#) [Schedule](#) [Run Now](#)

7. **Configure WBEM / WMI.** This section enables you to configure the target Linux, Windows or HP-UX system to send WBEM indications or events to HP Systems Insight Manager.
8. Click **Run Now**. The **Task Results** page appears.

Subscribing to WBEM indications through the **Options** menu

1. Select **Options**→**Events**→**Subscribe to WBEM Events**. The **Step 1: Select Target Systems** page appears.
2. Select the target systems, and then click **Apply**. The **Step 1: Verify Target Systems** page appears.
3. Click **Next**. The **Step 2: Task Confirmation** page appears and provides details about the task that was created in the previous steps.
4. Click **Run Now** to add subscriptions for WBEM events on the target systems. The **Task Results** page appears.

Related procedure

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols
- Windows CMS

Related topic

- Installing and configuring protocols
- Global protocols

Secure Shell

SSH is used to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

You can download SSH from the HP Software Depot (<http://www.software.hp.com/>).

To install the SSH provider from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**. To configure OpenSSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents**→**Install OpenSSH**→**Configure secure shell (SSH) access**.

Related procedures

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols
- Windows CMS
- HP-UX and Linux CMS

Related topics

- Installing and configuring protocols
- Global protocols

WMI Mapper

WMI Mapper is an application based on the OpenPegasus Common Information Model Object Manager (CIMOM), which enables the client application accessing *Windows Management Instrumentation* (WMI) data using CIM/XML. Microsoft Windows systems are well instrumented with CIM data through WMI. However, WMI uses a proprietary protocol and the Windows operating system must make WMI requests which left the client application with managing Windows using a different model than other operating systems. WMI Mapper is the solution for helping client applications using CIM/XML over HTTP to access WBEM data on target Windows systems.

When clients send CIM/XML requests over HTTP, WMI Mapper parses these requests, dispatches all requests to the Windows WMI interface, the WMI Interface returns WMI responses to the dispatcher, XML is built based on responses, and then XML data is returned to client. WMI Mapper uses basic authentication over HTTPS to receive the user name and password, and then the credential is validated by the WMI Interface using Windows authentication. Because Microsoft's WMI Interface can connect to a local system or a remote Windows system, WMI Mapper can be installed on one target system, and used in a proxy mode. WMI Mapper uses WMI/DCOM protocol for getting WMI data from other Windows systems remotely.

The typical installation for HP Systems Insight Manager (HP SIM) Windows Central Management Server (CMS) includes installing WMI Mapper on the Windows CMS and used in proxy mode. Configuring WMI Mapper as a proxy for Windows CMS is complete after WMI Mapper is installed. Users who use an HP-UX CMS or Linux CMS, must install Mapper on a Windows system and configure the WMI Mapper as a proxy, either through the First Time Wizard or the HP SIM +**Options**→**Protocol Settings**→**WMI Mapper Proxy** menu.

Adding a WMI Mapper Proxy

1. Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**→**[New]**. The **Add WMI Mapper Proxy** section appears.
2. In the **Host** field, enter the full *Domain Name Service (DNS)* name or IP address of the WMI Mapper Proxy.
3. In the **Port number** field, enter a port number. The WMI Mapper Proxy uses this port number to communicate with the WMI client.
4. Click **OK** to save and close the **Add WMI Mapper Proxy** section, click **Apply** to save without closing the **Add WMI Mapper Proxy** section, or click **Cancel** to abort the save operation.

You can use the the Pegasus WMI Mapper service on Windows to stop and start WMI Mapper. Select **Start→Control Panel→Administrator Tools→Services→Peegasus WMI Mapper**.

Related procedures

- Adding a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy
- Editing a WMI Mapper Proxy

Related topic

- ▲ WMI Mapper Proxy

Pinging managed systems

Ping is a basic internet program that enables you to verify that an IP address exists and can accept requests. It works by sending Internet Control Message Protocol (ICMP) echo request packets to the target system and listening for ICMP echo response replies.

To ping systems the HP Systems Insight Manager (HP SIM) UI, select **Diagnose→Ping**.

Installing the HP ProLiant Support Pack

SSH is used to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

For HP-UX and Linux, download SSH from the HP Software Depot (<http://www.software.hp.com/>).

For Windows systems, install SSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents→Install SSH**. To configure SSH from the **Manage Communications** page, select **Quick Repair+Install Providers and Agents→Install OpenSSH→Configure secure shell (SSH) access**.

Related procedures

- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Setting global protocols

Related topics

- Installing and configuring protocols
- Global protocols

System Type Manager rules

Manufacturers assign unique system object identifiers to their SNMP instrumented products. System Type Manager enables you to customize identification by creating rules that map these system object identifiers to product categories and names of your choice. If you have installed a new system with SNMP installed and there is no existing rule to identify the system type, you must create a new rule.

To create a new SNMP rule,

1. Select **Options→Manage System Types**. The **Manage System Types** page appears.
2. Click **New**. The **New rule** section appears.

3. Enter the **System object identifier** information. Retrieve the system object identifier from a target system on your network by clicking **Retrieve from system**. The **Retrieve from system** section appears. The **System object identifier** field is required.

- a. In the **Object identifier** field, enter the object identifier.
 - b. In the **Community string** field, enter the community string if other than public, the default. The community string of the target system and the HP Systems Insight Manager (HP SIM) server must match to retrieve data.
 - c. In the **Target hostname or IP address** field, enter the IP address of the system you want to search.
 - d. Click **Get response** to show the **Response SNMP data type** and the **Response value**.
 - e. Click **OK** to close the **Retrieve from system** section, and place the response value in the **System object identifier**, **Object value** fields, or both.
4. Enter the **System object identifier compare rule**. Click the down arrow, and then select the appropriate rule. In most cases, this rule is **match**. You can set it to **starts with** if you know that a class of systems has system object identifiers that start with the value you have entered.

- (Optional) Specify **MIB variable object identifier** by clicking **Retrieve from MIB**. The **Retrieve from MIB** section appears.

You might need to do this action if you have systems that return the same system object identifier that you would like to classify as different products based on some SNMP variable that returns a different value for each class. For example, if you have Windows NT servers from different vendors that return the same Windows NT system object identifier, you can specify rules using the Windows NT system object identifier as the system object identifier and a vendor-specific MIB variable and value combination to create separate rules for each vendor.

Retrieve from MIB:

Select a MIB file and MIB variable to view the MIB variable details below. Clicking 'OK' will transfer this value to the MIB Variable OID field above.

MIB definition file name:	rfc1213.mib
MIB variable name:	sysDescr

MIB variable object identifier: 1.3.6.1.2.1.1.1
MIB variable access: READ-ONLY
MIB variable status: MANDATORY
MIB variable type: DISPLAYSTRING

OK Cancel

- Click the down arrow in the **MIB definition file name** box to select the MIB definition file.
 - Click the down arrow in the **MIB variable name** box to select the MIB variable name.
 - Click **OK** to close the **Retrieve from MIB** section, and place the **MIB variable object identifier** information in the field.
- Select the **Object value** by clicking **Retrieve from system**. The **Retrieve from system** section appears.
 - Enter the **Object identifier**, **Community string**, and **Target hostname or IP address**.
 - Click **Get response** to view the **Response SNMP data type** and the **Response value**.
 - Click **OK** to close the **Retrieve from system** section, and place the information in the **Object value** field.
 - Select the **Object value Data type** by clicking the down arrow and selecting either **string** or **integer**.
 - Select the **Object value Compare rule** by clicking the down arrow.
 - Enter a **Priority** (applies only if there is more than one rule with the same system object identifier).
 - In the **System type** field, click the down arrow, and then select the system type.
 - In the **Subtype** field, click the down arrow, and then select the system subtype.
 - In the **Product name** field, enter the product name for the new rule.
 - In the **Custom management page** field, enter a URL. The URL displays this web page as a system link on the **System Page** of systems identified using this rule. Enter the special keywords *\$ipaddress* and *\$hostname* anywhere in this URL. They are replaced by the actual IP address or host name of the system when the link is placed on the **System Page**.
 - Click **Launch** to verify that you can browse to the URL.
 - Click **OK** to save the new rule, or click **Cancel** to cancel all changes and close the **New rule** section.

Installing and configuring version control

In HP Systems Insight Manager (HP SIM), the software status indicates both the availability of software updates and how critical they are. If HP Version Control Agent (VCA) is installed on the system, clicking the software status icon for that system displays HP Version Control Agent Software Inventory page.

To update managed servers with the most current software, HP SIM provides software update capabilities that use the *HP Version Control Agent (VCA)* and *HP Version Control Repository Manager (VCRM)*.

For Windows operating systems, you must install the *HP Insight Management Agent 5.40* or later to obtain any inventory data. For Linux operating systems, you must install HP Server Management Application and Agents (hpsasm RPM) 7.00 or later to obtain any inventory data. HP recommends installing the current version that is in the same *HP ProLiant and Integrity Support Pack* as the VCA.



NOTE: If the Insight Management Agents are not installed, *software inventory* cannot be collected by the VCA. However, the VCA can still be used to install software.

HP Version Control Agent

The *HP Version Control Agent* (VCA) is an *HP Insight Management Agent* that is installed on a system to enable you to view the HP software and firmware that is installed on that system. The VCA can be configured to point to a *repository* being managed by the *HP Version Control Repository Manager* (VCRM), enabling easy version comparison and software updates from the repository to the system on which the VCA is installed.

The VCA provides *version control* and system update capabilities for a single HP system. The VCA determines system software status by comparing each *component* installed on the local system with the set of individual components or a specified ProLiant or Integrity Support Pack listed in the VCRM. While browsing to the VCA, you can update individual components or an entire ProLiant or Integrity Support Pack by clicking the install icon located next to the system software status icon.

HP Version Control Repository Manager

The *HP Version Control Repository Manager* (VCRM) is an HP Insight Management Agent that manages a directory of HP software and firmware components. The VCRM can be used without the *HP Version Control Agent* (VCA) to provide a listing of available software and firmware to load on the local machine. The VCRM is part of the HP Foundation Pack.

The VCRM is designed to be used in a one-to-many configuration with a VCA installed on each managed HP system to manage installed HP software and firmware. In conjunction with HP Systems Insight Manager (HP SIM), the VCRM, and VCAs provide enterprise-wide management of HP software and firmware on HP ProLiant and Integrity systems. Alone, the VCRM can be used to catalog and manage a repository of ProLiant and Integrity Support Packs and individual software and firmware from HP for HP ProLiant and Integrity systems.



NOTE: Although it is possible to install an *HP ProLiant and Integrity Support Pack* or *component* to the local machine using the VCRM, you cannot install the software on remote servers unless the VCA has been installed on the remote server and the install is initiated using the VCA.

Accessing VCRM from HP SIM

1. Select **Tools**→**System Information**→**System Management Homepage**.
2. Select the target system, and then click **Run Now**. See “Creating a task” for more information. The System Management Homepage appears.
3. From System Management Homepage, perform one of the following actions:
 - Click the **HP Version Control Repository Manager** link. The **VCRM Home** page appears.
 - Select **Tools**, and then click the **HP Version Control Repository Manager** link.

Accessing VCRM In-Place

Navigate to `https://hostname:2381/vcrepository` on the system that has the VCRM installed. The **VCRM Home** page appears.



NOTE: You can also access VCRM from the System Management Homepage (SMH).

Version control repository

The Version Control Repository must be downloaded and at least one VCA must be configured to access the VCRM server where it is to be placed. The VCA must have appropriate rights to the VCRM server, but it cannot use the administrator account.

HP Systems Insight Manager (HP SIM) enables you to specify an HP Version Control Repository Manager. The VCRM stores the latest HP ProLiant Support Packs providing the latest software.

Updating the repository:




There are several ways to update the repository:

- From the HP SmartStart CD
- From the HP SmartStart CD manually
- From the HP SmartSetup CD

See the *HP Version Control Repository Manager Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html> for additional information.

- From the VCRM.
 1. Users must be given authorization to access the VCRM through System Management Homepage by selecting **The Settings Page**→**Security**→**Update Groups**.
See the *HP Version Control Repository Manager Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>, in the **The Settings page** chapter for details.
 2. Point the VCA to the VCRM by selecting **Change Agent Settings** from the **VCA Home** page.
See the *HP Version Control Agent Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>, in the **The Home page** chapter for details.
 3. From the VCRM **Home** page, select **Configure the Repository and Automatic Update Settings**.
See the *HP Version Control Agent Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html> in the **Navigating the software** chapter and the **Home - Configuring Auto Update** section for details.
 4. From the VCRM **Catalog** page, select **Update from hp.com Now**

Specifying a Version Control Repository in HP SIM

1. Select **Options**→**Version Control Repository**. The **Version Control Repository** page appears.
2. Under **Select the default version control repository**, select a system that has the VCRM installed.
Note: The system that has the VCRM installed must be trusted. See “Trusted certificates” for more information regarding trust relationships. After the trust relationship is established, click **Last Update** to update the **Trusted?** column to **Yes**.
3. Under **Contents of selected version control repository**, click the  icon to drill down and view the contents of the selected Version Control Repository.
Note: To expand the tree to display all contents, click the  icon, located in the upper-right corner of the **Contents of selected version control repository** section. Click the  icon to collapse the listings.
Note: Click any column heading to sort by that column in ascending or descending order.
Note: This section displays systems that are authorized by the current user. If the current user is not authorized to view any systems with the HP Version Control Repository Manager, the system will not be listed in the **Select the default Version Control Repository** section. If there are no *discovered systems* running the VCRM, a message appears, indicating that no repository could be found.
4. Click **OK** to apply your selection. A message appears, indicating if the repository setting was successfully saved.
5. Click **OK** to close the dialog box.

Related topics

- Version Control Repository
- Version Control
- About the Version Control Agent
- About the Version Control Repository Manager

Managing MIBs

A *Management Information Base* (MIB) is a file that contains information that enables you to correctly interpret specific information from *systems* on your network and gives you a more precise view of the activity on your network. To take advantage of this capability, the MIB must be registered to HP Systems Insight Manager (HP SIM). See “Registering a MIB” for more information.

HP has defined MIBs for its systems, and these MIBs expose the rich management infrastructure that HP builds into its products. HP MIBs are already registered in the HP SIM *database*. You can find them in the directory `\hp\system insight manager\mibs` on a Windows CMS or `opt\mx\mibs` on a UNIX CMS. If you have third-party systems on your network, you can register the MIBs that accompany the systems. See “Registering a MIB” for more information regarding registering your MIBs. Registering enables the MIBs to be identified correctly and traps can be interpreted correctly to give you a more precise view of the activity on your network. Always register the most recent version of a third-party MIB.

Related procedures

- Registering a MIB
- Unregistering a MIB
- Compiling a MIB
- Editing a MIB

Viewing a MIB

After a *Management Information Base* (MIB) has been registered in the HP Systems Insight Manager (HP SIM) *database*, additional `mxmib` options, such as `mxmib -l` and `mxmib -t` can be used to view all MIBs added to the database and all traps associated with a particular MIB. Also, SNMP Trap Settings (**Options**→**Events**→**SNMP Trap Settings**) can be used to display all registered MIBs and their associated traps that are contained in the database. The Event Type, Description, Enable Trap Handling, Category, and Severity can be modified through this screen to further customize the information that is collected on the network. See “Editing a MIB” for more information regarding editing a MIB.



CAUTION: Do not rename, move, or delete MIB files from the directory after they are registered.



NOTE: For a MIB file to be listed as registered, the MIB file must reside in the `mibs` directory.

NOTE: The following HP SIM directories are default directories. However, the directories can vary depending on the directory specified during HP SIM installation.

To view a MIB file on a Windows operating system:

1. Navigate to the MIB directory at `c:/program files/hp/systems insight manager/mibs`.
2. Open the MIB file with an ASCII editor.
3. Enter `write cpqghost.mib` on the Windows command line.

To view a MIB file on a Linux or HP-UX operating system:

1. Enter `cd opt/mx/mibs`.
2. Run `mxmib -l` to view registered MIBs.
3. Enter `vi file.mib` from a shell prompt.

Related procedures

- Registering a MIB
- Unregistering a MIB
- Compiling a MIB
- Editing a MIB
- Configuring SNMP traps

Related topic

▲ Managing MIBs

Editing a MIB

The HP MIBs configuration (`.cfg`) file can be edited with trap specific information, such as:

- *TYPE*. The type is a simplified form of the actual trap name. Change the type if it does not adequately describe the device for you.
- *SEVERITY*. Some vendors use the default INFORMATIONAL for all severity levels. Change the severity to a level that reflects your judgment of the problem. Alternatively, you can change a Major or Critical severity for a trap message that is clearly not a critical situation in your environment. Only you know if this is the case. The only valid options for HP Systems Insight Manager (HP SIM) are: Critical, Major, Minor, Warning, and Informational.
- *MSG_FORMATTER*. This message formatting string is used to construct enhanced messages that might be sent to a pager or in an e-mail. This string can be modified in the REV or the MIB.
- *ENABLE*. By default all traps are enabled. Trap handling gives you control over the volume of messages. Disable nuisance messages, such as unnecessary informational messages or repeated trap messages, for an event that has not been corrected.
- *DESCRIPTION*. The description is vendor-supplied. Replace it with more specific instructions, a precise reference source, or a website referral.
- *CATEGORY*. The category lists the HP SIM category types and UNKNOWN.

To edit the `.cfg` file:

1. Navigate to the MIB directory:
 - For Windows operating systems, navigate to `\program files\hp\systems insight manager\mibs`.
 - For Linux or HP-UX operating systems, navigate to `/opt/mx/mibs`.
2. Run `mcompile mymib.mib` to create the `.cfg` file.
3. After the `.cfg` file is created, use an editor of your choice to edit the `.cfg` file.

To edit trap-specific information in HP SIM:

1. From HP SIM, select **Options**→**Events**→**SNMP Trap Settings**.

The **SNMP Trap Settings** page appears.

2. Select the MIB name.
3. Select the trap within the MIB to be edited.
4. Edit the file with your changes, and then click **OK** to save your changes.

Note: The changes made through the **SNMP Trap Settings** page are saved to the HP SIM *database* only. The `.cfg` and MIB files are not affected.

Related procedures

- Viewing a MIB
- Compiling a MIB
- Unregistering a MIB

Related topic

▲ Managing MIBs

Compiling a MIB

The `mcompile` command enables you to compile an *SNMP* MIB file into an intermediate format (`.cfg`) file that can be registered using the `mxmib` utility for use with HP Systems Insight Manager (HP SIM).

Observe the following tips:

- To compile a *MIB*, you must copy the `.mib` file to the the default MIB directory.
- Comment lines in MIB files start with "--" and end with a new line or the next occurrence of "--." Beware of MIBs with "-" characters across the entire line. These lines are intended to be comments. However, extra dashes have canceled the first set of "--" characters.

For example:

```
-- xyz comments out xyz.
```

However:

```
-- -- xyz effectively uncomments xyz.
```

- `mcompile` expects the *END* keyword at the end of a module on a line by itself. Be sure there is a new line in the MIB file after the *END* keyword.

To compile a MIB:

1. Navigate to the HP SIM root directory and open an MS-DOS® window or UNIX shell.
2. Run `mcompile` to compile an SNMP MIB file into an intermediate format (`.cfg`).

`mcompile` recognizes the `-d` option. This option changes to the specified directory to locate and process the MIB file. The `MxMib` expects the `.cfg` file to reside in MIBs directory. It is convenient to have both files in that directory as the output of `mcompile` (`.cfg`) will be in the directory where `mcompile` either compiles or is directed to compile in.

For example:

```
cd mibsdir
```

```
mcompile mymib.mib
```

or

if you are not running in the MIBs directory:

```
mcompile -d mibsdir mymib.mib
```

3. Run `mxmib` to register the MIB with HP SIM.

For example:

```
MxMib -a mymib.cfg
```

Related procedures

- [Registering a MIB](#)
- [Unregistering a MIB](#)
- [Viewing a MIB](#)
- [Editing a MIB](#)

Related topic

- ▲ [Managing MIBs](#)

Registering a MIB

HP Systems Insight Manager (HP SIM) ships with HP MIBs that are registered at installation. In addition, a number of precompiled *MIBs* are included in the form of `.cfg` files. These MIBs can be registered at your convenience. A number of those `.cfg` files have been edited. If the corresponding MIB is recompiled, then those edits are lost.

To view a list of currently registered MIBs, including MIBs that you have registered:

- In Windows, enter `dir "c:\program files\hp\systems insight manager\MIBs\ *.MIB"` at the command line.
- On UNIX, enter `ls /opt/mx/mibs/*.mib` at the command line.

To view MIBs that are preloaded and registered during HP SIM installation:

- In Windows, enter `type "c:\program files\hp\systems insight manager\MIBs\cfglist?.list"` at the command line.
- On UNIX, enter `cat /opt/mx/mibs/cfglist*.list` at the command line.



NOTE: These are the install directories. If you changed the install directory during the HP SIM installation, these commands must reference your path instead.

HP MIBs can be registered using the command line interface (CLI). The CLI is the same for all CMS types including Windows, Linux, and HP-UX.



NOTE: When registering a MIB, it is not always necessary to run `mcompile` on the MIB especially if the corresponding `.cfg` file to that MIB already exists. If you run `mcompile` on a MIB and a `.cfg` file exists, a new `.cfg` is generated, which supersedes the old `.cfg` file and any changes in the old file are not active. In most cases with an existing `.cfg` file, it is desirable to edit the `.cfg` file to make changes unless a new MIB has been furnished.

This `.cfg` file can then be registered to the HP SIM *database* using the `mxmib -a` or `mxmib -f` command.

Registering a MIB in HP SIM

1. Open an MS-DOS window or UNIX shell.
2. Use an editor of your choice to create a file containing a list of the `.cfg` files to be registered. One `.cfg` per line.
3. Run `mxmib -f cfglist.list` to import a list of MIBs into HP SIM. After the MIB is registered in HP SIM, you can use `mxmib` to list or delete the MIB from HP SIM.

Note: You can also use `mxmib -a mymib.cfg` to register a single MIB.

Note: The `.cfg` file being registered must be in the default MIBs directory.

Note: MxMib requires the `.cfg` file to reside in the MIBS directory where all the `.mib` and `.cfg` reside by default.

Updating a MIB

1. Download and copy MIBs and any matching `.cfg` files to the default `mibs` directory. The `mibs` directory is typically located at `c:\program files\hp\systems insight manager\mibs` for Windows and at `/opt/mx/mibs` for Linux and HP-UX.

Note: If a `.cfg` file is available and no customizations have been made, proceed to step 2.

2. Run `mcompile` to create and update any `.cfg` file that exists.

Note: If the old `.cfg` file had any customizations, these must be reapplied.

3. Run `mxmib -a updatedfile.cfg` to update the MIB data in the database.

Service trap and service MIB information

HP SIM ships with a version of the service MIB to support service traps sent by Open Service Event Manager (OSEM) and Web-Based Enterprise Services (WEBES). The service MIB is comprised of the `cpqservice.mib` and `cpqservice.cfg` files. To obtain the service MIB separately, see <http://h18023.www1.hp.com/support/svctools/> and select **Service MIB Zip file** under **WEBES** or **OSEM**. The zip file contains the `.mib` and `.cfg` files. HP recommends you review the `readme.txt` file contained in the zip file for compatibility instructions.

Beginning with OSEM 1.3.6, the tool must be configured to generate the new trap type by accessing the **Internal Settings** for OSEM: HP SIM trap revision. WEBES sends the trap by default.

Related procedures

- [Viewing a MIB](#)
- [Compiling a MIB](#)

- Unregistering a MIB
- Editing a MIB

Related topics

- Managing MIBs
- Service notification events

Unregistering a MIB

HP MIBs can be unregistered using the command line. The command line interface (CLI) is the same for all CMS types to include Windows, Linux, and HP-UX.

To unregister a MIB from HP SIM:

1. Open an MS-DOS window or UNIX shell.
2. Run `mxmib -d file.mib` to unregister the MIB in HP Systems Insight Manager (HP SIM).

Related procedures

- Viewing a MIB
- Compiling a MIB
- Registering a MIB
- Editing a MIB

Related topics

- Managing MIBs
- Service notification events

Presentation of SNMP traps in HP SIM

You can map a severity from a varbind to the event severity displayed in the event view. The mechanism uses two keywords annotated as comments within the trap definition (`VARBINDSEVERITY` and `SEVERITYMAP`). The following is an example of a trap definition:

```
sanEventTrap TRAP-TYPE
  ENTERPRISE sanEvent
  VARIABLES { sanEventEventCofde, sanEventIPAddress,
    sanEventSeverity, sanEventCategory,
    sanEventGroup, sanEventSourceType,
    sanEventSourceSubtype, sanEventURL,
    sanEventDesc }
  --#SEVERITY INFORMATIONAL
  --#TYPE "Rack power supply inserted"
  --#VARBINDSEVERITY 3
  --#SEVERITYMAP "Unknown = INFORMATIONAL,
    Other = INFORMATIONAL,
    Information = INFORMATIONAL,
    Warning = INFORMATIONAL,
    Minor = MINOR, Major = MAJOR,
    Critical = CRITICAL,
    Fatal = CRITICAL"
  --#ENABLE true
  --#CATEGORY "San Event Events"
  DESCRIPTION
    "This trap signals (using SNMP) an event
    has been received"
```

The `VARBINDSEVERITY` is a pointer that points to a varbind, which contains a severity. Varbinds start at the count of 1 and in the example below, `sanEventSeverity` is the third varbind as pointed to by `--#VARBINDSEVERITY 3`. The severity for the varbind must be defined as an enumeration.

The `SEVERITYMAP` is a mapping of agent severity to the HP Systems Insight Manager (HP SIM) supported severity. HP SIM only supports `CRITICAL`, `MAJOR`, `MINOR`, `WARNING`, and `INFORMATIONAL`. Therefore, all mappings must resolve to one of these severities. In the example above, you can see a mapping of Fatal to `CRITICAL` ("Fatal = CRITICAL"). When we receive in the varbind Fatal, it is translated to the HP SIM severity of Critical. The varbind value and therefore, the severity, might be varied by the agent as conditions change, so when a trap is received in HP SIM, the severity displayed is set by the agent when a trap was sent.

Related procedures

- Registering a MIB
- Unregistering a MIB
- Compiling a MIB
- Editing a MIB

Installing OpenSSH

HP Systems Insight Manager (HP SIM) custom tools and command line tools require that *Secure Shell* (SSH) be installed and configured on each of the managed systems to work properly. See *Secure Shell (SSH) in HP SIM 5.x* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more detailed information on SSH and the features in HP SIM that use SSH.

The OpenSSH install is run from the *Central Management Server* (CMS) and installs the OpenSSH service on to target Windows systems and then runs the `mxagentconfig` command to complete the configuration.



NOTE: To be sure that the install OpenSSH task runs successfully, sign-in as a user with *administrative rights*. If you are signed-in as another user, be sure the user name does not contain any non-ASCII characters.

NOTE: You can easily install OpenSSH on Windows managed systems using the Configure or Repair Agents feature. See "Windows CMS" for more information.

To install OpenSSH through the OpenSSH Install option:

1. Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install OpenSSH**. The **Install OpenSSH** page appears.
2. Select the target systems. See "Creating a task" for more information about selecting target systems.
3. Click **Next**.
4. From the **Enter credentials for an administrator account on the target system(s)**: section:
 - a. In the **User name** field, enter the Windows administrator user name.
 - b. In the **Password** field, enter the administrator password for the Windows user name entered in the previous step.
 - c. In the **Password (Verify)** field, re-enter the Windows administrator password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain.

Note: Leave **Domain** field blank if the administrator account on the target systems is a local account.

5. Click **Schedule** to schedule the install, or click **Run Now** to run the installation immediately. See "Scheduling a task" for more information about scheduling the installation.

If you clicked **Run Now**, the **Tasks Results** page appears. See "Viewing task results" for more information about the **Task Results** page.

Related procedures

- Creating a task
- Scheduling a task
- Viewing task results
- Initial ProLiant Support Pack Install

- Deploying OpenSSH to multiple systems using RDP
- Creating an OpenSSH task through the CLI

Deploying OpenSSH to multiple systems using RDP

OpenSSH can be installed on a target server using HP Rapid Deployment Pack (RDP), and then the HP Systems Insight Manager (HP SIM) public key can be copied to target systems.

Installing OpenSSH Using RDP

1. Copy the OpenSSH install component to the Deployment Server.
2. Create a new job.
3. Add a Copy File task by selecting **Add >> Copy File to**.
4. Ensure that the **Copy File** option is selected.
5. For the **Source path:**, enter the complete path where the OpenSSH installer is located. For example, if `OpenSSH_3.7.1p1-1.exe` is in folder `C:\temp\OpenSSH`, enter the source path as `C:\temp\OpenSSH\OpenSSH_3.7.1p1-1.exe`.
6. Under **Destination path:**, enter the location where you want this file to be copied on the target server. For example, if you want the file to be copied to the `C:\temp\OpenSSH` folder on the target server, enter the destination path as `C:\temp\OpenSSH\OpenSSH_3.7.1p1-1.exe`.
7. Click **Finish**.
8. Add a Run Script task to the job by clicking **Add >> Run Script**.
9. Ensure that the **Run this script** option is selected.
10. In the box below **Run this script**, enter the following:


```
C:\temp\OpenSSH\OpenSSH_3.7.1p1-1.exe /SILENT /NORESTART
```
11. Select the Windows radio button in the **In which OS would you like to run this script?** section.
12. Click **Finish**.
13. Drag this event and drop it on any system on which you want OpenSSH installed.

Copying the public key from HP SIM to the target systems

After OpenSSH is installed, create another script to copy the `dtfsshkey.pub` file (the public key) from the HP SIM server to the `.ssh` directory of the home directory of the administrator user on the target system.

1. Copy the `.dtfSshKey.pub` file from `..\Program Files\HP\System Insight Manager\config\sshtools\` folder on the HP SIM server to a local folder on the deployment server, and rename `.dtfSshKey.pub` to `authorized_keys2`.
 - a. Create a new job.
 - b. Add a Run Script task to the job by clicking **Add >> Run Script**.
 - c. Ensure that the **Run this script** option is selected.
 - d. In the box below **Run this script**, enter the following (assuming that administrator's home directory is `C:\Documents and Settings\Administrator`):


```
cd C:\Documents and Settings\Administrator\
mkdir .ssh
cd .ssh
del * /q
```
 - e. Select the Windows option in the **In which OS would you like to run this script?** section.
 - f. Enter the complete path where you have the `authorized_keys2` file as the **Source path:**. For example, if `authorized_keys2` is in folder `C:\temp\OpenSSH`, enter source path as `C:\temp\OpenSSH\authorized_keys2`.
 - g. Enter the location where you want this file to be copied on the target server under the **Destination path:**. For example, if the administrator's home directory is `C:\Documents and Settings\Administrator`, enter the destination path as `C:\Documents and Settings\Administrator\.ssh\authorized_keys2`.
 - h. Click **Finish**.

- i. Add a Run Script task to the job by clicking **Add >> Run Script**.
 - j. Ensure that the **Run this script** option is selected.
 - k. In the box below **Run this script**, enter the following command:


```
net stop opensshd
net start opensshd
```
 - l. Select the Windows option in the **In which OS would you like to run this script?** section.
 - m. Click **Finish**.
2. Drag this event and drop it on the target system where you want OpenSSH to be configured.

Related procedures

- Installing OpenSSH
- Initial ProLiant Support Pack Install
- Creating an OpenSSH task through the CLI

Creating an OpenSSH task through the CLI

Perform this procedure to create an OpenSSH task through the command line using the `mxtask` command in two ways:

- Entering all parameters through the command line
- Entering all parameters through an `.XML` file



NOTE: Tasks created from an `.XML` file are disabled when viewed in the task list. Tasks created from the command line are not disabled when viewed from the task list.

Creating an OpenSSH task

1. To see how to enter the information correctly, export an existing OpenSSH task.
 - a. Create an OpenSSH task. See “Installing OpenSSH” for more information.
 - b. Save the task as **SSH Task**.
2. From the command line, execute the following command:

```
mxtask -lf "SSH Task" > ssh.xml
```

The `ssh.xml` now contains the format required to create an OpenSSH task from the command line. The following is an example file.

```
<?xml version="1.0" encoding="windows-1252"?>
<task-list>
  <task name="Install OpenSSH 1" type="manual"
    owner="admin" state="enabled">
    <toolname>Install OpenSSH</toolname>
    <queryname></queryname>
    <scheduleinfo />
    <timefilter />
    <toolparams>
      <?xml version="1.0"?>
      <XObject
        className="com.hp.mx.portal.taskandjob.
```

```

    OpenSSHInstall.MxOpenSSHInstallCommandToolParameters"
classVersion="1.0">
  <Property name="driveLetter">
    <Simple>C:</Simple>
  </Property>
  <Property name="path">
    <Simple>C:\Program Files\HP\System Insight Manager\
      openssh\1118786323238</Simple>
  </Property>
  <Property name="component">
    <Simple>CP005309.EXE</Simple>
  </Property>
  <Property name="username">
    <Simple>administrator</Simple>
  </Property>
  <Property name="password">
    <Simple></Simple>
  </Property>
  <Property name="domain">
    <Simple></Simple>
  </Property>
</XeObject>
</toolparams>
</task>
</task-list>>

```

The OpenSSH task uses six parameters, even though the user is only asked for three parameters during the task creation from the GUI. The first three parameters must follow the example provided. For example:

- **driveLetter** Must be the drive on which HP Systems Insight Manager (HP SIM) is installed
- **path** Must be *full path to openssh dir\dir name*, where *dir name* is any name you select
- **component** Must be CP005309.EXE
- **username** Is a user account with administrative rights on the target systems
- **password** Is the password to the administrative account specified by user name
- **domain** Is the domain of the administrative user (leave this blank if the administrative user is a local account on the target systems)

Creating an OpenSSH task from the command line with an XML file

Execute:

```
mxtask -cf ssh.xml
```

Creating an OpenSSH task from the command line without an XML file

Execute:

```
mxtask -c taskname -q queryname -w schedule -t
  toolname -A toolparams
```

where *taskname* is the name you are giving the task, *queryname* is the name of an existing collection, *schedule* is Tmanual, *toolname* is the tool (installing OpenSSH), and *toolparams* are those listed previously.

For example:

```
mxtask -c "ssh1" -q "All Systems" -w Tmanual -t "Install OpenSSH"
  -A "<?xml version="1.0"?>
<XeObjectclassName="com.hp.mx.portal.taskandjob.
  OpenSSHInstall.MxOpenSSHInstallCommandToolParameters"
  classVersion="1.0">
<Property name="driveLetter">
<Simple>C:</Simple>
</Property>
<Property name="path">
<Simple>C:\hpsim\target\windows\stage\sim\openssh\
  1079128853916</Simple>
</Property>
<Property name="component">
<Simple>CP005309.EXE</Simple>
</Property>
</Property name="username">
<Simple>user1</Simple>
</Property>
</Property name="password">
<Simple>password</Simple>
</Property>
<Property name="domain">
<Simple>openview</Simple>
</Property>
</XeObject">
```

Related procedures

- Installing OpenSSH
- Deploying OpenSSH to multiple systems using RDP

PMP tools

HP Performance Management Pack (PMP) is an integrated performance management solution that detects and analyzes hardware bottlenecks on HP ProLiant servers, select HP Integrity servers, and MSA500/MSA1000/MSA1500 shared storage systems. PMP is automatically installed with HP Systems Insight Manager (HP SIM) and operates in integration with HP SIM. No software installation on the monitored servers is required, other than the Insight Management Agents. PMP analyzes performance information to determine if there is a building or existing performance bottleneck issue. You can interactively display this information, log the information to a database for later analysis or reporting, and set up proactive notification using the HP SIM notification mechanism.

PMP is best suited for the following:

Customers that want to know about and deal with server performance issues before they impact user productivity.

- PMP provides a concise overview of configuration anomalies that could impact performance, like faster drives on slower controllers, NICs set to half-duplex, PCI cards concentrated on a single PCI bus, and so forth.
- PMP provides early alerts of building performance bottleneck situations.
- PMP enables interactive and historical analysis of performance issues.
- PMP provides easy to understand recommendations for solving performance issues.

Customers that, because of budget constraints, cannot automatically replace servers every three years.

- PMP provides detailed information on the subsystem that causes performance constraints, enabling pinpointed upgrades to economically extend the useful life of a server.
- When economical upgrade possibilities are exhausted, PMP provides a summary report containing both a performance profile (showing for each of the subsystems the percentage of time that performance is out of spec) and a detailed server inventory for each subsystem.

Two PMP tools are available through HP SIM **Optimize** menu:



NOTE: These options are available only on a Windows system.

- **Online Analysis** Enables you to watch and analyze the real-time performance of a monitored server. It provides an intuitive interface to detail the performance status and inventory of monitored servers, processors, memory, storage, network connections, and host bus nodes for each server.

To access **Online Analysis**, select **Optimize**→**HP Performance Management Pack**→**Online Analysis**.

or

From the **All Systems** collection page, select the monitored server by clicking its status icon in the **PF** column.

To access help for this option, go to https://middle_tier:2381/pmp/help/Server_Status.htm, where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access `PMP_directory\Program Files\HP\Performance Management Pack\htm\help\Server_Status.htm`, where *PMP_directory* is the PMP directory on the server that PMP is installed.

- **Offline Analysis** Enables you to view recorded data sessions directly from the PMP repository and license servers for PMP.

To access **Offline Analysis**, select **Optimize**→**HP Performance Management Pack**→**Offline Analysis**.

To access help for this option, go to https://middle_tier:2381/pmptools/help/Offline Analysis.htm, where *middle_tier* is the name or IP address of the server on which HP SIM and PMP are installed, or access `PMP_directory\Program Files\HP\HP Performance Management Pack\PMPTools\htm\help\Offline Analysis.htm`, where *PMP_directory* is the PMP directory on the server on which PMP is installed.

See <http://h18013.www1.hp.com/products/servers/proliantessentials/valuepack/pmp/index.html> for more information about PMP and access to documentation.

Related topics

- PMP administrative options
- PMP reporting options

Replicate Agent Settings

Replicate Agent Settings is a source system configuration that can, during *task* setup, be edited and copied to a target system or group of *systems*.

To access Replicate Agent Settings, select **Configure**→**Replicate Agent Settings**. To select target systems, see “Creating a task” for more information. After you click **Next** the **Choose Source System** page appears. Select the source system. See “Creating a Replicate Agent Settings task” for more information.

Related procedure

- ▲ Creating a Replicate Agent Settings task

Related topics

- Replicate Agent Settings - Reference
- About secure task execution
- Replicating trusted certificates

Creating a Replicate Agent Settings task

The *Replicate Agent Settings tool* enables HP Systems Insight Manager (HP SIM) to retrieve and optionally edit Web Agent configuration settings from a source *system* and distribute that configuration remotely to one or more target systems through Web Agents.

To create a Replicate Agent Setting task:

1. Select **Configure**→**Replicate Agent Settings**. The **Replicate Agent Settings** window appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**.
4. Select a source system by selecting one of the following methods:
 - **You know the name of the system.** If you select this option, enter the name of the system in the box. Click **Next**.
 - **Pick the system from a list.** If you select this option, select a target system from the list of known systems that supports *Replicate Agent Settings*. Click **Next**.
Note: If the source system cannot be used, a message appears, informing you of the error. Select a different system from the **Choose Source System** page.
Note: If the trust relationship for a system is incorrectly configured, an error message appears. See “Replicate Agent Settings - Reference” for more information.

The **Choose Source Configuration Settings** page appears. The source system configurations display without any parameters selected.

5. Select the desired settings as needed. You can select each parameter individually. At least one must be selected to continue. You can also select to **Wake target systems from low power mode before configuring**. See “Replicate Agent Settings - Reference” for more information.
6. Select one of the following options to execute the task:
 - Click **Schedule** to schedule when the task should run. See “Scheduling a task” for more information.
 - Click **Run Now** to run the task immediately. The **Task Results** page appears. See “Task results list” for more information.
 - Click **Previous** to return to the previous page.
Note: The Replicate Agent Settings task uses the Secure Task Execution (STE) feature. See “About secure task execution” for more information.

Related procedure

- ▲ Scheduling a task

Related topics

- Replicating trusted certificates
- Replicate Agent Settings - Reference
- About secure task execution

Replicate Agent Settings - Reference

Determining a trust relationship

When selecting the source system from the list, a trusted column displays that indicates whether a trust relationship exists between the management server and the indicated system. If a trust relationship is not configured for that system, that system is marked **no** in the trusted column.

Changing a trust relationship

To change a trust relationship for a system, click **configure** in the appropriate row. The HTTP server configuration page or **System Management Homepage** for the associated system appears.

Wake on LAN feature

Wake on LAN (WOL) is a feature that is used by HP Systems Insight Manager (HP SIM) to bring a target system that is in Advanced Configuration Power Interface (ACPI) Standby mode or powered off to full power. The Replicate Agent Settings feature can optionally use the WOL feature to wake target systems that are in low power mode so that they can be configured. A system can be remotely powered up if it is equipped with a WOL-enabled NIC, or it has ACPI support in the operating system. See the target ProLiant server documentation to determine if Remote WakeUp is supported by the server.

Replicate Agent Settings events

Replicate Agent Settings events are used to show the status of a Replicate Agent Settings task. They reflect successful or unsuccessful attempts of a Replicate Agent Settings task execution. They are logged in the job details for the corresponding Replicate Agent Settings task.

Related procedure

- ▲ [Creating a Replicate Agent Settings task](#)

Related topics

- [Replicate Agent Settings](#)
- [About secure task execution](#)
- [Replicating trusted certificates](#)

RPM Package Manager

The RPM Package Manager (RPM) is a powerful command line-driven package management system capable of installing, uninstalling, verifying, querying, and updating computer software packages. Each software package consists of an archive of files along with information about the package like its version, a description, and the like. There is also a related Application Program Interface (API), permitting advanced developers to bypass shelling out to a command line and to manage such transactions from within a native coding language. RPM has been integrated into HP Systems Insight Manager (HP SIM) through the **Deploy** menu.

The following procedures are available for RPM within HP SIM:

- **Install RPM.** See “Installing RPM” for more information.
- **Query RPM.** See “Querying RPM” for more information.
- **Uninstall RPM.** See “Uninstalling RPM” for more information.
- **Verify RPM.** See “Verifying RPM” for more information.

Related procedures

- [Installing RPM](#)
- [Querying RPM](#)
- [Uninstalling RPM](#)
- [Verifying RPM](#)

Installing RPM

Use this tool to install RPM Package Manager (RPM) on multiple Linux systems.

To install RPM:

1. Select **Deploy**→**RPM Package Manager**→**Install RPM**.
2. Select the target systems. See “Creating a task” for more information about selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[install-options] package-file**.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. See “Scheduling a task” for more information about scheduling the task.

Related procedures

- Querying RPM
- Uninstalling RPM
- Verifying RPM

Related topic

- ▲ RPM Package Manager

Uninstalling RPM

Use this tool to uninstall RPM Package Manager (RPM) on multiple Linux systems.

To uninstall RPM:

1. Select **Deploy**→**RPM Package Manager**→**Uninstall RPM**.
2. Select the target systems. See “Creating a task” for more information about selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[erase-options] package-name**.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. See “Scheduling a task” for more information about scheduling the task.

Related procedures

- Querying RPM
- Installing RPM
- Verifying RPM

Related topic

- ▲ RPM Package Manager

Querying RPM

This option is used to list installed RPM Package Manager (RPM) package versions and can be run on multiple Linux systems.

To query RPM package version:

1. Select **Deploy**→**RPM Package Manager**→**Query RPM**.
2. Select the target systems. See “Creating a task” for more information about selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, **[query-options] package-name**.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. See “Scheduling a task” for more information about scheduling the task.

Related procedures

- Installing RPM
- Uninstalling RPM
- Verifying RPM

Related topic

- ▲ RPM Package Manager

Verifying RPM

This procedure enables you to verify installed RPM Package Manager (RPM) packages installed and can be run on multiple systems.

To verify RPM:

1. Select **Deploy**→**RPM Package Manager**→**Install RPM**.
2. Select the target systems. See “Creating a task” for more information about selecting target systems.
3. Click **Next**. The **Step 2: Specify Parameters** page appears.
4. Enter the parameter, `[select-options] package-name`.
5. Click **Run Now** to run the tool, click **Previous** to return to the previous screen, or click **Schedule** to schedule when the task runs. See “Scheduling a task” for more information about scheduling the task.

Related procedures

- Querying RPM
- Installing RPM
- Uninstalling RPM

Related topic

- ▲ RPM Package Manager

Server Migration Pack

The HP Server Migration Pack - Universal Edition extends the functionality of the HP ProLiant Essentials Virtual Machine Management Pack by simplifying the server consolidation process. The HP Server Migration Pack - Universal Edition provides the following migration capabilities:

- **Physical-to-virtual (P2V) migration** Migrates a physical machine to a virtual machine guest within a Microsoft Virtual Server 2005 or VMware virtual machine host
- **Virtual-to-virtual (V2V) migration** Migrates a virtual machine guest between different virtualization layers, including Microsoft Virtual Server 2005, VMware ESX Server™, VMware Server™, and VMware GSX Server™
- **Virtual-to-physical (V2P) migration** Migrates a virtual machine guest within a Microsoft Virtual Server 2005 or VMware virtual machine host to a physical machine

You must have *administrative rights* to access SMP Universal related menu items.

Select **Options**→**Virtualization Management**→**Upload Drivers** and ensure that all of the necessary device drivers have been loaded on to the HP Systems Insight Manager (HP SIM) Central Management Server (CMS). If additional files are necessary, load these files from the original Windows or VMware media. Then, you can perform P2V, V2V, or V2P migrations from the **Deploy**→**Virtual Machine** menu items.

The SMP Universal is a companion product that works with an equivalent version of the Virtual Machine Management Pack.

SMP Universal licensing

The HP Server Migration Pack - Universal Edition uses HP ProLiant Essential products licensing. One license is used for each successful P2V, V2V, or V2P migration.

To add SMP Universal licenses:

1. Select **Deploy**→**License Manager**.
2. Select **Add New Product** or **Server Migration Pack** (if available).
3. Click **Manage Licenses**.
4. Click **Add Licenses** and follow the on-screen instructions.

Related procedures

- [Accessing the Server Migration Pack](#)
- [Adding licenses individually](#)

Accessing the Server Migration Pack

The physical-to-virtual (P2V), virtual-to-virtual (V2V), and virtual-to-physical (V2P) migrations can only be performed if at least one HP Server Migration Pack - Universal Edition license is available.

To access SMP Universal:

1. Select **Tools**→**Integrated Consoles**→**Server Migration Pack**. The **Server Migration Pack** page appears.
2. Select **Migration Options** to perform a P2V, V2V, or V2P migration.

Related topic

- ▲ [Server Migration Pack](#)

System Management Homepage

HP Systems Insight Manager (HP SIM) enables you to access the System Management Homepage of a system. The *System Management Homepage* (SMH) is a web-based application that provides a consolidated interface for single-system management. By aggregating the data from HP web-based agents and management utilities, the SMH provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server.

The SMH can be installed on Windows and Linux operating systems. On x86, the Setup Wizard performs the installation of the SMH and enables you to set the security options used by all of the Web Agents on the system. On Linux Itanium Processor Family (IPF), the System Management Homepage can be installed with default settings through a RPM Package Manager (RPM) package and configured by the `smhconfig` tool.

The SMH Replicate Agent Settings feature enables HP SIM to retrieve a set of configuration data from HP Web-enabled System Management Software on a reference system and distribute that configuration data to one or more target systems. In addition, some System Management Homepage parameters are replicable through HP SIM. See “Creating a Replicate Agent Settings task” for more information regarding Replicate Agent Settings.

Related procedure

- ▲ [Accessing the System Management Homepage](#)

Related topic

- ▲ [System Page](#)

Accessing the System Management Homepage

1. Select **Tools**→**System Information**→**System Management Homepage**.
2. Select target systems. See “Creating a task” for more information. The System Management Homepage appears.

Related procedures

- [Creating a Replicate Agent Settings task](#)
- [Accessing the Version Control Agent](#)
- [Accessing the Version Control Repository Manager](#)

Related topics

- [System Page](#)
- [System Management Homepage](#)

System Page

The **System Page** is used to display information that is related to a specific *system*. This page displays the following tabs:

- **System**. Includes general system and status information
- **Tools & Links**. Includes links to System Management pages, HP Systems Insight Manager (HP SIM) pages, and other useful links
- **Events**. Displays the event table view page for the system
- **Performance**. This tab is only available when virtual machine hosts and guests are discovered, and displays performance information.
- **Essentials**. This tab is only available for systems that might support other HP SIM partner applications and provides a description of the available software and a link to the HP website. You must have *administrative rights* or *operator rights* rights to view this tab.

You can access the **System Page** in two ways:

- Select **Tools**→**System Information**→**System Page**. Then select target systems.
- Click the system name in the **System Name** column on the system table view page.

Related topics

- [System table view page](#)
- [Tools & Links tab](#)
- [Navigating the event table view page](#)
- [System tab](#)
- [System tab for clusters](#)
- [System tab for a complex](#)
- [System tab for partitions](#)
- [System tab for a tape library](#)
- [System tab for a storage switch](#)
- [System tab for a storage host](#)
- [System tab for a storage array](#)

System tab

On the **System** tab, a status icon indicates the overall *health status* that is stored in the *database*. If a system is suspended, a disabled icon appears in place of the hardware status icon and software status icon. The **System Status** section contains more information on the *system* status.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.



NOTE: See “System tab for virtual machine hosts” for more information about the **System** tab for virtual machine hosts.

See “System tab for virtual machine guests” for more information about the **System** tab for virtual machine guests.

The **System** tab page for servers is divided into the following sections:

- System Status
- More Information
- Identification

- Firmware Revision
- Product Description
- HP Insight Power Manager
- Contact Information
- Asset Information
- Management Processor
- Host Server
- Storage Server
- Associations

System Status

This section includes the following information:

- **Health Status** The overall status for a system. It is obtained from *Web-Based Enterprise Management* (WBEM) *SNMP*, *Desktop Management Interface* (DMI), and the HTTP protocols with the most critical status displayed. A ping (ICMP or TCP reachable check) is always made. Click the **Health Status** link to access the System Management Homepage (SMH), if present. If the SMH is not present, the link accesses the **Property Page Status** page. If no option is available, the **Health Status** link is not present.
- **Management Processor Status** The management processor status (if available) links to a web server on the management processor.
- **Software Status** The software status icon links to the system software Version Control Agent if available.
- **Disabled Status** A system that is suspended has a disabled icon in the **HW** and **SW** columns on the system table view page.
- **Vulnerability Status** The vulnerability status of a system is the indicator summation of security and configuration weaknesses as determined by an external security scan of the system.
- **Contract and Warranty Status** The **Contract and Warranty Status** is available when you have a Windows CMS and the HP Service Essentials Remote Support Pack is installed. You can view Contract and Warranty status updates for HP systems that have contract and warranty data collection enabled. Click the **Contract and Warranty Status** icon to view the **Contract and Warranty Details** page for the system.
Note: See “Suspending or resuming contract and warranty data collection for a single system” for information about contract and warranty data collection.
Note: See “Editing system properties for a single system” or “Editing system properties for multiple systems” for information about entering contract and warranty information for single or multiple systems.
- **Aggregate Event Status** The **Aggregate Event Status** is a summary of all of a system's uncleared events. This status is updated whenever an event is added, updated, or removed. To view the **System Page Events** tab for a system, click the **Aggregate Event Status** icon.



NOTE: If a system is currently in a suspended mode, the **System Page** displays a disclaimer under **System Status**, stating Monitoring of the system is suspended until, and gives a date and time for monitoring to resume.

Partner applications might have their own status registered with the *Central Management Server* (CMS). If so, these statuses are displayed under **Health Status** and as status columns on the system table view page. For example, the **System Security Vulnerability Status** links to detailed information about the system status with regard to Vulnerability and Patch Management Pack.

See “System status types” for more information about system status types.

More Information

This section provides more detailed information about the system and lists all system information tools available for the system. The following links are available:

- **System Management Homepage** SMH is launched if available.
- **Property Page** The **Property** pages are launched if available.
- **Partition Manager View** The Partition Manager is launched if available.
- **Virtual Manager Host View** The Virtual Manager Host View is launched if available.

Identification

This section is expanded whenever you access the **System Page** the first time.



NOTE: This section can be expanded by clicking  or collapsed by clicking .



IMPORTANT: *Desktop Management Interface* identification is only supported on Windows and HP-UX-based *Central Management Server* (CMS) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.

The items available in this section include:

- **Address** The IP address that has been discovered for the system.
- **Preferred System Name** The name shown for the system. When available, it defaults to the host name from DNS. You can override this setting through the **Edit System Properties** link under the **Tools & Links** tab.
- **Network Name** The fully qualified DNS name, if available. Reverse DNS lookups by IP address must be enabled and match a forward lookup.
- **UUID** A unique identifier from the agent or other instrumentation on the system.
- **Serial Number** The serial number of the system.

Orphan systems



A system described as an orphan system is a system for which HP Systems Insight Manager (HP SIM) detects that both the IP address and name have been reallocated to another system. Occasionally, this reallocation can happen through simultaneous DHCP address assignment changes and a system rename. Other causes can be caused by a move of the operating system from one blade to another through different virtualization mechanisms, such as a physical-to-physical system move or replacement of a system board that has not been configured the same as the original system board.

In HP SIM, orphan systems can be named one of three ways, with the first naming convention that HP SIM can use. The following lists three ways orphan system can be named:

- **<serialNumber>** Where *<serialNumber>* is replaced with the serial number of the system.
- **<serialNumber>-<devKey>-<oldName>** Where *<serialNumber>* is replaced with the serial number of the system, *<devKey>* is replaced with the devKey on the system, and *<oldName>* is replaced with the old system name.
- **<devKey>** Where *<devKey>* is replaced with the devKey on the system.

Firmware Revision





NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section includes the following:

- **Executable** The name of the executable.
- **Manufacturer** The vendor of the installed firmware.
- **Version** The version string for the installed firmware. The version can include major, minor, revision, and build information.
- **Build Number** The build number of the software.
- **State** The client application uses the *InstallState* from the bundle, and the *InstallSoftwareIdentity* association from the bundle's components to determine which *Software Identity* objects in the bundle are installed and which are missing. This field can contain the values: **Installed**, **Partial**, or **None**.
- **Classification** The classification field provides a means to describe the software. For example, the field might contain **Firmware** or **Application Software** among other descriptive strings.
- **Firmware Category** The firmware category field displays values related to the category of software, such as Network Interface Card (NIC) driver, NIC firmware, System Management Software, and so on.

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section includes the following information:

- **Product ID** The identification number that, when added to the serial number of the server, enables HP Support to uniquely identify HP systems
- **System Type** The basic system type returned from identification
- **System Subtype** The system subtype returned from identification
- **Product Model** The product model (name) as defined by the manufacturer
- **Hardware Description** The description of the hardware obtained from the **Edit System Properties** page
- **OS Name** The operating system name for the system used for filtering in operating system-based system collections
- **OS For Tool Filtering** The short name of the operating system used for tool filter definition files
- **OS Description** The detailed description of the operating system (for example, service pack information)
- **OS Version** The numerical representation of the operating system version
- **Management Protocols** The management protocols that have responded when attempting to identify the system
Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.
- **Server Role** The user-specified server role from the ProLiant agents that can be set from the System Management Homepage
- **Comments** The user-specified comments from the SNMP or other agents
- **Current Running Applications** A list of all applications currently running on the system

HP Insight Power Manager

HP Insight Power Manager (IPM) is an *HP Systems Insight Manager* (HP SIM) plug-in that aggregates power data, and provides remote control regardless of operating system type and enables you to monitor historical power consumption and heat dissipation to effectively manage those resources. It extends the unified infrastructure framework by providing new levers into the server and enabling policy-based power and thermal management. For more information, see [HP Insight Power Manager - Getting started](#).



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This option displays a graph and analysis section for a single system, if IPM is installed/configured on HP SIM and if the selected server supports IPM and is licensed. For more information about licensing IPM, see “License manager”. See [HP Insight Power Manager - Report](#) or click help while viewing the HP Insight Power Manager graph for information about how to use the features of IPM.

Contact Information

This section includes the following information:

- **Location** A user-specified field from the agents for the physical location of the system
- **Contact** The user-specified contact of the system from the agents

Note: Many of the fields in the contact and product description sections can be overridden locally on the CMS through the **Edit System Properties** pages. See “Editing system properties for a single system” for more information.

Entitlement Information

- **Start Date** The starting date of the contract or warranty.
- **End Date** The end date of the contract or warranty.
- **Type** The contract type, if a service contract exists.
- **Status** The current contract or warranty status.
- **Last Collection** The date that contract and warranty data was last collected.

Asset Information

This section includes **Asset Number**, which is the asset number of the system.

Management Processor

This section appears only if a management processor is available. It includes the following information:

- **Name** The display name (Preferred Name) of the management processor used to manage the system
- **Address** The IP address of the management processor used to manage the system
- **Model** The model name of the management processor for this system

Host Server

This section includes the following information:

- **Name** The host server name with a link to the host server System page
- **Slot** The slot number of the host server
- **Model** The product model of the host server

Storage Server

The following section includes the following information for servers that have a storage server associated:

- **Name** The storage server name with a link to the storage server System Page
- **Slot** The slot number of the storage server System Page
- **Model** The product model of the storage server

Associations

This section includes the following information:

- **Enclosure Name** The name of the enclosure, if the system is in an enclosure (for example, a p-Class server blade)
- **Rack Name** The name of the rack, if the enclosure is in a rack that could be discovered
- **Slot** The slot number that the system is positioned within the enclosure
- **Server Dimensions** The dimensions in millimeters of the system, if available

Related topics

- [System Page](#)
- [Tools & Links tab](#)
- [System tab for virtual machine hosts](#)
- [Navigating the event table view page](#)

System tab for management processors

On the **System** tab, a status icon indicates the overall *health status* that is stored in the *database*. If a system is suspended, a disabled icon appears in place of the hardware status icon.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

The **Identity** page is divided into the following sections:

- [System Status](#)
- [Identification](#)
- [Product Description](#)

System Status

This section includes:

- **Health Status** The overall status for a system. It is obtained from *Web-Based Enterprise Management (WBEM) SNMP*, *Desktop Management Interface (DMI) Status Polling* tasks, or all three. A ping (ICMP or TCP reachable check) is always made. Click the **Health Status** link to access management processor home page.

See “System status types” for more information about system status types.

- **Contract and Warranty Status** The **Contract and Warranty Status** is available when you have a Windows CMS and the HP Service Essentials Remote Support Pack is installed. You can view Contract and Warranty status updates for HP systems that have contract and warranty data collection enabled. Click the **Contract and Warranty Status** icon to view the **Contract and Warranty Details** page for the system.

Note: See “Suspending or resuming contract and warranty data collection for a single system” for information about contract and warranty data collection.

Note: See “Editing system properties for a single system” or “Editing system properties for multiple systems” for information about entering contract and warranty information for single or multiple systems.

- **Aggregate Event Status** The **Aggregate Event Status** is a summary of all of a system's uncleared events. This status is updated whenever an event is added, updated, or removed. To view the **System Page Events** tab for a system, click the **Aggregate Event Status** icon.

Identification

This section is expanded whenever you access the **System Page** the first time.



NOTE: This section can be expanded by clicking  or collapsed by clicking .



IMPORTANT: DMI identification is only supported on Windows and HP-UX-based *Central Management Server* (CMS) installs. In addition, only like operating systems can be identified. For example, Windows-based CMSs can identify Windows-based DMI, and HP-UX-based CMSs can only identify HP-UX-based DMI systems.

The following items available in this section:

- **Address** The IP address that has been discovered for the system.
- **Preferred System Name** The name shown for the system. When available, it defaults to the host name from DNS. You can override this through the **Edit System Properties** link under the **Tools & Links** tab.
- **Network Name** The fully qualified DNS name, if available. Reverse DNS lookups by IP address must be enabled and match a forward lookup.
- **Serial Number** The serial number of the system.

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section includes the following:

- **System Type** The basic system type returned from identification
- **Product Model** The product model (name) as defined by the manufacturer
- **Hardware Description** The description of the hardware obtained from the **Edit System Properties** page
- **Management Protocols** The management protocols that have responded when attempting to identify the system
Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.

Entitlement Information

- **Start Date** The starting date of the contract or warranty.
- **End Date** The end date of the contract or warranty.
- **Type** The contract type, if a service contract exists.
- **Status** The current contract or warranty status.
- **Last Collection** The date that contract and warranty data was last collected.

Related topics

- [System Page](#)
- [Tools & Links tab](#)
- [Navigating the event table view page](#)





System tab for virtual machine hosts

After clicking a virtual machine host in the HP Systems Insight Manager (HP SIM) console, to display the following configuration information for the host, click the **System** tab.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

The **System** tab includes the following information:

- **System status** This section indicates the status of the virtual machine host using the following color-coded icons:

Status icon	Icon meaning	Description
	Normal	The virtual machine host is licensed and is currently communicating with the Virtual Machine Management Pack.
	Minor	The virtual machine host is licensed but is not currently communicating with the Virtual Machine Management Pack.
	Major	The Virtual Machine Management Pack Agent is installed on the server, but the server is not a virtual machine host.
	Critical	The Virtual Machine Management Pack Agent is installed on the virtual machine host, but the host is not licensed.
	No icon	The Virtual Machine Management Pack Agent is not installed on this server or not registered to the Virtual Machine Management Pack.

- **Health Status** The overall status for a system. It is obtained from *Web-Based Enterprise Management (WBEM) SNMP*, *Desktop Management Interface (DMI)*, and the HTTP protocols, with the most critical status being displayed. A ping (ICMP or TCP reachable check) is always made. To access the System Management Homepage (SMH), click the **Health Status** link. If the SMH is not present, the link accesses the **Property Page Status** page. If no option is available, the **Health Status** link is not present.
See "System status types" for more information about the system status types.
- **Vulnerability status**
- **Virtual Machine Management Status** The status of the virtual machine status.
If the virtual machine host or guest is not managed by HP ProLiant Essentials Virtual Machine Management Pack, this status becomes a hyperlink. Click the link for additional information on how to manage virtual machine hosts and guests.
- **Identification** The address, preferred system name, and network name. See "System tab" for more information about these fields.
- **Product Description**
 - **Product ID** The alphanumeric name used to identify the product.
 - **System type** The basic system type returned from identification.

- **System subtype** The system subtype returned from identification. The virtual machine host is present in this field.
- **Product model** The system model name returned from identification.
- **Hardware description** Details of the physical system on which the software is running.
- **OS name** The operating system used.
- **OS for tool filtering** The type of operating system being used for filtering.
- **OS description** The level of operating system being used.
- **OS version** The version of the operating system.
- **Management protocols** States the protocols being used for tool filtering.
- **Virtual machine host configuration details** This section displays virtualization and disk information.
 - **Virtualization** Virtualization layer type.
 - **Performance alert** Displays the threshold values set by the user. For example, **When over 44% CPU for more than 55 minutes.**
 - **Storage details** Displays disk space information.
- **Virtual machines** This section displays a list of virtual machines associated with the virtual machine host.
 - *unnamed* This option is used to select a virtual machine on which action is to be taken.
 - **Status** Displays the status of the virtual machine.
 - **State** Displays the state of the virtual machine.
 - **VM name** Displays the name of the virtual machine.
 - **System IP address** Displays the IP address of the virtual machine.
 - **Legend** Click the **Legend** link to display the **VMM Status Icon Legend** window that displays the icons and their definitions.
- **Contact information** This section displays the physical location of the equipment and the e-mail address of the contact.
- **Disk partitions** This section displays a list of virtual machines controlled by the host.
 - **Disk name** The name of the disk.
 - **Partition** The partition on the drive the disk is found.
 - **Capacity** The capacity of the disk.
 - **%Used** The percentage of the disk that has been used.
 - **Format** The format type of the disk.
 - **Type** The type of disk used.
- **Associations** This section displays a list of virtual machines that are hosted by this virtual machine host.



NOTE: Depending on the host configuration, additional details might be displayed.

Related topics

- System Page
- Virtual machine host performance
- System tab for virtual machine guests
- System tab

System tab for virtual machine guests

After clicking a virtual machine guest in the HP Systems Insight Manager (HP SIM) console, click the **System** tab to display the following configuration information for the guest.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

The **System** tab includes the following information:

- **System status** The health and virtual machine status is depicted using color-coded icons and includes the following information:
 - **Health Status** The overall status for a system. It is obtained from *Web-Based Enterprise Management (WBEM) SNMP*, *Desktop Management Interface (DMI)*, and the HTTP protocols, with the most critical status being displayed. A ping (ICMP or TCP reachable check) is always made. To access the System Management Homepage (SMH), click the **Health Status** link. If the SMH is not present, the link accesses the **Property Page Status** page. If no option is available, the **Health Status** link is not present.
See "System status types" for more information about the system status types.
 - **Vulnerability status**
 - **Virtual Machine Management Status** The status of the virtual machine status.
If the virtual machine host or guest is not managed by HP ProLiant Essentials Virtual Machine Management Pack, this status becomes a hyperlink. Click the link for additional information on how to manage virtual machine hosts and guests.
- **Identification** The address, preferred system name, and network name are displayed. See "System tab" for more information about these fields.
- **Product Description**
 - **System type** The type of system on which the software is running.
 - **System subtype** Identifies a virtual machine host or guest.
 - **Product model** Identifies the platform type.
 - **Hardware description** The details of the physical system on which the software is running.
 - **OS name** The operating system used.
 - **OS for tool filtering** The type of operating system being used for tool filtering.
 - **OS description** The level of operating system being used.
 - **OS version** The version of the operating system.
 - **Management protocols** States the protocols being used for tool filtering.

- **VM control** Virtual machine status is listed, and the controls enable you to launch the Remote Desktop and the Remote Console, as well as start, stop, reset, and pause the virtual machine. Click **Legend** for detailed status legend information.
- **Virtual machine configuration details**
 - **Virtual machine host** The system name of the virtual machine host.
 - **Virtualization** The virtualization technology installed on the virtual machine host.
 - **Alternate host** Displays the failover host set by the user.
 - **Configuration file** The name and location of the configuration file.
 - **Configuration folder** The name and location of the configuration folder.
 - **Memory** The amount of memory on the virtual machine host.
 - **Virtual NIC** The type of network card and MAC address.
 - **Virtual disk** The type of virtual disk, location, mode, and capacity.
 - **CD/DVD RM** Details about the drive.
- **Virtual machine backups** This section displays information about the backups for the virtual machine.
 - **Source host** The source host name.
 - **Source path** The source path.
 - **Configuration file** The configuration file name.
 - **Virtualization layer** The virtualization layer.
 - **Backup repository** The backup repository information.
 - **Backup repository location** The location of the backup repository.
 - **Date** The date of the last backup.
- **Virtual machine disk partitions** This section displays a list of virtual machines controlled by the host.
 - **Disk name** The name of the disk.
 - **Partition** The partition on the drive the disk is found.
 - **Capacity** The capacity of the disk.
 - **%Used** The percentage of the disk that has been used.
 - **Format** The format type of the disk.
 - **Type** The type of disk used.
- **Associations** This section displays a list of virtual machines that are hosted by this virtual machine host.

Related procedures

- [Virtual machine controls - Launching the remote console](#)
- [Virtual machine controls - Starting or resuming virtual machine guests](#)
- [Virtual machine controls - Shutting down or stopping virtual machine guests](#)
- [Virtual machine controls - Suspending virtual machine guests](#)
- [Virtual machine controls - Resetting or restarting virtual machine guests](#)

Related topics

- [System Page](#)
- [Virtual machine guest performance](#)
- [System tab for virtual machine hosts](#)

Virtual machine controls - Launching the remote console



IMPORTANT:

- Microsoft Virtual Server 2005 remote console is only supported with Microsoft Internet Explorer browsers.
- VMware Management Interface must be installed on VMware GSX Server VM hosts to launch the remote console.
- If you are launching a remote console from a VMware host, VMware Remote Console application must be installed on the system from which you are launching remote console.

1. From the HP Systems Insight Manager (HP SIM) **All Systems** page, click the virtual machine host or the virtual machine guest to access the **System Page**.
2. Click **Launch Remote Console**.

Related procedures

- [Virtual machine controls - Starting or resuming virtual machine guests](#)
- [Virtual machine controls - Shutting down or stopping virtual machine guests](#)
- [Virtual machine controls - Suspending virtual machine guests](#)
- [Virtual machine controls - Resetting or restarting virtual machine guests](#)

Related topics

- [System Page](#)
- [System tab for virtual machine guests](#)
- [Virtual machine guest performance](#)

Virtual machine controls - Starting or resuming virtual machine guests



NOTE: A virtual machine guest can only be started or resumed if it is currently stopped, shut down, or paused.

To start or resume a virtual machine guest from the HP Systems Insight Manager (HP SIM) toolbar:

1. From the **All Systems** page, select the virtual machine guests to be suspended or paused.
2. Select **Deploy**→**Virtual Machine**→**Start Virtual Machine**.
3. Verify the target system, and then click **Next**. Virtual machine source information appears.
4. Confirm the details, and then click **Schedule** or **Run Now**. See “Scheduling a task” for more information about scheduling a task.

To start or resume a virtual machine guest from the virtual machine host of guest **System Page**:

1. Click **Start/Resume**.
2. Verify the target system, and then click **OK** when prompted.

If the virtual machine guest is currently stopped or paused, the guest is started or resumed. If the virtual machine guest is currently suspended to disk (only possible with Microsoft Virtual Server 2005), selecting **Resume Virtual Machine Guest** restores the virtual machine guest to the previous state and powers on the virtual machine guest.

When the power-on process is complete, the status is updated to a Normal. The **Start** button is displayed, and the **Shutdown/Stop**, **Pause**, and **Reset** buttons are enabled.

If a virtual machine guest becomes stuck during the start process, the HP ProLiant Essentials Virtual Machine Management Pack displays **User Intervention** and the status is updated to Major.

Related procedures

- Virtual machine controls - Launching the remote console
- Virtual machine controls - Shutting down or stopping virtual machine guests
- Virtual machine controls - Suspending virtual machine guests
- Virtual machine controls - Resetting or restarting virtual machine guests

Related topics

- System Page
- System tab for virtual machine guests
- Virtual machine guest performance

Virtual machine controls - Resetting or restarting virtual machine guests

To reset or restart a virtual machine guest from the HP Systems Insight Manager (HP SIM) toolbar:

1. From the **All Systems** page, select the virtual machine guests to be suspended or paused.
2. Select **Deploy**→**Virtual Machine**→**Reset Virtual Machine**.
3. Verify the target system, and then click **Next**. Virtual machine source information appears.
4. Confirm the details, and then click **Schedule** or **Run Now**. See “Scheduling a task” for more information about scheduling a task.

To reset or restart a virtual machine guest from the virtual machine host or guest **System Page**:

1. Click **Reset/Restart**.
2. Verify the target system, and then click **OK** when prompted.

For Microsoft Virtual Server 2005 virtual machine guests, select **Reset** or **Restart** when prompted. Selecting **Reset** powers off and then powers on the virtual machine guest. Selecting **Restart** shuts down the virtual machine operating system and then powers off and powers on the virtual machine guest.



CAUTION: Unsaved data is lost if you click **Reset**.

When the reset or restart process is complete, the status is updated to Normal. The **Shutdown/Stop, Pause,** and **Reset** buttons are enabled, and the **Start** button is disabled.

Related procedures

- Virtual machine controls - Starting or resuming virtual machine guests
- Virtual machine controls - Shutting down or stopping virtual machine guests
- Virtual machine controls - Suspending virtual machine guests
- Virtual machine controls - Launching the remote console

Related topics

- System Page
- System tab for virtual machine guests
- Virtual machine guest performance

Virtual machine controls - Suspending virtual machine guests



NOTE: A virtual machine guest can only be suspended if it is currently powered on and running.

To suspend a virtual machine guest from the HP Systems Insight Manager (HP SIM) toolbar:

1. From the **All Systems** page, select the virtual machine guests to be suspended or paused.
2. Select **Deploy**→**Virtual Machine**→**Suspend Virtual Machine**.
3. Verify the target system, and then click **Next**. Virtual machine source information appears.
4. Confirm the details, and then click **Schedule** or **Run Now**. See “Scheduling a task” for more information about scheduling a task.

To suspend a virtual machine guest from the virtual machine host or guest **System Page**:

1. Click **Pause**.
2. Verify the target system, and then click **OK** when prompted.

For Microsoft Virtual Server 2005 virtual machine guests, select **Suspend to disk** or **Pause VM** when prompted. Selecting **Suspend to disk** saves the current state and releases the virtual machine host memory used by the virtual machine. Selecting **Pause VM** suspends the virtual machine execution but retains the virtual machine state in the virtual machine host memory.

When the suspend to disk or pause process is complete, the status is updated to Disabled. The **Stop**, **Pause**, and **Reset** buttons are disabled, and the **Start** button is enabled.

Related procedures

- Virtual machine controls - Starting or resuming virtual machine guests
- Virtual machine controls - Shutting down or stopping virtual machine guests
- Virtual machine controls - Launching the remote console
- Virtual machine controls - Resetting or restarting virtual machine guests

Related topics

- System Page
- System tab for virtual machine guests
- Virtual machine guest performance

Virtual machine controls - Shutting down or stopping virtual machine guests



NOTE: A virtual machine guest can only be shut down if it is currently powered on and the Microsoft Virtual Server Additions of the VMware Tools are installed on the virtual machine guest.

1. From the **All Systems** page, select the virtual machine guests to be suspended or paused.
2. Select **Deploy**→**Virtual Machine**→**Stop Virtual Machine**.
3. Verify the target system, and then click **Next**. Virtual machine source information appears.
4. Confirm the details, and then click **Schedule** or **Run Now**. See “Scheduling a task” for more information about scheduling a task.

To shut down or stop a virtual machine guest from the virtual machine host or guest **System Page**:

1. Click **Shutdown/Stop**.
2. Verify the target system, and then click **OK** when prompted.

For Microsoft Virtual Server 2005 virtual machine guests, select **Stop VM** or **Shutdown VM** when prompted. Selecting **Stop VM** powers off the virtual machine guest immediately without saving the current state. Selecting **Shutdown VM** shuts down the virtual machine operating system and then powers off the virtual machine guest.



CAUTION: Unsaved data is lost if you select **Stop VM**.

When shutdown or stop process is complete, the status is updated to Disabled. The **Stop**, **Pause**, and **Reset** buttons are disabled, and the **Start** button is enabled.

Related procedures

- Virtual machine controls - Starting or resuming virtual machine guests
- Virtual machine controls - Launching the remote console
- Virtual machine controls - Suspending virtual machine guests
- Virtual machine controls - Resetting or restarting virtual machine guests

Related topics

- [System Page](#)
- [System tab for virtual machine guests](#)
- [Virtual machine guest performance](#)

Virtual machine host performance

After clicking a virtual machine host in the HP Systems Insight Manager (HP SIM) console, click the **VM Performance** tab to display the performance information for the host. Activity for the most recent 1, 5, 15, 30, or 60 minutes can be displayed. If the amount of time requested exceeds the amount available, all available information is reported.

- **Virtual machine host performance** The following performance information is provided for VMware ESX Server, VMware GSX Server, VMware Server and Microsoft Virtual Server 2005 hosts, except where noted.
 - **Processor utilization (x CPUs)** The processor utilization on the host, including utilization by the virtual machines. The number of processor cores or threads on the virtual machine host is reported as x CPUs.
 - **Virtual machine processor utilization** The processor consumption by all of the virtual machines on this host. Processor resources consumed by a virtual machine before powering off the virtual machine are not included.
 - **Reserved capacity (All running virtual machines)** The sum of the Reserved System Capacity values for all virtual machines currently powered on (Microsoft Virtual Server 2005 only).
 - **CPU min (All running virtual machines)** The sum of the CPU Min values for all virtual machines currently powered on divided by the resources available on the host (VMware ESX Server only).
 - **Memory utilization** The total amount of memory currently in use on the host. The utilization bar indicates the memory utilization as a percentage of the physical memory configured.
 - **Virtual machine memory** The total amount of memory currently in use by virtual machines executing on the host. Memory consumed by a virtual machine before powering off the virtual machine is not included. The utilization bar indicates the virtual machine memory as a percentage of the physical memory configured (Microsoft Virtual Server 2005 and VMware ESX Server).
 - **Network throughput** The network traffic transmitted and received on this host. Virtual machine network throughput is included for VMware ESX Server.
 - **Network transmission throughput** The network traffic transmitted by this host. Virtual machine network transmission throughput is included for VMware ESX Server. The utilization bar represents the transmission percentage of the network throughput.
 - **Network receive throughput** The network traffic received by this host. Virtual machine network receive throughput is included for VMware ESX Server. The utilization bar represents the receive percentage of the network throughput.
 - **Storage throughput** The storage read by this host and all virtual machines on the host. The utilization bar represents the read percentage of storage throughput.
 - **Storage read throughput** The storage read by this host and all virtual machines on the host. The utilization bar represents the read percentage of storage throughput.
 - **Storage write throughput** The storage written by the host and all virtual machines on the host. The utilization bar represents the write percentage of storage throughput.
- **Virtual machine performance** The value averages displayed in this section are relative to the duration of the virtual machine host activity. Resources consumed by a virtual machine before powering off the virtual machine are not included.

- **CPU** The CPU percentage consumed by the virtual machine relative to the total processor capacity of the virtual machine host.
- **vCPU** The CPU percentage consumed by the virtual machine relative to its resource allocation.
- **Memory** Physical host memory consumed by the virtual machine (VMware ESX Server and Microsoft Virtual Server 2005).
- **Network** Network throughput for the virtual machine. The utilization bar indicates the virtual machine network throughput as a percentage of the total network throughput on the virtual machine host.
- **Storage** Storage throughput for the virtual machine. The utilization bar indicates the virtual machine storage throughput as a percentage of the total storage throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Threshold settings** A virtual machine host-specific threshold can be evaluated.
- **Threshold interval** The number of minutes of utilization data averaged to calculate the measured value.
- **Threshold value** The maximum utilization value that provides a Normal status.
- **Measured interval** The number of minutes of utilization data averaged to calculate the measured value.
- **Measured value** The average utilization over the most recent measured interval.
- **State** The current state of the threshold. The state can be:
 - **Unknown** Indicates that the number of utilization samples available is less than the threshold interval.
 - **Normal** Indicates that sufficient utilization samples are available, and the measured value is less than or equal to the threshold value.
 - **Exceeded** Indicates that sufficient utilization samples are available, and the measured value is greater than the threshold value.

Related topics

- [System Page](#)
- [System tab for virtual machine hosts](#)
- [Virtual machine guest performance](#)

Virtual machine guest performance

After clicking a virtual machine guest in the HP Systems Insight Manager (HP SIM) console, click the **VM Performance** tab to display performance information for the guest. Select the appropriate time frame at the top of the screen for which to display information.

- **Virtual machine performance**
 - **Virtual processor utilization (vCPU)** The CPU percentage consumed by the virtual machine relative to the resource utilization. The **Host Processor Utilization on 1 CPU** value is reported for VMware GSX Server and VMware Server.
 - **Host processor utilization on x CPUs** The CPU percentage consumed by the virtual machine relative to the number of physical processors (x) on which the virtual machine can execute.
 - **Host processor utilization on all CPUs** The CPU consumed by the virtual machine, relative to the total virtual machine host processors.

- **Memory utilization** The physical host used by the virtual machine. The utilization bar indicates the virtual machine memory utilization as a percentage of the physical memory configured on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Network throughput** The network traffic transmitted and received by the virtual machine. The utilization bar indicates the virtual machine network throughput as a percentage of the total network throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Network transmit throughput** The network traffic transmitted by the virtual machine. The utilization bar indicates the virtual machine Network Transmit Throughput as a percentage of the total network throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Network receive throughput** The network traffic received by the virtual machine. The utilization bar indicates the virtual machine network receive throughput as a percentage of the total network throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Storage throughput** The storage read and written by this virtual machine. The utilization bar indicates the virtual machine storage throughput as a percentage of the total storage throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Storage read throughput** The storage read by this virtual machine. The utilization bar indicates the virtual machine storage read throughput as a percentage of the total storage throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Storage write throughput** The storage written by this virtual machine. The utilization bar indicates the virtual machine storage write throughput as a percentage of the total storage throughput on the virtual machine host (VMware ESX Server and Microsoft Virtual Server 2005).
- **Resource Allocation** The bars indicate the virtual machine allocation relative to the capacity available on the virtual machine host.
 - **VMware ESX Server VMs** This section includes the following information:
 - **CPU min** The cpu.min value reported by VMware ESX Server.
 - **CPU max** The cpu.max value reported by VMware ESX Server.
 - **CPU shares** The cpu.shares value reported by VMware ESX Server.
 - **Microsoft Virtual Server 2005 virtual machine** This section includes the following information:
 - **Reserved capacity** The reserved system capacity value reported by Microsoft Virtual Server 2005 relative to one CPU.
 - **Maximum capacity** The maximum system capacity value reported by the virtual server relative to one CPU.
 - **Relative weight** The relative weight value reported by the virtual server.
- **Threshold settings** A virtual machine-specific threshold can be evaluated. This section includes the following information:
 - **Threshold interval** The number of minutes of utilization data that must be available before the threshold is evaluated.
 - **Threshold value** The maximum utilization value that provides a Normal status.
 - **Measured interval** The number of minutes of utilization data that is averaged when calculating the measured value.
 - **Measured value** The average utilization over the most recent Measured Interval minutes.
 - **State** The current state of the threshold, which can be:

- **Unknown** Indicates that the number of utilization samples available is less than the threshold interval.
- **Normal** Indicates that sufficient utilization samples are available, and the measured value is less than or equal to the threshold value.
- **Exceeded** Indicates that sufficient utilization samples are available, and the measured value is greater than the threshold value.

Related topics

- [System Page](#)
- [System tab for virtual machine guests](#)
- [Virtual machine host performance](#)

System tab for clusters

Based on the type of cluster provider and the version of cluster providers, not all properties are available at all times. If a property does not have a value, the property does not appear on this page. This page is for all clusters except for MSCS clusters. They are monitored using Cluster Monitor. See “[Cluster Monitor](#)” for more information.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Health Status

Each link under **Health Status** links to the **System Page** of a cluster member. The cluster status is a combination of the cluster member statuses included in the cluster. The most critical status is displayed.

Identification

- **Address** The IP address of the cluster.
- **Preferred System Name** The name shown for the system. When available, it defaults to the host name from DNS. You can override this through the **Edit System Properties** link under the **Tools & Links** tab.
- **Network Name** The fully qualified DNS name, if available. Reverse DNS lookups by IP address must be enabled and match a forward lookup.

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

- **Cluster Name** The name of the cluster
- **System Type** The basic system type returned from identification
- **Cluster Type** The basic cluster type returned from identification
- **Product Model** The product model (name) as defined by the manufacturer
- **OS Name** The longer operating system name for the system used for filtering in operating system-based system collections

- **OS For Tool Filtering** The short name of the operating system used for tool filter definition files
- **Management Protocols** The management protocols that have responded when attempting to identify the system
Note: If more protocols are expected, verify the credentials configured on the **System Protocol Settings** page.

Related topics

- [System Page](#)
- [System tab](#)

System tab for a complex

A complex is a container type system and contains nPartitions. Additional links are available on the **System Page** to access detailed information when a complex system is selected. Included here are the areas that are unique to a complex. See “[System tab](#)” for additional information about the tab.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Health Status

Each link under **Health Status** links to the **System Page** of a partition. The health status of a complex is a combination of all the health statuses of each partition included in the complex. The most critical status is displayed.

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section includes the following information:

- **Complex Name** The name of the complex returned from identification
- **Complex Type** The HP Systems Insight Manager (HP SIM) managed system type.
- **Complex Subtype** This field describes the additional roles of the complex. For example, HP Instant Capacity.
- **Product Name** The product name as defined by the manufacturer
- **Serial Number** The serial number of the complex returned from identification
- **Product Number - Current**
- **Product Number - Original**
- **Complex Profile Revision**
- **Active Service Processor Location**

Summary of Components

For a Complex Participating in iCOD:

- **Computer Cabinets**
- **I/O Cabinets** A cabinet is the Superdome's hardware box, which contains the cells, Guardian Service Processor (GSP), internal I/O chassis, I/O fans, cabinet fans, and power supplies.

- **nPartitions** The partition of an HP server, comprising a group of cells (containing CPUs and memory) and I/O chassis (containing I/O systems)
- **Authorized iCAP Cells**
- **Unlicensed iCAP Cells**
- **Authorized iCAP Processors**
- **Unlicensed/iCOD Processors**
- **DIMMs** The DIMM memory chips installed
- **Licensed Memory (GB)**
- **Unlicensed/iCOD Memory (GB)**
- **Chassis**
- **I/O Cards**
- **iCOD**
- **iCOD Balance**

For a Complex Not Participating in iCOD:

- **Computer Cabinets**
- **I/O Cabinets**
- **nPartitions**
- **Cells**
- **CPUs**
- **DIMMs**
- **Memory (GB)**
- **I/O Chassis**
- **I/O Cards**
- **iCOD**

Related topics

- [System Page](#)
- [System tab](#)
- [System tab for partitions](#)

System tab for partitions

The **System Page** for a partition follows the same layout as a server **System Page**. However, it is extended to include unique information that applies to partitions only.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

The following sections include only the unique information for a partition. See “[System tab](#)” for additional information about the tab.

Identification

The **Identification** section is expanded whenever you access the **System Page** for the first time. The items available under this section include:

- **nPartition Name**
- **nPartition Number**
- **Host Name**

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

- **CPU Architecture**
- **Cell Compatibility**
- **Firmware Revision**
- **Primary Boot Path**
- **HA Alternate Boot Path**
- **Alternate Boot Path**

Summary of Components

- **Active Cells**
- **Inactive Cells**
- **Active Processors**
- **Inactive Processors**
- **Number of Licensed Processors**
(Only available for partitions that participate in Instant Capacity.)
- **DIMMs**
- **Memory (GB)**
- **I/O Chassis**
- **I/O Cards**

Associations

▲ **Complex Name**

Related topics

- [System Page](#)
- [System tab](#)
- [System tab for a complex](#)

System tab for a storage host

A storage host is a server, desktop, or workstation that is connected by a host bus adapter (HBA) to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a storage host is selected. Included here are the areas that are unique to storage hosts. HP Systems Insight Manager (HP SIM) displays data supplied by each HBA's *SMI-S provider*. If an HBA's SMI-S provider

does not supply data for a particular property, the property does not appear on this page. See “System tab” for additional information about the tab.

The Host Bus Adapters section shows the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. See “Data collection” for additional information about data collection tasks.

If this host is managed by HP Storage Essentials, the **Host Bus Adapters** and **LUNs** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage host.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Product Description



NOTE: This section can be expanded by clicking or collapsed by clicking .

In addition to the Product Description information on the “System tab”, this section can include:

System Subtype Storage systems use the following subtypes:

- **Storage.** A system that is identified as part of the storage infrastructure
 - **SMI.** A system that was discovered through an *SMI-S provider*
 - **Storage Essentials Managed.** A system that is managed by HP Storage Essentials
-



NOTE: If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

Host Bus Adapters



NOTE: This section can be expanded by clicking or collapsed by clicking .

This section lists the installed Fibre Channel HBAs.

- **Element Name** The name of the HBA.
 - **WWN** The node world wide name of the HBA.
 - **Status** The HBA's WBEM operational status. See “WBEM operational status types” for additional information about WBEM status.
-



NOTE: Click to view HBA property and port information.

Properties





NOTE: This section can be expanded or collapsed by clicking and .

- **Product Name** The product name for the HBA (for example, a model number)
- **Product Vendor** The HBA vendor
- **Product Identifying Number** A unique identifier for the HBA (for example, a serial number)
- **Product Version** The HBA product version
- **Driver Version** The installed HBA driver version
- **Driver Manufacturer** The manufacturer of the HBA driver

- **Firmware Version** The installed HBA firmware version
- **Firmware Manufacturer** The HBA firmware manufacturer
- **BIOS/FCode Version** The installed BIOS/FCode version
- **BIOS/FCode Manufacturer** The BIOS/FCode manufacturer

Ports




NOTE: This section can be expanded by clicking  or collapsed by clicking .

- **Element Name** The port number.
- **WWN** The port's World Wide Name.
- **Port Type** The port type (see "Port types" for additional information.)
- **Status** The port's WBEM operational status (see "WBEM operational status types" for additional information about WBEM status.)

LUNs



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section lists the LUNs in use by the host.

- **LUN Name** The name of a LUN in use by the selected host.
- **LUN Number** The number by which the LUN (as seen through this port) is known to the storage host.
- **Storage Device** The name of the storage device that contains the listed LUN. Click the storage device name to view the storage device **System Page**.

A link from a LUN to a storage device appears in this column only if the LUN is reported by the *SMI-S provider* of the storage array on which the LUN resides and with the same Name property used by the HBA's SMI-S provider. If these conditions are not met but the HBA's SMI-S provider reports the LUN, the LUN's storage device is listed as **Unknown**.

- **HBA Name** The name of the HBA that connects the host to the LUN.
- **Port WWN** The port number through which the host connects to the LUN.
- **LUN Size** The usable size of the LUN.
- **RAID Level** The LUN's RAID level. RAID level information is available only if a LUN is matched up to a volume on a storage device. See "System tab for a storage array" in the **Storage Volumes** section for additional information about RAID levels.

Related topics

- System Page
- System tab
- Port types
- Data collection

System tab for a storage switch

A storage switch is a Fibre Channel switch that is connected to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a storage switch is selected. Included here are the areas that are unique to storage switches. HP SIM displays data supplied by the switch's *SMI-S provider*. If the SMI-S provider does not supply data for a particular property, the property does not appear on this page. See "System tab" for additional information about the tab.



The Ports and Status Summary sections show the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. See “Data collection” for additional information about data collection tasks.

If this switch is managed by HP Storage Essentials, the **Ports** and **Status Summary** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage switch.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

In addition to the Product Description information on the “System tab”, this section includes the following information:

- **System Subtype** Storage systems use the following subtypes:
 - **Storage.** A system that is identified as part of the storage infrastructure
 - **SMI.** A system that was discovered through an *SMI-S provider*
 - **Storage Essentials Managed.** A system that is managed by HP Storage Essentials
-



NOTE: If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

- **Product Name** The product name for the switch (for example, a model number)
- **Product Vendor** The switch vendor
- **Product Identifying Number** A unique identifier for the switch (for example, a serial number)
- **Product Version** The switch product version
- **Firmware Version** The installed firmware version
- **Firmware Manufacturer** The firmware manufacturer
- **BIOS/FCODE Version** The installed BIOS/FCODE version
- **BIOS/FCODE Manufacturer** The BIOS/FCODE manufacturer
- **Management Proxies** The servers that manage the switch through a *management protocol* such as WBEM
- **Software Version** The version of the software installed on this system
- **Software Manufacturer** The manufacturer of the software installed on this system



NOTE: Some vendors enter firmware details in the **Software Version** and **Software Manufacturer** fields instead of the **Firmware Version** and **Firmware Manufacturer** fields. These fields might display data about any software related to the system.

Ports



NOTE: This section can be expanded by clicking  or collapsed by clicking .

- **Port Number** The port number
- **WWN** The port's World Wide Name
- **Port Type** The port type (see "Port types" for additional information about port types.)
- **Status** The port's WBEM operational status (see "WBEM operational status types" for additional information about WBEM status.)

Status Summary



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section summarizes the status information in the Ports section.

- **Status** The WBEM operational status (see "WBEM operational status types" for additional information about WBEM status.)
- **Count** The number of ports with the listed status

Related topics

- [System Page](#)
- [System tab](#)
- [WBEM operational status types](#)
- [Port types](#)
- [Data collection](#)

System tab for a storage array

A storage array is a disk array that uses a Fibre Channel controller to connect to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a storage array is selected. Included here are the areas that are unique to storage arrays. HP SIM displays data supplied by the array's *SMI-S provider*. If the SMI-S provider does not supply data for a particular property, the property does not appear on this page. See "System tab" for additional information about the tab.

The Ports, Storage Volumes, and Capacity Information sections show the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. See "Data collection" for additional information about data collection tasks.

If this storage array is managed by HP Storage Essentials, the **Ports**, **Storage Volumes**, and **Capacity Information** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this storage array.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Product Description



NOTE: This section can be expanded by clicking or collapsed by clicking .

In addition to the Product Description information in “System tab”, this section can include the following information:

- **System Subtype** Storage systems use the following subtypes:
 - **Storage.** A system that is identified as part of the storage infrastructure
 - **SMI.** A system that was discovered through an *SMI-S provider*
 - **Storage Essentials Managed.** A system that is managed by HP Storage Essentials
-



NOTE: If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype.

- **Product Name** The product name for the array, for example, a model number
 - **Product Vendor** The storage array vendor
 - **Product Identifying Number** A unique identifier for the storage array (for example, a serial number)
 - **Product Version** The array product version
 - **Firmware Version** The installed firmware version
 - **Firmware Manufacturer** The firmware manufacturer
 - **BIOS/FCode Version** The installed BIOS/FCode version
 - **BIOS/FCode Manufacturer** The BIOS/FCode manufacturer
 - **Management Proxies** The servers that manage the selected array through a *management protocol*, such as WBEM
 - **Software Version** The version of the software installed on this system
 - **Software Manufacturer** The manufacturer of the software installed on this system
-



NOTE: Some vendors enter firmware details in the **Software Version** and **Software Manufacturer** fields instead of the **Firmware Version** and **Firmware Manufacturer** fields. These fields might display data about any software related to the system.

NOTE: If this storage array is managed by HP Storage Essentials, data is not displayed for the **Product Name**, **Product Vendor**, **Product Identifying Number**, and **Product Version**.

Ports



NOTE: This section can be expanded by clicking or collapsed by clicking .

If HP Systems Insight Manager (HP SIM) has discovered controllers that manage this array's ports, they are displayed as expandable elements in the **Ports** table. If no controllers were discovered, the table lists only port details.

Controller Details

- **Element Name** The name of the controller
- **LUN Count** The number of connections made through this controller
- **Status** The controller's WBEM operational status (see “WBEM operational status types” for additional information about WBEM status.)



NOTE: Click  to view specific port details.

Port Details

- **Element Name** The port name
- **WWN** The port's World Wide Name
- **Port Type** The port type (see "Port types" for additional information about port types.)
- **LUN Count** The number of connections made through this port
- **Status** The port's WBEM operational status (see "WBEM operational status types" for additional information about WBEM status.)

Storage Volumes



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section lists the array's storage volumes. Storage volumes are logical volumes on an array (for example, LUNs).


- **Volume Name** The storage volume name.
- **Visible to Host(s)** The storage volume is accessible to the listed hosts.
- **Block Size** The storage volume's block size in bytes.
- **Number of Blocks** The total number of blocks on the storage volume.
- **Total Size** The storage volume's total size.
- **RAID Level** The RAID level of the storage volume. Typically, this value is supplied by the array's SMI-S provider. If the SMI-S provider does not supply a value, HP Systems Insight Manager calculates the RAID level based on the values for Package Redundancy and Data Redundancy as follows:

Package redundancy	Data redundancy	RAID level
0	1	RAID 0
1	1	RAID 5
1	2	RAID 1
2	1	RAID 6
2	2	RAID 15/51

If the RAID value is calculated by HP Systems Insight Manager, an asterisk is added to the RAID value (for example **RAID 5***).

Capacity Information



NOTE: This section can be expanded by clicking  or collapsed by clicking .

The Capacity Information table lists the available capacity metrics for storage arrays in the **Metric** column and the corresponding disk space value in the **Size** column. For each metric, the disk space value is expressed as a percentage of the array's total capacity. The metrics in the **Capacity Information** table are also displayed as percentages in a pie chart below the table. If any value in the table shows an **Undetermined** value, the pie chart is not displayed.

HP SIM discovers external LUs (a feature of External Storage XP) on XP arrays that are managed by Command View XP Advanced Edition. When an XP array has external LUs, the **Total Capacity** value is higher than the total capacity of all of the disks in that XP array because it includes the capacity from the external LUs.

- ▲ **Total Capacity** This is the total capacity of the array and it can be used in the following ways:
- **Raw** Space that is not configured for a specific purpose.
 - **Assigned** Space that is assigned to pools of storage that can be configured into storage volumes (LUNs).
 - **Allocated** Space configured as storage volumes, but not connected through a port. Applications cannot access this space until it is assigned to a port.
 - **Exposed** Space configured as storage volumes that is connected through one or more ports. Applications can access this space.
 - **RAID Overhead** Space on the array that is not directly usable because it is being used to provide redundancy. For example, if 100 GB is allocated for a RAID 1 (mirrored) storage volume, 50 GB are directly usable (Allocated or Exposed), and 50 GB is RAID Overhead to provide the mirrored copy of the data.
 - **Other** Space that is not accounted for by the previously listed categories. Other space is typically space that is required for metadata.

Related topics

- [System Page](#)
- [System tab](#)
- [Port types](#)
- [Data collection](#)

System tab for a tape library

A tape library is a tape drive that is connected to a storage area network (SAN). Additional links are available on the **System Page** to access detailed information when a tape library is selected. Included here are the areas that are unique to tape libraries. HP SIM displays data supplied by the tape library's *SMI-S provider*. If the SMI-S provider does not supply data for a particular property, the property does not appear on this page. See "System tab" for additional information about the tab.



The Ports, Media Access Devices, and Changer Devices sections show the date, time, and duration of the last data collection task. If you want to update the data, click the **Last Update** link, and schedule or run a Data Collection task. See "Data collection" for additional information about data collection tasks.

If this tape library is managed by HP Storage Essentials, the **Ports**, **Media Access Devices**, and **Changer Devices** sections do not appear on this page, and an **SE System Properties** link appears in the **Storage Essentials Pages** section on the **Tools & Links** tab. Click the **SE System Properties** link to view the Storage Essentials device page for this tape library.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

Product Description



NOTE: This section can be expanded by clicking  or collapsed by clicking .

In addition to the Product Description information on the "System tab", this section includes the following information:

- **System Subtype** Storage systems use the following subtypes:

- **Storage.** A system that is identified as part of the storage infrastructure
- **SMI.** A system that was discovered through an *SMI-S provider*
- **Storage Essentials Managed.** A system that is managed by HP Storage Essentials



NOTE: If a system is managed by HP Storage Essentials, it does not show the **SMI** subtype

- **Product Name** The product name for the tape library (for example, a model number)
- **Product Vendor** The tape library vendor
- **Product Identifying Number** A unique identifier for the tape library (for example, a serial number)
- **Product Version** The tape library product version
- **Firmware Version** The installed firmware version
- **Firmware Manufacturer** The firmware manufacturer
- **BIOS/FCode Version** The installed BIOS/FCode version
- **BIOS/FCode Manufacturer** The BIOS/FCode manufacturer
- **Management Proxies** The servers that manage the selected tape library through a *management protocol*, such as WBEM
- **Software Version** The version of the software installed on this system
- **Software Manufacturer** The manufacturer of the software installed on this system



NOTE: Some vendors enter firmware details in the **Software Version** and **Software Manufacturer** fields instead of the **Firmware Version** and **Firmware Manufacturer** fields. These fields might display data about any software related to the system.

Ports





NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section lists the tape library's Fibre Channel ports.

- **Element Name** A user-friendly name for the port.
- **WWN** The port's World Wide Name.
- **Port Type** The port type. See "Port types" for additional information about port types.
- **Status** The port's WBEM operational status. See "WBEM operational status types" for additional information about WBEM status.

Media Access Devices




NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section lists the following information about the tape library's storage media (for example, data cartridges or disk drives):

- **Name** The name of the storage media.
- **Status** The media access device's WBEM operational status. See "WBEM operational status types" for additional information about WBEM status.
- **Firmware Version** The installed firmware version.

Changer Devices



NOTE: This section can be expanded by clicking  or collapsed by clicking .

This section lists the tape library's changer devices, for example, the tape drive robotics.

- **Name** The name of the changer device.
- **Status** The changer device's WBEM operational status. See “WBEM operational status types” for additional information about WBEM status.
- **Firmware Version** The installed firmware version.

Related topics

- System Page
- System tab
- WBEM operational status types
- Port types
- Data collection

Port types

HP Systems Insight Manager (HP SIM) displays port types for storage systems. If the values are supplied by a storage system's *SML-S provider*, the port link technology and port type are displayed.

The possible port link technologies are **Unknown, Other, Ethernet, IB, FC, FDDI, ATM, Token Ring, Frame Relay, Infrared, BlueTooth, and Wireless LAN.**

The port type is displayed if it is one of the following:

- **N-Port.** A node port
- **NL-Port.** A node port that supports Fibre Channel arbitrated loop (FC-AL)
- **E-Port** An expansion port that connects fabric elements (for example, Fibre Channel switches)
- **F-Port.** A fabric (element) port
- **FL-Port.** A fabric (element) port that supports FC-AL.
- **B-Port.** A bridge
- **G-Port.** A generic port
- **Other.** Any port type that does not fit the previously described categories

Related topics

- System tab for a tape library
- System tab for a storage switch
- System tab for a storage host
- System tab for a storage array

Tools & Links tab

The system links that you can view depend on the *Discovery* configuration, the correct installation of agents and protocols, and the polling tasks that interrogate the *system*. The **Tools & Links** tab includes:

- System Management Pages
- System Web Application Pages
- HP Systems Insight Manager Pages
- Storage Essentials Pages



NOTE: In some cases, depending on the DNS configurations, you might need to use the IP address or a Fully Qualified DNS name to make the links work appropriately. See “Configuring the system link” for more information.

The **Quick Launch** link provides instant access to a short list of frequently used tools. Place your cursor over the link to expand the menu and view the tools available for the systems that are currently displayed. Selecting a tool from this list bypasses the target verification page of the Task Wizard, regardless of the Task Wizard settings. Tools launched with this menu cannot be scheduled. The menu can be customized by clicking the **Customize** link in the **Quick Launch** menu.

System Management Pages

This section includes links that are provided by the HTTP Web Management on the system. These links are for system management and status. If the system does not have Insight Management Agent, this section is not displayed. Some of the available links include the following:

- **HP Version Control Agent**
- **HP Version Control Repository Manager**
- **HP Insight Management Agent**

System Web Application Pages

This section includes a list of web applications hosted by the system. Some of the available links include:

- **VMware Management Interface**
- **Default Web Server**
- **HP SIM**

HP Systems Insight Manager Pages

This section contains links that are generated by HP Systems Insight Manager (HP SIM). Some of the available links include:

- The **Data Collection Report** link displays the data collection report for the system in a separate report results window.



NOTE: The storage tables in HP SIM's Data Collection reports are not populated with data because HP SIM's SMI-S data collection is disabled.

NOTE: The Data Collection report is not available for clusters.

- The **System Protocol Settings** link points to the **Protocol Settings**, where you can set the protocol settings for this individual system only.
- The **Edit System Properties** link enables users with *administrative rights* to reconfigure some of the system properties for a single system through its system page. This link is not available if you do not have administrative rights.

See “Editing system properties for multiple systems” for information about setting system properties for multiple systems.

- The **Suspend/Resume Monitoring** link enables you to set the timer for suspending monitoring, which enables a system to be excluded from the status polling, identification, data collection, and the automatic event handling features of HP SIM. The available suspend lengths include the predetermined increments of 5 minutes, 15 minutes, 1 hour, and 1 day. The suspend feature can be turned on indefinitely. This link is only available to users with administrative rights.

See “Suspending or resuming system monitoring for multiple systems” for information about suspending or resuming monitoring for multiple systems.

Storage Essentials Pages

This section is added when HP Storage Essentials is installed. See your HP Storage Essentials documentation for details about the links that are added.

Related procedures

- Editing system properties for a single system
- Suspending or resuming system monitoring for a single system
- Editing system properties for multiple systems
- Suspending or resuming system monitoring for multiple systems

Related topics

- System Page
- Editing system properties for a single system
- Suspending or resuming system monitoring for a single system

Essentials tab

The **Essentials** tab is available on the **System Page** of systems that might support other HP Systems Insight Manager (HP SIM) partner applications. This tab provides a description of the available software and a link to the HP web site where you can get further details. Only *administrative rights* and *operator rights* users can view the Essentials tab.

When new information is available on the **Essentials** tab, the tab is highlighted with an Informational icon: ⓘ. After you view the **Essentials** tab, the icon is removed until new information is available.

Related topics

- System Page
- Partner applications

Version Control

The *HP Version Control Repository Manager (VCRM)* and *HP Version Control Agent (VCA)* are web-enabled HP Insight Management Agents. HP Systems Insight Manager (HP SIM) uses these Insight Management Agent and others to facilitate Software Update and tasks related to it.

In general, HP Insight Management Agents 4.0 and later are web enabled, and they provide in-depth subsystem status and fault information on servers, workstations, desktops, and notebooks, communicating directly with HP SIM when they are launched. Web-enabled agents are accessible directly through a browser or through HP SIM.

HP SIM provides the following version control tools:

- **Install Software and Firmware.** Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install Software and Firmware**.
- **Initial HP ProLiant Support Pack Install.** Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Initial HP ProLiant Support Pack Install**.

Related procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install
- Installing ROM firmware updates
- HP Version Control Agent reports

Related topics

- Creating a Replicate Agent Settings task
- About the Version Control Agent
- About the Version Control Repository Manager

- About integration
- About multiple system management
- About software repositories

About the Version Control Agent

The *HP Version Control Agent (VCA)* is an *HP Insight Management Agent* that is installed on a system to enable you to view the HP software and firmware that is installed on that system. The VCA can be configured to point to a *repository* being managed by the *HP Version Control Repository Manager (VCRM)*, enabling easy version comparison and software updates from the repository to the system on which the VCA is installed.

The VCA provides *version control* and system update capabilities for a single HP system. The VCA determines system software status by comparing each *component* installed on the local system with the set of individual components or a specified ProLiant or Integrity Support Pack listed in the VCRM. While browsing to the VCA, you can update individual components or an entire ProLiant or Integrity Support Pack by clicking the install icon located next to the system software status icon.

The VCRM and the VCA are integrated with the *System Management Homepage (SMH)*, which is the standard single-server management tool in the HP Foundation Pack. HP Systems Insight Manager (HP SIM), also part of the HP Foundation Pack, uses the VCRM and VCA to facilitate software versioning, update, and tasks related to it.

The VCA is available for Windows and Linux operating systems. The VCA is an integrated part of the System Management Homepage that is designed to display the *available software* inventory of the system on which it is installed. The VCA also allows the installation, comparison, and update of system software from a repository that is managed by the VCRM.

Users with administrator or operator privileges can access the VCA to maintain the *software inventory* of the system manually. The installation of components and configuration activities are logged to a log file at the system. The *VCA logs* activities, such as software installations. However, installations done outside the VCA do not appear in this log.

The VCA enables you to view the software installed on selected HP equipment, the available updates, and whether the installed software is compliant with the latest updates found in the selected repository. In addition, you can add or update HP software on the system remotely, using the browser interface of the VCA.

You can use the *Replicate Agent Settings* feature in HP SIM to update multiple servers with VCA settings. See “*Windows CMS*” for more information regarding the **Replicate Agent Settings** feature.

The VCA allows the following tasks:

- Viewing the currently installed software
- Selecting an VCRM as a reference point for obtaining software updates
- Selecting a ProLiant or Integrity Support Pack as a managed baseline
- Viewing the details associated with a ProLiant or Integrity Support Pack or individual software component that is in the version control repository
- Installing a ProLiant or Integrity Support Pack or individual software component from the version control repository
- Printing the installed software inventory and software status
- Managing the VCA log

In addition to maintaining the software inventory of the system, the VCA integrates with HP SIM. This integration enables administrators to take advantage of the Software Update capabilities of the agent.

Additional resources

For additional resources, go to <http://www.hp.com/servers/manage>.

Related procedures

- Installing Software and Firmware
- Installing ROM firmware updates

- Initial ProLiant Support Pack Install
- HP Version Control Agent reports

Related topics

- Version Control
- About integration
- About multiple system management
- About software repositories

About the Version Control Repository Manager

The *HP Version Control Repository Manager* (VCRM) is an HP Insight Management Agent that manages a directory of HP software and firmware components. The VCRM can be used without the *HP Version Control Agent* (VCA) to provide a listing of available software and firmware to load on the local machine. The VCRM is part of the HP Foundation Pack.

The VCRM is designed to be used in a one-to-many configuration with a VCA installed on each managed HP system to manage installed HP software and firmware. In conjunction with HP Systems Insight Manager (HP SIM), the VCRM, and VCAs provide enterprise-wide management of HP software and firmware on HP ProLiant and Integrity systems. Alone, the VCRM can be used to catalog and manage a repository of ProLiant and Integrity Support Packs and individual software and firmware from HP for HP ProLiant and Integrity systems.



NOTE: Although it is possible to install an *HP ProLiant and Integrity Support Pack* or *component* to the local machine using the VCRM, you cannot install the software on remote servers unless the VCA has been installed on the remote server and the install is initiated using the VCA.

The VCRM permits the following tasks:

- Viewing the contents of the repository, such as HP ProLiant Support Packs or component details
- Configuring Automatic Update to proactively deliver new ProLiant software from HP as it is made available
- Uploading a support pack to the repository from a CD or other accessible media using the **Upload a Support Pack** feature
- Creating HP ProLiant and HP Integrity Support Packs
- Deleting HP ProLiant and HP Integrity Support Packs and components
- Copying HP ProLiant and HP Integrity Support Packs and components to another repository
- Configuring components in the repository that are flagged as requiring configuration
- Updating from HP.com now
- Rescanning the repository and rebuilding the catalog
- Managing the log
- Installing selected components at the local (browser client) system

Additional resources

For additional resources, go to <http://www.hp.com/servers/manage>.

Related procedures

- Installing Software and Firmware
- Installing ROM firmware updates
- Initial ProLiant Support Pack Install
- HP Version Control Agent reports

Related topics

- [Version Control](#)
- [About integration](#)
- [About multiple system management](#)
- [About software repositories](#)

About integration

For software versioning and updating, HP Systems Insight Manager (HP SIM) relies on the VCRM and the VCA. By using these applications, HP SIM provides a single view of the software status for all managed ProLiant or Integrity servers, plus the capability to update software and firmware on those servers through its powerful query and task features. Updates can be scheduled and applied to specific sets of servers based on predetermined criteria, including applying updates only to those systems that require an update.

To take full advantage of the software update capabilities of HP SIM, ensure that the following conditions are met:

- Every managed target server on the network has the VCA installed and is configured to use a repository.
- Every repository that is to be used has the VCRM installed.
- You can optionally use the automatic update feature of the VCRM to update all repositories with the latest software from HP automatically.

Related procedures

- [Installing Software and Firmware](#)
- [Installing ROM firmware updates](#)
- [Initial ProLiant Support Pack Install](#)
- [HP Version Control Agent reports](#)

Related topics

- [Version Control](#)
- [About the Version Control Agent](#)
- [About the Version Control Repository Manager](#)

About software repositories

The practice of updating HP ProLiant Support Packs and components using VCRM from a single or multiple repositories saves time and is key to standardizing software maintenance and update procedures on distributed *systems*.

For maximum manageability and flexibility across operating system platforms, each repository that is created should conform to the following conditions:

- Located on a local drive with write access
- Updated automatically by the VCRM
- Managed by VCRM.

When a repository has been created, the repository must be populated with HP ProLiant Support Packs and components before being updated on the target HP systems. Although it is optional, the easiest and most efficient way to update a repository is by using the Automatic Update feature of the VCRM. The Automatic Update feature of the VCRM enables you to schedule an automatic population of the repository. However, the repository can be updated in any, or combination of any, of the following ways:

- The Automatic Update feature of the VCRM
- The Upload HP ProLiant Support Pack feature of the VCRM, which enables users to easily copy HP ProLiant Support Packs from a SmartStart CD or other accessible media
- Manually downloading the software into the repository from <http://www.hp.com>

Related procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install
- HP Version Control Agent reports

Related topics

- Version Control
- About integration
- About the Version Control Agent
- About the Version Control Repository Manager

About multiple system management

The Software Update capabilities of HP Systems Insight Manager (HP SIM) includes the following features:

- **Initial HP ProLiant Support Pack Install.** This feature enables you to install the latest desired HP ProLiant Support Pack from the specified VCRM. It is for use only on target systems **not** running the HP Version Control Agent. This feature is only available on Windows systems. If the VCA is already installed on managed systems, you can use the Install Software and Firmware task to update.
- **Install Software and Firmware.** This feature enables you to automatically update HP ProLiant Support Packs and components on HP systems managed by HP SIM. The target systems must have the VCA installed.
- **Searching by systems with Software/Firmware.** This search criterion enables you to quickly create and display a list of systems with specific software or firmware versions. For example, a user with *administrative rights* might want to locate and display all HP systems with HP Insight Management Agent earlier than a defined version. The search can then be used with the Install Software and Firmware Task to update the systems to the current version of Insight Management Agent.
- **Software Version Status Polling.** Software and firmware upgrade statuses are retrieved from the VCA on target systems. Software and firmware inventories are also retrieved from those systems during this task.
- **Replicate Agent Settings.** This feature allows HP SIM to retrieve Web Agent configuration settings from a source device and distribute that configuration to one or more target devices through their Web Agents.

All of these system software management enhancements rely on the tight integration of HP SIM with the HP Version Control Repository Manager and the HP Version Control Agent.

Related procedures

- Installing Software and Firmware
- Initial ProLiant Support Pack Install
- HP Version Control Agent reports

Related topics

- Version Control
- About integration
- About software repositories
- Replicating trusted certificates

Accessing the Version Control Agent

Access the *HP Version Control Agent* (VCA) GUI from any network client using a web browser. For information about which browsers are supported, see the *HP Version Control Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.



IMPORTANT: If an *HP Version Control Repository Manager* (VCRM) has not been configured, only the Software and Firmware Inventory of items currently installed on the system are displayed on the **Home** page. The VCA settings must be configured for full functionality.

IMPORTANT: For Windows operating systems, you must install the *HP Insight Management Agent 5.40* or later to obtain any inventory data. For Linux operating systems, you must install HP Server Management Application and Agents (hpsasm RPM) 7.00 or later to obtain any inventory data. HP recommends installing the current version that is in the same *HP ProLiant and Integrity Support Pack* as the VCA.



IMPORTANT: For Windows operating systems, you must install the *HP Insight Management Agent 5.40* or later to obtain any inventory data. For Linux operating systems, you must install HP Server Management Application and Agents (hpsasm RPM) 7.00 or later to obtain any inventory data. HP recommends installing the current version that is in the same *HP ProLiant and Integrity Support Pack* as the VCA.



NOTE: If the Insight Management Agents are not installed, *software inventory* cannot be collected by the VCA. However, the VCA can still be used to install software.

NOTE: Login accounts that have Administrator or Operator privileges defined in the System Management Homepage can access all features of the VCA.

Logging in to the VCA

To access the VCA with access to all available features, you must log in to the System Management Homepage with **administrator** or **operator** level access. To log in to the VCA:

1. Navigate to `https://hostname:2381`. The **Login** page appears if **Anonymous Access** is disabled. If **Anonymous Access** is enabled, the **System Management Homepage** page appears.
2. After you have logged in, you can browse directly to the VCA by entering `https://hostname:2381/vcagent` in the browser address field, or you can open it in a new browser window by clicking the HP Version Control Agent link from the System Management Homepage under **Integrated Agents** or in the **Version Control** status box on the **Home** tab. The **VCA** page appears.



NOTE: You can also access VCA from the System Management Homepage (SMH).

Related procedure

- Accessing the Version Control Repository Manager
- HP Version Control Agent reports

Related topics

- System Page
- System Management Homepage

Accessing the Version Control Repository Manager

You can access an HP Version Control Repository Manager through one of the following methods:

- Accessing a VCRM from HP Systems Insight Manager (HP SIM)
- Accessing a VCRM directly

Accessing VCRM from HP SIM

1. Select **Tools**→**System Information**→**System Management Homepage**.
2. Select the target system, and then click **Run Now**. See “Creating a task” for more information. The System Management Homepage appears.
3. From System Management Homepage, perform one of the following actions:
 - Click the **HP Version Control Repository Manager** link. The **VCRM Home** page appears.
 - Select **Tools**, and then click the **HP Version Control Repository Manager** link.

Accessing VCRM In-Place

Navigate to `https://hostname:2381/vcrepository` on the system that has the VCRM installed. The **VCRM Home** page appears.



NOTE: You can also access VCRM from the System Management Homepage (SMH).

Related procedure

- Accessing the Version Control Agent
- HP Version Control Agent reports

Related topics

- System Page
- System Management Homepage

Version Control status icons



NOTE: Click a **Software Status** icon to access the *HP Version Control Agent (VCA)*. If the VCA cannot be accessed, help displays that describes how to configure the VCA or trust relationship on that system.

NOTE: There is a **Software Status** icon for every server except HP-UX.

Version Control status

The status is based on comparing the installed versions against versions in the *repository*.





Icon	Status
	There are different reasons why an Unknown status icon might display: <ul style="list-style-type: none">• The VCA does not have an <i>HP Version Control Repository Manager (VCRM)</i> configured.• The configured VCRM is not reachable or does not respond to HTTP requests (for example, the system or service is down or the password has been changed).• An VCA cannot be detected on the system or cannot communicate with the VCA.

Status values when no Reference Support Pack is set




Note: The status is that of the latest version of the component in the configured repository.

Icon	Status
	This update contains critical bug fixes. HP requires that you apply this update at your earliest convenience.
	The repository contains a version of this component that might contain bug fixes or new hardware support. HP recommends that you review information about this version and apply this update appropriately.
	The installed software versions are the same or newer than the latest versions available at the VCRM.

Status values when a Reference Support Pack is set but the exact match setting is not selected

Icon	Status
	This update contains critical bug fixes. HP requires that you apply this update at your earliest convenience.
	This update might contain bug fixes or new hardware support. HP recommends that you review information about this version and apply this update appropriately.
	The installed software versions are the same or newer than the versions in the Reference Support Pack.
	The <i>Reference Support Pack</i> configured at the VCA is no longer valid at the configured VCRM.

status values when a Reference Support Pack is set and the exact match is selected

Icon	Status
	The installed version does not match the version of the same item in the Reference Support Pack, and the VCA settings specify that an exact match is expected.
	The installed software versions are the same or later than the versions in the Reference Support Pack.
	The Reference Support Pack configured at the VCA is no longer valid at the configured VCRM.

When the *overall software status* indicates that an item is not current, identify the software or firmware items that have available updates, read the item descriptions, and determine whether the update is appropriate for the server.

In the event a repository has been configured and a Reference Support Pack has not, the status is based on a comparison between the installed software or firmware versions and the newest components available from the configured repository.

In the event a repository and Reference Support Pack have been configured, the status is based on a comparison between the installed software or firmware versions and the software or firmware versions in the Reference Support Pack.

Related procedures

- Installing Software and Firmware
- Installing ROM firmware updates
- Initial ProLiant Support Pack Install
- HP Version Control Agent reports

Related topics

- About the Version Control Agent
- About the Version Control Repository Manager

HP Version Control Agent reports

HP Systems Insight Manager (HP SIM) provides a predefined Software and Firmware Baseline Information report. This report is very useful if you want to print the software and firmware baseline information contained in the repository which is reported by the HP Version Control Agent (VCA).

The Software and Firmware Baseline Information report displays information provided by the HP Version Control Agent on Windows and Linux systems. If a system is running HP-UX, the report appears blank since the VCA is not supported on HP-UX systems.

See “Reporting views” for specific details about the fields that are displayed in Software and Firmware Baseline Information report.

To run the Software and Firmware Baseline Information report:

1. Select **Reports**→**New Report**. The **New Report** window appears.
2. Add multiple or single targets:
 1. To add targets, you can choose one of two radio buttons above the drop-down selection box, either the **Collection** option or the **Search** option which is used to indicate the method of target selection or click **Cancel** which will result in no additions.

Note: You are not allowed to select individual events for Targets or Filters, so the ability to search will not be available when those selections are made. The two radio buttons will not be present in these cases.
 2. Choosing the **Collection** option will allow you to select targets from the drop-down selection box.
 3. If you choose the **Search** option, the drop-down selection box and **View Contents** button will be replaced with the **Quick Search** user interface. Type a **Device Name** into the **Text Field** and then click **Search**.

Note: If there are **Device Names** that match the characters typed in the **Text Field**, a dynamic list is displayed with those matches.
 4. If you select one of the **Device Names** displayed in the dynamic list, a **System Table** containing the selected system will be displayed below the **Quick Search** user interface. Items displayed in the **Search Results** table will be selected (checked) by default and the **Apply** button will be enabled as long as there is at least one item from the **Search Results** table selected. Only items that are selected will be added when you click **Apply**.

Note: The maximum number of **Device Names** displayed is six.
 5. If you click **Search**, a **Basic Search** using common attributes will be performed using the characters typed into the **Text Field**. The results will be displayed in the **Search Results** table below the **Quick Search** user interface.

While the search user interface remains open, the **Task Wizard** will retain a reference to the **Query** object created to perform the **Dynamic Query** generation used when performing searches. Each new search term will be added to this **Query** object and a new **Dynamic Query** will be generated. The **Task Wizard** will release its reference to the search **Query** when you close the search user interface or by clicking **Cancel** or **Apply**.

Note: A barbershop pole will be seen while **Basic Search** results are loading.

Once you choose the system to add, the **Select <item> itself** checkbox is checked by default and the **Apply** button and **View Contents** button are enabled. You can choose to click **Apply** or **View Contents**.

To remove a target, select **Remove Targets**.

3. To filter target selections, complete the following.
 - a. Click **Add Event Filter**.
 - b. From the **Add filters by selecting from** dropdown box, select an event filter. If you do not select an event filter, an error message appears.
 - c. Click **Apply** to apply the filter to the target systems (or, click **Cancel** to cancel adding a filter). The **Filtered by** table appears below the list of selected target systems.


Note: If the target selections are events instead of systems, the button changes to **Add System Filter** and you can select from different system collections. Unlike event filters, you can select multiple system filters.

4. To modify an event filter, click **Modify Event Filter**.

Note: If the filters are systems, you will see an **Add System Filters** and **Remove Filters** buttons. If there is only one event filter, the **Remove Filters** button will simply remove the single event filter. If you have more than one event filters, the **Remove Filters** button will open a sub-pane that you may select the event filters to remove.

 - a. From the **Add filters by selecting from** dropdown box., select an event filter. If you do not select an event filter, an error message appears.
 - b. Click **Apply** to change the event filter and apply the filter to the target systems, or click **Cancel** to cancel editing the filter.

Note: If the target selections are events instead of systems, the button does not change to **Modify System Filter** you will have the option to select either the **Add System Filters** or **Remove Filters**. It is possible to have one or more system and event combination collections already selected. If there are combination collections selected, they will provide filtering.
5. To remove a filter, select the filter(s) from the sub-pane that you wish to remove and click **Remove Filters**.
6. Click **Next**.
7. After you click **Next**, the **Step 2: Specify Parameters** page appears.
 - a. In the **Report Name** field, enter a name for the report.

Important: Report names cannot contain any of the following characters: < > ' & \ ` , # + | % ; / \\ ! ~ @ \$ ^ * = { } [] " : and ?
 - b. Click  next to **General** to expand the tree.
 - c. Select **Software Firmware Baseline Information**. The tree displays the items available for the report.

The following fields are available:

 - System Name
 - Description
 - Version
 - Software Firmware Baseline Name
 - Software Firmware Baseline Version
 - Latest Version
 - Configured Repository
 - d. Deselect any of the items that you do not want to include in the report.
8. Click **Run Report**. The report appears.

Related procedures

- System reporting
- Adding a report

Related topics

- Reporting
- Printing reports
- Reporting views

Installing Software and Firmware

To update managed servers with the most current software, HP SIM provides software update capabilities that use the *HP Version Control Agent (VCA)* and *HP Version Control Repository Manager (VCRM)*.


Automated software updates through HP SIM have the following restrictions:


- Updates can be performed only on ProLiant servers that have the VCA installed and trust the HP SIM server. The Install Software and Firmware feature can only be used with third-party systems running the VCA.
Note: See “Trusted certificates” for information regarding trust relationships. After the trust relationship is established, click **Last Update** to update the display to trusted.
- Updates require HP ProLiant Support Pack or components, version 5.3 or later. The Install Software and Firmware feature does not support third-party software.
- Updates are supported on Linux, Windows NT 4.0, Windows 2000, and Windows Server 2003 operating systems.
- Updates cannot be made on the CMS.

To install software and firmware:

1. Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install Software and Firmware**. The **Install Software and Firmware** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**.
4. Under **Select Items to Install**, select the repository from which to retrieve the catalog.

Note: This section only displays *systems* that are authorized by the current *user* name.

5. Under **Contents of selected version control repository**, click the  icon to drill down and view the contents of the Version Control Repository that you selected.

Note: To expand the tree to display all contents, click the  icon located in the upper-left corner of the **Contents of selected Version Control Repository** section. Click the  icon to collapse the listings.

Select the components you want to install.

6. Click **Next**.
The **Select Install Options** section appears. The items are installed in the order in which they are listed.
7. (Optional) To reorder the items, select the item to reorder and perform one of the following actions
 - Click **Move Up** to advance the item up.
 - Click **Move Down** to move the item down.
8. Select **Force downgrade or re-install if necessary** if you are installing software that is earlier than or the same as the version currently installed. This option is disabled by default.
9. Select **Bring systems to full power before install** if you want to bring systems to full power before the installation. If this option is not selected, the installation is attempted and might fail because the system was not running at full power.

Note: The targeted system must support Magic Pocket technology to be brought to full power.

If selected, the target systems are brought to full power before the install is selected.

10. (Optional) Clear the **Reboot systems if necessary after successful install** option if you do not want to reboot after the installation. However, the successful *task* status indicates that a reboot is required to complete the update.
11. Click **Schedule** to configure a time for the update to occur. See “Scheduling a task” for more information about scheduling the task. Click **Previous** to return to the previous screen, or click **Run Now** to immediately install the software.

If you click **Schedule**, the **Schedule Task** section appears.

Firmware deployment to switches

When deploying firmware to switches, verify that the following conditions are met:

- When updating HP switch firmware, only switch devices and a single switch firmware component are selected.
- The switch firmware image version always matches the switch firmware boot image.
- Some older switch components do not generate a log file. However, the switch update status can be found by running the ProLiant Interconnect Switch Upgrade tool. This tool is installed automatically as part of an Install Software/Firmware Task to a switch device.

Related procedures

- [Installing ROM firmware updates](#)
- [Scheduling a task](#)
- [Task results list](#)
- [HP Version Control Agent reports](#)




Related topics

- [Version Control](#)
- [Replicating trusted certificates](#)

Installing ROM firmware updates

HP Systems Insight Manager provides update capabilities that enable you to update managed servers with the most current ROM firmware updates.

To update ROM firmware:

1. From HP SIM, position your cursor in the **Search** field, and enter criteria for the specific models to be ROM flashed. Click **Search**. The systems appear.
Searching for specific models is necessary because different models require different ROM firmware updates.
2. Select the systems to be updated, or you can select the column header to select all of the systems.
3. Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Install Software and Firmware**. The **Install Software and Firmware** page appears.
4. Select the systems to be updated, and then click **Next**.
5. Under **Select Items to Install**, select the HP Version Control Repository Manager(VCRM). The contents of the selected repository appear.
6. Under **Contents of selected version control repository**, click the  icon to drill down and view the contents of the Version Control Repository that you selected.
Note: To expand the tree to display all contents, click the  icon located in the upper-left corner of the **Contents of selected Version Control Repository** section. Click the  icon to collapse the listings.
After drilling down in the repository, select the server, the operating system and the BIOS to be updated. Scroll down the BIOS list and find the matching server type and select the most current BIOS versions. You can select additional items such as the ProLiant and Integrity Support Pack or array firmware if applicable.
7. Click **Next**. The **Select Install Options** section appears. The items are installed in the order in which they are listed.
8. (Optional) To reorder the items, select the item to reorder and perform one of the following actions
 - Click **Move Up** to advance the item up.
 - Click **Move Down** to move the item down.
9. Select **Force downgrade or re-install if necessary** if you are installing software that is older than or the same as the version currently installed. This option is disabled by default.

10. Select **Bring systems to full power before install** if you want to bring systems to full power before the installation. If this option is not selected, the installation is attempted and might fail because the system was not running at full power.
Note: The targeted system must support Magic Pocket technology to be brought to full power. If selected, the target systems are brought to full power before the install is selected.
11. (Optional) Clear the **Reboot systems if necessary after successful install** option if you do not want to reboot after the installation. However, the successful *task* status indicates that a reboot is required to complete the update.
12. Click **Run Now** to update the software. This process may take several seconds. The **Task Results** page appears indicating whether the updates succeeded or failed.

Related procedure

- Installing Software and Firmware
- HP Version Control Agent reports

Related topic

- ▲ Version Control

Initial ProLiant Support Pack Install

The Initial HP ProLiant Support Pack Install task enables you to install an *HP ProLiant Support Pack* from a Windows *Central Management Server* (CMS) to a Windows managed system when you do not have any *HP Insight Management Agents*, especially the *HP Version Control Agent*, installed. This task also configures the *systems* to use the trust *certificate* from HP Systems Insight Manager (HP SIM) and the setting to use the desired *HP Version Control Repository Manager* (VCRM).



NOTE: The Initial HP ProLiant Support Pack Install feature is only supported on Windows Central Management Servers.

The target system must be a Windows system. The Install Software and Firmware feature in HP SIM requires that the HP Version Control Repository Manager (VCRM) be installed and populated on servers containing a repository. Installing the VCRM is not part of this procedure. For more information regarding installing the VCRM, see the *HP Version Control Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

You can use the Configure or Repair Agents task to setup managed systems simultaneously which also installs the VCA from Windows CMSs to Windows managed systems. For more information, see see "Windows CMS".



NOTE: You must have Windows administrator privileges on target systems to install a HP ProLiant Support Pack.

NOTE: The Install Software and Firmware and HP Version Control Agent (VCA) tasks are only available to systems running a properly configured VCA. Running the Initial HP ProLiant Support Pack task enables you to install the VCA quickly and easily.

NOTE: For more information regarding HP ProLiant Support Packs, see the *HP ProLiant Support Pack and Deployment Utilities User Guide* at <http://www.hp.com/servers/psp>.

NOTE: More than one Initial HP ProLiant Support Pack Install tasks cannot be run simultaneously. If you execute a second task before the first one is complete, the second task starts after the first task completes.

To install a HP ProLiant Support Pack:

1. Select **Deploy**→**Deploy Drivers, Firmware and Agents**→**Initial HP ProLiant Support Pack Install**. The **Initial ProLiant Support Pack Install** page appears.
2. Add multiple or single targets:

1. To add targets, you can choose one of two radio buttons above the drop-down selection box, either the **Collection** option or the **Search** option which is used to indicate the method of target selection or click **Cancel** which will result in no additions.

Note: You are not allowed to select individual events for Targets or Filters, so the ability to search will not be available when those selections are made. The two radio buttons will not be present in these cases.

2. Choosing the **Collection** option will allow you to select targets from the drop-down selection box.
3. If you choose the **Search** option, the drop-down selection box and **View Contents** button will be replaced with the **Quick Search** user interface. Type a **Device Name** into the **Text Field** and then click **Search**.

Note: If there are **Device Names** that match the characters typed in the **Text Field**, a dynamic list is displayed with those matches.

4. If you select one of the **Device Names** displayed in the dynamic list, a **System Table** containing the selected system will be displayed below the **Quick Search** user interface. Items displayed in the **Search Results** table will be selected (checked) by default and the **Apply** button will be enabled as long as there is at least one item from the **Search Results** table selected. Only items that are selected will be added when you click **Apply**.

Note: The maximum number of **Device Names** displayed is six.

5. If you click **Search**, a **Basic Search** using common attributes will be performed using the characters typed into the **Text Field**. The results will be displayed in the **Search Results** table below the **Quick Search** user interface.

While the search user interface remains open, the **Task Wizard** will retain a reference to the **Query** object created to perform the **Dynamic Query** generation used when performing searches. Each new search term will be added to this **Query** object and a new **Dynamic Query** will be generated. The **Task Wizard** will release its reference to the search **Query** when you close the search user interface or by clicking **Cancel** or **Apply**.

Note: A barbershop pole will be seen while **Basic Search** results are loading.

Once you choose the system to add, the **Select <item> itself** checkbox is checked by default and the **Apply** button and **View Contents** button are enabled. You can choose to click **Apply** or **View Contents**. To remove a target, select **Remove Targets**.

3. Click **Next**. The **Step 2: Enter Windows credentials** page appears.

Step 3: Enter Windows credentials

This tool allows you to install a Support Pack to systems that are not running the Version Control Agent (VCA). The VCA will be installed as part of this task so that future software and firmware updates can be performed using the Install Software and Firmware tool in the Deploy menu.

Enter credentials that possess local administrative rights on the target system(s). The "Install and initialize SSH (Secure Shell)" option on the next screen will also use these credentials; it is designed to use the local administrator account for access to the system and for running SSH tools. If the local administrator account has been disabled or another account with administrative privileges is used, the account should be specified in the setting `WindowsAdminUserName`. See the white paper *Secure Shell (SSH) in HP Systems Insight Manager 5.0*. The login account used here is for connecting to the system to install the ProLiant Support Pack and OpenSSH, and for setting up the authorization between HP Systems Insight Manager and the managed system. Note that this account must be a direct member of the Administrators group on the manage system; the account will automatically be added to this group if needed.

User name:	<input type="text"/>
Password:	<input type="password"/>
Password (Verify):	<input type="password"/>
Domain:	<input type="text"/>

< Previous

Next >

4. On the **Enter Windows credentials** page:
 - a. In the **User name** field, enter the Windows administrator user name for the target system.
 - b. In the **Password** field, enter the administrator password for the Windows user name entered in step a.
 - c. In the **Password (Verify)** field, reenter the Windows administrator password exactly as it was entered in the **Password** field.
 - d. In the **Domain** field, enter the Windows domain.
Note: This field can be left blank if the system is not part of a domain.
5. Click **Next**. The **Select a Windows Support Pack** page appears.
6. Under **Step 3: Select a Version Control Repository**, select a source repository system from which to retrieve the catalog.

Initial ProLiant Support Pack Install

Targets: hpsim2, hpsim3

Select a Version Control Repository

Last update: Tue, 4/17/2007, 12:59 PM IST

	Name	Status	Product Name	Trusted?
<input type="radio"/>	cn762900fx		ProLiant BL20p G3	no [configure]
<input checked="" type="radio"/>	hpsim1		ProLiant DL380 G4	yes [configure]
<input type="radio"/>	hpsim2		ProLiant DL380 G4	yes [configure]
<input type="radio"/>	hpsim3		ProLiant DL380 G4	yes [configure]

Select a Support Pack to install



System Software Baseline

- Install and initialize SSH (Secure Shell)
- Force downgrade or reinstall the same version
- Reboot systems if necessary after successful install

The following fields display:

- **Name.** This field displays the name of the system.
- **Status.** This field displays the status of the system.
- **Product Name.** This field displays the name of the product.
- **Trusted?.** This field indicates whether the system trust relationship has been configured. To configure a trust relationship, click **configure**. See "Trusted certificates" for more information.

Note: This section displays systems that are authorized by the current user name. If the current user is not authorized to view the systems, a message appears, indicating that the user does not have authorization rights on the system.

7. Under **Select a Support Pack to Install**, select a support pack to install. Click the icon to drill down and view the contents of the Version Control Repository that you selected.
Note: To expand the **System Software Baseline** to display all contents, click the icon located in the upper-left corner of the **Select a Support Pack to Install** section. Click the icon to collapse the listings.
8. (Optional) Select **Install and initialize SSH (Secure Shell)** if you want to install and configure OpenSSH on the target systems. This option is disabled by default. See "Installing OpenSSH" and the *Secure Shell (SSH) in HP Systems Insight Manager white paper* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more detailed information on SSH and the features in HP SIM that use SSH.
9. (Optional) Select **Force downgrade or re-install the same version** if you are installing an HP ProLiant Support Pack that is earlier than or the same as the version currently installed. This option is disabled by default.
10. (Optional) If you do not want to reboot after the installation, clear the **Reboot systems if necessary after successful install** option, which is selected by default. However, the system must be rebooted for the new HP ProLiant Support Pack to be available.
11. Click **Next**. The **Configure Support Pack** page appears.
 - The following options display:
 - Click **Configure System Management Homepage** to set up the Support Pack to establish a trust relationship with System Management Homepage when it is installed on target systems.

The **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page appears.

Note: If the Support Pack has already been configured, you can omit this step.

Note: See “Trusted certificates” for more information about setting up a trust relationship. After the trust relationship is established, click **Last Update** to update the status to trusted.

To configure the System Management Homepage:

- a. From the **Welcome to the Configuration Wizard for the HP System Management Homepage Component** page, click **Next**. The **Operating Systems Groups** page appears.
- b. In the **Group Name** field, enter the name of an operating system group that you want to assign (for example, `vcadmin`).
- c. In the **Operating Level** field, select the appropriate level for the new group from the dropdown list.

Note: The default **Administrators Groups** always have administrative access.

- d. Click **Add** to assign the group. The new group appears under the operating system group to which it was assigned.

Note: You can add up to five entries per operating system group.

- e. Click **Next**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
- f. Select one of the following options:
 - **Anonymous Access** Anonymous Access is disabled by default. Enabling **Anonymous Access** enables a user to access the *System Management Homepage* (SMH) without logging in. Select this option to allow anonymous access.
Caution: HP does not recommend the use of anonymous access.
 - **Local Access** Local Access is disabled by default. Enabling Local Access enables a user to locally gain access to the System Management Homepage without being challenged for authentication, which means that any user with access to the local console is granted full access if **Administrator** is selected. If **Anonymous** is selected, any local user has access limited to unsecured pages without being challenged for a user name and password.
Caution: HP does not recommend the use of local access unless your management server software enables it.
- g. Click **Next**. You can click **Save** to save your changes up to this point, or click **Cancel** to discard the changes and close the wizard.
- h. Select one of the following Trust Mode security options:
 - **Trust by Certificate** Sets the *System Management Homepage* (SMH) to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security because it requires certificate data and verifies the digital signature before allowing access. If you do not want to enable any remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by avoiding importing any certificates.



NOTE: HP strongly recommends using this option because it is more secure.

To trust by certificate:

1. Select **Trust by Certificate**, and then click **Next**.
2. In the **Certificate Name** field, click **Browse** to select the certificate file. After the certificate file is selected, the certificate data appears on the screen.

3. Click **Add**. The certificate appears under **Certificate Files**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- **Trust by Name** Sets the System Management Homepage to accept certain configuration changes only from servers with the HP SIM names designated in the **Trust By Name** field. The **Trust By Name** option is easy to configure. For example, you might use the **Trust By Name** option if you have a secure network with two separate groups of administrators in two separate divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server name submitted.



NOTE: HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

The server name option must meet the following criteria:

- Each server name must be less than 64 characters.
- The overall length of the server name list is 1,024 characters.
- Special characters must not be included as part of the *server name*: ~ ' ! @ # \$ % ^ & * () + = \ " : ' < > ? , | .
- Semicolons are used to separate *server names*.

To trust by name:

1. Select **Trust by Name**, and then click **Next**.
 2. In the **Trusted Server Name** field, enter the server name to be trusted.
 3. Click **Add**. The trusted system name appears under the **Trusted Servers** list. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
 4. Click **Next**. The **IP Binding** page appears.
- **Trust All** Sets the System Management Homepage to accept certain configuration changes from any system.



NOTE: HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

To trust all servers:

1. Select **Trust All**. You can click **Save** to save your changes up to this point or click **Cancel** to discard the changes and close the wizard.
 2. Click **Next**. The **IP Binding** page appears.
- i. IP Binding specifies from which IP addresses the *System Management Homepage* (SMH) accepts requests and provides control over which nets and subnets requests are processed.

Administrators can configure the System Management Homepage to only bind to addresses specified in the **IP Binding** page. A maximum of five subnet IP addresses and netmasks can be defined.

An IP address on the server is bound if it matches one of the entered IP Binding addresses after the mask is applied.



NOTE: The System Management Homepage always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, then the System Management Homepage is only available to 127.0.0.1. If IP Binding is not enabled, you bind to all addresses.

To configure IP Binding:

1. Select **IP Binding**. The **IP Binding** page appears.
2. Enter the IP address.
3. Enter the netmask.
4. Click **Add**. The IP binding configuration is saved and appears under the **IP Binding List**.
5. Click **Next**. The **IP Restricted Login** page appears.

- j. The IP Restricted Login enables the *System Management Homepage* (SMH) to restrict login access based on the IP address of a system.

You can set address restriction at installation time or by it can be set by administrators from the **IP Restricted Login** page

- If an IP address is excluded, it is excluded even if it is also listed in the included box.
- If there are IP addresses in the inclusion list, then only those IP addresses are allowed login access with the exception of *localhost*.
- If no IP addresses are in the inclusion list, then login access is allowed to any IP addresses not in the exclusion list.

To include or exclude IP addresses:

1. In the **From** field, enter the IP addresses to include or exclude. You can enter an IP address range to be included or excluded by entering a beginning IP address in the **From** field and an ending IP address in the **To** field.
2. From the **Type** field, select **Include** or **Exclude**.
3. Click **Add** to add the IP address or IP address range to the **Inclusion List** or **Exclusion List**.
4. Click **Save**. The **HP System Management Homepage Login** page for the System Management Homepage system appears. For more information about System Management Homepage, see the *System Management Homepage Online Help* at <http://h18013.www1.hp.com/products/servers/management/agents/documentation.html>.

- Click **Configure VCA** to set up the VCA in the selected Support Pack.

Note: If the VCA has already been configured, you can omit this step.

To configure the VCA:

- a. In the **Computer Name** field, enter the name of the system where the VCRM is installed.
- b. In the **Login Account** field, enter the login name used to connect to the VCRM on the system specified.
Note: Use a login account that has administrative privileges, but do not use the login name **Administrator**.
- c. In the **Login Password** field, enter the password associated with the login name specified.
- d. Click **Save** to save your settings. Click **Cancel** to discard your settings and close the **VCA Setup** page.
- e. Click **Next**.

12. Back in HP SIM, click **Next** to start the HP ProLiant Support Pack download. The **Download Support Pack** page appears.

13. After the support pack is downloaded, click **Schedule** to create a scheduled task for the Initial HP ProLiant Support Pack Install to run or click **Run Now** to run the task immediately.

Related procedures

- [Installing Software and Firmware](#)
- [Setting up managed systems](#)

Related topic

- ▲ [About the Version Control Repository Manager](#)

WBEM-based tools

Several Web-Based Enterprise Management (WBEM)-based tools are available in HP Systems Insight Manager (HP SIM), including the following:

- Property pages
- System Fault Management
 - Note:** If System Fault Management is not installed, HP SIM cannot recognize or see WBEM indications.
- WBEM providers

Related topics

- [Property Pages](#)
- [System Fault Management overview](#)
- [WBEM providers overview](#)

Property Pages

The *Web-Based Enterprise Management* (WBEM) name and password pairs entered under **Options**→**Protocol Settings**→**Global Protocol Settings** also control the amount of data displayed on the **Property** pages. If the root name and password pair is not available, many of the properties are omitted because the target system providers require root access. The **Property** pages are used to view WBEM properties on remote target *systems* (HP-UX, HP-UX IPF, Linux Itanium Processor Family (IPF), Linux x86, Windows, and Dec Alpha) and can be accessed in two ways:

- From the **System Page** on the **System** tab, click **Properties**. The **Property** pages display for the target system.
- Select **Tools**→**System Information**→**Properties**. Select the target system and click **Run now**. The **Property** pages display for the target system.

The supported versions for indications on Linux IPF include:

- RHEL4
- RHEL5
- SLES9
- SLES10

Also, the HP ProLiant Support Pack 3.90 or later should be installed on the system.

The **Property** pages open in a new window if launched from the **Systems Page** or from the **Tools** menu. The **Property** pages include three tabs:

- **Identity**. Displays WBEM properties that help describe the target system on the network. These properties can include such physical aspects as location, local time, operating system characteristics, and owner information. The computer system status is based on the status returned from the WBEM Computer System provider.
- **Status**. Displays WBEM properties that help determine the status of the system. At a minimum, you can determine the memory status and process status. Depending on the target system installation of WBEM, you might be able to determine status on all of the major computer subsystems. A status icon for each component appears next to each of the status properties. The computer system status is determined by information collected through the WBEM protocol and the information provided by the Windows Management Instrumentation (WMI) provider. See “[System status types](#)” for more information about the hardware status icons that can be displayed.



NOTE: When you click the FC HBA link on the Property Pages **Status** tab, you will receive an error message. The reason for this, is that even though FC control is not present on the system the FC HBA hot link might be displayed on the **Status** tab. For an FC HBA, HP SIM cannot anticipate if there will

be instances present and might display this link. If there are instances present, the Common Information Model (CIM) Client connection might have timed out.

- **Configuration.** Displays an inventory of the target system based on WBEM properties. At a minimum, this inventory includes operating system information, but it might also include information on CPUs, disk drives, file systems, motherboards, software installations, and networks.
-



NOTE: The date and time displayed on the **Property** pages indicates the time on the target system.

NOTE: OpenWBEM is not supported.

System Fault Management overview

System Fault Management (SFM) is a suite of advanced hardware fault technologies that protects hardware against failures and reports predictive information and corrective action events. SFM is available for HP 9000 systems running version 2 update 2, and Integrity servers running HP-UX 11i version 2 update 2.

SFM integrates into HP Systems Insight Manager (HP SIM) using industry-standard *Web-Based Enterprise Management* (WBEM) instrumentation.

Integration among standards-compliant system management applications, as with HP SIM, provides a holistic and comprehensive view of HP 9000 systems' and HP Integrity servers' health.

SFM uses industry-standard *Desktop Management Task Force* (DMTF) WBEM to provide advanced system level monitoring capabilities to protect hardware against failures that could interrupt system operation.

In addition, SFM allows for configuration of notification thresholds for reporting predictive information and corrective action events. Configurable thresholds enable system administrators to customize notifications to match the desired availability service level.

SFM includes providers to gather and model information and deliver it to the network management application through an industry standard interface (that is, using CIM specifications, through XML over HTTP).

The CPU Instance Provider gathers information about the central processors of an HP 9000 server.

The Memory Instance Provider gathers information about the memory configuration of an HP 9000 server.

The EMS Wrapper Provider translates hardware events from Event Monitoring System (EMS) hardware monitors into a form that is compatible with WBEM.

SFM is available in HP SIM by selecting a system with SFM installed and selecting **Tools**→**System Information**→**System Page**.

See http://h20293.www2.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=SysFaultMgmt&jumpid=reg_R1002_USEN for additional information about SFM.

WBEM providers overview

HP WBEM Management Providers enable you to remotely monitor system configuration and status. The Management Providers report information about the system on which they are used. Information is provided over the *Web-Based Enterprise Management* (WBEM) industry-standard protocol. A *Central Management Server* (CMS) using HP Systems Insight Manager (HP SIM) gathers, organizes, and displays the information in reports enabling you to monitor system use and troubleshoot problems.

The management provider package contains a set of provider modules that plug in to the HP WBEM Services package. The providers extend the basic functions of the HP WBEM Services package by providing additional information about the hardware and operating system.

The provider package can supply the following categories of information in response to WBEM queries. For more information see the HP WBEM Provider Data Sheets available separately.

- Power supplies: Name, ID, description, status, and availability
- Disk SMART sensors: System, state (online, failed/asserted, or unknown)
- Disk drives: ID, capabilities, size, block size
- Disk partitions, logical systems, and logical disks: ID, bootable, and type
- Physical memory: Description, bank label, capacity, and memory type

- Physical memory statistical information: Single-bit errors, double-bit errors, and predictive failure indicator
- Network adapters: Address, speed, maximum speed, duplex indicator, and count of octets transmitted and received
- PCI systems: ID, vendor, grant time, and latency
- Physical media: Name, hot swap capability, capacity, manufacturer, model, serial number, version, and other information
- SCSI controllers: ID, name, description, and protocol

HP WBEM Providers are available from the Linux link at <http://www.software.hp.com>. WBEM providers for other HP equipment and operating systems are also available separately.

WBEM is a replacement for the SNMP network management protocol. WBEM providers perform a similar role to SNMP agents of publishing information about a managed system. HP Integrity servers can also be remotely managed using the HP SNMP Agents, which are available separately from <http://www.software.hp.com>.



CAUTION: The current release of HP WBEM Providers cannot coexist with the HP Insight Management Agent. This restriction will be removed in a future release. HP recommends Insight Management Agent be installed on production machines managed using SNMP, and the HP WBEM Providers be installed for evaluation of WBEM only.

See <http://h71028.www7.hp.com/enterprise/cache/13219-0-0-225-121.html> for additional information about WBEM Providers for Linux.

Available MSA tools

The following list of the *multiple-system aware* (MSA) tools are available in HP Systems Insight Manager (HP SIM):

- Deploy SSH Public Key
- Ignite-UX Console
- Ignite-UX Restricted Console
- Create or Modify Recovery Archive
- Create or Modify Tape Recovery Archive
- Install or Recover System
- Install Software
- Remove Software
- Software Distributor Job Browser
- Copy Depot Software
- Remove Depot Software
- SD Job Browser
- Subscribe to WBEM Events
- Install WLM Configuration
- Retrieve WLM Configuration
- Syntax Check on the Systems Insight Manager Server Configuration
- Syntax Check Configuration
- Install OpenSSH
- Initial ProLiant Support Pack Install
- Install Software and Firmware

1.3 Partner applications

HP Systems Insight Manager (HP SIM) partner applications extend the breadth of HP system coverage and improve the lifecycle management capabilities for your HP servers as plug-in tools or .TDEF files.



NOTE: If you are looking for information about a tool that is not listed on this page or referenced in this help system, it might be a custom tool or a tool provided by a company other than HP. Ask your administrator for assistance.

HP Integrity Essentials plug-ins

Feature	HP product	HP-UX	Linux	Windows	OpenVMS
Configuration management	Availability Manager				X
	HP-UX webmin-based Admin	X			
	Integrated Lights-Out	X	X	X	X
	Intelligent Networking Pack	X	X	X	
	Management Processor	X	X	X	
	Partition Manager	X	X	X	
	HP Serviceguard Manager				
	System Management Homepage				
Software deployment	Ignite-UX	X			
	Security Patch Check	X			
	Software Distributor-UX	X			
	Software Package Builder	X			X
	VMS Loader				
Virtualization and automation management	Capacity Advisor	X			
	Class Scheduler				X
	Global Workload Manager	X	X		X
	HP-UX Workload Manager	X	X		
	OpenView GlancePlus	X	X	X	X
	OpenView Performance Agent	X	X		
	Process Resource Manager				
	Virtualization Manager				

HP ProLiant Essentials plug-ins

Feature	Description
Configuration management	<ul style="list-style-type: none"> • Integrated Lights-Out Advanced Pack Control ProLiant servers remotely through a web browser. Built into HP ProLiant systems. Non-operating system dependent. • Intelligent Networking Pack Minimize the risk of outages caused by network failures or virus attacks. Runs on Windows only. • Performance Management Pack Identify systems with performance bottlenecks. Runs on Windows and Linux. • Rack and Power Management Grow with your datacenter demands for power protection and rack space. Runs on Windows only. • HP Insight Power Manager Monitor historical power consumption and heat dissipation and manage these resources.
Software deployment	<ul style="list-style-type: none"> • HP BladeSystem Integrated Manager Access all tools needed to configure and manage an HP BladeSystem Integrated Manager in HP Systems Insight Manager environment. Runs on Windows, Linux, and HP-UX. • Insight Management Agents Review in-depth system hardware configuration and status data, performance metrics, system thresholds and software version control information. Runs on Windows and Linux. • HP Rapid Deployment Pack Automate unattended deployment of HP BladeSystem Integrated Manager in HP Systems Insight Manager and ProLiant hardware. Runs on Windows and Linux. • Vulnerability and Patch Management Pack Identify and close security vulnerabilities before they result in unplanned downtime. Runs on Windows and Linux.
Virtualization and automation management	<ul style="list-style-type: none"> • HP Server Migration Pack - Universal Edition Convert between physical and virtual, virtual and virtual, and virtual and physical systems. Runs on Windows and Linux. • Workload Management Pack Control and dynamically allocate system resources. Runs on Windows only.

HP Storage Essentials plug-ins

All of these plug-ins install on Windows only.

Feature	Description
Application storage management	<ul style="list-style-type: none"> • Exchange Viewer Microsoft Exchange availability and performance views. • File System Viewer High performance file-level storage resource management (SRM) capabilities. • Oracle Viewer Oracle database availability and performance views. • SQL Viewer SQL database availability and performance views.

Feature	Description
Configuration management	<ul style="list-style-type: none"> • NAS Manager Comprehensive Network Attached Storage (NAS) management capabilities. • Provisioning Manager Heterogeneous host-to-array path provisioning wizard. • HP Storage Essentials Enterprise Edition Main console for open, heterogeneous LAN management.
Reporting	<ul style="list-style-type: none"> • Backup Manager Visualization of backup elements, dependency management, and reports. • Chargeback Manager Assign tiers and create asset-based chargeback management. • Global Reporter View roll-up reporting of multiple Storage Essentials instances. • Report Designer Develop customer reports for your storage infrastructure.

HP Infrastructure Resource Management plug-ins

Feature	HP Product	Managed Systems
Client management software	HP Client Manager Web JetAdmin	HP business desktop, workstation, notebook, and tablet PCs. HP management supported printers and third-party network peripherals.

Related topics

- [Managing with tasks](#)
- [Viewing task results](#)
- [Array Configuration Utility overview](#)
- [HP BladeSystem overview](#)
- [HP Client Manager overview](#)
- [Event Monitoring Service overview](#)
- [GlancePlus overview](#)
- [HP-UX Bastille overview](#)
- [Ignite-UX overview](#)
- [Integrated Lights-Out overview](#)
- [HP Integrity Essentials overview](#)
- [HP OpenView Storage Data Protector overview](#)
- [HP OpenView Performance Agent overview](#)
- [HP OpenView Storage Management Appliance overview](#)
- [Partition Manager overview](#)
- [HP ProLiant Essentials applications](#)
- [Software Distributor overview](#)
- [HP Storage Essentials overview](#)
- [HP StorageWorks Command View EVA overview](#)
- [HP StorageWorks Command View SDM overview](#)
- [HP StorageWorks Command View Tape Library overview](#)
- [HP StorageWorks Command View XP overview](#)

- HP StorageWorks Command View XP Advanced Edition overview
- HP StorageWorks 1000 Modular Smart Array overview
- System Fault Management overview
- HP ProLiant Essentials Vulnerability and Patch Management Pack overview
- HP Virtual Server Environment overview
- WBEM providers overview
- Web JetAdmin overview
- PMP tools
- HP Process Resource Manager overview
- RPM Package Manager
- Security Patch Check overview
- HP Serviceguard Manager overview
- Server Migration Pack
- Webmin overview
- Workload Manager overview

HP Integrity Essentials overview

HP Integrity Essentials is an optional plug-in for HP Systems Insight Manager (HP SIM) that enables you to add powerful lifecycle features while continuing to benefit from common security and configuration management.

HP SIM and HP Integrity Essentials help you control IT infrastructure with unified management of your HP Integrity server environment running:

- HP-UX 11i
- Windows
- Linux
- OpenVMS

HP Integrity Essentials for HP-UX 11i

HP Integrity Essentials provides modular, integrated system management software for complete Integrity server management for multiple operating systems, including HP-UX 11i.

Software deployment

- Ignite-UX provides for fast deployment.
- Software Distributor distributes software for HP-UX.
- Software Package Builder allows easy updates to HP-UX.
- Security Patch Check and Patch Assessment Tool improves system security.

Configuration management

- HP Integrity Essentials Virtualization Manager provides comprehensive, integrated configuration, and management of all Virtual Server Environment elements.
- HP Integrity Essentials Capacity Advisor provides ongoing capacity planning simulating placement of application workloads.
- *System Management Homepage* (SMH)/System Administration Manager provides basic HP-UX management.
- Partition Manager creates and manages hard partitions.
- HP-UX Bastille provides security hardening /lock down.

- HP-UX Webmin-based Admin allows open source tools to plug in.
- Serviceguard Manager manages Serviceguard clusters.

Workload management

- Process Resource Manager provides workload management.
- Secure Resource Partitions provides secure application stacking.
- HP-UX Workload Manager is an intelligent policy engine for the HP Virtual Server Environment.
- Global Workload Manager is the intelligent policy engine for multisystem Virtual Server Environments.
- OpenView GlancePlus and Performance Agent provide performance monitoring.

Remote server management

- Integrated Lights-Out (iLO) manages entry level Integrity servers.
- Management Processor manages mid-range and high-end Integrity servers.

HP Integrity Essentials for Windows

Deployment and configuration

- Integrity Essentials Foundation Pack for Windows is a complete toolset to install, configure, and manage HP Integrity servers with Windows Server 2003.
- Smart Setup CD provides easy server configuration and the latest HP drivers, firmware utilities, and management assets.
- HP Performance Management Pack enables you to create and manage hard partitions (nPars).
- System Management Homepage (*HP Insight Management Agents*) provides a consolidated view of an individual server.
- *HP Version Control Agent (VCA)* and *HP Version Control Repository Manager (VCRM)* provide easy system software maintenance.
- NIC Configuration Utility enables you to configure and monitor HP Network Interface Controllers.
- HP Performance Management Pack enables you to detect and analyze performance bottlenecks for HP Integrity servers.

Remote server management

- Integrated Lights-Out (iLO) manages entry-level Integrity servers.
- Management Processor manages mid-range and high-end Integrity servers.

HP Integrity servers with Linux

Central administration

HP SIM is the foundation for the HP unified server-storage management strategy. It is a multiple operating system, hardware-level management product that supports HP Integrity, HP ProLiant, and HP 9000 servers. HP SIM is easily extensible, integrating other HP management products and value-add plug-ins such as HP Integrity Essentials.

The HP OpenView enterprise-level management solution System Management Homepage (Insight Management Agents) provides a consolidated view of an individual server.

HP Integrity Essentials provides modular, integrated system management software for complete Integrity server management for multiple operating systems, including Linux.

HP Integrity Essentials for Linux

Deployment and configuration

Enablement Kit for Linux, including SystemImager, delivers all the latest, compatible HP drivers, firmware, utilities, and Insight Management Agents and manages the installation of the operating system.

HP Integrity Essentials Capacity Advisor provides ongoing capacity planning simulating placement of application workloads.

System Management Homepage provides a consolidated view of an individual server

Partition Manager creates and manages hard partitions (nPars), and Serviceguard Manager manages Serviceguard clusters.

Workload management

Global Workload Manager is the intelligent policy engine for multisystem Virtual Server Environments.

OpenView GlancePlus and Performance Agent offer performance monitoring.

Remote server management

Integrated Lights-Out (iLO) manages entry-level Integrity servers.

Management Processor manages mid-range and high-end Integrity servers.

HP Integrity servers with OpenVMS

Central administration

HP SIM is the foundation for the HP unified server-storage management strategy. It is a multiple operating system, hardware-level management product that supports HP Integrity and HP 9000 servers. HP SIM is easily extensible, integrating other HP management products and value-added plug-ins such as HP Integrity Essentials.

OpenView, the HP enterprise-level management solution, includes OpenView Operations Agent for seamless management from OpenView Operations.

HP Integrity Essentials provides modular, integrated system management software for complete Integrity server management for multiple operating systems, including OpenVMS.

HP Integrity Essentials for OpenVMS

Configuration management

Availability Manager is a real-time performance monitor for OpenVMS. Insight Management Agents enable HP SIM Partition Manager to create and manage hard partitions (nPars).

Workload management

Availability Manager is a real-time performance monitor for OpenVMS.

Insight Management Agents enable HP SIM Partition Manager to create and manage hard partitions (nPars).

Remote server management

Integrated Lights-Out (iLO) manages entry-level Integrity servers.

Management Processor manages mid-range and high-end Integrity servers.

Related topics

- [Partner applications](#)
- [HP BladeSystem overview](#)
- [Event Monitoring Service overview](#)
- [GlancePlus overview](#)
- [HP-UX Bastille overview](#)

- Ignite-UX overview
- Integrated Lights-Out overview
- Management processor tools
- HP OpenView Storage Data Protector overview
- HP OpenView Performance Agent overview
- Partition Manager overview
- HP Process Resource Manager overview
- Security Patch Check overview
- HP Serviceguard Manager overview
- Software Distributor overview
- Webmin overview
- Workload Manager overview

Event Monitoring Service overview

Event Monitoring Service (EMS) is a system monitoring application designed to facilitate real-time monitoring and error detection for HP products in the enterprise environment. This framework provides centralized management of hardware systems and system resources and provides immediate notification of hardware failures and system status.

HP EMS reports information that helps you detect loss of redundant resources, thus exposing single points of failure and eliminating the threat to data and application availability. HP EMS capabilities cover the entire system: system components, storage, and network interfaces.

To access the Event Monitoring Services in HP Systems Insight Manager (HP SIM), select **Diagnose**→**Event Monitoring Service**.

See <http://docs.hp.com/en/B7612-90015/ch01s01.html> for more information and access to documentation.

HP-UX Bastille overview

HP-UX Bastille is a security hardening/lockdown tool that can be used to enhance the security of the HP-UX operating system. It provides customized lockdown on a system by system basis, addressing many of the recommendations from several popular security scanning tools and checklists.

Features and benefits

- Configures daemons and system settings to be more secure
- Turns off unneeded services such as `pwgrd`
- Helps create chroot jails that partially limit the vulnerability of common Internet services such as web servers and Domain Name System (DNS)
- Educates users through its user interface
- Configures Security Patch Check to run automatically
- Configures an IPFilter-based firewall
- Returns the security configuration to the state before Bastille was run with the `revert` feature

HP-UX Bastille must be downloaded and installed from the HP website.

See http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA for more information and access to documentation.

GlancePlus overview

HP OpenView GlancePlus Pak provides you with a single product for managing a system's availability and performance. It is an integrated product that includes the following components:

- HP OpenView GlancePlus
- HP OpenView Performance Agent

As an integrated product, the GlancePlus Pak includes the real-time diagnostic capabilities of GlancePlus and the historical data collection capabilities of the Performance Agent. The performance agent is used with other availability and performance management products, providing an integrated real-time and historical performance management solution.

With GlancePlus Pak, you can handle a wide range of system performance and availability problems to get the best from your system and the applications running on it.

To access GlancePlus Pak, select **Tools**→**performance monitors**.

See <http://www.managementsoftware.hp.com/products/gppak2k/index.html> for more information and access to documentation.

Ignite-UX overview

Ignite-UX addresses the need for HP-UX system administrators to perform system installations and deployment, often on a large scale. It provides the means for creating and reusing standard system configurations. It provides the ability to archive a standard system configuration and to use that archive to replicate systems, with the added benefit of speeding up the process. It also permits post-installation customizations and is capable of both interactive and unattended operating modes.



NOTE: This product is available for HP-UX systems only.

After Ignite-UX has been installed, you can access its features within HP Systems Insight Manager (HP SIM) by selecting **Deploy**→**Ignite-UX**.

See <http://docs.hp.com/en/IUX/> for more information and access to documentation for Ignite-UX.

Integrated Lights-Out overview

Basic system management functions, diagnostics, and essential Lights-Out functionality are included as core components of Integrated Lights-Out (iLO) supported servers. The standard features of iLO are referred to as iLO Standard. Advanced remote administration functionality, referred to as iLO Advanced, can be licensed with the optional Integrated Lights-Out Advanced Pack for HP Integrity Servers.

iLO functionality on HP Integrity servers is similar to that offered on HP ProLiant servers to ensure a common user experience between HP ProLiant and Integrity platforms.

The key iLO Standard features on Integrity servers include:

- **Web GUI** Enables you to access the iLO from anywhere using any standard browser.
- **Virtual Power** Provides full remote control of the server power button.
- **Remote text console** Provides an operating system-independent, text-based console to display and control remote host server activities such as shutdown and start-up.
- **Virtual Serial Port** Provides access serial port applications such as Windows Server 2003 Emergency Management Services and Text Telephone (TTY) sessions over your LAN.
- **Command line and scripting interfaces** Provides flexible operation, configuration, and maintenance.
- **Secure Sockets Layer (SSL) encryption** Ensures that all data transmitted between iLO processors and client browsers is secure.
- **iLO and server diagnostics** Provides detailed status logs.
- **Domain Name System (DNS)/Dynamic Host Configuration Protocol (DHCP)**

- **Remove Firmware Update**
- **Intelligent Platform Management Interface (IPMI) over LAN**

The iLO Advanced Pack includes the following key features:

- Directory Services Integration for iLO User Management using Lightweight Directory Access Protocol (LDAP)-based Directory Services
- Secure Shell (SSH encryption) support for secure access to iLO
- iLO Group Actions for managing multiple systems using HP Systems Insight Manager (HP SIM)

See <http://h71028.www7.hp.com/enterprise/cache/98327-0-0-0-121.html/> for more information and access to documentation for iLO for HP Integrity servers.

Partition Manager overview

Partition Manager provides system administrators with a convenient graphical user interface to configure and manage nPartitions on HP server systems. Using Partition Manager, you can perform complex configuration tasks without needing to remember commands and parameters. You select nPartitions, cells, I/O chassis, or other components from the graphical display, then select an action from a menu.

With HP Systems Insight Manager (HP SIM), you can perform the following tasks:

- Modify nPartitions
- View and modify nPartitions
- View and modify Remove Complex

Depending on the version of Partition Manager that you are running, you can access it in HP SIM from the **Tools**→**Partition Manager** menu or the **Configure**→**Partition Management** menu.

See <http://docs.hp.com/en/PARMGR2/index.html> for more information and access to documentation.

Security Patch Check overview

Security Patch Check is a tool that analyzes the currency of a system with respect to security bulletins. It recommends actions for security vulnerabilities that have not been fixed by previously performed patches, updates, removals, or, where logged by the user, manual actions. The actions might include updates, software removals, or manual actions. Use of the Security Patch Check software tool can help efficiently improve system security but does not guarantee system security.

Security Patch Check performs the following functions:

- ▲ Generates a report of recommended security actions that are applicable and not installed or applied
 - Helps automate the process of checking for security patches, updates, or manual actions missing from a system
 - Warns about patches with warnings that are present on the system being analyzed
 - Integrates with HP Systems Insight Manager (HP SIM) by enabling you to get the patch catalog and to run Security Patch Check

To access the Security Patch Check features within HP SIM, select **Configure**→**Security**.

HP Serviceguard Manager overview

HP Serviceguard Manager is a graphical user interface that provides configuration, status-monitoring, and administration of high availability clusters created by HP Serviceguard. The Serviceguard Manager management station can be an HP-UX, Linux, or Windows system. Using Serviceguard Manager, you can view the status of all the clusters on your network through color-coded icons. From this high-level perspective, you can drill down and proactively manage specific clusters, nodes, and packages.

Serviceguard clusters are identified and associated through SNMP and provide a mechanism to view cluster information by running HP Serviceguard Manager if it is registered with HP Systems Insight Manager (HP SIM).



NOTE: If you have systems that have both SNMP and WBEM Serviceguard cluster awareness agents installed and you previously ran HP SIM 4.x, you must run discovery again for Serviceguard cluster information to be obtained through WBEM.

You can access HP Serviceguard Manager through one of the following methods:

- From the system table view page, select a system that is an HP Serviceguard Cluster. HP SIM searches the database for the first system that belongs to the cluster and Serviceguard Manager is launched with that system.
 - From the system table view page, click a container system that has a cluster member. The cluster member is passed to Serviceguard Manager. You can also select the row that includes the container system and launch Serviceguard Manager from the menu by selecting **Tools**→**Integrated Consoles**→**HP Serviceguard Manager**.
 - From the system table view page, click a cluster node. The cluster node is passed to Serviceguard Manager. You can also select the row that includes the container system and then launch Serviceguard Manager from the menu by selecting **Tools**→**Integrated Consoles**→**HP Serviceguard Manager**.
 - Access the **HP Serviceguard Manager** page by selecting **Tools**→**Integrated Consoles**→**HP Serviceguard Manager**. The **HP Serviceguard Manager** page appears.
-



NOTE: If you have not used HP Serviceguard Manager before HP SIM 5.0, you can download the latest version from: <http://www.hp.com/go/softwaredepot> and click **HP Serviceguard Manager**. When you install HP Serviceguard Manager, it recognizes HP SIM and automatically registers it for you. If you used HP Service Manager 4.02 with previous versions of HP SIM, when you upgrade to HP SIM to 5.0, the tool HP Serviceguard Manager 4.02 is still available.

See <http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B8325BA> for more information and to download the software.

Related topics

- [Navigating the system table view page](#)
- [Navigating the Cluster Table View Page](#)

Software Distributor overview

Software Distributor (SD) is the HP-UX administration tool set used to deliver and maintain HP-UX operating systems and layered software applications. SD is delivered as part of HP-UX. You do not need to download it separately.

SD works with you. System administrators use SD to manage software on HP PA-RISC and Itanium-based systems. Software packagers use SD to organize, standardize, and distribute software to customers. HP-UX partners use SD as the primary tool for building and testing complete solutions for the enterprise and technical desktop.



NOTE: This product is available for HP-UX systems only.

To access SD through HP Systems Insight Manager (HP SIM), select **Deploy**→**Software Distributor**.

To view SD logs, select **Tasks & Logs**→**View Software Distributor Agent Log** and **Tasks & Logs**→**View Software Distributor Daemon Log**.

See <http://www.docs.hp.com/en/SD/> for more information and access to documentation.

Webmin overview

Webmin is a web-based interface for system administration for UNIX and Linux. Using HP Systems Insight Manager (HP SIM), you can set up user accounts, Apache, DNS, file sharing, and so on. Webmin consists of a miniserver and many Common Gateway Interface (CGI) programs, which directly update system files such as `/etc/inetd.conf` and `/etc/passwd`. The web server and all CGI programs are written in Perl 5 and use no external modules, which means that you only need a Perl binary to run Webmin.

Because Webmin supports the concept of modules (for example, PhotoShop plug-ins), you can develop and distribute your own Webmin modules for any purpose and distribute them under any license (such as General Public License (GPL), commercial, or shareware).

To access Webmin in HP SIM, select **Tools**→**Integrated Consoles**→**Webmin**. The **Webmin** page appears. Select a target system, and then click **Run Now**.

Workload Manager overview

HP-UX Workload Manager (HP-UX WLM) is a resource management tool that provides automatic CPU resource allocation and application performance management based on prioritized service level objectives (SLOs). In addition, real memory and disk bandwidth allocations can be set to fixed levels in the configuration.

The following features are available within HP Systems Insight Manager (HP SIM):

- Workload Manager Console
- Activate WLM Configuration
- Enable WLM
- Install WLM Configuration
- Restart WLM
- Stop WLM
- Syntax Check Configuration
- Syntax Check on HP SIM Configuration
- Truncate Statistics Log Files
- View Workload Manager Log Files
- View Workload Manager Statistics Log Files
- Ability to Launch Workload Manager from the GUI

To access the Workload Manager features within HP SIM, select **Optimize**→**Workload Manager, Tasks & Logs**→**Workload Manager Log Files**, and **Tasks & Logs**→**Workload Manager Statistics Log Files**.

See <http://h20338.www2.hp.com/hpux11i/cache/328328-0-0-0-121.html> for more information.

HP OpenView Storage Data Protector overview

HP OpenView Storage Data Protector is software that manages backup and recovery from both disks and tapes, delivering maximum data protection while providing continuous business operations. The software is designed to simplify and centralize backup and recovery operations by integrating a variety of techniques to eliminate backup windows. These range from online backup, open file backup, and instant recovery or zero-downtime backups. Its proven industry-leading instant recovery features and several other integrated disaster recovery alternatives meet the demands of the most complex enterprises so that they can recover critical data within minutes.

Data Protector simplifies the use of complex backup and recovery procedures with the fastest installation, automated routine tasks, and easy-to-use features. The ideal solution to reduce complexity while remaining reliable and scalable to grow from single-server environments to the largest distributed enterprise infrastructures, providing broad compatibility of operating systems, applications, drives, libraries, and disk arrays.

It also provides tracking and management of offline storage media, maximizes media operations productivity and increases data availability by automating the tracking and management of removable storage media. With media operations, customers can manage the complete lifecycle of removable storage media, shortening recovery time, reducing financial and business risks from lost data, and minimizing opportunities for human error.

HP OpenView Storage Data Protector is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page** only after the application has been installed. See “Tools & Links tab” for information about accessing the **System Page**.

See <http://h18006.www1.hp.com/products/storage/software/dataprotector/index.html> for more information and access to documentation.

HP OpenView Performance Agent overview

The HP OpenView Performance Agent logs and collects data and, then, sends alarms about that data when necessary. The agent is installed on each system you plan to monitor.

With its powerful end-to-end application response measurement capabilities, the Performance Agent is the core enabling technology in any service management strategy.

HP OpenView Performance Agent must be downloaded and installed from the HP website.

See <http://www.managementsoftware.hp.com/products/ovperf/index.html> for more information and access to documentation.

HP Insight Power Manager overview



NOTE:

NOTE:

HP OpenView Storage Management Appliance overview

The HP OpenView Storage Management Appliance is a centralized, appliance-based monitoring and management solution for the storage area network (SAN). Connected directly to the fabric, it performs management functions outside the data path and without involving host computers, allowing data transfers to proceed independently between computers and storage systems.

The Storage Management Appliance optimizes SAN availability and performance while streamlining manageability by enabling policy-based automation of repetitive storage management tasks. It provides an intuitive, web-based interface and storage management aggregation point, enabling you to organize, configure, visualize, monitor, and provision storage from anywhere, anytime. The Storage Management Appliance includes HSG Element Manager and provides support for HP OpenView Storage Operations Manager. This combined solution delivers easy-to-use tools for centralized management of Enterprise Virtual Array and Enterprise Modular Array (EMA)/Modular Array (MA) arrays on the SAN, as well as the foundation for comprehensive enterprise storage resource management across multivendor platforms in the network storage infrastructure.

The Storage Management Appliance supports a variety of additional value-added storage management applications from HP, as well as popular virus protection, backup, system management, and UPS software products. The Storage Management Appliance provides the following features:

- Unobtrusive, centralized appliance for storage management
The HP OpenView Storage Management Appliance provides an unobtrusive, centralized point for managing and monitoring the SAN and other networked storage systems. Designed to connect directly to the SAN fabric, the Storage Management Appliance performs management functions without involving host computers.
- SAN availability and performance optimization
Strategically located out of the SAN data path, the Storage Management Appliance enables data transfers to proceed independently between computers and storage systems whether it is operating. The Storage Management Appliance optimizes SAN availability and performance while streamlining SAN manageability.
- Web-based interface for storage management
Included with the Storage Management Appliance, HP OpenView Storage Management Appliance software provides a web-based aggregation and entry point for centralized storage management. This intuitive interface enables you to organize, visualize, configure, and monitor storage from a single navigation point on the SAN. The Storage Management Appliance software provides a launch site for a variety of value-added HP storage management applications and provides navigation links to directly manage storage components on the SAN.
- HSG Element Manager
This easy-to-use, graphical storage configuration and monitoring tool centralizes storage management across network and multivendor platforms. Included with the HP OpenView Storage Management

Appliance, HSG Element Manager reduces the job of storage management to simple point-and-click, across the switched Fibre Channel SAN. It provides for easy configuration of HP StorageWorks HSG80/60 storage systems as well as field replaceable unit (FRU) level fault detection and notification, through an SNMP agent with MIB event logging. This new version introduces a provider for the Storage Networking Industry Association Storage Management Initiative Specification (SMI-S), enabling greater multivendor manageability in the enterprise network storage infrastructure.

HP OpenView Storage Management Appliance is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See <http://h18006.www1.hp.com/products/sanworks/managementappliance/index.html> for more information and access to documentation.

HP Process Resource Manager overview

HP Process Resource Manager (PRM) enables the system administrator to focus the appropriate amount of system resources exactly where you need them. This powerful resource management tool runs as in addition to HP-UX. When PRM is enabled, groups of users or applications are guaranteed a specified portion of the total system central processing unit (CPU) processing cycles, of the available real memory resources, and of the disk bandwidth to logical volume-managed (LVM) systems.

PRM is a resource management tool used to control the amount of resources that processes use during peak system load (at 100% CPU, 100% memory, or 100% disk bandwidth utilization). PRM can guarantee a minimum allocation of system resources available to a group of processes through the use of PRM groups.

A PRM group is a collection of users and applications that are joined together and assigned certain amounts of CPU, memory, and disk bandwidth. The two types of PRM groups are FSS PRM groups and PSET PRM groups. An FSS PRM group is the traditional PRM group, whose CPU entitlement is specified in shares. This group uses the Fair Share Scheduler (FSS) in the HP-UX kernel within the system's default processor set (PSET). A PSET PRM group is a PRM group whose CPU entitlement is specified by assigning it a subset of the system's processors (PSET). Processes in a PSET have equal access to CPU cycles on their assigned CPUs through the HP-UX standard scheduler.

Reasons to use PRM

- Improve the response time for critical users and applications.
- Set and manage user expectations for performance.
- Allocate shared servers based on budgeting.
- Ensure that an application package in a Serviceguard cluster has sufficient resources on an active standby system in the event of a failover.
- Ensure that critical users or applications have sufficient CPU, memory, and disk bandwidth resources.

Users who at times run critical applications might at other times engage in relatively trivial tasks. These trivial tasks can compete in the users' PRM group with critical applications for available CPU and real memory. For this reason, it is often useful to separate applications into different PRM groups or create alternate groups for a user. You can assign a critical application its own PRM group to ensure that the application gets the needed share of resources.

- Restrict the CPU, real memory, and disk bandwidth resources available to relatively low-priority users and applications during times of heavy demand.

For example, mail readers can consume significant disk bandwidth when users first come into work or return from lunch. Therefore, you might want to assign a mail application to a PRM group with small resource allocations and restrict the amount of resources mail can use during such times of heavy demand on the system.

- Monitor resource consumption by users or applications.

Assigning a group of users or applications to separate PRM groups can be a good way to keep track of the resources they are using.

Accessing Process Resource Manager from HP SIM

Select **Optimize**→**Process Resource Manager**. Four options are available:

- Process Resource Manager Console
- Display Resource Usage
- List Resource Availability
- Launch PRM from the GUI

If the system has the PRMSIMTools bundle installed, the available options are:

- Monitor PRM Groups
- Configure PRM Groups
- Display Resource Usage
- List Resource Availability

Go to: <http://www.hp.com/go/prm> for more information about PRM.

HP Virtual Server Environment overview

The HP Virtual Server Environment (VSE) encompasses several fully integrated, complementary components that enhance the functionality and flexibility of your server environment.

The following are key VSE applications:

- **HP Integrity Essentials Virtualization Manager** Virtualization Manager is easy-to-use virtualization management software that reduces complexity by providing unified visualization and management of physical and virtual servers. Virtualization Manager provides a central point of control that enables you to manage all the resources in your VSE. It is a powerful way to connect IT resources to real business needs. See http://h71028.www7.hp.com/enterprise/cache/262377-0-0-225-121.html?jumpid=reg_R1002_USEN for more information.
- **HP Integrity Essentials Global Workload Manager (gWLM)** Global Workload Manager (gWLM) is a multisystem, multi-operating system workload manager that serves as an intelligent policy engine in the HP Virtual Server Environment. It simplifies the deployment of automated workload management policies across multiple HP-UX 11i or Linux servers and provides centralized monitoring and reporting providing improved server utilization and maintaining service levels. HP Global Workload Manager is available for HP-UX 11i and Linux. See <http://h71028.www7.hp.com/enterprise/cache/257279-0-0-0-121.html> for more information.
- **HP Integrity Essentials Capacity Advisor** HP Integrity Essentials Capacity Advisor is the industry's first lightweight, integrated tool for ongoing capacity planning, simulating placement of application workloads to help IT administrators improve server utilization. Capacity Advisor provides planning capability for the intelligent control of the HP Virtual Server Environment. See <http://h71028.www7.hp.com/enterprise/cache/262379-0-0-0-121.html> for more information.
- **HP Systems Insight Manager (HP SIM)** HP Systems Insight Manager (HP SIM) combines the best of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver hardware fault, asset, and configuration management for all of your HP systems. HP SIM can be easily extended to deliver rapid deployment and performance management for workload and partition management for Integrity and HP 9000 systems.

If installed, HP Virtual Server Environment can be accessed through HP SIM by selecting **Tools**→**VSE Management**.

Go to HP Virtual Server Environment at <http://www.hp.com/go/vse> for more information about VSE and see www.hp.com/go/integrityessentials to access documentation. See the *VSE Management Quick Start Guide* as a quick way to get started using VSE.

HP ProLiant Essentials applications

HP ProLiant Essentials includes software to assist in managing your ProLiant servers. ProLiant Essentials Services can help you perform the following tasks:

- Contain server-related acquisition and operating costs.
- Reduce the risks associated with change.
- Improve overall IT manageability.
- Decrease application downtime by speeding problem detection and resolution.
- Increase service efficiency and productivity.

The applications listed here are considered partner applications with HP Systems Insight Manager (HP SIM) and are all available automatically with an installation of HP SIM or by download from the HP website.

Monitor and Alert

- HP BladeSystem Integrated Manager
- HP Intelligent Networking Pack
- HP Insight Management Agent

Analyze and Control

- HP Power Regulator
- HP Performance Management Pack
- Insight Diagnostics
- Workload Management Pack

Provision and Patch

- HP Array Configuration Utility
- HP BladeSystem Setup through iLO
- HP ProLiant Essentials Vulnerability and Patch Management Pack
- HP ProLiant Support Pack
- Rapid Deployment Pack
- SmartStart Scripting Toolkit

Recovery and Scale

- HP Server Migration Pack - Universal Edition
- HP ProLiant Essentials Virtual Machine Management Pack
- VMware+ProLiant Essentials Bundle

Remote Management

- Integrated Lights-Out Standard Edition
- Integrated Lights-Out Advanced Edition
- Lights-Out 100 Remote Management
- Remote Insight Lights-Out Edition II

Enterprise Management

- HP OpenView Storage Data Protector
- HP OpenView Storage Management Appliance
- HP OpenView Storage Operations Manager

Other HP Management

- HP Client Manager
- HP OpenView Storage Area Management
- Web Jetadmin

for more information about HP ProLiant Essentials and links to the above partner applications, see <http://h18013.www1.hp.com/products/servers/management/index.html>.

Related topics

- PMP tools
- HP ProLiant Essentials Vulnerability and Patch Management Pack overview
- Array Configuration Utility overview
- Server Migration Pack
- Management processor tools
- HP OpenView Storage Management Appliance overview
- Workload Manager overview
- HP BladeSystem overview
- RPM Package Manager
- Web JetAdmin overview
- HP Client Manager overview

Array Configuration Utility overview

The HP Array Configuration Utility (ACU) software for Smart Array controllers and the StorageWorks Enclosure 4x00 family of products makes it easy to configure and expand your disk drive arrays. This web-based tool is intuitive. By using its Configuration Wizards, your array controller is set up and ready to use in minutes. ACU is also versatile: use it to locally or remotely configure your array controller, add additional disk drives to an existing configuration, or completely reconfigure your disk drive array. Additionally, innovative features such as Online Capacity Expansion, Logical Drive Capacity Extension, and RAID Level Migration enable you to change your array configuration and settings as your storage needs change.

HP Array Configuration Utility is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See <http://h18000.www1.hp.com/products/servers/proliantstorage/software-management/acumatrix/index.html> for more information.

HP BladeSystem overview

HP is delivering *HP BladeSystem Integrated Manager* as a component in HP Systems Insight Manager (HP SIM) to provide streamlined management access for the HP BladeSystem Integrated Manager in HP Systems Insight Manager. The HP BladeSystem Integrated Manager in HP Systems Insight Manager is comprised of blade computer systems, integrated connectivity to data and storage networks, and shared power subsystems.

The HP BladeSystem Integrated Manager in HP Systems Insight Manager integrated management environment enables users to quickly navigate their HP blade environments, including blades servers and desktops, enclosure infrastructures, racks, and integrated switches, through hierarchical tree views. Users can conveniently configure, deploy, and manage individual or groups of blade systems. Additionally, users can quickly set up logical groups of blade systems for convenient management and control.

Finally, the HP BladeSystem Integrated Manager in HP Systems Insight Manager integrated management environment works seamlessly within the expanding HP SIM environment, including ProLiant Essential Value Packs and third-party plug-ins to HP SIM. Version 2.1 of HP BladeSystem Integrated Manager in HP Systems Insight Manager is installed automatically with HP SIM 5.0 with SP5 for Windows and HP SIM 5.0 with Update 2 for HP-UX and Linux. HP BladeSystem Integrated Manager in HP Systems Insight Manager builds on the current leading capabilities in HP SIM for managing blades, including automatically generated, interactive blade system rack views.

HP BladeSystem Integrated Manager in HP Systems Insight Manager is available by selecting **Tools**→**Integrated Consoles**→**HP BladeSystem**.

See <http://h18004.www1.hp.com/products/servers/management/bsme/index.html> for more information, and see the *HP BladeSystem Integrated Manager Environment in HP SIM 5.2* at <http://18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

HP Client Manager overview

HP Client Manager is the foundation for all of the HP Client Management Solutions, providing the following:

- The infrastructure, data repository, and web-based console for the other HP Client Management Solutions from Altiris
- Task-based user interface, improved QuickStart screen, and streamlined setup and installation for faster software productivity
- Support for HP business desktops, notebooks, and workstations
- Integration with HP Systems Insight Manager (HP SIM) for client hardware management from the HP SIM console
- Ability to configure Wake on LAN (WOL) to remotely manage HP PCs even when they are powered on
- Scalable, web-based hardware and BIOS management for HP and Compaq clients
- Complete hardware inventory down to the component level
- Hardware change notification
- Client health monitoring and proactive diagnostics
- Update management (intelligent software distribution/BIOS flashing)

HP Client Manager is available through HP SIM, after being downloaded and installed from **Tools**→**Integrated Consoles**→**HP Client Manager Console**.

See http://h18000.www1.hp.com/im/client_mgr.html for information and access to documentation.

HP ProLiant Essentials Vulnerability and Patch Management Pack overview

Protect against hackers, worms, and Trojans that exploit software security vulnerabilities, using the HP ProLiant Essentials Vulnerability and Patch Management Pack, the all-in-one vulnerability assessment and patch management tool integrated into HP Systems Insight Manager (HP SIM). The Vulnerability and Patch Management Pack simplifies and consolidates the proactive identification and resolution of issues that can affect server availability into one central console.

The Vulnerability and Patch Management Pack delivers comprehensive vulnerability assessment and advanced patch management features to accelerate the remediation of vulnerabilities and reduces the risk of exploits.

The Vulnerability and Patch Management Pack is available from the **VPM** column on the system table view page. See “Navigating the system table view page” for more information.

See <http://www.hp.com/servers/proliantessentials/vpm> for more information and access to documentation.

Web JetAdmin overview

HP Web Jetadmin is a simple peripheral management software for remotely installing, configuring, and managing a wide variety of HP and third-party network peripherals using only a standard web browser. It can be used to proactively solve problems before they affect user productivity.

HP Web Jetadmin is available through HP Systems Insight Manager (HP SIM), after being downloaded and registered, by selecting **Tools**→**Integrated Consoles**→**WebJet Admin**.

See <http://h20338.www2.hp.com/Hpsub/cache/423231-0-0-225-121.html> for more information and access to documentation.

HP Storage Essentials overview

HP Storage Essentials is a suite of value-added plug-ins that offer advanced heterogeneous storage management functionality including storage area network (SAN) management, storage resource management, provisioning, and application infrastructure monitoring. HP Storage Essentials includes a core product and the following modules:

- **Enterprise Edition.** Main console for open, heterogeneous SAN management
Note: Enterprise Edition is required to have access to the remaining modules
- **Provisioning Manager.** Heterogeneous host-to-array path provisioning wizard
- **Chargeback Manager.** Asset-based chargeback management and tier assignment
- **Oracle Viewer.** Oracle database availability and performance views
- **Exchange Viewer.** Exchange database availability and performance views
- **Sybase Viewer.** Sybase database availability and performance views
- **File System Viewer.** File system scanning to reclaim wasted space
- **Global Reporter.** Roll-up reporting of multiple HP Storage Essentials Server instances
- **Report Designer.** Develop customer reports for storage infrastructure

Storage Essentials uses the latest industry standards, such as J2EE, SMI-S, WBEM, and WMI, to ensure that your storage management infrastructure is extendable and will support both HP and third-party technology, which enables you to use the technology appropriate to your needs and avoid vendor lock-in.

HP Storage Essentials is available through HP Systems Insight Manager (HP SIM) from the **Tools, Deploy, Diagnose, Optimize, Reports, Tasks & Logs**, and **Options** menus. See your HP Storage Essentials documentation for details about these menu items.

The HP Storage Essentials Agent Deployment Pack is available to streamline the Storage Essentials CIM Extensions installation. The deployment pack enables you to use HP SIM to install the Storage Essentials CIM extensions on remote hosts. You must install the CIM extensions on your storage hosts to use them with Storage Essentials. For more information about the deployment pack, see version 5.00.01 and later of the *HP Storage Essentials Installation Guide*. The HP Storage Essentials documentation is available at <http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docId=179111&taskId=101&prodTypeId=12169&prodSeriesId=463512>.

See “Changes to HP SIM storage functionality when HP Storage Essentials is installed” for information about the changes that occur in HP SIM when HP Storage Essentials is installed.

Related topics

- HP StorageWorks Command View EVA overview
- HP StorageWorks Command View SDM overview
- HP StorageWorks Command View Tape Library overview
- HP StorageWorks Command View XP overview
- HP StorageWorks Command View XP Advanced Edition overview
- HP StorageWorks 1000 Modular Smart Array overview

Storage device managers

HP Systems Insight Manager (HP SIM) allows you to start supported storage device managers from a link on the **Tools & Links** tab on the **System Page**. You can start the following device managers:

- HP StorageWorks Command View EVA
- HP StorageWorks Command View SDM
- HP StorageWorks Command View for Tape Libraries

- HP StorageWorks Command View XP
- HP StorageWorks Command View XP Advanced Edition
- HP StorageWorks Modular Smart Array 1000

Related topics

- HP StorageWorks Command View EVA overview
- HP StorageWorks Command View SDM overview
- HP StorageWorks Command View Tape Library overview
- HP StorageWorks Command View XP overview
- HP StorageWorks Command View XP Advanced Edition overview
- HP StorageWorks 1000 Modular Smart Array overview

HP StorageWorks Command View EVA overview

HP StorageWorks Command View EVA is a comprehensive software suite designed to simplify, enhance, and maximize the high-performance HP StorageWorks Enterprise Virtual Array (EVA) family of storage array products.

Command View EVA provides simplicity without compromise as it complements the HP StorageWorks Enterprise Virtual Array user. It offers storage administrators a single storage management solution for all your Enterprise Virtual Array management needs. It automates and aggregates storage management to reduce time-consuming manual tasks. Growing capacity is simple, because you can easily and dynamically expand logical unit numbers (LUNs) and add physical drives online to quickly meet changing business needs without application downtime. It provides easy and fast configuration of LUNs and redundant array of independent disk (RAID) groups. For mission-critical applications, you can take advantage of proactive remote services using the HP Instant Support Enterprise Edition and HP Solutions support to ensure continuous EVA uptime.

HP StorageWorks Command View EVA is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See <http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html> for more information and access to documentation.

HP StorageWorks Command View SDM overview

HP StorageWorks Command View SDM acts as a centralized management platform through a common user interface from which the value-added software solutions can be launched. Command View scalability ranges from management of a single array to multiple arrays all from a single management console. Command View SDM provides customers with a choice of user interfaces: GUI, CLI, or web browser. Included in Command View SDM is event/trap forwarding capabilities to network management frameworks enabling network administrators to be aware of any changes in their storage environment. You can also link with HP Systems Insight Manager (HP SIM) for initial consolidation of your storage and server environments. Command View SDM supports the emerging SMI-S storage standard, reducing manual integration for basic management capabilities.

Command View has been integrated with high level management frameworks such as OpenView Network Node Manager, CA Unicenter TNG, BMC Patrol, and Tivoli NetView. These integrations empower the network administrator by providing the ability to manage HP storage devices from the network management console.

HP StorageWorks Command View SDM is available through HP SIM from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See http://www.hp.com/products1/storage/products/disk_arrays/modular/commandview/index.html for more information and access to documentation.

HP StorageWorks Command View Tape Library overview

HP StorageWorks Command View Tape Library Software is the next step in the HP Extended Tape Library Architecture (ETLA), a key component of the HP Adaptive Infrastructure strategy. This software delivers tape libraries that are both self-aware and self-managed, automatically maintained, continuously available,

network-aware, resilient, secure, and adaptable. The HP tape libraries provide the reliability, interoperability, and advanced functionality required for enterprise SAN environments.

HP StorageWorks Command View Tape Library Software is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See <http://h18006.www1.hp.com/products/storageworks/tlarchitecture/index.html> for more information.

HP StorageWorks Command View XP overview

HP StorageWorks Command View XP provides centralized, web-based management for XP disk arrays. It enables collaboration among global team members, eliminating the need for travel to remote locations and increasing the efficiency of your administrator.

Graphical mapping and Fibre Channel diagnostic capabilities provide early warning to conditions that might be hampering the performance of HP storage, ensuring that your data is always available. Command View contains SNMP scripts, making it easy to integrate into leading network management frameworks.

HP StorageWorks Command View XP is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See http://www.hp.com/products1/storage/products/disk_arrays/xpstoragesw/commandview/index.html for more information and access to documentation.

HP StorageWorks Command View XP Advanced Edition overview

HP StorageWorks Command View XP Advanced Edition for XP disk arrays combines the best features of Command View XP together with additional wizard-based modules that are easy to use. It provides for seamless integration into higher level management utilities such as Storage Essentials. It can centrally manage, configure, provision, and monitor XP disk arrays.

HP StorageWorks Command View XP Advanced Edition for XP disk arrays is available through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information on accessing the **System Page**.

HP StorageWorks 1000 Modular Smart Array overview

The HP StorageWorks 1000 Modular Smart Array (MSA1000) is a 2-GB Fibre Channel storage system for the entry-level to midrange storage area network (SAN). The MSA1000 reduces the complexity and risk of SAN deployments. The powerful but easy-to-use management software makes it ideal for departmental and remote location SANs. With the addition of two more drive enclosures and the new 300-GB drives, it can control up to 42 drives allowing capacity of 12 TB. All configuration, management, partitioning, and licensing software come standard with no extra charges.

The HP exclusive optional embedded eight-port SAN switches or three-port hubs give cost-effective and space saving methods of creating a SAN environment. The MSA1000 supports Windows (32 and 64-bit), NetWare, and Linux (32 and 64-bit) operating systems. It also supports Tru64 UNIX, OpenVMS, or HP-UX operating systems.

The MSA1000 is accessible through HP Systems Insight Manager (HP SIM) from the **Tools & Links** tab on the **System Page**. See “Tools & Links tab” for information about accessing the **System Page**.

See <http://h18006.www1.hp.com/products/storageworks/msa1000/index.html> for more information and access to documentation.

HP Service Essentials Remote Support Pack

Overview

The HP Service Essentials Remote Support Pack provides proactive remote monitoring, automated diagnosis, and troubleshooting to help improve the availability of HP-supported servers and storage devices in your data center. The Remote Support Pack reduces cost and complexity in support of systems and devices. The Remote Support Pack securely communicates service incident information through your firewall and/or Web proxy to the HP Support Center for reactive support.

Remote Support Software Manager

The Remote Support Software Manager is installed on the CMS during the HP SIM installation. The Remote Support Software Manager is included for Typical HP SIM installations, and is the default for Custom installations. The Remote Support Software Manager installation is non-interactive. Once installed, the Remote Support Software Manager application can be launched from the CMS. After the HP SIM installation is complete, you must configure the Remote Support Software Manager to fit your enterprise specifications. Once configured, the Remote Support Software Manager downloads and installs the most current suite of Remote Support applications, including:

- Remote Support tool
- Remote Support Common Components (MC3)
- Open Service Event Manager (OSEM)

See the *HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows at HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about setting up Remote Support Pack with HP SIM.

Remote Support tool

The Remote Support tool facilitates the submission of service incidents from monitored devices and establishes remote connectivity back to HP for reactive support based on service obligation. The Remote Support tool is accessed through the HP SIM interface and coordinates remote monitoring and event status for qualified devices in the Enterprise. It provides automated case creation and handling, and supplies entitlement information such as warranty and contract attributes to HP SIM.

You can access, configure, register, and use the Remote Support tool with HP SIM by selecting **Options**→**Remote Support Configuration and Services**. The Remote Support Configuration and Services page allows you to enable Remote Support for eligible systems.

See “Service notification events” for information about viewing service incidents in HP SIM.

See “Viewing contract and warranty information” for information about viewing contract and warranty information in HP SIM.

Remote Support Common Components

The Remote Support Common Components collect configuration data to determine the unique identification of devices, and supply this information to the Remote Support tool.

Open Service Event Manager

OSEM analyzes SNMP events and data for serviceable events, provides automated diagnosis of hardware problems, supplies recommended actions and customer self repair procedures, and submits service notifications to HP SIM and the Remote Support tool.

See “Service notification events” for information about viewing service incidents in HP SIM.

Using HP SIM with the Remote Support Pack

When you use the Remote Support Pack and HP SIM together on a Windows CMS, you can monitor and view contract and warranty data for HP systems in the HP SIM user interface. Contract and warranty data is obtained through communication with HP data centers. Information such as a system's serial number, product ID, or contract ID is sent to HP data centers in order to retrieve the warranty and contract details.

See “Viewing contract and warranty information” for details about where you can view Remote Support information in the HP SIM user interface.

Related topics

- Suspending or resuming contract and warranty data collection for a single system
- Suspending or resuming contract and warranty data collection for multiple systems
- Editing system properties for a single system
- Editing system properties for multiple systems
- Service notification events

- About default system functions
- Viewing contract and warranty information
- Contract and warranty status types
- Viewing contract and warranty status
- About default system functions
- Navigating the system table view page
- System tab
- System tab for management processors
- Reporting
- Search criteria
- Navigating the event table view page
- Default shared collections

Viewing contract and warranty information

Introduction

The **Contract and Warranty Status** is available when you have a Windows CMS and the HP Service Essentials Remote Support Pack is installed. You can view Contract and Warranty status updates for HP systems that have contract and warranty data collection enabled. Click the **Contract and Warranty Status** icon to view the **Contract and Warranty Details** page for the system.

The following requirements must be met in order to view contract and warranty data in HP Systems Insight Manager (HP SIM):

- The HP SIM CMS must have connectivity to <http://www.hp.com>.
- The Remote Support Pack software must be installed and properly configured. The Remote Support Software Manager is installed on the Central Management Server during the HP SIM installation. After the HP SIM installation is complete, you must configure the Remote Support Software Manager to fit your enterprise specifications. Once configured, the Remote Support Software Manager will download and install the Remote Support tool. The Remote Support tool must be installed, configured, and registered before you can retrieve contract and warranty data. See the *HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows at HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about setting up Remote Support Pack with HP SIM.
- To collect contract and warranty data for a system, the system's serial number, product ID, and country code must be present in the system properties. In most cases, the serial number and product ID are obtained during HP SIM's identification process. You can enter a serial number and product ID if needed. It is important to specify the correct country code to ensure accurate information. If HP SIM cannot obtain a country code, it defaults to *US*. If you have a support contract, enter an entitlement or obligation identifier and entitlement type if you want to view contract data.
See "Editing system properties for a single system" or "Editing system properties for multiple systems" for instructions on editing system properties.

Viewing contract and warranty information

You can view contract and warranty information by:

- Clicking the **CW** icon in the system table view page. See "Navigating the system table view page" for more information.
- Clicking the **Contract and Warranty status** link on the system page. See "System Page" for more information.
- Viewing a **Warranty-Contract** report. See "Reporting" for more information.
- Searching for systems with contracts or warranties that expire in a specified number of days. See "Performing an advanced search for systems" for more information.

- Configuring alerts for systems with expiring contracts or warranties. See “Creating an automatic event handling task” for more information.
- Viewing the initial and monthly contract and warranty data collection tasks. See “Navigating the All Scheduled Tasks page” and “About default system functions” for more information.
- Viewing the **Remote Support Eligible** collection, which lists systems the Remote Support Pack supports if you choose to enable them for support and are entitled to support. If a system is enabled without proper entitlement, events are submitted to the Remote Support tool, but they are not monitored and will not trigger a response.



NOTE: If you receive an incorrect response for a particular HP brand system after clicking the **CW** icon on the system table view page, there might be an entitlement issue with the system. This is not a Remote Support or an HP SIM issue. Please contact HP support. You must have a valid serial number and product ID along with any contract or Care Pack numbers that are applicable.

Collecting contract and warranty data

The following tasks are used to collect contract and warranty data:

- **Initial contract and warranty collection.** This task collects contract and warranty data from newly discovered systems. If the required system properties are not entered for a new system or automatically collected by HP SIM during *identification*, contract and warranty data will not be collected.
- **Monthly contract and warranty collection** This task collects contract and warranty data every month. If the required system properties are not entered for a system or automatically collected by HP SIM during identification, contract and warranty data will not be collected.



NOTE: See “Editing system properties for a single system” or “Editing system properties for multiple systems” for instructions on editing system properties.

If you want to run the Contract and Warranty Collection task immediately for an updated system, select **Options**→**Contract and Warranty Data Collection**. See “Creating a task” for more information.



IMPORTANT: Running the contract and warranty collection task more than once a month is not recommended or needed since the data does not often change.

Related topics

- Suspending or resuming contract and warranty data collection for a single system
- Suspending or resuming contract and warranty data collection for multiple systems
- Editing system properties for a single system
- Editing system properties for multiple systems
- Service notification events
- About default system functions
- Contract and warranty status types
- Viewing contract and warranty status
- About default system functions
- Navigating the system table view page
- System tab
- System tab for management processors
- Reporting
- Search criteria
- Navigating the event table view page

- Default shared collections
- HP Service Essentials Remote Support Pack

Viewing contract and warranty status

Overview

The **Contract and Warranty Status** page is available when you click the **CW** icon on the system table view page or the **Contract and Warranty Status** link on the system page. This page lists **System Information** and contract and warranty details.



NOTE: If you receive an incorrect response for a particular HP brand system after clicking the **CW** icon on the system table view page, there might be an entitlement issue with the system. This is not a Remote Support or an HP SIM issue. Please contact HP support. You must have a valid serial number and product ID along with any contract or Care Pack numbers that are applicable.

NOTE: A system can have multiple contracts and warranties.

System Information

- **System Name.** The system name or IP address.
- **Serial Number.** The system serial number. This can be the serial number discovered by HP SIM or the number you entered in the **Customer-Entered serial number** field on the **Edit System Properties** page.
- **Product ID/Number** The product number. Typically, the product number is the number used to order a system.
- **Product Line.** Details about the product line.

Contract

- **CCRN (Customer Contract Reference Number).** The reference used for the contract as renewed over time.
- **Active Contract.** This value is **true** if an active contract exists.
- **Start Date.** The start date of an active contract.
- **End Date.** The end date of an active contract. If no end date is available, this field is blank.
- **Contract Status.** The possible values are:
 - A: Active.
 - F: The start date is in the future.
 - X: Expired.
 - E: There is no end date.
 - I: The agreement is informal. This status might mean that the agreement is not finalized.
 - B: Delivery blocked
 - C: Cancelled.
- **Active Obligation.** This value is **true** if there is an active support contract for a system.

The contract start and end date is listed for each contract item along with the following information:

- **Status** The possible values are:
 - A: Active.
 - F: The start date is in the future.
 - X: Expired.

- E: There is no end date.
- I: The agreement is informal. This status might mean that the agreement is not finalized.
- B: Delivery blocked
- C: Cancelled.
- **Service Level.** The level of service specified in the offer. This includes the amount of time HP has to react to an issue, the time to resolution for a set of issues, and the type of response HP will use to react to an issue.
- **Deliverables.** A description of services offered with this contract, for example, onsite support or parts and materials.

Warranty

- **Warranty Type.** The type of warranty, for example, Base Warranty, Bundled Warranty, or HP Care Pack.
- **Start Date.** The start date of an active warranty.
- **Extension.** The number of days that this warranty has been extended.

The warranty start and end date is listed for each warranty item along with the following information:


- **Status.** The possible values are:
 - A: Active.
 - F: The start date is in the future.
 - X: Expired.
 - E: There is no end date.
 - I: The agreement is informal. This status might mean that the agreement is not finalized.
 - B: Delivery blocked
 - C: Cancelled.
- **Service Level.** The level of service specified in the warranty. This includes the amount of time HP has to react to an issue, the time to resolution for a set of issues, and the type of response HP will use to react to an issue.
- **Deliverables.** A description of services offered with this warranty, for example, onsite support or parts and materials.






Related topic

- [Suspending or resuming contract and warranty data collection for a single system](#)
- [HP Service Essentials Remote Support Pack](#)
- [Contract and warranty status types](#)
- [Editing system properties for a single system](#)

Contract and warranty status types

If you have a Windows Central Management Server (CMS) and the HP Service Essentials Remote Support Pack is installed, you can monitor contract and warranty status in the HP SIM user interface. Contract and warranty status is shown by the following status types:

Status Icon	Icon Meaning	Description
	Major	The contract or warranty is expired

Status Icon	Icon Meaning	Description
	Minor	<ul style="list-style-type: none"> Contract information is temporarily unavailable. The contract expires in 30 days.
	Warning	The contract expires in 90 days.
	Normal	The system has a valid contract or warranty.
	Unknown	No contract information was found. The system might not have a serial number or product ID.
	Disabled	The Do not collect contract and warranty data for this system option is set for the system.

Related topic

- [HP Service Essentials Remote Support Pack](#)
- [Viewing contract and warranty information](#)
- [Viewing contract and warranty status](#)
- [Suspending or resuming contract and warranty data collection for a single system](#)
- [Suspending or resuming contract and warranty data collection for multiple systems](#)
- [Editing system properties for a single system](#)
- [Editing system properties for multiple systems](#)
- [Navigating the system table view page](#)
- [System tab](#)
- [System tab for management processors](#)

Suspending or resuming contract and warranty data collection for a single system

The **Suspend/Resume Contract and Warranty Data Collection** link allows you to exclude this system from contract and warranty data collection. When a system is suspended, it has a disabled **Contract and Warranty Status**.



NOTE: To complete this procedure, you must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the system you want to update.

To suspend or resume contract and warranty data collection on a single system:

1. Select **Tools**→**System Information**→**System Page**. The **System Page** appears.

Note: You can also access the **System Page** by selecting a system name in the **System Name** column of the system table view page.
2. Select the target system. See "Creating a task" for more information.
3. Select the **Tools & Links** tab.
4. Click the **Suspend/Resume Contract and Warranty Data Collection** link. The **Suspend/Resume Contract and Warranty Data Collection** page appears.
5. Select or clear the **Do not collect contract and warranty data for this system** check box to suspend or resume contract and warranty data collection.
6. Click **OK** to apply the changes or click **Cancel** to cancel changes. After clicking **OK** or **Cancel** you are returned to the **Tools & Links** tab.

Related procedure

- ▲ Suspending or resuming contract and warranty data collection for multiple systems

Related topics

- System Page
- Contract and warranty status types
- HP Service Essentials Remote Support Pack
- Viewing contract and warranty information
- Editing system properties for a single system
- Editing system properties for multiple systems

Suspending or resuming contract and warranty data collection for multiple systems

The **Suspend/Resume Contract and Warranty Data Collection** link allows you to exclude the target systems from contract and warranty data collection. When a system is suspended, it has a disabled **Contract and Warranty Status**.



NOTE: To complete this procedure, you must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the systems you want to update.

To suspend or resume contract and warranty data collection on multiple systems:

1. Select **Options**→**System Properties**→**Suspend or Resume Contract and Warranty Data Collection**. The **Suspend or Resume Contract and Warranty Data Collection** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. You can click **Add Targets** to add additional systems or select targets and click **Remove Targets** to remove the systems.
4. Select or clear the **Do not collect contract and warranty data for target systems** check box to suspend or resume contract and warranty data collection.
5. Click **Previous** to select different target systems, click **Schedule** to schedule the task, or click **Run Now** to run the task immediately.

Related procedure

- ▲ Suspending or resuming contract and warranty data collection for a single system

Related topics

- System Page
- System tab
- Tools & Links tab
- Suspending or resuming contract and warranty data collection for a single system

14 Reporting

HP Performance Management Pack reporting

HP Performance Management Pack (PMP) reports are available through HP Systems Insight Manager (HP SIM) on Windows systems. See “PMP reporting options” for more information.

To view the System Information Reporting options,

select **Reports**→**HP Performance Management Pack Reports**→**Static Analysis Report**.

System Information Reporting

The HP SIM System Information Reporting feature enables you to generate reports. In addition to generating reports, you can create customer-defined report configurations and edit, copy, and delete report configurations. All *users* with sign-in access to HP SIM can generate reports.



NOTE: To add a new report, see “Adding a report”.

The System Information Reporting feature provides you with the following options:

- **Managing Reports.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears.
- **Running Reports.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report that you want to run. Select the **HTML**, **XML**, or **CSV** report format. Click **Run Report**.
- **Creating New Reports.** Select **Reports**→**New Report**. The **New Report** page appears.
- **Creating New Reports from the Manage Reports Page.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Click **New**. The **New Report** section appears.
- **Editing Reports.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report that you want to edit, and then click **Edit**. The **Edit Report** section appears.
- **Copying Reports.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report that you want to copy, and then click **Copy**. The **Copy report** section appears.
- **Running Reports in HTML Format.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report you want to run in HTML format, select **HTML**, and then click **Run Report**.
- **Running Reports in XML Format.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report you want to run in XML format, select **XML**, and then click **Run Report**.
- **Running or Downloading Reports in CSV Format.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report you want to run, or download the report in Comma Separated Value (CSV) format, select **CVS**, and then click **Run Report**.
- **Showing SQL Queries.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report you for which want to view the SQL details, select **Run Report**, and then on the report itself, click **Show SQL queries**.
- **Deleting Reports.** Select **Reports**→**Manage Reports**. The **Manage Reports** page appears. Select the report to be deleted, and then click **Delete**.

Snapshot comparison

Snapshot comparisons enable you to compare up to four systems (with the same operating system) to each other or to compare a single system to itself and observe changes over time. See “Snapshot comparison reporting” for more information.

To view a snapshot comparison, select **Reports**→**Snapshot Comparison**. The **Snapshot Comparison** page appears. Select target systems, and then click **Next**.

Related procedures

- System reporting
- Adding a report
- Editing a report
- Copying a report
- Snapshot comparison reporting
- PMP reporting options

Related topics

- System license information reporting
- Printing a cluster collection view
- Printing an event collection view
- Printing reports
- Reference information
- Reporting views
- User and user group reports
- Toolbox report
- Authorizations report

System reporting

A generated report provides you with the following information:

- Report name
- Associated system collection



NOTE: The Associated system collection information is not displayed if there is no collection selected to run the report.

- Report run date and time

Reports can be run in the following formats:

- **HTML (Recommended for viewing).** This option displays the report in HTML format.
- **XML.** This option displays the report in XML format.
- **CSV.** This option displays the report in CSV format.



NOTE: The default sort order is based on the system name.

NOTE: You can click any column heading to sort in ascending or descending order.

NOTE: You can also access the **Manage Reports** page from the **Manage** section of the HP Systems Insight Manager (HP SIM) **Home** page by clicking the **Manage inventory reports** link.

Running an existing report in HTML format

To view a report, HP recommends that you use the HTML format.

To run a report in HTML format:

1. Select **Reports**→**Manage Reports**.
2. Select the report you want to view.
3. Under **Format for generated report**, select **HTML (Recommended for viewing)**.
4. Click **Run Report**. The report appears.

The HTML report enables you to **Show SQL queries**. See “Showing SQL” for more information.

Selecting the sort order

The Reporting feature enables you to sort the data after it displays in the **Report Results** page.

- **Ascending Order.** Click the column heading you want to sort by once. The data queries in ascending alphabetical order.
- **Descending Order.** Click the column heading you want to sort by twice. The data queries in descending alphabetical order.

Viewing an existing report in XML format

1. Select **Reports**→**Manage Reports**.
2. Select the report you want to view.
3. Under **Format for generated report**, select **XML**.
4. Click **Run Report**. The XML report appears.

Viewing an existing report in CSV format

1. Select **Reports**→**Manage Reports**.
2. Under **Report Name**, select the report you want to view.
3. Under **Format for generated report**, select **CSV**.
4. Click **Run Report**. If the browser system has no application associated with .CSV files, then the .CSV file is displayed in the browser window. If you have an application associated with .CSV files, then the .CSV file is displayed in the specified application.

If you are using Internet Explorer and an application such as Excel is installed on the browser system and the .CSV file extension is associated with that application, the **Save As** dialog box appears. Click **Save**.

5. Name the file, and in the **Save as type** field, select a format in which to save the file from the dropdown list. Click **Save**. The report is saved.

Printing an existing report

From the **Report Results** page, select **File**→**[Print]** from your browser.

Command line interface

Use the `mxreport` command to perform this task from the command line interface (CLI). For assistance with this command, see the HP-UX or Linux manpage by entering `man mxreport` at the command line. See “Using command line interface commands” for more information about the command and a link to the manpage.

Related procedures

- Adding a report
- Editing a report
- Copying a report

Related topic

- ▲ Reporting

Adding a report

You can save the report configuration for future use or generate a one-time report.

A report configuration is a customer-defined set of preferences that pulls specified criteria from the *database* tables and places it in a report in the specified format. The report configurations can be saved and used to run a report at a later date with live data.

You must have administrative or *operator rights* to create, save, edit, copy, or delete report configurations. In addition, you must have *administrative rights* to view a license *key*. *Users* with *user rights* can run the authorized report configurations only.

You can also create a new report by selecting **Reports**→**Manage Reports**→**[New]**.

If Customer 1 with administrative rights generates a report and a private collection, then Customer 2 with administrative rights is allowed to generate a report using the report configuration and private collection that Customer 1 created. Customer 2 is allowed to edit, save, copy, and delete the report configuration but cannot delete the private collection created by Customer 1.

Adding a new report

1. Select **Reports**→**New Report**. The **New Report** window appears.
2. Add multiple or single targets:
 1. To add targets, you can choose one of two radio buttons above the drop-down selection box, either the **Collection** option or the **Search** option which is used to indicate the method of target selection or click **Cancel** which will result in no additions.

Note: You are not allowed to select individual events for Targets or Filters, so the ability to search will not be available when those selections are made. The two radio buttons will not be present in these cases.
 2. Choosing the **Collection** option will allow you to select targets from the drop-down selection box.
 3. If you choose the **Search** option, the drop-down selection box and **View Contents** button will be replaced with the **Quick Search** user interface. Type a **Device Name** into the **Text Field** and then click **Search**.

Note: If there are **Device Names** that match the characters typed in the **Text Field**, a dynamic list is displayed with those matches.
 4. If you select one of the **Device Names** displayed in the dynamic list, a **System Table** containing the selected system will be displayed below the **Quick Search** user interface. Items displayed in the **Search Results** table will be selected (checked) by default and the **Apply** button will be enabled as long as there is at least one item from the **Search Results** table selected. Only items that are selected will be added when you click **Apply**.

Note: The maximum number of **Device Names** displayed is six.
 5. If you click **Search**, a **Basic Search** using common attributes will be performed using the characters typed into the **Text Field**. The results will be displayed in the **Search Results** table below the **Quick Search** user interface.

While the search user interface remains open, the **Task Wizard** will retain a reference to the **Query** object created to perform the **Dynamic Query** generation used when performing searches. Each new search term will be added to this **Query** object and a new **Dynamic Query** will be generated. The **Task Wizard** will release its reference to the search **Query** when you close the search user interface or by clicking **Cancel** or **Apply**.

Note: A barbershop pole will be seen while **Basic Search** results are loading.

Once you choose the system to add, the **Select <item> itself** checkbox is checked by default and the **Apply** button and **View Contents** button are enabled. You can choose to click **Apply** or **View Contents**.

Note: If you choose to change the selected item in the drop-down selection box, the **Select <item> itself** text will be updated to reflect the change.

Note: If the **Select <item> itself** checkbox is unchecked, the **Apply** button will become disabled.

Selecting **View Contents** will display the **Table View** or **Tree View** of the selected item and the **Apply** button will become disabled.

Note: When **View Contents** is selected, the **Target Selection Page** displays a barbershop pole and the message *"Please wait while the data is loading"* while the **Table View** or **Tree View** is loading.

Once you select items from the displayed **Table View** or **Tree View**, the **Apply** button becomes enabled.

Note: If the **Select <item> itself** checkbox is checked while a **Tree View** is displayed, the **Tree View** will be closed and the **Apply** button will become enabled. If you uncheck the **Select <item> itself** checkbox, the **Tree View** will not be redisplayed. You must click **View Contents** in order to have the **Tree View** displayed again.

3. To filter target selections, complete the following.
 - a. Click **Add Event Filter**.
 - b. From the **Add filters by selecting from** dropdown box, select an event filter. If you do not select an event filter, an error message appears.
 - c. Click **Apply** to apply the filter to the target systems (or, click **Cancel** to cancel adding a filter). The **Filtered by** table appears below the list of selected target systems.

Note: If the target selections are events instead of systems, the button changes to **Add System Filter** and you can select from different system collections. Unlike event filters, you can select multiple system filters.



4. To modify an event filter, click **Modify Event Filter**.

Note: If the filters are systems, you will see an **Add System Filters** and **Remove Filters** buttons. If there is only one event filter, the **Remove Filters** button will simply remove the single event filter. If you have more than one event filters, the **Remove Filters** button will open a sub-pane that you may select the event filters to remove.

 - a. From the **Add filters by selecting from** dropdown box., select an event filter. If you do not select an event filter, an error message appears.
 - b. Click **Apply** to change the event filter and apply the filter to the target systems, or click **Cancel** to cancel editing the filter.

Note: If the target selections are events instead of systems, the button does not change to **Modify System Filter** you will have the option to select either the **Add System Filters** or **Remove Filters**. It is possible to have one or more system and event combination collections already selected. If there are combination collections selected, they will provide filtering.

5. To remove a filter, select the filter(s) from the sub-pane that you wish to remove and click **Remove Filters**.
6. **Next.** Click **Next** to specify parameters and to run or save the report.
7. After you click **Next**, the **Step 2: Specify Parameters** page appears.
 - a. In the **Report Name** field, enter a name for the report.

Important: Report names cannot contain any of the following characters: < > ' & \ ` , # + | % ; / \\ ! ~ @ \$ ^ * = { } [] " : and ?
 - b. In the **Select items to show in report** section, select all of the categories or items to include in the report. You can click the  icon to expand a category, and then select specific items or click the  icon to collapse a category.
 - c. After you have selected all items to include in the report, select one of the following options:
 - **Show all systems in the same table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and the selected data items appear as column headers in the report. All *systems* appear in the same table.
 - **Show each system in a separate table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and all the selected data items appear as column headers. Each system appears in an individual table.

8. Under **Format for generated report**, select from the following options:
 - **HTML (Recommended for viewing).** This option displays the report in HTML format.
 - **XML.** This option displays the report in XML format.
 - **CSV.** This option displays the report in CSV format.
9. To save the report configuration, click **Save Report**. If the report already exists, the **overwrite report** message appears. Click **Cancel** if you do not want to overwrite the existing report.
10. Click **Run Report**.

The new report appears, providing you with the **Show SQL Queries** option:

Selecting the sort order

The Reporting feature enables you to sort the data when it displays on the **Report Results** page.

- **Ascending Order.** Click the column heading you want to sort by once. The data requeries in ascending alphabetical order.
- **Descending Order.** Click the column heading you want to sort by twice. The data requeries in descending alphabetical order.

Printing the report

On the **Report Results** page, select **File**→**[Print]** from your browser.

Command line interface

Use the **mxreport** command to perform this task from the command line interface (CLI). For assistance with this command, see the HP-UX or Linux manpage by entering `man mxreport` at the command line. See “Using command line interface commands” for more information about the command and a link to the manpage.

Related topics

- System reporting
- Editing a report
- Copying a report

Related topic

- ▲ Reporting

Editing a report

HP Systems Insight Manager (HP SIM) enables you to edit existing report configurations. You can save these updated report configurations over the existing report configuration, or you can save it as a new report configuration.





NOTE: You must have *administrative rights* or *operator rights* to create, save, edit, copy, or delete report configurations. In addition, you must have administrative rights to view a license *key*. Users with *user rights* cannot edit the report configurations.

You can also access the **Manage Reports** page from the HP SIM **Home** page, **Manage** section by clicking the **Manage inventory reports** link.

To edit an existing report:

1. Select **Reports**→**Manage Reports**. The **Manage Reports** window appears.
2. Select the report to edit, and then click **Edit**. The **Edit Report** page displays.

3. After you click **Next**, the **Step 2: Specify Parameters** page appears.
 - a. In the **Report Name** field, enter a name for the report.
Important: Report names cannot contain any of the following characters: < > ' & \ ` , # + | % ; / \\ ! ~ @ \$ ^ * = { } [] " : and ?
 - b. In the **Select items to show in report** section, select all of the categories or items to include in the report. You can click the  icon to expand a category, and then select specific items or click the  icon to collapse a category.
 - c. After you have selected all items to include in the report, select one of the following options:
 - **Show all systems in the same table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and the selected data items appear as column headers in the report. All *systems* appear in the same table.
 - **Show each system in a separate table.** This option displays all categories and items selected in the **Select items to show in report** section in the report. The selected categories appear as tables, and all the selected data items appear as column headers. Each system appears in an individual table.
4. Under **Format for current run of generated report (format not saved with report)**, select from the following options:
 - **HTML (Recommended for viewing).** This option displays the report in HTML format.
 - **XML.** This option displays the report in XML format.
 - **CSV.** This option displays the report in CSV format.
5. To save over the existing report configuration, click **Save Report**.
Note: To save an existing report as a report with a new name, enter a new report name in the **Report Name** field, and then click **Save Report**. The new report is saved and added to the report list on the **Manage Reports** page.
 A dialog box appears, asking you to confirm your intention to save the report. Click **OK** to save, or click **Cancel** to abort. If the report already exists, the **overwrite report** message appears. Click **Cancel** if you do not want to overwrite the existing report.
6. To view the report, click **Run Report**. You can click **Previous** to return to the target selection page. You can click **Cancel** to abort the report creation process.

Command line interface

Use the `mxreport` command to perform this task from the command line interface (CLI). For assistance with this command, see the HP-UX or Linux manpage by entering `man mxreport` at the command line. See “Using command line interface commands” for more information about the command and a link to the manpage.

Related procedures

- Adding a report
- Showing SQL
- System reporting

Related topic

- ▲ Reporting

Copying a report

HP Systems Insight Manager (HP SIM) enables you to copy report configurations from an existing report configuration. You can edit the newly copied configurations to create a new report.



NOTE: You must be signed-in to HP SIM with *administrative rights* or *operator rights* to copy report configurations. If you are not signed-in with administrative or operator rights, the copy option is not available.

NOTE: You can also access the **Manage Reports** page from the **Manage** section of the HP SIM **Home** page, by clicking the **Manage inventory reports** link.

To copy a report configuration:

1. Select **Reports**→**Manage Reports**. The **Manage Reports** window appears.
2. Select the report to copy, and then click **Copy**. The **Copy report** section appears.
3. In the **Report Name** field, enter a name for the new report configuration.

Important: Report names cannot contain any of the following characters: < > ' & \ ` , # + | % ; / \\
! ~ @ \$ ^ * = { } [] " ' : and ?

4. Click **OK**.

The **Copy report** section closes, and the copied report configuration appears in the **Manage Reports** section.

Command line interface

Use the `mxreport` command to perform this task from the command line interface (CLI). For assistance with this command, see the HP-UX or Linux manpage by entering `man mxreport` at the command line. See “Using command line interface commands” for more information about the command and a link to the manpage.

Related procedures

- System reporting
- Adding a report
- Editing a report
- Showing SQL
- Snapshot comparison reporting

Related topic

- ▲ Reporting

Deleting a report

You can permanently delete a report configuration from the **Manage Reports** page.

To delete a report configuration:

1. Select **Reports**→**Manage Reports**. The **Manage Reports** page appears.
2. Select the report configuration to be deleted.
3. Click **Delete**. A dialog box displays asking you to confirm your intention to delete the selected report.
4. Click **OK** to permanently delete the report configuration. You can click **Cancel** to abort the delete operation.

Related procedures

- System reporting
- Editing a report
- Copying a report

Related topic

- ▲ Reporting

Showing SQL

You can view the SQL details behind a report. The **SQL Queries** page details all SQL queries that are used to generate the report.

To show the SQL queries:

1. Select **Reports**→**Manage Reports**. The **Manage Reports** page appears.
2. Select the report for which you want to see the SQL details.
3. Click **Run Report**. The report appears.
4. Click the **Show SQL queries** link.
The **SQL Queries** page appears.

Related procedure

- ▲ System reporting

Related topic

- ▲ Reporting

Reporting views

Reporting uses the following *database* views to generate reports.

Database views

Several database views are included with HP Systems Insight Manager (HP SIM). These views can be used to generate reports in HP SIM. The following views are available:

R_ArrayControllers	R_Batteries	R_CellularSysCell
R_CellularSysParComplex	R_CellularSysPartition	R_CellularSysParIOChassis
R_ChangerDevices	R_CPU	R_deviceLicenseInfo
R_DIMMSlots	R_EventSummary	R_Fans
R_HPVMGuests	R_InstalledBoards	R_Inventory
R_lockdownStatus	R_LogicalDisks	R_MediaAccessDevices
R_NetworkInterface	R_OperatingSystem	R_PhysicalDisks
R_PowerSupply	R_Process	R_Racks
R_Software	R_SWFWBaselineInformation	R_StorageDeviceInventory
R_StorageDeviceControllers	R_StorageHostBusAdapters	R_StoragePorts
R_StorageLogicalUnits	R_StorageDeviceCapacity	R_UnixOSDetails
R_UnixLogicalMemory	R_UnixIODevices	R_WarrantyContract
R_UnixIPRoute	R_HPUXFileSystem	R_HPUXVolumeGroup
R_HPUXLogicalVolume	R_HPUXLogicalVolume	R_HPUXNetworkDetails
R_HPUXKernelParam	R_HPUXSoftwareBundle	R_HPUXSoftwareProduct

R_ArrayControllers

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
BoardName	Board name
Model	Controller model
Version	Controller Product Revision number
FirmwareRev	Board firmware revision
SerialNumber	Controller Serial number
SlotNumber	Slot number in the system
SnapshotID	Snapshot ID
Tag	Tag

R_Batteries

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
SerialNumber	Serial number
AssetNumber	Asset tag number
SnapshotID	Snapshot ID
Tag	Tag

R_CellularSysCell

Column name	Description
DeviceKey	Device key
DeviceName	Name of the system
CellID	Cell ID number
CellType	Cell type
ComplexName	Complex name
PartitionID	Partition ID
TotalMemoryInstalled	Total memory installed
TotalMemoryOK	Total memory OK
TotalCPUInstalled	Total CPU installed
TotalCPUOK	Total CPU OK
CabinetNumber	Cabinet location
SlotNumInCabinet	Cell location
State	State of the cell
BoardSpeed	Cell speed
CellArchitecture	Cell architecture
FirmwareRevision	Firmware revision
SnapshotID	SnapshotID

R_CellularSysParComplex

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
ComplexName	Complex name
ComputeCabinets	Number of compute cabinets in the complex
IOCabinets	Number of IOX cabinets in the complex
SnapshotID	SnapshotID
MaxPartitionsSupported	Maximum partitions supported
ProductName	Product name

R_CellularSysPartition

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
PartitionName	Partition name
IPAddress	IP address
TotalCPUCore	Number of CPUs in the partition
InstalledCells	Number of installed cells in the partition
PoweredonCells	Number of powered up cells in the partition
CoreCell	Index to cpqSeCellTablePtr for core cell in the partition
CoreCellCabinet	Index to cpqSeCellTablePtr for core cell in the cabinet
HasInterleaveMemory	When set, indicates that there is an interleaved memory configured in the partition
#ActiveCells	Number of alive cells
OSType	Operating system type
SnapshotID	SnapshotID

R_CellularSysParIOChassis

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
PartitionName	Partition name
CabinetNumber	Represents the cabinet to which the I/O chassis belongs
IOBayNumber	Indicates the bay in the cabinet where the I/O chassis resides
IOChassisNumber	The I/O chassis number that is unique across the bay
SnapshotID	SnapshotID

R_ChangerDevices

Column name	Description
DeviceKey	Device key
DeviceID	Device ID
SnapshotID	Snapshot ID
Name	Name of changer device
FirmwareVersion	Firmware version
OperationalStatus	Status
SystemName	Name of parent system

R_CPU

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
CPUType	Type of CPU

Column name	Description
CPU Speed	CPU speed
SlotNumber	Slot number in the system
SnapshotID	Snapshot ID
FirmwareID	Processor firmware ID
ProcessorLoad	Processor load
ProcessorAllocated	Processor status: 1=Allocated; 0=Not allocated
Location	Location for 64-bit Intel® platform systems (This field is blank for all other systems.)
CellNumber	Cell number
ArchitectureRevision	Architecture revision
FirmwareRevision	Firmware revision
DataWidth	Data width
DeviceID	Device ID
WorkingSetSize	Size of working set

R_deviceLicenseInfo

Column name	Description
deviceKey	System key
numberLicPurchased	The number of licenses purchased for this key
numberLicUsed	Actual number of licenses in use for this particular license key and system
keyVer	The version of the key in use
licKey	The key the customer has entered (This column can be blank if you restrict the Integrated Lights-Out (iLO) response to HP SIM requests for license information. This column is not displayed if you do not have permission to view license keys.)
licType	The type of license on the system
licDate	The date the license was applied
productName	The name of the product
productVer	The version of the product; can be blank
expirationDate	The date the product expires
collectDate	The date the collection last took place by HP SIM
DeviceName	Name of system associated with system key
licStatus	License status
SnapshotID	SnapshotID
deviceKey	Device key
deviceSN	Device serial number
nodeName	Device name

Column name	Description
licenseType	0001b – Flexible Quantity License (FQL) 0010b – Demo (time) 0011b – BETA 0100b – Demo License (seats and time) 0101b – Activation Key Agreement (AKA) 0110b – reserved 0111b – Free Flexible Quantity License (FFQL) 1000b – Subscription License 1001b – Site License (SITE) 1010b – Maintenance License (ML)
productName	Product name
productVersion	Product version
seatsUsed	Number of seats used
daysMax	Maximum number of days
daysUsed	Number of days used
status	Status
pexpire	License expiration date, if any
licenseSource	Displays Purchased or Free trial
pupgrade	Updates and upgrades: For iLO2, always displays Purchase Separately For servers: Included if the license has not been used Included until <date> if the license is in use
support	Technical support: For iLO2, always displays Purchase Separately For servers: Included if the license has not been used Included until <date> if the license is in use
SnapShotID	Snap shot ID

R_DIMMSlots

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
FormFactor	Type of memory module installed
MemorySize	Memory size in kilobytes
PartNumber	Memory module manufacturer part number
SerialNumber	Memory module serial number
SlotNumber	Slot number in the system
MemoryType	Memory type
MemoryTech	Technology type of memory module installed
Location	Location for 64-bit Intel® platform systems (This field is blank for all other systems.)
SnapshotID	Snapshot ID

Column name	Description
LocationID	Location ID
Description	Description
BankLabel	Bank label
Tag	Tag

R_EventSummary

Column name	Description
DeviceName	Name of the event
Severity	Event severity
Type	Event type
CallStatus	Reference to string map for third-party status
CallID	Used for HP Service Essentials Remote Support Pack/WEBES event ID
ClearedStatus	Event cleared status
ReceivedTime	Event received time
ModifiedTime	Event modified time
ClearedTime	Event cleared time
Description	Detail description of the event
AssignedTo	Assigned to user
Comment	Comments

R_Fans

Column name	Description
DeviceKey	Device key
DeviceName	Name of the system
FanName	Name of the fan
HwLocation	Hardware location
Type	Fan type
DeviceID	Device ID of the fan
Description	Description of the fan
Version	Version number of the fan
Manufacturer	Manufacturer of the fan
SerialNumber	Serial number of the fan
ActiveCooling	Active cooling status
SnapshotID	SnapshotID
PhysicalPosition	Physical position of the fan

R_HPVMGuests

Column name	Description
DeviceKey	Device key
DeviceName	Name of the guest system

Column name	Description
IPAddress	Host IP address
VMName	VM guest name
VMNumber	VM guest ID
UUID	UUID
VMHostSysName	VM host name
VMHostVersionNum	VM host version number
OSType	OS type
NumvCPUs	Number of vCPUs
CPUEntitlement	CPU entitlement plus units
MemorySize	Amount of memory plus units
SnapshotID	SnapshotID

R_InstalledBoards

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
BoardName	Board name (for example, PCI SCSI controller, and so on)
BoardModel	Board model
BoardRevision	Board revision
BoardFirmware	Board firmware
BoardSerial	Board serial number
Slot	Slot number in the system
SnapshotID	Snapshot ID
Location	Location for 64-bit Intel® platform systems (This field is blank for all other systems)
Tag	Tag

R_Inventory

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
ProductName	Product name
ProductID	Product ID
MemorySize	Memory size
ROMVersion	ROM version
SerialNumber	Serial number
AssetTag	Asset tag
OSName	Operating System name
IPAddress	IP address
IPLongValue	IP address in decimal value
OSVendor	Operating system vendor

Column name	Description
SnapshotID	Snapshot ID
DeviceOwner	Owner of the system
Location	Location of the system
ProductType	Type of system (for example, server, client, workstation, and so on)
DeviceStatus	Hardware status of the system
DeviceBootTime	System Boot Up Time
ProductSubType	Product subtype
ProductTypeStr	Product type
ServerRole	Server role
numberOfCPU	Indicates the number of CPU in the device

R_lockdownStatus

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
LastScanName	Name of last vulnerability scan
LastScanDate	Date of last vulnerability scan
LastVulChk	Vulnerability DAT file used in last scan
Critical	Number of Critical vulnerabilities found in the last scan
Major	Number of Major vulnerabilities found in the last scan
Minor	Number of Minor vulnerabilities found in the last scan
LPatchDate	Date and time of last patch event
PatchRqd	Number of patches required (total)
PatchMiss	Number of patches not included (total)
Warning	Number of vulnerability Warnings found in the last scan
SnapshotID	SnapshotID

R_LogicalDisks

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
Description	Which logical drive (for example, c: [FAT])
SizeMB	Size of the logical drive in megabytes
UsedMB	Size of used space in megabytes
UsedPercent	Percentage of the used space
SnapshotID	Snapshot ID

R_MediaAccessDevices

Column name	Description
DeviceKey	Device key

Column name	Description
DeviceID	DeviceID
SnapshotID	SnapshotID
Name	Name of media access device
FirmwareVersion	Firmware version
OperationalStatus	Status
SystemName	Name of parent system

R_NetworkInterface

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
Description	Description
MacAddress	MAC address
IPAddress	IP address
InputErrors	Input errors
OutputErrors	Output errors
Speed	Interface speed (bits/s)
Duplex	Adapter Duplex state
FullDuplex	Flag indicating that the adapter is operating in full duplex mode
InterfaceName	Interface name
SubnetMask	Subnet mask
BroadcastAddress	Broadcast address
InterfaceState	Status information to indicate whether the logical system is enabled (3), disabled (4), some other (1), or unknown (2) state
DHCPEnabled	Indicates whether DHCP is enabled
IPLongValue	IP address in decimal value
SnapshotID	Snapshot ID
OperationalStatus	Operational status
ProtocolType	Protocol type
MaxDataSize	Maximum data size
PortType	Port type

R_OperatingSystem

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
Description	Description of the operating system type
Version	Version number of the operating system
SubDesc	Additional description (for example, Service Pack, Rev information)
OSType	Operating system type (for example, Windows 2000)
SnapshotID	Snapshot ID

Column name	Description
OSVendor	Operating system vendor

R_PhysicalDisks

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
DeviceType	System type (for example, CSCI disk)
DriveModel	Drive model
DriveSize	Drive size
DriveFirmware	Drive firmware
TransferMode	Mode of transfer for ATA drives
DriveSerial	Drive serial number
DriveVendor	Drive vendor (for example, HP)
Slot	Slot number in the system
DriveLoc	The drive number attached to the port
DrivePort	The port
DriveChassis	Populated only for Fibre Channel attached drives, the name of the chassis that contains the physical disk drive
DriveServiceTime	The total number of hours that a physical drive has been operating under the system driver
HardReadErrors	The number of read errors that have occurred on a drive that could not be recovered by the ECC algorithm of the physical drive or through retries
HardWriteErrors	The number of write errors that could not be recovered by a physical drive
DeviceID	Device ID
SnapshotID	Snapshot ID

R_PowerSupply

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
DeviceID	System ID
ModelName	Model name
SerialNumber	Serial number
FirmwareRev	Firmware revision
ConditionVal	Condition value
MaxCapacity	Maximum capacity in watts
UsedCapacity	Used capacity in watts
RedundancyState	Redundancy state of the power supply
Status	Status of the fault tolerant power supply system
Condition	Condition of this power supply
SnapshotID	Snapshot ID

Column name	Description
Description	Description
Type	Type of power supply
PhysicalLocation	Physical location of the power supply
Manufacturer	Manufacturer of the power supply
PowerSupplyIdentifier	Name of the power supply

R_Racks

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
RackName	The associated rack name
EnclosureName	The associated enclosure name
SerialNumber	Serial number
Model	Model name
Type	Type
SlotNumber	Slot number
SnapshotID	Snapshot ID

R_Software

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
SnapshotID	Snapshot ID
Description	Software description (for example, Server Agent Service, or Storage Agent Service)
Version	Version number
Executable	Name of the executable
TypeValue	Type value
Status	Software status
Date_	Date the software item
Type	Type of software (for example, agent, application, or driver)
FirmwareCategory	Displays firmware category

R_StorageDeviceInventory

Column name	Description
DeviceKey	System key
DeviceName	Unique name for the system
ControllerName	Name of the controller
WorldWideName	World Wide Name (WWN) or IP address
Vendor	The name of the product supplier
Model	Commonly used product name

Column name	Description
ProductRevision	Product version information
FirmwareVersion	Version information related to the software
SerialNumber	Product identification such as serial number
Status	System status
PortCount	The total number of ports on this system
PortUtilized	The number of ports on this system that has something connected
SnapshotID	Snapshot ID

R_StorageDeviceControllers

Column name	Description
DeviceKey	System key
DeviceName	Unique name for the storage array
ControllerName	Friendly name for the controller
WorldWideName	WWN
Vendor	Vendor
Model	Model
ProductRevision	Product version information
FirmwareVersion	Version info related to the software
SerialNumber	Product identification such as serial number
Status	The controller status
PortCount	The total number of ports on this system
PortUtilized	The number of ports on this system that have something connected
SnapshotID	Snapshot ID

R_StorageHostBusAdapters

Column Name	Description
DeviceKey	System key
DeviceName	Name of the host
HBAType	Friendly name of the host bus adapter (HBA)
WorldWideName	Node WWN of HBA
Vendor	Vendor
Model	Model of the HBA
Status	Status of the HBA
ProductRevision	Product version information
DriverVersion	Version of the driver for the HBA
FirmwareVersion	Firmware version of the HBA
FCode_BIOSVersion	FCode/BIOS version of the HBA
SerialNumber	Product identification such as serial number
PortCount	The total number of ports on this system
PortUtilized	The number of ports on this system being used

Column Name	Description
SnapshotID	Snapshot ID

R_StoragePorts

Column name	Description
DeviceKey	System key
DeviceName	Name of the SAN host, interconnect system, or storage system
PortName	Friendly name of the port
Number	Port number
WorldWideName	WWN of HBA
ControllerHBAName	The name of the parent (For ports on host system, this would be the HBA.)
Status	The status of the port
Type	FC-GS port type
LinkTech	The link technology supported by this adapter
Speed	The speed of the established link in bits per second (bps)
MaxSpeed	The maximum speed of the port in bits per second (bps)
SnapshotID	Snapshot ID

R_StorageLogicalUnits

Column name	Description
DeviceKey	System key
DeviceName	Unique name for the storage system
LUNName	Friendly name of the Logical Unit Number (LUN)
ID	VPD
Status	The status of the LUN
ExtentStatus	Additional status information on the LUN
LUNSize	The capacity of the LUN in bytes
RAIDLevel	Use heuristic based on StorageSetting qualifier to determine the RAID level
StoragePool	The name of the storage pool from which this LUN was carved
SnapshotID	Snapshot ID

R_StorageDeviceCapacity

Column name	Description
DeviceKey	System key
DeviceName	Name of storage system
ID	Unique ID of storage system
rawcapacity	Total capacity of a storage array in bytes
unassigned	Space that is not yet assigned to a storage pool for configuration into storage volumes (LUNs)
otherRaw	Space that is not configured for a specific purpose

Column name	Description
assigned	Space that is assigned to pools of storage that can be configured into storage volumes (LUNs)
raidovrassigned	Assigned space that is reserved for RAID overhead
unallocated	Assigned space that is not configured as LUNs or reserved for RAID overhead
otherassigned	Any assigned space that is not in the RAID Overhead, Un-Allocated, or Allocated categories
carved	The amount of space used in creating LUNs (if LUN is mirrored, this is the total space used by the LUN and not the space usable by the initiator.)
overhead	Allocated space (space configured as storage volumes) that is reserved for RAID overhead
presented	The amount of usable bytes that have been assigned to ports
unpresented	The number of usable bytes that have been carved into LUNs but are not assigned to a port
usable	The amount of allocated space minus space that is reserved for RAID overhead
snapshotId	Snapshot ID

R_SWFWBaselineInformation

Column name	Description
DeviceName	System name
DeviceKey	Device key
SnapshotID	Snapshot ID
Description	Description
Version	Installed version
R_BaselineName	Software or firmware baseline name
SWFWBaselineVersion	Software or firmware baseline version
LatestVersion	Latest version
ConfiguredRepository	Configured repository

R_Process

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
ID	ID
Name	Name of the process
State	Process state
Priority	Process priority
SnapshotID	Snapshot ID

R_UnixOSDetails

Column name	Description
DeviceKey	System key

Column name	Description
DeviceName	Name of the system
OSName	Name of the operating system
OSVersion	Operating system version
Capability	Operating system capability
SystemUptime	System boot up time
NumUsers	Number of users
NumProcesses	Number of processes
MaxProcesses	Max processes
TimeZone	System date and time
Snapshot ID	Snapshot ID

R_UnixLogicalMemory

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
SwapSpaceName	Swap space name
SwapType	Swap type
SwapSpaceSize	Swap space size
SwapSpaceMinSize	Swap space minimum size
SwapSpaceMaxSize	Swap space maximum size
SwapSpaceReservedSize	Swap space reserved size
SnapshotID	Snapshot ID

R_UnixIODevices

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
DeviceType	System type
DeviceDescription	System description
DeviceIdentifier	System identifier
DeviceStatus	System status
DeviceErrors	System errors
HardwarePath	Hardware path
HardwareType	Hardware type
DeviceClass	System class
AssociatedDriver	System driver
SnapshotID	Snapshot ID

R_WarrantyContract

Column name	Description
DeviceKey	Device key
DeviceName	System or component name that is covered by the contract
EntitlementType	Warranty or Contract displays
ContractID	Contract number
Startdate	Start date of warranty or contract
Enddate	End date of warranty or contract
ExpirationStatus	Entitlement status enum
Offers	Detail information regarding warranty or contract
Obligation ID	Contract or warranty obligation ID
Response Time	Response time for warranty or contract service
Coverage Window	Hours of available support
Service Level	Level of service specified in the offer
SnapshotID	SnapshotID

R_UnixIPRoute

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
RouteDestination	Route destination
RouteMask	Route mask
RouteGateway	Route gateway
SnapshotID	Snapshot ID

R_UnixSensors

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
SensorName	Sensor name
SensorID	Sensor ID
SensorType	Sensor Type
SnapshotID	Snapshot ID

R_HPUXFileSystem

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
MountPointName	Mount point name
MountSpecialDeviceName	Mount special system name
RemoteMountPointName	Remote mount point name

Column name	Description
FileSystemType	File system type
FileSystemAccess	File system access
FileSystemBootable	File system bootable
TotalInodes	Total inodes
FreeInodes	Free inodes
DataCapacity	Data capacity
FreeCapacity	Free capacity
MinFreeSpace	Minimum free space
SnapshotID	Snapshot ID

R_HPUXVolumeGroup

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
VolumeGroupName	Volume group name
AccessPermission	Access permission
Status	Status
ExtentSize	Physical extent size
Capacity	Volume group capacity
Allocation	Volume group allocated
FreeSpace	Free space
MaxNumPhysicalVol	Maximum number of physical volume
MaxNumPhysicalExtent	Maximum number of physical extent
NumDefinedPhysicalVol	Number of defined physical volume
NumActivePhysicalVol	Number of active physical volumes
MaxNumLogicalVol	Max number of logical volumes
SnapshotID	Snapshot ID

R_HPUXLogicalVolume

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
LogicalVolName	Logical volume name
AccessPermission	Access permission
Status	Logical volume status
ExtentSize	Logical extent size
Capacity	Logical volume capacity
SchedulePolicy	Schedule policy
AllocationPolicy	Allocation policy
SnapshotID	Snapshot ID

R_HPUPhysicalVolume

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
PhysicalVolName	Physical volume name
Status	Physical volume status
ExtentSize	Physical extent size
Capacity	Physical volume capacity
AllocatedPhysicalExtent	Allocated physical extent
FreePhysicalExtent	Free physical extent
SnapshotID	Snapshot ID

R_HPUNetworkDetails

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
DomainName	Domain name
Search	Search list
ServerIPAddress	Server IP address
ServerType	Server type: Unknown (0), Other (1), None (2), Master Server (3), Slave Server (4)
ServerWaitFlag	Server wait flag
ServerAddress	Server address
SnapshotID	Snapshot ID

R_HPULKernelParam

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
ParameterName	Parameter name
ParameterValue	Parameter value
SnapshotID	Snapshot ID

R_HPUSoftwareBundle

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
BundleName	Bundle name
VendorTag	Vendor tag
Architecture	Architecture
Revision	Revision
Caption	Caption

Column name	Description
ModificationTime	Modification time
Size_	Size
LayoutVersion	Layout version
OSName	Operating system name
OSRelease	Operating release
IsPatch	IsPatch
InstallSource	Install source
InstallDate	Install date
SnapshotID	Snapshot ID

R_HPUXSoftwareProduct

Column name	Description
DeviceKey	System key
DeviceName	Name of the system
Specification	Product software specification
ProductName	Product name
Architecture	Architecture
Revision	Revision
VendorTag	Vendor tag
Caption	Product caption
ModificationTime	Modification time
Size_	Size
OSName	Operating system name
OSRelease	Operating system release
IsPatch	IS patch
InstallSource	Install source
InstallDate	Install date
SnapshotID	Snapshot ID

Related topics

- [Reporting](#)
- [Snapshot comparison reporting](#)

Snapshot comparison reporting

Snapshot Comparisons enable you to compare up to four systems (with the same operating system) to each other or to compare a single system to itself and observe changes over time. To perform historical trend analysis for a single system, such as compare snapshot data, you must have already collected at least two sets of snapshot data (by way of **Options**→**Data Collection**) for that system and select **Append new data set (for historical trend analysis)** in the **Step 2: Specify How to Save Data** page.

To run a snapshot comparison:

1. Select **Reports**→**Snapshot Comparison**. The **Snapshot Comparison** window appears.
2. Select target systems. See “[Creating a task](#)” for more information.

3. Click **Next**. You can click **Previous** to return to the **Target Selection** page.
Select two to four snapshots for the systems from the **Select Snapshots** page.
The following warnings are possible:
 - Some system OS types are unknown.
 - More than one operating system type is selected.
 - Only one operating system type comparison is supported.
 - If one target is selected, this target must have at least two snapshots. You must select between two and four snapshots to compare.
 - If more than one target is selected, you can select one snapshot for each system.
The target systems selected should be of the same operating system for the snapshot comparison feature to work.
4. Click **Next**.
5. From the **Select Categories and Baseline** page, select the categories to be included in the snapshot comparison. The **Category Name** column displays the category, and the **Description** column displays a brief description of the category.
6. From the **Select snapshot comparison baseline** section, select an item against which to run the comparison.
7. Click **Run Reports**. The **View the results** page displays listing the results. You can click **Previous** to return to the **Select Snapshots** page.

Related procedures

- System reporting
- Adding a report
- Editing a report

Related topic

- ▲ Reporting

PMP reporting options

Three *HP Performance Management Pack* (PMP) reports are available through HP Systems Insight Manager (HP SIM):



NOTE: PMP reporting is only available on a Windows system.

- **Static Analysis Report** Displays configuration pertaining to server components: processors, memory, network connections, storage, and host buses.
To access **Static Analysis Report**, select **Reports**→**HP Performance Management Pack Reports**→**Static Analysis Report**.
To access help for this option, go to https://middle_tier:2381/pmptools/help/StaticAnalysisReport.htm, where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\HP Performance Management Pack\PMPTools\htm\help\StaticAnalysisReport.htm, where *PMP directory* is the PMP directory on the server where PMP is installed.
- **System Summary Report** Displays the percentage of time the server remains in a bottleneck state, the overall performance utilization of the server for each of its components, and the server configuration details.
To access **System Summary Report**, select **Reports**→**HP Performance Management Pack Reports**→**System Summary Report**.
To access help for this option, go to https://middle_tier:2381/pmptools/help/SystemSummaryReport.htm, where *middle_tier*

is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\HP Performance Management Pack\PMPTools\htm\help\SystemSummaryReport.htm, where *PMP directory* is the PMP directory on the server where PMP is installed.

- **CSV File Generator** Displays, in detail, the logged data from the PMP repository for all server components in a .csv file for import into desktop analysis or report tools.

To access **CSV File Generator**, select **Reports**→**HP Performance Management Pack Reports**→**CSV File Generator**.

To access help for this option, go to

https://middle_tier:2381/pmptools/help/CSVFileGenerator.htm, where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\HP Performance Management Pack\PMPTools\htm\help\CSVFileGenerator.htm, where *PMP directory* is the PMP directory on the server where PMP is installed.

Related topics

- [PMP tools](#)
- [PMP administrative options](#)

15 Administering systems and events

Users with *administrative rights* can administer HP Systems Insight Manager (HP SIM). Administration of HP SIM involves the following tasks:

- Configuring basic settings using the First Time Wizard
- Configuring and running *automatic* and *manual discovery*
- Identifying systems
- Managing hosts and template files
- Managing system types by creating, editing, and deleting SNMP and *Desktop Management Interface (DMI)* rules
- Setting global and single system protocol settings
- Configuring and running status polling tasks
- Configuring automatic event handling by creating and editing tasks, deleting events, and configuring e-mail, modem, event filter, SNMP trap, and status change event settings
- Configuring cluster and system settings
- Running data collection tasks
- Customizing the **Home** page options
- Selecting and maintaining default HP Version Control Repository Manager for advanced searches and tasks such as installing software and firmware
- Managing toolboxes
- Managing authorizations
- Managing users
- Monitoring the Audit Log
- Creating, editing, exporting, importing, and synchronizing server certificates
- Creating, deleting, exporting, and importing trusted system certificates
- Setting up managed systems
- Setting system properties for multiple systems
- Suspending or resuming system monitoring for multiple systems
- Specifying the HP Version Control Repository Manager
- Running HP Performance Management Pack (PMP) administrative tools from HP SIM
- Configuring security settings
- Modifying identification through System Type Manager
- Managing system keys



NOTE: You must be a user with *administrative rights* on a system to access the **Options** menu and perform HP SIM administration tasks. Additionally, to configure users, authorizations, and toolboxes, you must have the **Allow this user to configure other users, authorizations and tool boxes** option selected.

Related procedures

- Viewing the Audit Log
- Configuring the audit log file
- Creating new users
- Creating new toolboxes
- Creating new user groups
- Creating new authorizations

- Updating authorizations
- Editing user accounts and user groups
- Editing toolboxes
- Deleting user accounts and user groups
- Deleting toolboxes
- Deleting authorizations
- User and user group reports
- Toolbox report
- Authorizations report
- Exporting a server certificate
- Editing a server certificate
- Creating a server certificate
- Importing a server certificate
- Deleting trusted certificates
- Exporting trusted certificates
- Importing trusted certificates
- Requiring trusted certificates
- Configuring cluster resource settings
- Configuring node resource settings
- Creating a data collection task
- Configuring automatic discovery
- Adding a system manually
- Disabling or enabling a discovery task
- Creating a new discovery task
- Editing a discovery task
- Deleting a discovery task
- Running a discovery task
- Configuring automatic discovery general settings
- Adding systems in a hosts file to the HP SIM database
- Deleting a hosts file
- Editing a hosts file
- Creating a new hosts file
- Creating a new discovery template file
- Editing a discovery template
- Deleting a discovery template
- Clearing events
- Deleting events
- Editing automatic event handling tasks
- Enabling or disabling automatic event handling tasks
- Viewing task definitions
- Configuring e-mail settings
- Configuring modem settings for paging
- Creating an automatic event handling task

- Managing event handling tasks
- Configuring event filters for registered SNMP traps
- Configuring SNMP traps
- Configuring status change events
- WBEM indications
- Setting up managed systems
- Version Control Repository
- PMP administrative options
- Setting global protocols
- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system
- Adding a WMI Mapper Proxy
- Editing a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy
- Configuring sign-in events
- Configuring the system link
- Configuring browser timeout options
- Hardware status polling
- Software status polling
- Creating STM rules
- Editing STM rules
- Deleting STM rules
- Editing system properties for multiple systems
- Suspending or resuming system monitoring for multiple systems
- Version Control Repository
- PMP administrative options
- Configuring SSH bypass properties

Related topics

- Users and authorizations
- Audit log
- Server certificates
- Possible certificate errors
- Data collection
- Discovery and identification
- Events
- Discovery filters
- Identification
- Protocols
- Global protocols
- WMI Mapper Proxy
- Networking and security
- About login
- About secure task execution

- Status polling
- Managing system types
- Protocol functionality

Events

Managing *events* in HP Systems Insight Manager (HP SIM) includes the following:

- **Automatic Event Handling** Enables you to manage automatic event handling tasks, create new automatic event handling tasks, and configure e-mail and modem settings.
 - **Managing Tasks** Enables you to view definitions, copy tasks, edit tasks, view task results, disable or enable tasks, or delete existing Automatic Event Handling tasks. You can also create a new Automatic Event Handling task. Select **Options**→**Events**→**Automatic Event Handling**→**Manage Tasks**.
See “Managing event handling tasks” for more information.
 - **Creating a New Task** Enables you to create a new Automatic Event Handling task. Select **Options**→**Events**→**Automatic Event Handling**→**New Task**.
 - **E-mail Settings** Enables you to set up the various e-mail settings needed when sending an e-mail because of an event action. You can access the **E-mail Settings** page using one of two methods:
 - Select **Options**→**Events**→**Automatic Event Handling**→**E-mail Settings**.
 - From the HP Systems Insight Manager (HP SIM) introductory page, click **e-mail** in the **Do this now to finish the installation** section.

E-mails are sent to alert users of problems. Because mail systems differ in their requirements, ask your e-mail administrator to verify whether you need the following information:

- SMTP host name of the outgoing mail server, such as *mail.company.com*. This server receives the mail messages from HP SIM and begins routing them to the recipient.
- The name of the management server e-mail address. This address appears in the **From** field of any e-mail sent from HP SIM. The user can be a system name. Enter the full domain address in the form *server@domain.com*, as the sender.



NOTE: Some e-mail systems require a valid From user before they accept the message. HP suggests that a valid e-mail account be used for this purpose.

- **Modem Settings** This feature is available to users with *administrative rights* only and is available for Windows systems only.
Set up a modem to use for alphanumeric paging. Before you send a page from the HP SIM server, set up the modem on the server. Be sure you know the COM port used by the modem to send the page.
You can access the **Modem Settings for Paging** page using one of two methods:
 - Select **Options**→**Events**→**Automatic Event Handling**→**Modem Settings**.
 - From the HP SIM introductory page, click **paging** in the **Do this now to finish the installation** section.
- **Clearing Events** Select **Options**→**Events**→**Clear Events**. Select the target events to clear and click **Clear**. See “Clearing events” for more information.
- **Deleting Events** This option is used to delete events from the *database*.



NOTE: Events can be deleted from the event view page. See “Customizing event collections” for more information.

Select **Options**→**Events**→**Delete Events**. After you select the targets and the **Tasks Results** page appears, select the events to delete and click **Delete**. The events are deleted from the *database*. See “Deleting events ” for more information.

- Event Filter Settings** Event filtering is a way to filter *SNMP traps* you receive from discovered *systems*. The default setting is to accept all registered SNMP traps from all discovered systems. You can specify the severity of the traps you want to see and use the IP address ranges to create a subset of systems whose traps you can receive or ignore. For example, you can use event filtering to ignore informational traps. This feature is available to users with administrative rights. See “Managing MIBs” for information about compiling MIBs.

To access **Event Filter Settings**, select **Options**→**Events**→**Event Filter Settings**.
- SNMP Trap Settings** SNMP trap settings is available to users with administrative rights and is used to view or edit trap details for a registered MIB.

SNMP traps enable you to tailor trap messages to your specific network needs. Trap messages can be cryptic, poorly written, and incomprehensible. You can modify the MIB information in the database representation. You can also modify a `.cfg` file of the MIB. HP recommends that you never modify an actual MIB. To access SNMP trap settings, select **Options**→**Events**→**SNMP Trap Settings**. See “Editing a MIB” for more information about editing MIBs.

See “Configuring SNMP traps” for more information about SNMP trap settings.
- Status Change Event Settings** This page is used to configure the settings for sending status change events for systems when hardware status changes. To access, select **Options**→**Events**→**Status Change Event Settings**.

See “Configuring status change events” for more information.
- Subscribing to WBEM Events** Select **Options**→**Events**→**Subscribe to WBEM Events**.

See “Subscribing to WBEM indications” for more information.
- Unsubscribing to WBEM Events** Select **Options**→**Events**→**Unsubscribe to WBEM Events**.

See “Unsubscribing to WBEM indications” for more information.

OpenWBEM is not supported.

Example automatic event handling tasks

HP SIM ships with three example automatic event handling tasks which are disabled by default. When the **Automatic Event Handling - Manage Tasks** page is displayed, you can select one of the example tasks and click **View Definition**.

- example - all desktop information events** This task is triggered when an informational event is received from the discovered desktop systems and this task clears the event. The same task can be edited to change the action of the system criteria. See “Editing automatic event handling tasks” for more information about editing automatic event handling tasks.
- example - all linux MIB updates** This task is triggered when a MIB update events request is received from all managed Linux target systems that are discovered and Identified in HP SIM. The same task can be edited and saved as new task. See “Editing automatic event handling tasks” for more information about editing automatic event handling tasks.
- example - all server failed sign-in events** This task is triggered when a failed sign-in attempt is made. Sign-in failure might be caused by an invalid user account, sign-in attempt from an excluded IP address, or because the sign-in attempt failed authentication. See “Editing automatic event handling tasks” for more information about editing automatic event handling tasks.

Related procedures

- Configuring e-mail settings
- Configuring modem settings for paging
- Creating an automatic event handling task
- Managing event handling tasks
- Configuring event filters for registered SNMP traps
- Configuring SNMP traps

- Configuring status change events
- Deleting events
- Clearing events
- Viewing task definitions

Related topics

- Managing event handling tasks
- Creating a paging task based on e-mail notification
- Examples of e-mail pages
- Creating a paging task based on e-mail notification

About administering events

Managing *events* include the following tasks:

- Automatic event handling
- Delete events
- Event filter settings
- SNMP trap settings
- Status change event settings

Automatic event handling

Automatic event handling enables you to define an action that HP Systems Insight Manager (HP SIM) performs when an event is received. Users who want to access this feature require *administrative rights*.

Four options are available under Automatic Event Handling:

- **New Task.** Used to create new Automatic Event Handling tasks.
- **Manage Tasks.** Used to manage existing Automatic Event Handling tasks.
- **Configure e-mail settings.** Used to send e-mails to alert users of problems. Because mail systems differ in their requirements, ask your e-mail administrator to verify whether you need the following information:
 - SMTP host name of the outgoing mail server, such as *mail.company.com*. This server receives the mail messages from HP SIM and begins routing them to the recipient.
 - The name of the management server e-mail address. This address appears in the **From** field of any e-mail sent from HP SIM. The user can be a system name. Enter the full domain address, in the form *server@domain.com*, as the sender.



NOTE: Some e-mail systems require a valid From user before they accept the message. HP suggests that a valid e-mail account be used for this purpose.

- **Configure modem settings (Windows only).** This feature is available to users with administrative rights.
Set up a modem to use for alphanumeric paging. Before you can send a page from the HP SIM server, set up the modem on the server. Be sure you know the COM port used by the modem to send the page to set up the modem in HP SIM.

Access the **Automatic Event Handling** page to edit or delete an existing rule by clicking **Automatic Event Handling** in the **Do this now to finish the installation** section of the HP SIM introductory page.

Delete events

This task is used to delete events from the *database*.



NOTE: Events can be deleted from the event view page. See “Customizing event collections” for more information.

Event filter settings

Event filtering is a way to filter *SNMP traps* you receive from discovered *systems*. The default setting is to accept all registered SNMP traps from all discovered systems. You can specify the severity of the traps you want to see and use the IP address ranges to create a subset of systems whose traps you can receive or ignore. For example, you can use event filtering to ignore informational traps. This feature is available to users with administrative rights. See “Managing MIBs” for information about compiling MIBs.

Options for filtering events

Events are registered or unregistered. Registered events are SNMP traps that are recognized by HP SIM from systems that have been discovered. Unregistered events are traps from systems that were discovered but whose system information is not part of the HP SIM *MIBs* database. Only registered events have a severity level. See “Event severity types” for information about event severity types.

You can specify IP ranges for accepting or discarding traps. Enter one system or range per line, or separate the ranges and systems with a semicolon (;).

You can also filter traps using SNMP Extensions.

SNMP trap settings

This feature is available to users with administrative rights and is used to view or edit trap details for a registered MIB.

SNMP traps enable you to tailor trap messages to your specific network needs. Trap messages can be cryptic, poorly written, and incomprehensible. You can modify the MIB information in the database representation. You can also modify a `.cfg` file of the MIB. HP recommends that you never modify an actual MIB. See “Editing a MIB” for more information about editing MIBs.

Status change event settings

This page is used to configure the settings for sending status change events for systems when hardware status changes.

Related procedures

- Configuring e-mail settings
- Configuring modem settings for paging
- Creating an automatic event handling task
- Managing event handling tasks
- Configuring event filters for registered SNMP traps
- Configuring SNMP traps
- Configuring status change events

Related topics

- Events
- Examples of e-mail pages
- Creating a paging task based on e-mail notification

Managing event handling tasks

Perform the following procedures to create, edit, copy, view definition, view task results, enable or disable, or delete automatic event handling tasks.



CAUTION: If you delete an automatic event handling task, the task is permanently deleted and cannot be restored.

The **Automatic Event Handling - Manage Tasks** page includes a table that shows all automatic event handling tasks and how the task was set up.

Name	Page	E-mail	CMS Tool	Forward	Assign	Clear	Log	Last Run
example - all desktop informational events						✓		Disabled
example - all linux MIB updates						✓	✓	Disabled
example - all server failed sign-in events							✓	Disabled

View Definition: example - all desktop informational events

Task name: example - all desktop informational events
Owner: gtd@hp.com:admin
Time filter: None defined
Events:
severity is Informational
Systems:
system type is Desktop
Action(s):
Clear event

To manage automatic event handling tasks:

1. Select **Options**→**Events**→**Automatic Event Handling**→**Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task.
3. Click one of the following:
 - **New** to create a new automatic event handling task. See “Creating an automatic event handling task” for more information.
 - **Edit** to edit the task. The edit wizard appears, which is similar to the page for creating a new automatic event handling task, but the fields are prepopulated with the current settings for the task. An additional field is available to reassign the task owner. See “Editing automatic event handling tasks” for more information.
 - **Copy** to replicate the configuration details of an existing task. A **Copy Task** page appears below the task list. Specify a new task name in the **Task name** box. Click **OK**, and a new and separate task is created. See “Copying automatic event handling tasks” for more information.
 - **View Definition** to view the task. The entire configuration for the selected task, such as task name, owner, time filter, event, system criteria, actions, modem settings, and e-mail settings, appear. See “Viewing task definitions” for more information.
 - **Task Results** to view the task result details for a selected task below the list. See “Viewing event task results” for more information.
 - **Disable** to disable a task. See “Enabling or disabling automatic event handling tasks” for more information.
 - **Delete** to delete the task. A confirmation box appears. Click **OK** to delete, or click **Cancel** to cancel the deletion. See “Deleting events ” for more information.

Example automatic event handling tasks

HP SIM ships with three example automatic event handling tasks which are disabled by default. When the **Automatic Event Handling - Manage Tasks** page is displayed, you can select one of the example tasks and click **View Definition**.

- **example - all desktop information events** This task is triggered when an informational event is received from the discovered desktop systems and this task clears the event. The same task can be edited to change the action of the system criteria . See “Editing automatic event handling tasks” for more information about editing automatic event handling tasks.
- **example - all linux MIB updates** This task is triggered when a MIB update events request is received from all managed Linux target systems that are discovered and Identified in HP SIM. The same task can be edited and saved as new task. See “Editing automatic event handling tasks” for more information about editing automatic event handling tasks.
- **example - all server failed sign-in events** This task is triggered when a failed sign-in attempt is made. Sign-in failure might be caused by an invalid user account, sign-in attempt from an excluded IP address, or because the sign-in attempt failed authentication. See “Editing automatic event handling tasks” for more information about editing automatic event handling tasks.

Related procedures

- [Configuring e-mail settings](#)
- [Configuring modem settings for paging](#)
- [Creating an automatic event handling task](#)
- [Managing event handling tasks](#)
- [Configuring event filters for registered SNMP traps](#)
- [Configuring SNMP traps](#)
- [Configuring status change events](#)
- [Deleting events](#)
- [Clearing events](#)
- [Viewing task definitions](#)

Related topics

- [Managing event handling tasks](#)
- [Creating a paging task based on e-mail notification](#)
- [Examples of e-mail pages](#)
- [Creating a paging task based on e-mail notification](#)

You must have administrative rights to view the automatic event handling example tasks.

Related procedures

- [Creating an automatic event handling task](#)
- [Editing automatic event handling tasks](#)
- [Copying automatic event handling tasks](#)
- [Viewing task definitions](#)
- [Viewing event task results](#)
- [Enabling or disabling automatic event handling tasks](#)
- [Deleting events](#)
- [Configuring e-mail settings](#)
- [Configuring modem settings for paging](#)

Related topics

- Events
- Examples of e-mail pages

Creating an automatic event handling task

Perform the following procedure to create a new automatic event handling task to define a response to a specific *event*.



NOTE: If you create an automatic event handling task and you do not select a predefined collection that has event and system information in it, and then you use the `mxtask -lf` command to create an `.XML` file that can be used to create another task, the task and collection that are associated with the task are placed in the `.XML` file. If you delete the task, the collection is deleted along with the task. Therefore, the `.XML` file can no longer be used to create a new task with the collection that is referenced in the `.XML` file. Any time you create an automatic event handling task that includes selecting event information and then system information, that information is stored in a hidden collection that is unavailable for use by any task other than the immediate task. See the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

1. Select **Options**→**Events**→**Automatic Event Handling**→**New Task**. The **Automatic Event Handling - New Task** page appears.
2. Enter a name in the **Task name** field, or accept the default, and then click **Next**. The **Select event collection** page appears.
3. Select one of the following:
 - a. Use this event collection
 - i. Select an event collection from the dropdown list.

Note: Select an event collection. The event collection is a collection that is defined by event attributes. The event collection might be a combination collection containing system information. If the collection contains system information, step iii will not appear. If you select an event collection that contains additional event collections, you will receive an error message.
 - ii. (Optional) Click **View Definition** to view the collection attributes that define the event collection.

Note: This field is displayed if you selected an existing private or shared event collection. If the collection was created using the Automatic Event Handling feature that enables you to select event and system information, this will not be displayed.
 - iii. Click **Next**. The **Select system collection** page appears. If the event collection contains system information, the select system collection process will not be displayed. Instead, the **Select actions** page will appear.
 - b. Use event attributes that I will specify
 - i. Click **Next**. The **Select events** page appears.
 - ii. Select event search criteria for defining the task:
 - List criteria
 - Comparison option
 - Value for the criteria or comparison options selectedTo add additional search criteria, click **Add**.

See “Performing an advanced search for events” for more information about event searches.
 - c. Click **Next**. The **Select system collection** page appears.

4. Select one of the following options:
 - a. Use this system collection
 - i. From the dropdown list, select a system collection.
 - ii. Click **View Definition** to view the collection attributes or the members of the system collection that is selected.
 - iii. Click **Next**. The **Select action** page appears.
 - b. Use system attributes that I will specify
 - i. Click **Next**. The **Select systems** page appears.
 - ii. Select system search criteria for defining the task:
 - List criteria
 - Comparison option
 - Value for the criteria or comparison options selected
 To add additional search criteria, click **Add**.
 See "Performing an advanced search for events" for more information about event searches.
 - iii. Click **Next**. The **Select actions** page appears.
5. Select from the following options:
 - Send page (Windows only)
 1. Add users to be paged from the dropdown list of users by clicking **>>**. Click **<<** to remove selected users from the list of users to be paged. The pager number for an HP Systems Insight Manager (HP SIM) user is set on the **Users and Authorizations** page. See "Creating new users" for more information. If a user name in the **Users** list is inactive, the pager information for the user has not been configured. You can add the user to the list of users to be paged, but pager messages are not sent to this user until the pager information is provided.
Note: If you select a user that does not have pager information set, the **Pager Information** section expands where you can enter the information.
 2. Enter the paging information.
 - **Phone number** Enter the pager phone number of the user associated with this user account if you are using a Windows operating system. If the **Phone number** field is left blank, the paging information is not saved. This field does not apply to user groups.
 - **PIN number** Enter the PIN number associated with the pager phone number.
 - **Message length** Select how many characters can be accepted in the paging message from the dropdown list.
 - **Baud rate** Select the appropriate baud rate for the pager from the dropdown list.
 - **Data format** Select the appropriate data format for the pager from the dropdown list.
 - Click **Apply**. A dialog box appears stating that the changes were successful. Click **OK** to close the box.
 - Send e-mail

In the **To** field, enter the list of e-mail addresses that should receive the notification, separating each entry with a comma.

In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each entry with a comma.

In the **Subject** field, enter a note describing the subject of the e-mail.

In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:

- **Standard.** A default message format that sends a text e-mail message to the recipients.
- **Pager/SMS.** An e-mail message format that sends a message to the recipients with the same information and format as a pager message.
- **HTML.** An e-mail message format that sends a message to the recipients that looks like the **HTML Event Details** page.

In the **Encoding** field, select from the following formats:

- **Western European (ISO-8859-1)**
 - **Unicode (UTF-8)**
 - **Japanese (ISO-2022-JP)**
 - **Japanese (Shift_JIS)**
 - **Japanese (EUC-JP)**
 - **Chinese (GB18030)**
 - **Chinese (Big5)**
 - **Korean (EUC-KR)**
- Run custom tool

Select a custom tool from the **Name** dropdown list. Custom tools are created under the **Tools**→**Custom Tools**→**New Custom Tool** option, and then select **CMS tool**. See “Creating a new CMS tool” for more information.
 - Assign

Enter the name of the person to whom to assign the task. The event is assigned to this user when received. Setting this field allows you to do searches assigned to this person.
 - Forward as *SNMP trap*

Enter a system name or IP address in the **Name or IP** field, and then click **>>** to add it to the **Trap recipients** box.

Click **Delete** if you want to delete a recipient after selecting the name in the **Trap recipients** box. Use the up and down arrows to scroll to the recipient to delete.
 - Write to system log

On Windows NT and Windows XP systems, the event details are written to the Application Log, and the **Source** column of the Event Log is listed as **HP SIM** for the logged event. On Linux and HP-UX systems, the event details are logged to the system log, which is usually located in the file `/var/log/messages` on Linux and in `/var/adm/syslog/syslog.log` on HP-UX.
 - Clear event

Received events are cleared based on the criteria selected when task executes.
6. After you have made your selections, click **Next**. The **Select time filter** page appears.
 7. Select the **Use time filter** checkbox if you want to use time filters, and then select an option from the dropdown list.
 - a. Click **Manage Filters** if you want to set user-defined filters. See “Applying a time filter” for more information.
 - b. Select the **View time filter** checkbox. A time filter window appears, showing the times selected.

If the **Use time filter** checkbox is not selected, actions are triggered whenever the events matching the selected criteria are received.

If the **Use time filter** checkbox is selected, actions are triggered **only** when they occur during the days and times specified by the selected time filter.
 - c. When you have entered the information, click **Next** to continue with the next step. The **Review summary** page appears. The task name, owner, time filters, event collections, system collections, and actions information is displayed. If a paging or e-mail option was selected, the modem and e-mail settings are displayed, along with buttons to change the settings.

- (Optional) Click **Edit modem settings** to edit the modem settings, or click **Edit email Settings** to edit the SMTP settings. See “Configuring modem settings for paging” or “Configuring SNMP traps” for more information.

Note: The event and system search criteria appear at the bottom of the page. This information can be extremely complex and long. Therefore, you might need to scroll down to view all of the criteria.

- Click **Finish** to create the new task.

Related procedure

- Managing event handling tasks
- Configuring e-mail settings
- Configuring event filters for registered SNMP traps
- Configuring modem settings for paging
- Configuring status change events
- Configuring SNMP traps
- WBEM indications

Related topics

- Events
- Examples of e-mail pages

Editing automatic event handling tasks

Two users cannot edit Automatic Event Handling tasks at the same time. The first user to click Finish will have their changes saved. The second user will receive an error message, stating `Unable to modify task`.

- Select **Options**→**Events**→**Automatic Event Handling**→**Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.

Note: once a task is selected on the **Automatic Event Handling - Manage Tasks** page, the task summary displayed when clicking **View Definition** automatically appears.

- Select the task to edit, and then click **Edit**. The **Edit task** section appears.
- Follow the on-screen instructions.

See “Creating an automatic event handling task” for more information about each of the steps.

Note: Select an event collection or an event combination collection. The event collection is a collection that is made up of event attributes. If you select an event collection that contains additional event collections, you will receive an error message.

Related procedures

- Creating an automatic event handling task
- Copying automatic event handling tasks
- Viewing task definitions
- Viewing event task results
- Enabling or disabling automatic event handling tasks
- Deleting events
- Configuring e-mail settings
- Configuring modem settings for paging

Related topics

- Events
- Examples of e-mail pages

Copying automatic event handling tasks

1. Select **Options**→**Events**→**Automatic Event Handling**→**Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select the task to copy, and then click **Copy**. The **Copy task** section appears.
3. In the **Task name** field, enter a name for the new task.
4. Click **OK**. The task is copied with a new name and placed in the list of Automatic Event Handling tasks.

Related procedures

- Creating an automatic event handling task
- Editing automatic event handling tasks
- Viewing task definitions
- Viewing event task results
- Enabling or disabling automatic event handling tasks
- Deleting events
- Clearing events
- Configuring e-mail settings
- Configuring modem settings for paging

Related topics

- Events
- Examples of e-mail pages

Viewing task definitions

Complete the following procedure to view the entire task configuration for a selected task. These configuration options were set when creating the task.

1. Select **Options**→**Events**→**Automatic Event Handling**→**Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task, and then click **View Definition**. The **View Definition** section appears, displaying the following information:
 - **Task name** The name given to the task when it was created
 - **Task owner** The user that created the task
 - **Time filters** The times that the task will run
 - **Event collection** The event collection that was selected when the task was created
Note: This field is displayed if you selected an existing private or shared event collection. If the collection was created using the Automatic Event Handling feature that enables you to select event and system information, this will not be displayed.
 - **Events** The event search criteria set for the task
 - **Systems** The system collection selected for the task
 - **Action(s)** The actions selected when the task was created, such as send e-mail and write to system log
 - **E-mail settings** The e-mail settings set when the task was created

See “Creating an automatic event handling task” for more information about each of the settings.



NOTE: If the task was created with no event or system information in the collection selected, the **Events** or the **Systems** field will show **None Defined**. If you edit the task, you will be forced to select the event or

system information for the collection. Prior to HP SIM 5.1, if no system or event information was included in the task, the All Systems and All Events collections were displayed respectively.

Related procedures

- Creating an automatic event handling task
- Editing automatic event handling tasks
- Copying automatic event handling tasks
- Viewing event task results
- Enabling or disabling automatic event handling tasks
- Deleting events
- Configuring e-mail settings
- Configuring modem settings for paging

Related topics

- Events
- Examples of e-mail pages

Viewing event task results

1. Select **Options**→**Events**→**Automatic Event Handling**→**Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task to view the task results, and then click **Task Results**. The **Task details** section appears. See “Task results list” for more information about the details displayed.

Related procedures

- Creating an automatic event handling task
- Editing automatic event handling tasks
- Copying automatic event handling tasks
- Viewing task definitions
- Enabling or disabling automatic event handling tasks
- Deleting events
- Configuring e-mail settings
- Configuring modem settings for paging

Related topics

- Events
- Examples of e-mail pages

Enabling or disabling automatic event handling tasks



NOTE: This option is especially useful for notification tasks imported from Insight Manager 7, which are imported into HP Systems Insight Manager (HP SIM) in a disabled state. You can edit these tasks, verify that the settings are accurate, and then enable the tasks by clicking **Enable**.

NOTE: The button label changes depending on if the task is currently enabled or disabled.

1. Select **Options**→**Events**→**Automatic Event Handling**→**Manage Task**. The **Automatic Event Handling - Manage Tasks** page appears.
2. Select a task to enable or disable.
3. If the task is enabled and you want to disable it, click **Disable**, or if the task is disabled and you want to enable it, click **Enable**.

Related procedures

- Creating an automatic event handling task
- Editing automatic event handling tasks
- Copying automatic event handling tasks
- Viewing task definitions
- Viewing event task results
- Deleting events
- Configuring e-mail settings
- Configuring modem settings for paging

Related topics

- Events
- Examples of e-mail pages

Configuring e-mail settings

To configure HP SIM to send e-mail notifications through automatic event handling:

1. Access the Simple Mail Transfer Protocol (SMTP) host and CMS e-mail settings through the First Time Wizard or choose **Options**→**Events**→**Automatic Event Handling**→**Email Settings**. The **Email Settings** page appears.
2. Enter the SMTP host name. The SMTP host is the outgoing e-mail server that the CMS uses to send e-mail notifications.
3. In the **Sender's e-mail address** box, enter the e-mail address that the management server uses when sending e-mail notifications.
4. To authenticate your SMTP server, select **Server Requires Authentication**.
5. Enter the account user name and password in the corresponding boxes.
6. **Note** If you did not enter a valid Simple Mail Transfer Protocol (SMTP) host, HP SIM notifies you that it cannot send e-mail notifications. If you do not want to enter e-mail settings now, click **OK**, or to enter a valid SMTP host, click **Cancel**.

If you are changing the e-mail settings from the **Options**→**Events**→**Automatic Event Handling**→**Email Settings** page, click **OK** to save changes.



NOTE: If the **Server Requires Authentication** option is selected, and you enter incorrect account information, e-mail event notifications do not reach the intended recipients.

Additional e-mail settings

The `globalsettings.props` contains properties that can be set for additional information to be included in email messages.

EmailPrefixUserSubject

To have user defined information (from the e-mail information on the **Actions** page) displayed first on the subject line of an e-mail, you must change the `EmailPrefixUserSubject` property in the `globalsettings.props` file to True. Otherwise, HP Systems Insight Manager (HP SIM) defined information is displayed first. The `globalsettings.props` file is located at:

- **On Windows** It is typically located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`.
- **On HP-UX and Linux** It is located at `/etc/opt/mx/config/globalsettings.props`.

The HP SIM service should be restarted after the flag is set. To restart:

- **If `EmailPrefixUserSubject = false`** The format of the subject line is Device Name: Short Description from Alert: User's Defined Subject.
- **If `EmailPrefixUserSubject = true`** The format of the e-mail subject line is User's Defined Subject: Device Name: Short Description from Alert.



IMPORTANT: This property does not need to be configured for the e-mail feature to work. This property is automatically set to false in the `globalsettings.props` file and does not need to be changed unless you want user defined text to appear before the HP SIM text in the subject line.

EmailKeywords

To include event information in an e-mail message, edit the *EmailKeywords* property in the `globalsettings.props` file.



NOTE: The HP SIM service must be restarted if any of the keywords change.

Keywords supported in the *EmailKeywords* property:

Keyword	Description
TID	Trap ID
TDESC	Trap description
TSDESC	Short description about trap
TNAME	Trap name
TNOTENUM	Trap notice number
TRCVD	Trap received time
TADDR	Trap source address
TENTOID	Enterprise trap OID
TNOTSEV	Trap severity
TASSIGNTO	Trap assigned to
TCOMMENT	Trap comments
DNAME	Device name
DDISCOV	Device discovered time
DURL	Device URL
HDR	Header which can be used to format message

Related procedures

- [Managing event handling tasks](#)
- [Creating an automatic event handling task](#)
- [Configuring event filters for registered SNMP traps](#)
- [Configuring modem settings for paging](#)
- [Configuring status change events](#)
- [Configuring SNMP traps](#)
- [WBEM indications](#)

Related topics

- [Using the First Time Wizard](#)
- [Events](#)

- About administering events
- Examples of e-mail pages
- Creating a paging task based on e-mail notification

Configuring modem settings for paging

Perform the following procedure to specify the COM port used by the modem to send pager messages.



NOTE: You can configure modem settings in Windows only.

To set modem settings for paging:

1. Select **Options**→**Events**→**Automatic Event Handling**→**Modem Settings**. The **Modem Settings** page appears.
2. From the **COM port** field, select the appropriate COM port. See your modem documentation for details.
3. Click **OK** to save the setting.

Related procedures

- Creating an automatic event handling task
- Editing automatic event handling tasks
- Copying automatic event handling tasks
- Viewing task definitions
- Viewing event task results
- Enabling or disabling automatic event handling tasks
- Deleting events
- Configuring e-mail settings

Related topics

- Events
- Examples of e-mail pages

Clearing events

1. Select **Options**→**Events**→**Clear**. The **Clear Events** page appears.
2. Select the target events. Refer “Creating a task” for more information about selecting targets.
3. Click **Apply**.
4. Click **Run Now** to clear the events immediately and view the **Task Results** page, or click **Schedule** to schedule the deletion. See “Scheduling a task” for more information about scheduling the task to run.



NOTE: When an event is cleared in HP Systems Insight Manager (HP SIM), it is also cleared in HP Storage Essentials.

When an event is cleared in HP Storage Essentials, it is also cleared in HP SIM.

Related procedures

- Configuring e-mail settings
- Configuring modem settings for paging
- Creating an automatic event handling task
- Managing event handling tasks
- Configuring event filters for registered SNMP traps
- Configuring SNMP traps
- Configuring status change events
- Deleting events

Related topics

- Events
- Examples of e-mail pages
- Service notification events

Deleting events

This task is used to delete events from the database.

1. Select **Options**→**Events**→**Delete**. The **Delete Events** page appears.
2. Select the target events. See “Creating a task” for more information about selecting targets.
3. Click **Apply**.
4. (Optional) Click **Add Targets** to add additional events to delete, or click **Remove Targets** to remove events from the deletion process.
5. Click **Run Now** to delete the events immediately and view the **Task Results** page, or click **Schedule** to schedule the deletion. See “Scheduling a task” for more information about scheduling the task to run



NOTE: Deleting an event in HP SIM causes the same event to be deleted in HP Storage Essentials.

Related procedures

- Configuring e-mail settings
- Configuring modem settings for paging
- Clearing events
- Creating an automatic event handling task
- Managing event handling tasks
- Configuring event filters for registered SNMP traps
- Configuring SNMP traps
- Configuring status change events

Related topics

- Events
- Examples of e-mail pages
- Service notification events

Configuring event filters for registered SNMP traps

1. Select **Options**→**Events**→**Event Filter Settings**. The **Event Filter Settings** page appears.
2. Select **Accept Unregistered Events** to accept unregistered events, or clear the box to not accept unregistered events. This option is disabled by default.
3. Select **Accept Registered Events with Severity** to accept registered events with a certain severity or multiple severities. This option is disabled by default.
4. Select the severities you want to accept. The available options are Critical, Major, Minor, Warning, and Informational.
5. Enter the IP ranges to accept in the **Accept Traps from Discovered Systems in IP Ranges:** box. By default, traps are accepted from all discovered systems.
6. (Optional) Enter IP ranges in the **Discard Traps from Discovered Systems in IP Ranges:** box to discard traps from certain systems.
Note: Enter one system or range per line, and separate the ranges and systems with a semicolon (;). Enter an asterisk (*) to accept or delete traps from all ranges.
7. Click **OK** to accept settings.

Related procedures

- Managing event handling tasks
- Creating an automatic event handling task
- Configuring e-mail settings
- Configuring modem settings for paging
- Configuring status change events

Related topics

- Events
- Managing MIBs

Configuring SNMP traps

Perform the following procedure to view and edit user-modifiable attributes associated with *SNMP traps*.

To configure SNMP traps:

1. Select **Options**→**Events**→**SNMP Trap Settings**. The **Snm Trap Settings** page appears.
2. Select the *MIB* name from the **MIB Name** dropdown list.
3. Select the trap name from the **Trap Name** dropdown list. The **Event Type** and **Description** change according to the trap name selected.
4. (Optional) Change the **Event Type**.
5. (Optional) **Edit the Description**.
6. Select **Yes** or **No** in the **Enable Trap Handling** box.
7. Select the category from the **Category** dropdown list.
8. Select the severity from the **Severity** dropdown list. The available options are Informational, Warning, Minor, Major, and Critical.
9. Click **OK** to save the settings.

SNMP trap fields

Field Names	Description
MIB Name	Select a MIB name from the dropdown list. All the remaining fields change according to the MIB name selected.
Trap Name	The default trap name is completed when a MIB name is selected in the MIB Name field. However, you can modify it by selecting a different trap name in the dropdown list.
Event Type	The type is a reflective form of the actual trap name. Change the type if it does not adequately describe the system for you.
Description	The description is vendor-supplied. Replace it with more specific instructions, a precise reference source, or a website referral.
Enable Trap Handling	Most traps are enabled. Trap handling gives you control over the volume of messages. Turn off nuisance messages, such as unnecessary informational messages, or repeated trap messages for an event that has not been corrected.
Category	The category lists the HP Systems Insight Manager (HP SIM) category types and Unknown.
Severity	Some vendors use the default Informational for all severity levels. Change the severity to a level that reflects your judgment of the problem. Alternatively, you can change a Major or Critical severity for a trap message that is clearly not a critical situation in your environment. Only you know if this is the case. The only valid options for HP SIM are Critical, Major, Minor, Warning, and Informational.

Modifying traps

To modify a specific trap, such as *cpqIDELogicalDriveStatusChange*, to have trap information included in e-mail messages, you can edit the MIB *cfg*. You can add keywords to the *MSG_FORMATTER* field, and then you must reregister the MIB, after making changes, by using the *mxmib -a cpqide.cfg* command.

For example:

```
#MSG_FORMATTER "$V3V#Ide Controller Model: # $V4V#Controller Slot Number: #
$V5V#Controller Index: # $V6V#Ide Logical Drive Index: # $V7V#Logical Drive
Status: # $tid#Trap ID: # $tname#Trap Name: # $trcvd#Trap Received Time: #
```

You can also edit the *globalsettings.props* file and modify the *EmailKeywords* property. "Configuring e-mail settings", in the "EmailSettings" section for additional information on changing the *EmailKeywords* property.

For SNMP traps, the MIB *cfg* file is the default location that HP SIM looks for keywords. If keywords are not defined here, then HP SIM looks at the *EmailKeywords* property in the *globalsettings.props* file.

Related procedures

- [Configuring e-mail settings](#)
- [Configuring event filters for registered SNMP traps](#)
- [Configuring modem settings for paging](#)
- [Managing event handling tasks](#)
- [Creating an automatic event handling task](#)
- [Configuring status change events](#)
- [WBEM indications](#)

Related topics

- [Events](#)
- [Examples of e-mail pages](#)
- [Managing MIBs](#)
- [Properties for globalsettings.props file](#)

Configuring status change events

Perform the following procedure to configure the sending of status change *events* for *systems* when hardware status changes to and from a Critical (unreachable) state only.

To configure status change event settings:

1. Select **Options**→**Events**→**Status Change Event Settings**. The **Status Change Event Settings** page appears.
2. Two options are available on this page. Select one or both of the options.
 - **Enable creation of system status change events.** This option causes a system unreachable event to be sent whenever a system cannot be reached by a ping through the Hardware Status Polling task. Enabling this option causes a system reachable event to be created whenever the system is reachable again.
 - **Automatically clear unreachable system status change events when system is reachable.** If this option is enabled, when a system that was previously unreachable starts to respond, the previous unreachable event is marked with a cleared state.
3. Click **OK** to apply changes.

Related procedures

- [Managing event handling tasks](#)
- [Creating an automatic event handling task](#)
- [Configuring e-mail settings](#)
- [Configuring event filters for registered SNMP traps](#)

- Configuring modem settings for paging
- Configuring SNMP traps
- WBEM indications

Related topics

- Events
- Examples of e-mail pages

WBEM indications

HP Systems Insight Manager (HP SIM) enables you to add and remove subscriptions to Web-Based Enterprise Management (WBEM) indication events through the GUI. You can also add and remove subscriptions to WBEM indication events from the *command line interface* (CLI). If you do not subscribe to WBEM indication events for a system that supports them, any WBEM events that occur will not appear on the event table view page.

OpenSSH must be installed and set up on the *Central Management Server* (CMS) with the keys enabled for SSH. See “Installing OpenSSH” for more information.

WBEM events support HP-UX, Linux, and SMI-S devices (such as storage, switches, and tape libraries). WBEM events for HP-UX and Linux systems require WBEM services 2.0 to be installed on the managed systems. Each managed system must have the correct event provider installed (for example, the EMS wrapper indication (event) provider on HP-UX). See “Setting up managed systems” for information about installing WBEM services and providers. The `mxwbemsub` command requires root privilege on HP-UX or Linux. OpenSSH is only used when menu tools are executed. If `mxwbemsub` is executed at the command line, it does not require OpenSSH.

Instant capacity (iCAP) properties for cells and processors for a complex is collected and displayed using the HP-UX WBEM. Data collection collects software and firmware information from HP-UX, NSK, Linux Integrity, and ProLiant boxes whenever the providers are available. See “Setting up managed systems” for information about installing WBEM services and providers.



NOTE: The iCAP provider is available on HP-UX 11i v3 (11.31), HP-UX 11i v2 (11.23) and HP-UX 11i v1 (11.11) which can only be installed on HP 9000 servers.

The supported versions for indications on Linux IPF include:

- RHEL4
- RHEL5
- SLES9
- SLES10

Also, the HP ProLiant Support Pack 3.90 or later should be installed on the system.

To set the port on which WBEM indications are received, edit the `globalsettings.props` file and the `WBEM_indications_Listener_Port` property. The default value for the port is 50004 (`WBEM_indications_Listener_Port=50004`). If this port is unavailable, edit the file and assign a suitable value. If HP SIM is running, stop the service and restart it for the new port to be accessed. If WBEM event subscriptions have been set up with the default port settings, delete and add the subscriptions again so that the new port is used when WBEM events are sent to the CMS.

You can subscribe and unsubscribe to WBEM indication events. To access these options, select **Options**→**Events**→**Subscribe to WBEM Events** and **Options**→**Events**→**Unsubscribe to WBEM Events**.

Related procedures

- Subscribing to WBEM indications
- Unsubscribing to WBEM indications

Related topics

- WBEM indications
- Creating a task
- Scheduling a task
- Task results list

Subscribing to WBEM indications



NOTE: OpenWBEM is not supported.

1. Select **Options**→**Events**→**Subscribe to WBEM Events**. The **Step 1: Select Target Systems** page appears.
2. Select the target systems, and then click **Apply**. The **Step 1: Verify Target Systems** page appears.
3. Click **Next**. The **Step 2: Task Confirmation** page appears and provides details about the task that was created in the previous steps.
4. Click **Run Now** to add subscriptions for WBEM events on the target systems. The **Task Results** page appears.

Related procedure

- ▲ Unsubscribing to WBEM indications

Related topics

- WBEM indications
- Creating a task
- Scheduling a task
- Task results list

Unsubscribing to WBEM indications



NOTE: OpenWBEM is not supported.

1. Select **Options**→**Events**→**Unsubscribe to WBEM Events**. The **Step 1: Verify Target Systems** page lists all of the targets with subscriptions to WBEM indication events.
2. If you do not want to delete a target's WBEM indication events subscription, select the checkbox next to the target and click **Remove Targets**.
3. Click **Next**. The **Step 2: Task Confirmation** page appears and provides details about the task that was created in the previous steps.
4. Click **Run Now** to remove subscriptions for WBEM indication events on the target systems. The **Task Results** page appears.

Instead of clicking **Run Now**, you can click **Schedule** to schedule the task for a later time. See “Scheduling a task” for more information.



NOTE: You can also list subscriptions and move subscriptions to a new destination through the CLI using the `mxwbemsub` command. See “Using command line interface commands” for more information.

Related procedure

- ▲ Subscribing to WBEM indications

Related topics

- WBEM indications
- Creating a task
- Scheduling a task
- Task results list

Subscribing to health lifecycle events

HP Systems Insight Manager (HP SIM) enables you to add and remove health lifecycle event subscriptions for HP NonStop Kernel servers. This procedure is performed using the *command line interface* (CLI). If you subscribe to health lifecycle events for an HP NonStop Kernel server, when the server's status changes, notification is sent to HP SIM and the server status is updated immediately in the GUI instead of waiting for the next status collection.

1. Sign into the CLI. See “Signing in” for instructions.
2. Enter one of the following commands:

- To add a health lifecycle event subscription for one or more servers, enter:

```
mxwbemsub -a [destination] ( ( -n nodenames ) | ( -f filename ) ) [-t health]
```

The target system (node) names can be entered through the command line or an input file. Each system name, entered on the command line or in a file, can be the IP address, hostname, or fully-qualified name of the system. You can specify the destination CMS for the subscriptions. If the destination is not included, the default is the CMS on which the command is run.

- To remove a health lifecycle event subscription for one or more servers, enter:

```
mxwbemsub -r [destination] ( ( -n nodenames ) | ( -f filename ) ) [-t health]
```

The target system (node) names can be entered through the command line or an input file. Each system name, entered on the command line or in a file, can be the IP address, hostname, or fully-qualified name of the system. This command can delete subscriptions from another CMS. If a CMS is not specified, the default is to remove subscriptions from the CMS on which the command is run.



NOTE: See the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for detailed information about `mxwbemsub`.

Related topics

- [Signing in](#)
- [Using command line interface commands](#)

Check event configuration

Use this tool any time to verify if a system is configured for receiving events either from SNMP traps or *Web-Based Enterprise Management* (WBEM) indications. To receive SNMP events, the Central Management Server (CMS) IP address must be in the trap destination list on the managed systems. However, this tool only checks for Windows systems which have an System Management Homepage (SMH) trust relationship with CMS. To receive WBEM indications, the WBEM Services installed on the managed system must support sending indications and the subscription must be created from the CMS.

If this task has not run, the **Manage Communications Event** column displays the informational icon.

1. Select **Options**→**Events**→**Check Event Configuration**. The **Check Event Configuration** page appears.
2. Select the target events. Refer “Creating a task” for more information about selecting targets.
3. Click **Apply**.
4. Click **Run Now** to view results, or click **Schedule** to schedule the task. See “Scheduling a task” for more information about scheduling the task to run.

Related topics

- [Scheduling a task](#)
- [Managing Communications](#)

Examples of e-mail pages

Automatic Event Handling allows the sending of a system's home page URL in an e-mail address if that system has a home page. If the system does not have a home page, then Automatic Event Handling sends a URL that points to the HP SIM **System Page** of the system on the current Central Management Server (CMS).



NOTE: The URL specified in an e-mail message is displayed only if the format is set to standard.

Three types of e-mail pages can be sent from HP Systems Insight Manager (HP SIM):

- Standard
- Pager/SMS
- HTML

See "Creating an automatic event handling task" for more information about each type of page.

Example of a standard e-mail page

```
From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: System A: Storage System side panel is removed (Ver. 3):
Standard E-mail format
```

```
Event Name: Storage System side panel is removed (Ver. 3)
URL: https://systemname:2381
Event originator: System A
Event Severity: Major
Event received: 28-Apr-2004, 17:03:47
```

```
Event description: Storage System side panel is removed. The side
panel status has been set to removed. The storage system`s side
panel is not in a properly installed state. This situation may result
in improper cooling of the drives in the storage system due to
air flow changes caused by the missing side panel.
User Action: Replace the storage system side panel.
```

```
Status: sidePanelRemoved
```

Example of a Pager/SMS page

```
From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: System A: Storage System side panel is removed
(Ver. 3): Pager
SMS Format E-mail testing
```

```
System A, Storage System side panel is removed (Ver. 3),Status:
```

sidePanelRemoved

Example of an HTML page

From: Doe, John
Sent: Wednesday, April 28, 2004 5:04 PM
To: Doe, Jane
Cc: Smith, Jim; Jones, Beth
Subject: qaunit1: Storage System side panel is removed (Ver. 3): HTML
Format E-mail testing

Event Identification and Details	
Event Severity	Major
Cleared Status	Not cleared
Event Source	qaunit1
Associated System	qaunit1
Associated System Status	Minor
Event Time	28-Apr-2004, 17:03:47 CDT
Description	Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel. User Action: Replace the storage system side panel.
Assignee	May-HTML
Comments	

Trap Details	
Variable Description	Value
An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	QAUNIT1
The Trap Flags. This is a collection of flags used during trap delivery. Each bit has the following meaning: Bit 5-31: RESERVED; Always 0. Bit 2-4: Trap Condition 0= Not used (for backward compatibility) 1= Condition unknown or N/A 2= Condition ok 3= Condition degraded 4= Condition failed 5-7= reserved Bit 1: Client IP address type 0= static; entry 1= DHCP entry Bit 0: Agent Type 0= Server 1= Client NOTE: bit 31 is the most significant bit, bit 0 is the least significant.	0
Drive Box Side Panel Status. This value will be one of the following: other(1) The agent does not recognize the status. You may need to upgrade your software. sidePanelInPlace(2) The side panel is properly installed on the storage system. sidePanelRemoved(3) The side panel is not properly installed on the storage system. noSidePanelStatus(4) This unit does not support side panel status monitoring.	sidePanelRemoved

Where *qaunit1* is the system name.

Related procedures

- Managing event handling tasks
- Creating an automatic event handling task
- Configuring event filters for registered SNMP traps
- Configuring modem settings for paging
- Configuring e-mail settings

Related topic

- ▲ Events

Service notification events

The HP Services analysis tools, *Web-Based Enterprise Services (WEBES)*, and *Open Service Event Manager (OSEM)*, generate service notifications to HP Systems Insight Manager (HP SIM) through a specific *SNMP trap* type or *Simple Object Access Protocol (SOAP)* event if analysis has determined that there are serviceable events.

The SNMP trap capability is supported in WEBES 4.4.1 or later and OSEM 1.3 or later, and has been part of HP SIM since version 4.0. The SOAP event notification is supported with WEBES 5.0, OSEM 1.4.1, and HP SIM 5.2.

To download these tools and for installation instructions, go to <http://h18023.www1.hp.com/support/svctools/>.

OSEM can also be obtained from the *Smart Start Management CD*.

If *HP Service Essentials Remote Support Pack* is installed, the service notification provided by WEBES and OSEM also provides status about remote support incidents. See “HP Service Essentials Remote Support Pack” for more information about Remote Support Pack.

Host configuration and setup

No special setup of OSEM is required as long as these tools are on the same system as HP SIM because the service traps are normally sent to *localhost* by default and you accept the default SNMP settings. If OSEM is on a separate system from HP SIM, you must perform the procedure outlined in the *How to Change the HP SIM Host Name* section of the *OSEM Installation Guide*.

In the case of WEBES, enter `desta snmp` from the operating system command line.

You are prompted for the system to send the service traps to and you must enter the HP SIM system name regardless of whether WEBES and HP SIM are on the same system.

If you do not use Public for the SNMP community string, OSEM will not perform SNMP Gets properly. For this to happen, you must set the **HP Systems Insight Manager trap community name** field to the desired value in the OSEM **Settings: Internal**.

HP SIM handling of service event notifications

Upon receipt of service trap notifications from WEBES or OSEM, HP SIM handles them in much the same way as any other management events.

There are two ways to view these events:

- View them under **All Events**, which is always done by default.
- View them under event collections using the **Advanced Search** capability.
 - For HP SIM 4.x, you must use Advanced Search and search for events where the event category selection name is **HP Service Events** and type name is **any**. From here, you can select **View** to see the HP Service Events, or you can select **Save As** to create a collection category. This collection can be viewed under the left pane based on the location where you saved it.
 - For HP SIM 5.0 and later, this search is performed by default with the **All HP Service Events** collection, located under **Events**→**Service Events** in the **System and Event Collections** panel.

On the event table view page, the **Event Type** is shown as **A Service Incident has been reported (Type x)**, where Type x is the version of the SNMP trap or SOAP event. See the table under “Service trap notification details” for a list of differences between the service event notification types. The **System Name** and **Event Time** refer to the failing system or subsystem and time the error was reported. The **Severity** is shown as **Major** because the service notification is only sent if analysis has determined that a maintenance action should be performed and because the service trap contains information in addition to what can be found in the original events such as SNMP traps sent by Insight Management Agents. Beginning with HP SIM 5.0 with SP3, the severity follows the severity assigned by the OSEM or WEBES event type. For most events the severity will still be shown as **Major** indicating these are hardware events requiring service intervention and are submitted as incidents by the Remote Support Pack software. For service events generated as a result of test traps or that provide customer notification only, the severity is **Informational**.

In WEBES, notification is sent based on operating system event log analysis so there might be other traps sent by management agents.

HP SIM Service Notification overview and setup information

HP SIM 5.0 ships with a Service MIB to properly recognize service traps sent by OSEM and WEBES. HP recommends using the version of the Service MIB that shipped with HP SIM. If you need to replace the MIB, download it from <http://h18023.www1.hp.com/support/svctools/> by selecting **Service MIB Zip file** under

WEBES or OSEM, and instructions will be provided on the version to select. The zip file contains the .mib and .cfg files, and a readme file.

There are currently two versions of the MIB, which are based on the version of HP SIM being used, and the service trap type being sent by WEBES or OSEM; there are currently three types or revisions of the service trap. A new type of notification known as type 4 is done through SOAP, but does not require the MIB. See the table under "Service trap notification details" for a list of differences between the service event notification types.

Although the new version of the Service MIB recognizes all three service event trap types, it does not work properly if compiled or updated into HP SIM 5.0 with SP5.

To update the new service MIB with HP SIM, perform the following procedure on the system running HP SIM:

1. Open an MS-DOS window or UNIX shell.
2. Change to the directory containing the MIBs.
 - **For Windows:**
c:\program files\hp\systems insight manager\mibs
 - **For Linux:**
/opt/mx/mibs
3. Copy the new cpqservice.mib and cpqservice.cfg files to the mibs directory.
4. Run mxmib -a cpqservice.cfg to update the new service MIB.

To configure the service trap type to send, for OSEM, go to **Settings: Internal** and set the **HP Systems Insight Manager trap revision** field to the desired type. For WEBES, after the command `desta snmp on` is entered, you must select the desired type when prompted by the question: Which revision of the service trap should be sent (Type 2 or 3) [2]:.

If you are using HP SIM 5.1, Remote Support Pack A.05.00, and OSEM 1.4.1, duplicate service events might occur since service traps and SOAP events will both be sent. You can configure HP SIM to display or sort based on the service trap type, or you can de-register the service MIB so that only SOAP events are used.

Service trap notification details

To view details about the service notification from the event table view page, select the **A Service Incident has been reported** option you are interested in under **Event Type** in the table, to view the service event itself.

Refer to the following table for differences between the four service event types as well as compatibility with HP SIM, WEBES, OSEM, and Remote Support Pack. The last row shows the varbinds supported in the event. Each varbind is capable of storing 256 bytes of information. The description of each varbind for all three trap types can be found by perusing the latest Service MIB. As can be seen from the table, Type 3 provides the most information and uses the maximum number of varbinds supported by HP SIM per trap, for a total of 22 varbinds. HP SIM 5.0 with SP3 also provides formatting enhancements such as the ability to concatenate multiple varbinds into one field (for example, the Recommended Action 1 through 3 fields now shows up as one Recommended Action field).

The service trap consists of several types of information:

- Basic trap information, such as event identification, status, and description.
- Source information identifying the attributes of the failing system and time of error.
- Severity provided in Type 3 to indicate the severity level based on the event type.
- URL link to WEBES or OSEM event analysis, which opens the WEBES or OSEM Event Viewer, providing detailed analysis and troubleshooting information specific to the event.
- URL link to the Remote Support Pack software and case status for the particular event. If you are running version A.05.00 of the Remote Support Pack, this will link to a new Properties page.



NOTE: This link is only available if Remote Support Pack is installed and status has been received properly from the Remote Support Pack software.

- Recommended action that provides information on the service action to perform to correct the problem and might include information such as failing location, system identification, and parts callout. The following table shows this support beginning with Type 2. Type 3 traps extend this by adding 4 FRUList varbinds which provide detailed information, such as spare part number, information about the Replaceable Units, and 2 FRULocation varbinds that help identify the physical location of the Replaceable Units.
- URL link to customer self-repair procedure, if available, and provides written instructions and videos to help you perform the recommended action

Note: This information is only available in the Service MIB that ships with HP SIM 5.0 or greater and for service traps sent by OSEM 1.3.6 or WEBES 4.4.1.

Service trap Type 1	Service trap Type 2	Service trap Type 3 or SOAP event Type 4
Ships with HP SIM 4.x	Ships with HP SIM 5.0 and HP SIM 5.0 with SP2	Type 3 ships with HP SIM 5.0 with SP3 Type 4 ships with HP SIM 5.1
Supported by OSEM prior to version 1.3.6	Supported by OSEM 1.3.6 and 1.3.7a, and versions of WEBES from 4.4.1 and prior to 4.5	Type 3 supported by OSEM 1.4 and WEBES 4.5 Type 4 supported by OSEM 1.4.1
	Default trap type in OSEM 1.3.6, 1.3.7a, 1.4, 1.4.1; user must select in WEBES	Type 3 can be configured beginning with OSEM 1.4 and WEBES 4.5 Type 4 are automatically sent when Remote Support Pack A.05.00 is installed
Compatible with Remote Support Pack beginning with A.03.50	Compatible with Remote Support Pack beginning with A.03.50	Type 3 is compatible with Remote Support Pack beginning with A.03.50 Type 4 requires Remote Support Pack A.05.00
sysName ServiceIncidentSeverity ServiceIncidentStatus ServiceIncidentInformation ServiceIncidentEvent ServiceIncidentUniqueID ServiceIncidentTimeofOriginalEvent ServiceIncidentSourceSystemName ServiceIncidentIPAddressOfSource ServiceSEIncidentInformation ServiceIncidentIdentifier ServiceIncidentReceiveTrapOID ServiceIncidentFilterOID ServiceIncidentFilterValue	sysName ServiceIncidentStatus ServiceIncidentInformation ServiceIncidentEvent ServiceIncidentUniqueID ServiceIncidentTimeofOriginalEvent ServiceIncidentSourceSystemName ServiceIncidentIPAddressOfSource ServiceSEIncidentInformation ServiceIncidentIdentifier ServiceIncidentReceiveTrapOID ServiceRecommendedAction1 ServiceRecommendedAction2 ServiceRecommendedAction3 ServiceCustomerSelfRepairInstructionURL	ServiceIncidentSourceSystemName ServiceIncidentIPAddressOfSource ServiceEventSeverity ServiceIncidentStatus ServiceIncidentInformation ServiceIncidentEvent ServiceIncidentUniqueID ServiceIncidentTimeofOriginalEvent ServiceAnalyzerSystemName ServiceSEIncidentInformation ServiceIncidentIdentifier ServiceIncidentReceiveTrapOID ServiceRecommendedAction1 ServiceRecommendedAction2 ServiceRecommendedAction3 ServiceFRUList1 ServiceFRUList2 ServiceFRUList3ServiceFRUList4 ServiceLocation1 ServiceLocation2 ServiceCustomerSelfRepairInstructionURL

OSEM port discovery

HP SIM discovers the OSEM application on port 2069. To view this, perform one of the following:

- In HP SIM, access the All Systems view, and then select a system from the **System Name** column. Click the **Tools & Links** tab to verify if OSEM is displayed under the **System Web Application Pages**. If it is displayed, that means that HP SIM has discovered the OSEM application on port 2069. By selecting OSEM, the OSEM Event Viewer is displayed.
- Use Advanced Search and perform the following: Search for systems where web agent is OSEM and select **View** to see which systems have OSEM installed, and then continue as in the previous bullet to see the OSEM link

Related procedures

- Registering a MIB
- Unregistering a MIB

Related topic

- ▲ Default shared collections

Examples of event tasks

Examples for different event tasks that you might want to include in your portfolio include the following:

- **Deleting cleared server events** This example demonstrates how to create an event collection and creating and scheduling a task to delete cleared server events.
- **Deleting information events** This example demonstrates how to create an event collection and creating and scheduling a task to delete informational events on a set schedule.
- **Send e-mail when a system reaches a critical state** This example demonstrates how to create an event collection and creating and scheduling an Automatic Event Handling task to send an e-mail when systems reach a Critical state.
- **Creating a paging task** This example demonstrates how to create an Automatic Event Handling task to send a page when a system reaches a Critical, Major, or Minor status.

Related procedures

- Creating a task to delete all cleared events
- Creating a task to delete events older than 30 days
- Creating a paging task based on e-mail notification
- Creating a task to send an e-mail when a system reaches a critical state

Creating a paging task based on e-mail notification

You can set up a notification *task* that causes HP Systems Insight Manager (HP SIM) to send an e-mail that can then be forwarded to a BlackBerry, cell phone (for example, SMS), and other paging interface application whenever the *Central Management Server* (CMS) receives a Critical, Major, or Minor event.



IMPORTANT: When using time filters, you can use on-call style e-mails or pages. If you want one person to be notified during business hours and another at night, create two different tasks and set the time filter appropriately.



NOTE: This same type of task configuration can be applied to a Paging Task to use a modem in the HP SIM server to page through a BlackBerry or alphanumeric pager.

NOTE: Paging is only supported on a CMS running Windows.

To create the task:

1. Select **Options**→**Events**→**Automatic Event Handling**→**New Task**. The **Automatic Event Handling - New Task** page appears.
2. In the **Task name** field, enter a name for the task, such as **Important Events for e-mail-Pager Task**.
3. Click **Next**. The **Select event collection** page appears.
4. Select **Use attributes that I will specify**.
5. If a new event collection is created, then in the first selection box (criteria selection), select **severity**. Otherwise, a list of all event collections is displayed.
 - a. In the second selection box (comparison selection), select **is**.
 - b. In the third selection box (value selection), select **Critical**.
 - c. Click **Add** to add the Major and Minor severities to the task.
 - d. Repeat steps through, and in the third selection box, select **Major** and **Minor**.
 - e. Click **Next**. The **Select system collection** page is displayed.
6. Select **Use attributes that I will specify**.
7. Click **Next**. The **Select systems** page is displayed.
 - a. In the first selection box (criteria selection), select **system name**.
 - b. In the second selection box (comparison selection), select **(any)**.
 - c. In the third selection box (value selection), select **system name**.
 - d. Click **Next**. The **Select actions** page appears.
8. Select **Send e-mail**.
 - a. In the **To** address field, enter the e-mail address to which you want the notification sent (multiple addresses can be added so that a group is notified). A **CC** address can also be added so that a manager or supervisor is also notified.
 - b. In the **Subject** field, enter your subject. For example, **HP Systems Insight Manager Events**.
 - c. In the **Message Format** section, change the option to **Pager/SMS**. This option sends a condensed e-mail format that is similar to a paging task in HP SIM, which is the ideal way to send alerts to a BlackBerry or cell phone type of hardware (or when Telephony Application Programming Interface (TAPI) is not available and an e-mail-to-paging provider is being used).
 - d. Click **Next**. The **Review summary** page appears.
9. Click **Next**. The **Select time filter** section appears.
10. Select **Use time filter** and select **Nights and Weekends**, unless you want to receive the e-mail 24 hours per day. If so, clear **Use time filter**. See “Applying a time filter” for more information.
11. Click **Finish** to create the new task.

Related procedures

- [Creating an automatic event handling task](#)
- [Managing event handling tasks](#)
- [Scheduling a task](#)
- [Applying a time filter](#)

Creating a task to delete all cleared events

The following example describes how to create a task to delete all cleared server events from the HP Systems Insight Manager (HP SIM) database. This task is useful to include in your management portfolio because deleting cleared events on a regular basis empties the database of unnecessary entries and improves system performance.

The following task has two segments:

- Creating an event collection that contains the events you want to delete
- Creating and scheduling the task to delete all cleared server events and run the task

Creating the event collection

1. Select **Search** panel, and then click **Advanced Search**. The **Advanced Search** page appears.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (*criteria* selection), click the down arrow, and then select **cleared state**.
4. From the second selection box (comparison selection), click the down arrow, and then select **is**.
5. In the third selection box (value selection), select **cleared**.
6. Click **Add** to add the system type criteria.
7. From the first selection box (*criteria* selection), click the down arrow, and then select **system type**.
8. From the second selection box (comparison selection), click the down arrow, and then select **is**.
9. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **server**.
10. (Optional) Click **View** to view the search results.
11. Click **Save As** to save the event collection.
12. In the **Name** field, enter a name for the collection, such as **Delete Cleared Server Events**.
13. Under **Place in Folder**, select to save the collection in **Events by Severity** to have it available to other users.
14. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Creating and scheduling the task

1. Select **Options**→**Events**→**Clear Events**. The **Clear Events** page appears.
2. Select the **Delete Cleared Server Events** collection. Select **Select "Delete Cleared Server Events" itself**.
3. Click **Apply**.
4. Click **Schedule**.
5. In the **Task name** box, give the task a name, such as **Delete Cleared Server Events**.
6. In the **Refine schedule** section, select the scheduling option that you prefer. See "Scheduling a task" for more information about scheduling the task.
7. Click **Done**. The task is now scheduled, and the **All Scheduled Tasks** page appears.
To run this task at any time, select **Tasks & Logs**→**View Task Results**. Then select **Delete Informational Events** from the table, and then click **Run Now**. See "Running a scheduled task" for more information.

Related procedures

- Performing an advanced search for events
- Saving collections
- Deleting events from the database

Related topic

- ▲ Navigating the tree view page

Creating a task to delete events older than 30 days

Use this task to delete events based on a set of criteria. For example, you might create a task called Delete Informational Events that deletes all informational events that are more than six weeks old.



NOTE: You must have *administrative rights* to delete security events.

Creating the collection

1. Select **Search** panel, and then click **Advanced Search**. The **Advanced Search** page appears.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (*criteria* selection), click the down arrow, and then select **severity**.
4. From the second selection box (comparison selection), click the down arrow, and then select **is**.

5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Informational**.
6. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Normal**.
7. Click **Add** to select Normal severity.
8. From the first selection box (*criteria* selection), click the down arrow, and then select **severity**.
9. From the second selection box (comparison selection), click the down arrow, and then select **is**.
10. In the third selection box (value selection), select **Normal**.
11. Click **Add** to select Normal severity.
12. From the first selection box (*criteria* selection), click the down arrow, and then select **event time**.
13. From the second selection box (comparison selection), click the down arrow, and then select **older than** and select **30 days**.
14. (Optional) Click **View** to view the search results.
15. Click **Save As** to save the event collection.
16. In the **Name** field, enter a name for the collection, such as **Delete Insignificant Events**.
17. Under **Place in Folder**, select to save the collection in **Events by Severity** to have it available to other users.
18. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Scheduling the task

1. Select **Options**→**Events**→**Delete Events**. The **Delete Events** page appears.
2. Select the **Delete Insignificant Events** collection. Select the **Select "Delete Informational Events" itself** checkbox.
3. Click **Apply**.
4. Click **Schedule**.
5. In the **Task name** box, give the task a name, such as **Delete Informational Events**.
6. In the **Refine schedule** section, select **Every 1 week(s) on Saturday at 12:00 AM**, or select the day and time that you want the task to run.
7. Click **Done**. The task is now scheduled, and the **All Scheduled Tasks** page appears.
To run this task at any time, select **Tasks & Logs**→**View Task Results**. Then select **Delete Informational Events** from the table, and then click **Run Now**. See "Running a scheduled task" for more information.

Related procedures

- [Performing an advanced search for events](#)
- [Creating a task](#)
- [Scheduling a task](#)
- [Deleting events](#)
- [Saving collections](#)
- [Running a scheduled task](#)

Related topic

- ▲ [Navigating the tree view page](#)

Creating a task to send an e-mail when a system reaches a critical state

The following instructions set up an automatic event handling task to be run when a discovered system goes to a Critical status.

Creating the collection

1. Select **Search** panel, and then click **Advanced Search**. The **Advanced Search** page appears.
2. Select **events** from the **Search for** dropdown list.
3. From the first selection box (*criteria* selection), click the down arrow, and then select **severity**.

4. From the second selection box (comparison selection), click the down arrow, and then select **is**.
5. In the third selection box (value selection), the available values for a given criteria or comparison combination are given. Select **Critical**.
6. (Optional) Click **View** to view the search results.
7. Click **Save As** to save the event collection.
8. In the **Name** field, enter a name for the collection, such as **Critical Events**.
9. Under **Place in Folder**, select to save the collection in **Events by Severity** to have it available to other users.
10. Click **OK** to save the collection, or click **Cancel** to cancel the save operation.

Configuring HP SIM to send e-mail

1. Select **Options**→**Events**→**Automatic Event Handling**→**E-mail Settings**. The **E-mail Settings** page appears.
2. Specify the SMTP host in the **SMTP Host** box.
3. Specify the e-mail address that the management server uses when sending e-mail notifications in the **Sender's Email Address** box.
4. To authenticate your SMTP server, select the **Server Requires Authentication** checkbox.
5. Specify the account name in **Account name** box.
6. Specify the password in the **Password** box.
7. Click **OK** to save changes.

Configuring status change events

1. Select **Options**→**Events**→**Status Change Event Settings**. The **Status Change Event Settings** page appears.
2. Select **Enable creation of system status change events**. This option causes a system unreachable event to be sent whenever a system cannot be reached by a ping through the Hardware Status Polling task. Enabling this option causes a system reachable event to be created whenever the system is reachable again.
3. Click **OK** to apply changes.

Creating the task

1. Select **Options**→**Events**→**Automatic Event Handling**→**New Task**. The **Automatic Event Handling - New Task** page appears.
2. Select **with an existing event collection**.
3. On the **Step 1, Select name** page, enter a name for the task in the **Task name** box, such as **Send E-mail for Critical Status**.
4. Click **Next**. The **Step 2, Select existing event collection** page appears.
5. Select the **Critical Events** collection from the dropdown list.
6. Select **Send e-mail**.
 - ▲ In the **To** field, enter the list of e-mail addresses that should receive the notification.
In the **CC** field, enter any e-mail address that should receive a copy of the e-mail, separating each with a comma.
 - In the **Subject** field, enter a note describing the subject of the e-mail.
 - In the **Message Format** field, select from the following formats based on the encoding preference of the recipient:
 - **Standard**. A default message format that sends a text e-mail message to the recipients
 - **Pager/SMS**. An e-mail message formatted with the same information and format as a pager message is sent to the recipients
 - **HTML**. An e-mail message that looks like the **HTML Event Details** page is sent to the recipients

In the **Encoding** field, select from the following formats:

- **Western European (ISO-8859-1)**
- **Unicode (UTF-8)**
- **Japanese (ISO-2022-JP)**
- **Japanese (Shift_JIS)**
- **Japanese (EUC-JP)**
- **Chinese (GB18030)**
- **Chinese (Big5)**
- **Korean (EUC-KR)**

7. Click **Next**. The **Step 4, Select time filter** page appears.
8. Select the **Use time filter** box if you want to use time filters, and then select an option from the dropdown list.

Click **Manage Filters** if you want to set user defined filters. See [“Applying a time filter”](#) for more information.

9. Click **Next**. The **Step 5, Review summary** page appears. The **Task name**, the **selected event collection**, the **events**, **system criteria**, and **Action(s)** information are displayed.
10. If you want to edit the e-mail selections, click **Edit e-mail Settings** to edit the SMTP settings. See [“Configuring SNMP traps”](#) for more information.
11. Click **Finish** to create the new task.

Related procedures

- [Managing event handling tasks](#)
- [Configuring e-mail settings](#)
- [Configuring event filters for registered SNMP traps](#)

Status polling

Polling tasks track *system health status* for *systems* in the system list. They provide a simple means of assessing system health in the *event* that an *SNMP* trap or other event was not properly delivered to the management console. Hardware status polling must occur continuously to determine when systems go offline or performance degrades. You can customize polling tasks for specific systems to run at scheduled times. You can also create new polling tasks with different system or event lists to match your specific requirements.



NOTE: DMI Status polling is supported only on Windows Central Management Servers and target systems.

There are two default polling tasks:

- **Software Status Polling.** Use Software Status Polling to determine software version update status. This task is set to run every seven days, on Wednesday at midnight, by default. You can edit the task and run it at any time. This task performs the following functions:
 - Retrieves software and firmware inventory from systems
 - Determines the software and firmware update status
 - Sorts versions in the *database*

To access Software Status Polling, select **Options**→**Status Polling**→**Software Status Polling**.

- **Hardware Status Polling.** Used to track system status. There are two types of Hardware Status Polling Tasks:
 - **Hardware Status Polling for Non servers.** Used to collect status information for target systems that are not of a server, cluster, or management processor type. This task is configured to poll every 10 minutes and at startup by default and does not send status change events.
 - **Hardware Status Polling for Servers .** Used to collect status information for SNMP systems of type server, cluster, or management processor. This task is configured to poll every five minutes

and at startup by default and sends status change events that can be used set up a notification task based on the event.

To access Hardware Status Polling, select **Options**→**Status Polling**→**Hardware Status Polling**.

Related procedures

- Hardware status polling
- Software status polling

Related topic

- ▲ About default system functions

Software status polling

The following example describes how to set up a Software Version Status Polling Task that determines whether *managed systems* have software that is out of date. This task uses the All Servers list as the default list.



NOTE: One instance of this *task* is created by default when HP Systems Insight Manager (HP SIM) is installed. It runs on a weekly basis. Create this task only if it has been deleted.

To create a Software Status Polling Task:

1. Select **Options**→**Status Polling**→**Software Status Polling**.
2. Select target *systems* from the All Systems collection. The default selected is All Systems. See “Creating a task” for more information.
3. Click **Schedule** to schedule the task, or click **Run Now** to run the task immediately. See “Scheduling a task” for more information about scheduling the task.

Related procedure

- ▲ Hardware status polling

Related topics

- Status polling
- About default system functions

Hardware status polling

HP Systems Insight Manager (HP SIM) tracks *system health status*, using a predefined hardware status polling task. This *task* polls for updates on hardware status through the different protocols. The following example describes how to set up a task to poll *systems* using hardware status polling.



NOTE: One instance of this task is created by default when HP SIM is installed. It runs when new systems or events meet the search criteria. Create this task only if it has been deleted.

To create a Hardware Status Polling Task:

1. Select **Options**→**Status Polling**→**Hardware Status Polling**.
2. Select the target systems. See “Creating a task” for more information.
3. Click **Next**. The **Select Protocol Settings** section appears.
4. Select from the following protocols:

- *DMI*

Note: DMI is only available on Windows systems.

- *HTTP*
- *SNMP*
- *WBEM*

Note: By default, all protocols are selected. If all protocols are unselected, then the **Schedule** and **Run Now** buttons are disabled.

Note: WBEM hardware status polling can be bypassed if all of the following conditions are met:

- The `WBEMStatusPollingBypass` flag is set to enabled in the `globalsettings.props` file.
- The target system type is set to Server. See “Editing system properties for a single system” for more information about setting system properties for a single system.
- The target system sub type is set to ProLiant. See “Editing system properties for a single system” for more information about setting system properties for a single system.
- The SNMP Insight Agents are installed on the target.

After all of these conditions are met, the WBEM status is cleared.

5. Select **Timeout (in seconds)**:
 - **Use default (currently "4")**
 - **Use custom.** Timeout maximum is 120 seconds, with a minimum of one second.
6. Select the retry value:
 - **Use default (currently "1")**
 - **Use custom.** The retries maximum is 10 retries, with a minimum of 0 retries.
7. Select one of the following options to execute the task:
 - **Schedule.** Click **Schedule** to schedule when the task should run. See “Scheduling a task” for information about scheduling a task.
 - **Run Now.** Click **Run Now** to run the task now. The **Task Results Page** appears. See “Task results list” for information about the **Task Results Page**.
 - **Previous.** Click **Previous** to return to the previous page.

Related procedure

- ▲ [Software status polling](#)

Related topics

- [Status polling](#)
- [About default system functions](#)

WMI Mapper Proxy

The WMI Mapper Proxy is a configuration setting for WMI. The WMI Mapper receives client CIM/XML WBEM requests and converts the requests to *Windows Management Instrumentation* (WMI) requests. The WMI results are converted to CIM/XML format and returned to the Central Management Server (CMS). The *discovery* and *Identification* task uses the proxies in the WMI Mapper Proxy list to discover whether a *system* is a WMI-enabled system. If the system is WMI-enabled, then the identification information for that system based on that specific proxy is returned.

The WMI Mapper Proxy feature enables you to perform the following tasks:

- **Add a WMI Mapper Proxy.** Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**→**[New]**. The **Add WMI Mapper Proxy** section appears.
- **Edit a WMI Mapper Proxy.** Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**. Select the proxy to edit, and then click **[Edit]**. The **Edit WMI Mapper Proxy** section appears.
- **Delete a WMI Mapper Proxy.** Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**. Select the systems to delete, and then click **Delete**. A confirmation box appears. Click **OK** to delete the systems, or click **Cancel** to cancel the deletion.



NOTE: Sort any column by clicking the column heading.

Related procedures

- Adding a WMI Mapper Proxy
- Editing a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy
- Protocol functionality

Related topic

- ▲ Protocols

Adding a WMI Mapper Proxy

HP Systems Insight Manager (HP SIM) enables you to add a WMI Mapper Proxy to define a new proxy for HP SIM.



NOTE: You must have *administrative rights* to add, edit, or delete a WMI Mapper proxy.

To add a WMI Mapper Proxy:

1. Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**→**[New]**. The **Add WMI Mapper Proxy** section appears.
2. In the **Host** field, enter the full *Domain Name Service (DNS)* name or IP address of the WMI Mapper Proxy.
3. In the **Port number** field, enter a port number. The WMI Mapper Proxy uses this port number to communicate with the WMI client.
4. Click **OK** to save and close the **Add WMI Mapper Proxy** section, click **Apply** to save without closing the **Add WMI Mapper Proxy** section, or click **Cancel** to abort the save operation.

Related procedures

- Editing a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy

Related topic

- ▲ WMI Mapper Proxy

Editing a WMI Mapper Proxy

Edit a *Windows Management Instrumentation (WMI)* Mapper proxy to update the proxy information. You can only edit one proxy at a time.



NOTE: You must have *administrative rights* to add, modify, or delete the WMI Mapper Proxy.

To edit a WMI Mapper Proxy:

1. Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**.
2. Select the proxy to edit, and then click **Edit**. The **Edit WMI Mapper Proxy** section appears.
3. In the **Port number** field, change the port number. The WMI Mapper Proxy uses this port number to communicate with the WMI client.
4. Click **OK** to save, or click **Cancel** to abort the edit operation.

Related procedures

- Adding a WMI Mapper Proxy
- Deleting a WMI Mapper Proxy

Related topic

- ▲ [WMI Mapper Proxy](#)

Deleting a WMI Mapper Proxy

HP Systems Insight Manager (HP SIM) enables you to delete a *Windows Management Instrumentation* (WMI) Mapper proxy. The delete option enables you to delete all selected proxies. Delete is available only if one or more proxies are selected.



CAUTION: If you delete one or more WMI Mapper proxies, the deletion is permanent and the proxies cannot be restored.



NOTE: You must have *administrative rights* to add, modify, or delete the WMI Mapper Proxy.

To delete a WMI Mapper Proxy:

1. Select **Options**→**Protocol Settings**→**WMI Mapper Proxy**.
2. Select the systems you want to delete.

Note: Sort by any column by clicking that column heading.

3. Click **Delete**.

A message appears, asking you to confirm your intention to delete the WMI Mapper Proxy.

4. Click **OK** to confirm your intention to delete the WMI Mapper Proxy, or click **Cancel** to cancel the delete operation.

Related procedures

- [Adding a WMI Mapper Proxy](#)
- [Editing a WMI Mapper Proxy](#)

Related topic

- ▲ [WMI Mapper Proxy](#)

Protocols

You can use HP Systems Insight Manager (HP SIM) to set protocol settings for all *systems*, for a group of systems, or for an individual system.

To set protocol settings for all systems, access the **Global Protocol Settings** page in one of the following ways:

- Select **Options**→**Protocol Settings**→**Global Protocol Settings**.
- From the HP SIM introductory page, click **Protocol Settings** in the **Do this now to finish the installation** section.
- From the **Automatic Discovery - General Settings** page, click **Configure global protocol settings** in the **Discovery configuration** section.



NOTE: You can set some global protocol settings in the First Time Wizard. See “Using the First Time Wizard” for more information.

To set protocol settings for a single system or group of systems, access the **System Protocol Settings** page in one of the following ways:

- From the **All Systems** page, click the **System Name** link of the system to go to the **System Page** for that system, and then click the **System Protocol Settings** link on the **Tools & Links** tab page.
- From the HP SIM menu, select **Options**→**Protocol Settings**→**System Protocol Settings**, and then select the single system to set its protocol settings.

To set protocol settings for a single system:

1. Access the **System Protocol Settings** page by selecting **Tools**→**System Information**→**System Page**.
2. Select the target system.
3. Click **Run Now**.
4. Select **Links**→**System Protocol Settings**.

Related procedures

- Setting global protocols
- Setting protocols and credentials for a system or groups of systems
- Setting protocols for a single system

Related topic

- Global protocols
- Using the First Time Wizard

Setting global protocols

You can set default system-wide protocols settings. These defaults apply to all newly discovered *systems*. For passwords or community strings, the default list is repeated until one string works (if at all). HP recommends putting the most often used passwords or community strings first in the list. In the following procedure, all sections are optional but highly recommended for proper management of systems.



WARNING! If your environment's security policy includes account lockout after a specific number of failed attempts, system protocol settings should be used instead of global protocol settings. You cannot configure system protocol settings until discovery has been run once, making sure none of the account lockout accounts are configured in the global protocol settings. See “Setting protocols and credentials for a system or groups of systems” for information on configuring system protocol settings.



NOTE: If you access the **Global Protocol Settings** page from the **Automatic Discovery - General Settings** page, click **Automatic Discovery** at the top of the page to return to the **Automatic Discovery - General Settings** page. Otherwise, this option is not available.

NOTE: You can configure some global protocol settings in the First Time Wizard. See “Using the First Time Wizard” for more information.

To set global management protocol settings:

1. Select **Options**→**Protocol Settings**→**Global Protocol Settings**. The **Global Protocol Settings** page appears.
2. In the **Default ping settings** section, choose from the following:
 - (Recommended) **Use the Internet Control Message Protocol (ICMP) for system reachability (ping) check**. This is the default setting.
 - **Use the TCP protocol for system reachability (ping) check port number 80**. Select this if your company has disabled Internet Control Message Protocol (ICMP) on the corporate network or if the corporate policy mandates system firewall software to filter ICMP requests.

Windows XP has this feature built in and can prevent systems from being automatically discovered. This option enables you to run HP SIM and ping all available systems.

This option only applies to IP-based systems and is available for global, system-wide settings that are used when managing all systems in HP SIM. It is used by automatic discovery, hardware status polling, the ping tool, and any other tool that must verify system availability. This option is not available on a single-system basis.

When HP SIM attempts a connection request to a system, that system does not need any additional software running on it for this option to work. For example, HP does not require that a web server be running on port 80. Some networking systems might not respond to the TCP request, which is typically seen in low-end networking equipment. You can make manual additions, if necessary. However, this system displays as Critical if hardware status polling is run.

To use a port other than port 80, change the *NodeReachableTcpPort* property in the *globalsettings.props* file located in *C:\Program Files\HP\System Insight Manager\config\globalsettings.props* for Windows and in */etc/opt/mx/config/globalsettings.props* for HP-UX and Linux.

3. Set the **Default timeout** and the **Default retries**. If some systems are managed over a WAN or satellite link, use a larger time-out (for example, five seconds) with at least one retry. For a LAN, you can use a shorter time-out. You can configure this setting on a single-system basis. See “Setting protocols and credentials for a system or groups of systems” for more information about setting single-system protocols.
4. In the **Default WBEM settings** section, verify that **Enable WBEM** (the default) is selected to allow *Web-Based Enterprise Management* (WBEM) requests to be sent. Enter as many default user names and passwords as needed. If your network includes *storage systems*, enter the user name and password of each *SMI CIMOM* in this section. The identification process attempts each user name and password pair until a successful response is obtained. Future WBEM requests to that system use the user name and password that succeeded. For Windows-based systems, the user name should include the domain name, for example, *domainname\username*.

If you have WBEM systems and you do not enter a user name and password pair, the systems will not be discovered.

Order the name and password pairs such that root and administrator passwords are listed first and user and guest passwords are listed second. This order minimizes the search time.

HP recommends limiting WBEM user name and password pairs to 10 to reduce the overall discovery run time. To add more than 10 WBEM user name and password pairs, run the `mxnodesecurity -a -p wbem -c username:password` command for each additional set. You can also create an XML file that defines your system authorizations before running discovery. See “Example XML file to add more than 10 WBEM username and password pairs” for more information.

OpenWBEM is not supported.

5. In the **Default HTTP settings** section, select **Enable HTTP and HTTPS** if you need web-based agents and other HTTP port scans to be identified. HP recommends leaving this option enabled for proper management and discovery of systems.
6. In the **Default SNMP settings** section, verify that **Enable SNMP** (the default) is selected and specify values for **Default time out** and **Default retries**. For systems managed over a WAN or satellite link, use a larger time-out (for example, five seconds) with at least one retry. For a LAN, a shorter time-out can be used. You can configure these settings on a single-system basis.
7. (Optional) Enter the **Default write community string**. This value is case-sensitive. Only a few tools need this option set. Community strings are case-sensitive.

Note: The **Write community string** is optional and is required only for firmware updates on a GbE switch. If you must update the GbE switch firmware, you must first set the write community string from this page and then run the existing switch update task. Do not set this feature if the network is not trusted.

8. In the **Read community string** field, enter up to 10 read community strings. This value is case-sensitive. The identification process attempts communication with a system, using each of these communities in succession until a successful response is obtained. Future SNMP requests then use the community string that provided a successful response.

If you have SNMP systems and no read community string that match the systems are entered, the systems will not be discovered.

9. (Optional) In the **Default DMI settings** section, select **Enable DMI**, to enable *Desktop Management Interface* (DMI) identification to run on systems. DMI is used to manage some older desktops, HP-UX 11.0 servers, and some third-party servers. If you do not need to manage these kinds of systems, DMI can be disabled to improve discovery performance.

For HP-UX, HP recommends disabling DMI.

DMI is not currently supported on Linux systems and is not shown in the user interface.

If DMI is disabled and some systems no longer have a correct system type or product name, re-enable DMI.

10. Click **OK** to accept the settings.

If you accessed this page from the **Discovery** page, click **automatic discovery** to return to the **Discovery** page after making changes.

Related topics

- Protocols
- Global protocols
- Protocol functionality
- Using the First Time Wizard
- Entering WBEM settings

Setting protocols and credentials for a system or groups of systems

Configure single-system protocol settings to fine-tune settings for individual *systems* or a group of similar systems. This option is especially useful if some of your systems are accessed through a LAN, while others are accessed through a WAN. Configure systems accessed through the WAN with longer timeouts and increased retries.

If you selected a collection when first using this tool, you can click the collection link at the top of the page. A window appears, showing all systems in the collection chosen. Click **OK** to close the window. This link is not displayed if you selected a single system.



NOTE: Since the **System Protocol Settings** page is intended for a group of similar systems, it is initially filled with default settings based on the corresponding values from the **Global Protocol Settings** page. The initial settings might not match current values from an individual system.

To set protocol settings for a single system or a group of similar systems:

1. Select **Options**→**Protocol Settings**→**System Protocol Settings**.
2. In the **WBEM settings** section, select **Update values for this protocol** to enable updating the WBEM settings. If this is not selected, the settings are not updated. This option is disabled by default.
OpenWBEM is not supported.
3. In the **WBEM settings** section, select:
 - **Use global defaults.**
 - **Use values specified below.** Enter the **User name** and password fields or select corresponding **Use certificate instead.**

Specify whether a specific WBEM port is to be authenticated through a set of credentials or a certificate. To authenticate through a set of credentials, enter the **Port #**, **User name**, **Password**, and **Confirm Password** information. To authenticate through a certificate, enter the **Port #** and select **Use certificate instead**. Enter as many sets of these values as needed.

Note: The user name should include the domain name. For example, *domainname/username*.

Note: The **Port #** can be blank for a set if appropriate.

Note: Since each port number can only be associated with a user name and password, when the same port number (including a blank entry) is specified in more than one set (row) of WBEM credentials, only the last set with that port number value will be retained. In other words, when several sets of WBEM credentials sharing the same port number are specified, the last set with that same port number replaces all previous entries.

4. In the **SSH settings** section, select **Update values for this protocol** to enable updating the SSH settings. If this is not selected, the settings are not updated. This option is disabled by default.
5. In the **SSH settings** section, select from the following options:

- **Not applicable.**
- **Use values specified below.** Enter the **User name**, **Password**, and **Confirm password**.

Note: Information should be included in this section if your target *Secure Shell* (SSH) server does not support public key authentication.

Related procedures

- Setting global protocols
- Setting protocols for a single system

Related topics

- Protocols
- Global protocols

Setting protocols for a single system

Configure single-system protocol settings to fine-tune settings for an individual *system*. This page is accessed from the **Tools & Links** tab on the **System Page**.

To set protocol settings for a single system:

1. Select **Tools**→**System Information**→**System Page**.
2. Select target systems. See “Creating a task” for more information.
3. Click **Run Now**. The **System Page** appears.
4. Click the **Tools & Links** tab.
5. Under **HP Systems Insight Manager Pages**, click **System Protocol Settings**. The **System Protocol Settings** page appears.
6. In the **Ping (ICMP) settings** section, select **Update values for this protocol** to enable updating the ICMP settings. If this is not selected, the settings are not updated. This option is disabled by default.
7. In the **Ping (ICMP) settings** section, select one of the following:

- **Use global defaults.**
- **Use values specified below.** Enter the **Timeout (seconds)** and the **Retries**.

8. In the **WBEM settings** section, select **Update values for this protocol** to enable updating the WBEM settings. If this is not selected, the settings are not updated. This option is disabled by default.

OpenWBEM is not supported.

9. In the **WBEM settings** section, select:

- **Use global defaults.**
- **Use values specified below.** Enter the **User name** and password fields or select corresponding **Use certificate instead**.

Specify whether a specific WBEM port is to be authenticated through a set of credentials or a certificate. To authenticate through a set of credentials, enter the **Port #**, **User name**, **Password**, and **Confirm Password** information. To authenticate through a certificate, enter the **Port #** and select **Use certificate instead**. Enter as many sets of these values as needed.

Note: The user name should include the domain name. For example, *domainname/username*.

Note: The **Port #** can be blank for a set if appropriate.

Note: Since each port number can only be associated with a user name and password, when the same port number (including a blank entry) is specified in more than one set (row) of WBEM credentials, only the last set with that port number value will be retained. In other words, when several sets of WBEM credentials sharing the same port number are specified, the last set with that same port number replaces all previous entries.

10. In the **SNMP settings** section, select **Update values for this protocol** to enable updating the SNMP settings. If this is not selected, the settings are not updated. This option is disabled by default.

11. In the **SNMP settings** section, select from the following:

- **Use global defaults.**
- **Use values specified below.** Enter the **Timeout (seconds)**, **Retries**, **Read community string**, and the **Write community string**.

Note: The **Write community string** is optional and is required only for firmware updates on a GbE switch. If you must update the GbE switch firmware, you must first set the write community

string from this page and then run the existing switch update task. Do not set this feature if the network is not trusted.

12. In the **SSH settings** section, select **Update values for this protocol** to enable updating the SSH settings. If this is not selected, the settings are not updated. This option is disabled by default.
13. In the **SSH settings** section, select from the following options:
 - **Not applicable.**
 - **Use values specified below.** Enter the **User name**, **Password**, and **Confirm password**.
Note: Information should be included in this section if your target *Secure Shell* (SSH) server does not support public key authentication.
14. In the **Identification settings** section, **Also run system identification** is selected by default. If you do not want to run system identification, clear this box.
15. Click **OK** to save the settings, or click **Return to System Page** to return to the **System Page** for the system and not save changes.
Note: If the **OK** button is disabled, look for any bold red error messages and correct all the problematic entries to enable that button.

Related procedures

- Setting protocols and credentials for a system or groups of systems
- Setting global protocols

Related topics

- Protocols
- Global protocols

Example XML file to add more than 10 WBEM username and password pairs

To save time and effort, create an XML file that defines your system authorizations prior to running discovery. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
15.43.215.47
15.43.212.150
15.3.110.117
15.3.105.51
15.3.110.113
-->
<nodelist>
  <node name="system1">
    <credential protocol="wbem" username="root "
      password="pswd" />
  </node>
  <node name="system2">
    <credential protocol="wbem" username="root "
      password="pswd" />
  </node>
  <node name="system3">
    <credential protocol="wbem" username="root "
      password="pswd" />
  </node>
  <node name="system4">
    <credential protocol="wbem" username="root "
      password="pswd" />
  </node>
</nodelist>
```

```

</node>
<node name="system5">
  <credential protocol="wbem" username="euploid\administrator"
    password="pswd" />
</node>
</odelist>

```

The IP addresses of the systems to be discovered can be included in an XML comment as shown above so that it can be maintained at the same time as the XML file and copied and pasted into the **Ping inclusion ranges, system (hosts) names, templates, and/or hosts files** field when creating or editing a discovery task. See “Creating a new discovery task” for creating a new discovery task and see “Editing a discovery task” for more information about editing a task.

After the XML file is created it can then be imported into HP Systems Insight Manager (HP SIM) prior to running discovery using the following CLI command:

```
mxnodesecurity -a -f <path-to-xml-file>
```

HP recommends limiting the WBEM user name and password pairs to 10 to reduce the overall discovery run time.

Related procedure

- ▲ Setting global protocols

Related topics

- Protocols
- WMI Mapper Proxy
- Protocol functionality
- Entering WBEM settings

Global protocols

Managing a network is complex, and network management becomes even more complicated without standards. When an organization purchases multiple management tools, each with a different method of managing a particular hardware or software product, it must maintain and train network administrators in different tools. This process is both expensive and inefficient. To address this issue, standards committees have developed protocols for network management.

HP Systems Insight Manager (HP SIM) takes advantage of many different management protocol standards. This capability enables HP SIM to provide management support for a wide array of manageable devices.

SNMP

The Internet Engineering Task Force (IETF), the standards-rating body for the worldwide Internet, has defined a management protocol, *SNMP*, which has accumulated a major share of the market and has the support of over 20,000 different products. SNMP has its roots in the Internet community. The complexity of large international TCP/IP networks has provided the necessary incentive to develop a standard method of managing devices on the network.

Within the SNMP framework, manageable network devices (routers, bridges, servers, and so on) contain a software component called a management agent. The agent monitors the various subsystems of the network element and stores this information in a *Management Information Base* (MIB). The agents enable the device to generate traps, which can be configured to be sent to a trap destination server that is running HP SIM. Conceptually, the MIB is a database that can be written to and read by a management application using the SNMP protocol. There are two types of MIBs:

- **Internet Management MIBs.** These MIBs, standardized by the Internet community, include MIB-II, Remote Monitoring (RMON), and others and represent the core objects that are common across the

widest range of network devices implementing the Internet protocols. Examples of these objects include network protocols such as TCP/IP and network systems such as Ethernet network interfaces.

- **Vendor MIBs.** These MIBs represent objects that are unique to an individual vendor's product or product line. Over 500 vendors and organizations have created their own vendor MIBs. HP was the first personal computer company to develop a MIB-enabled SNMP management of system hardware.

SNMP supports both read and write (`GET` and `SET`) commands on attributes. Some vendors do not support the `SET` command because of the potential to allow an unauthorized person to alter critical parameters on a network element. HP SIM primarily only uses the SNMP `GET` command.

SNMP is associated with TCP/IP and used for monitoring systems on Ethernet networks because of its long association with the Internet.

Since its inception, SNMP itself has undergone several updates, including SNMP V2c and SNMP V3. HP SIM supports the original V1-compliant agents and the compilation of V1 and V2 MIBs. SNMP uses UDP port 161 for monitoring systems, while traps are received on port 162.

If your CMS is an HP-UX or Linux system, HP SIM might need to co-exist with other applications using port 162. To accomplish this, use the following procedure to assign HP SIM to use a different port.

1. Open the `globalsettings.props` file located at `/etc/opt/mx/config/globalsettings.props`.
2. Locate the `SnmpTrapPortAddress` property: `SnmpTrapPortAddress=162` .
3. Modify this property by changing the port value to a different port number.
4. Restart HP SIM.



NOTE: HP SIM will not receive traps from the application using port 162 unless the application is configured to forward traps to the port assigned to HP SIM.

NOTE: If the `SnmpTrapPortAddress` entry is deleted, HP SIM will default to port 162.

SNMP communication between systems is used to gather information about a system. HP SIM attempts SNMP communications based on the number of SNMP retries you specify and only stops when the communication is successful or the number of retries is exceeded. HP SIM also waits for SNMP responses between retries, based on the timeout period. Finally, HP SIM can only communicate through SNMP when the community string specified on the system and the community string specified for that system in HP SIM match. The community string, "public," is a commonly used default. However, you can specify any community string needed for your security requirements.



NOTE: Community strings on the managed system and the HP SIM community strings for the system must match to manage the system through SNMP. Some SNMP management agents also provide IP address filtering. Be sure the HP SIM IP address is in the allow list for any given SNMP agents.

DMI

The Desktop Management Task Force (DMTF), formed in 1992 and composed of leading PC industry vendors and corporations, established a common, platform-independent process for specifying methods of managing desktop hardware and software components. HP is a Steering Committee member of the DMTF and helped to define the task force's two pieces of technology: the *Desktop Management Interface* (DMI) software and the *Management Information Format* (MIF) language. DMI software serves as the liaison between desktop-resident management programs, manageable hardware, and software components on the computer. DMI is most commonly used for obtaining information from desktops, but some HP servers and workstations do support DMI.

HTTP

HP SIM also takes advantage of the industry-standard HTTP protocol (used to transfer information over the World Wide Web) for transportation of management information. Many systems support some kind of configuration "home page" that is supported over HTTP or the secure HTTPS protocol. HP SIM attempts to find HTTPS servers running on systems if the **Global Protocol Settings** page has this enabled. See "Setting global protocols" for more information.

WBEM

Web-Based Enterprise Management (WBEM) is one of the newest management protocols. This protocol leverages the industry-standard Common Information Model (CIM) as defined by the DMTF. HP SIM can communicate to systems directly using the WBEM protocol or to the Windows WMI systems using the WMI Mapper Proxy. HP SIM uses WBEM to communicate with storage system *SMI-S WBEM providers*. HP has been leading this effort through its association with the WBEM initiative. WBEM is an initiative supported by HP, Microsoft, Intel, BMC, Cisco, and 120 other platform, operating system, and application software suppliers.

When WBEM is enabled, the management console can obtain information from any *system* that supports WBEM. For WBEM to work, the correct user name and password must be provided for the given system. WBEM enables a larger set of server and storage manageability data to be collected and displayed on the **System Page** and in reports. The presence of WBEM enables the **Properties** pages and enables WBEM indications (events) to be displayed in event collections. Without HTTP enabled, HP SIM will not discover any web-based features on a system.



NOTE: HP SIM supports WBEM over HTTPS to ensure user supplied WBEM name and password pairs are protected.

NOTE: OpenWBEM is not supported.

Related procedures

- Setting global protocols
- Setting protocols and credentials for a system or groups of systems

Related topics

- Protocols
- WMI Mapper Proxy

Protocol functionality

The following table displays descriptions of management protocols displayed under **Management Protocols** on the **System Page** which displays protocols that have responded when attempting to identify the system.



NOTE: The Central Management Server (CMS) initiates the requests for all protocols except events.

Management Standard	Description	Functionality when enabled
Common Information Model (CIM)	A common definition of management information for systems, networks, applications, and services.	System identification, inventory, events
Common Information Model XML (CIM-XML)	A protocol using XML over HTTP to exchange CIM information; part of the WBEM suite of standards.	System identification
Desktop Management Interface (DMI)	DMI is an RPC-based protocol. To operate, DMI requires opening a number of ports through a firewall; therefore, DMI is not recommended for use through firewalls. It is largely being replaced by WBEM. Note: DMI is only used for non-HP systems running Windows NT and for versions of HP-UX prior to 11.0. WMI and WBEM are used for more recent versions.	System identification, inventory data, events
Hyper-Text Transfer Protocol (HTTP and HTTPS)		System identification, management tool launch, agent configuration

Management Standard	Description	Functionality when enabled
Internet Control Message Protocol (ICMP)	ICMP is a required protocol tightly integrated with IP. ICMP messages are delivered in IP packets and are used for out-of-band messages related to network operation. HP SIM can use ICMP messages to ping a managed system. However, some routers block ICMP messages so HP SIM provides an alternative ping using TCP. See "Setting global protocols" for more information.	Provides system reachability (ping) check during system discovery and before other operations
Management Information Base (MIB)	Part of the SNMP specification, the MIB is a model of the information to be managed through SNMP. It is equivalent to the Common Information Model (CIM) defined by WBEM.	System identification, inventory and events
Simple Network Management Protocol (SNMP)	SNMP is widely used for management but the widely implemented versions 1 and 2 have weak security. While no "set" operations are used by HP SIM, read access to system data may be visible on the network. SNMP is UDP-based; therefore, in many environments it is not considered a suitable protocol to pass through the firewall. Because SNMPv1 has a simple, clear-text "community," it provides a low level of security. However, SNMP may be suitable for some environments in which the network used for managing systems is relatively controlled.	System identification, Inventory and events
Secure Shell (SSH)	SSH is used for remote command execution. HP SIM uses SSH to run commands on managed systems.	Remote tool execution
System Management Architecture for Server Hardware (SMASH)	A DMTF initiative for common server management which enables vendor-independent management applications.	Consistent server management across vendors
Storage Management Interface - Specification (SMI-S)	An SNIA standard for storage management using WBEM.	System identification
Web-Based Enterprise Management (WBEM)	A DMTF program with widespread industry support with a set of standards including CIM, CIM-XML, and WS-Management. The CIM-XML protocol is most widely used with WBEM today, and the term WBEM is often used to mean this protocol. Note: Firewalls should be configured to allow the CMS to communicate with managed systems through default port 5989. If you have modified the default port setting for your WBEM provider, you must configure your firewall for the port number your WBEM provider on which it is actually configured."	Identification, inventory, and events
Web Services for Management (WS-Management)	A DMTF standard for exchanging management information using web services. WS-Management may be used to transport CIM as an alternative to CIM-XML.	Identification, inventory, and events

Management Standard	Description	Functionality when enabled
Windows Management Instrumentation (WMI)	WMI is Microsoft's implementation of WBEM. WMI runs over DCOM, which in turn, uses RPC. WMI is generally not suitable through firewalls because a number of ports must be opened and the management traffic cannot be separated from other DCOM requests. For Windows systems behind a firewall, HP recommends installing the WMI Mapper on a managed system in the secure network. This mapper allows standard CIM-XML requests through the firewall, and they are mapped to WMI requests on the managed system.	Identification, inventory, and events

Related topics

- System tab
- System Page
- Setting global protocols

Data collection

Data collection is used to gather data that can be used for reporting. This data can be collected and stored in the database in two ways. You can choose to maintain only the most recent data, enabling you to run reports or compare different systems to each other using Snapshot Comparison. Or, you can store all of the data collected over time, which enables you to use Snapshot Comparison to view trends on a single system.

Data collection uses *SNMP*, *Desktop Management Interface (DMI)*, *Web-Based Enterprise Management (WBEM)*, or a combination of the three protocols to gather information, which ensures you a comprehensive dossier on a system. However, OpenWBEM is not supported. Typically, DMI is instrumented on Windows-based desktop computers and laptops and on HP-UX systems. SNMP is instrumented on Windows-based servers, Linux systems and other networking systems, and can be used to interrogate Windows-based desktops. The WBEM protocol is used to collect data from storage systems such as arrays, tape libraries, Fibre Channel switches, and HBAs. Any device that has a HP Insight Management WBEM Providers for Windows Server 2003/2008 WBEM providers profile identified will have data collected through this provider taking precedence over Windows Management Instrumentation (WMI)/SNMP collection. Data can be collected from any storage system with an *SMI-S provider* that complies with the Storage Networking Industry Association's *Storage Management Initiative Specification*. For more information about SMI-S providers, see the HP SIM user guides located at *HP SIM 5.2 Installation Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html>, and then select the appropriate guide for your operating system.

Instant capacity (iCAP) properties for Cells and Processors for a Complex is collected and displayed using the HP-UX Web-Based Enterprise Management (WBEM). For HP-UX, the following software is required for essential HP Systems Insight Manager (HP SIM) functionality to operate. This software is installed by default as part of the latest HP-UX 11i v3 (11.3), HP-UX 11i v2 (11.23) and HP-UX 11i v1 (11.11) which can only be installed on HP 9000 servers.



NOTE: WBEM providers is only collected under the Web-Based Enterprise Management (WBEM).

After HP Systems Insight Manager (HP SIM) collects data initially, you can schedule a Data Collection task to specify systems and run the task with different schedules. In addition to the default Initial and Bi-Weekly Data Collection tasks built in to HP SIM, you can set up new data collection tasks targeting specific *managed systems*. If you are scheduling to **Overwrite existing data set (for detailed analysis)**, formerly known as Single Instance Data Collection task in Insight Manager 7, having it run once per week (smaller networks) to once per month (larger networks) should be adequate. If you are scheduling to **Append new data set (for historical trend analysis)**, it might be beneficial to run it more frequently, perhaps once per hour for your most important systems, realizing it consumes database storage space.

To create a Data Collection task from the toolbar, select **Options**→**Data Collection**.



NOTE: The Data Collection Report does not display CPU information for Netware systems.

NOTE: To enable data collection to collect data from any of the aforementioned instrumentation protocols, the corresponding protocol must be enabled, and the appropriate protocol settings must be specified, globally or for the specific target system. See “Setting global protocols” for more information about setting global protocol settings and “Setting protocols and credentials for a system or groups of systems” for more information about setting single system protocol settings.

NOTE: To enable collection of DMI data from a DMI-instrumented HP-UX system, be sure that the name of the server that the HP SIM runs on is added to the `/var/dmi/dmimachines` file of the target system.

NOTE: To enable collection of *Windows Management Instrumentation (WMI)* data from WMI-instrumented systems, a WMI Mapper Proxy must have been set up and specified through **Options**→**Protocol Settings**→**WMI Mapper Proxy**. See “Adding a WMI Mapper Proxy” for information about setting up a WMI Mapper Proxy.

Append new data set (for historical trend analysis)

The **Append new data set (for historical trend analysis)** option maintains trend information in separate historical entries. You can use the historical perspective for trend and usage analysis because records change over time. Information gathered by data collection is used in Snapshot Comparison and reports and can be used as *criteria* in system collections. With **Append new data set (for historical trend analysis)**, data detailing the system history is collected. Use **Append new data set (for historical trend analysis)** conservatively and sparingly to track problem systems or problem usage times. Do not overuse this task because it can create a considerable amount of data to be stored.



CAUTION: Do not delete the standard data collection task without replacing it with a substitute task that achieves a similar result. For example, removing the Data Collection task removes the capability for historical analysis and updating any information shown in reporting tables. You must refresh the page to see new data in reports.

Overwrite existing data set (for detailed analysis)

The **Overwrite existing data set (for detailed analysis)** option overwrites any previous information collected. The **Overwrite existing data set (for detailed analysis)** is useful as a snapshot at the current time because it overwrites old information with the current value.

You can view the current data set report from the **System Page**, which you can reach by selecting a system in a collection. See “System Page” for information about the **System Page**.

Running data collection consumes noticeable network resources. Proper scheduling might be appropriate.



IMPORTANT: Multiple instances of the same Status Polling or Data Collection tasks do not run simultaneously.

Initial data collection

The Initial Data Collection task is used to collect information from many systems that have DMI, SNMP, or WBEM running (for example, serial numbers and model numbers). This task is set to run by default when a new system or event meets the search criteria. You can view the Data Collection Report for a system after data has been collected by selecting it from the system table view page. This action displays the **System Page**, where you can select the **Data Collection Report** link from the **Tools & Links** tab. Other report formats are available from the Reporting tool. See “Reporting” for more information about reporting.

Bi-weekly data collection

The Bi-Weekly Data Collection task runs the **Overwrite existing data set (for detailed analysis)** option on all of the systems in the system default collection. The default schedule is to run every two weeks on Saturday at 12:00 a.m. You can view the Data Collection Report for a system after data has been collected by selecting it from the system table view page. This action displays the **System Page**, where you can select the **Tools & Links** tab and then click **Data Collection**.

Related procedures

- ▲ Creating a data collection task

Related topics

- Discovery and identification
- Protocols
- Reference information
- System Page
- Reporting

Creating a data collection task

Data collection is used to gather data that can be used for reporting. You can collect detailed data to use for reporting or for comparing different systems with Snapshot Comparisons, or you can collect less detailed data but collect it over time, which enables you to use Snapshot Comparisons to view trends on a single system.

To create a Data Collection task:

1. Select **Options**→**Data Collection**. The **Data Collection** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**.
4. Specify how to save data by selecting:
 - **Overwrite existing data set (for detailed analysis)**. Provides a network snapshot at a certain time
 - **Append new data set (for historical trend analysis)**. Provides trend and usage analysis
5. Select one of the following options to execute the task:
 - Click **Schedule** to schedule when the task should run. See “Scheduling a task”.
 - Click **Run Now** to run the task now. The **Task Results Page** appears. See “Task results list”.
 - Click **Previous** to return to the previous page.
6. Click **Done**.

View the task results by selecting the desired data collection task on the **All Scheduled Tasks** page. See “Task results list” for more information about the All Scheduled Tasks page.

Command line interface

Use the `mxtask` command to perform this task from the command line interface. For assistance with this command, see the HP-UX or Linux manpage by entering `mxtask` at the command line or the Windows command help. See “Using command line interface commands” for information about accessing the manpage.

Related topics

- Data collection
- Reference information

System properties

The Set System Properties tool enables you to set system properties for a single system or for multiple systems.



NOTE: System properties that are edited in HP Systems Insight Manager (HP SIM) are not transferred to HP Storage Essentials products.

You have two options for setting system properties:

- **Edit system properties for a single system** Select the **Tools & Links** tab on the **System Page**, and then click the **Edit System Properties** link.
- **Set system properties for multiple systems** Select **Options**→**System Properties**→**Set System Properties**.

The Suspend or Resume Monitoring tool enables you to suspend monitoring of a single system or multiple systems, which enables systems to be excluded from status polling, identification, data collection, and the automatic event handling features of HP SIM. The available suspend lengths include the predetermined increments of five minutes, 15 minutes, one hour, and one day. The suspend tool can also be turned on indefinitely. Configuration changes take effect immediately. To view the new settings for a system, click the **System** tab on the **System Page**. Changes made with this tool override previous settings. A system that is suspended appears with a disabled icon throughout HP SIM.

You can suspend or resume monitoring using one of the following methods:

- **Suspend or resume monitoring for a single system** Click the **Tools & Links** tab on the **System Page**, and then click the **Suspend/Resume Monitoring** link.
- **Suspend or resume monitoring for multiple systems** Select **Options**→**System Properties**→**Suspend or Resume Monitoring**.



NOTE: You must have *administrative rights* to access these tools.

Related procedures

- Editing system properties for a single system
- Editing system properties for multiple systems
- Suspending or resuming system monitoring for a single system
- Suspending or resuming system monitoring for multiple systems

Related topic

- ▲ System Page

Editing system properties for a single system

The **Edit System Properties** link allows you to re-configure system properties for a single system through its **System Page** which is made up of the following sections. You must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the system you want to update.



NOTE: It is possible to change system properties for multiple systems if care is not taken. Read all additional notes in this section to understand what precautions must be taken.

Examples

Setting Customer Company and Contact Information Globally

Setting Customer Company and Contact Information Individually

Setting Customer Company and Contact Information for Complex Deployments

Setting Customer Company and Contact Information Globally

The preferred method for setting customer company and customer contact information for multiple devices, is to use HP SIM **Set System Properties** task. The following example will set up all remotely monitored devices with the same information.

To ensure that properties are propagated to all existing discovered devices, perform the following steps:

1. Select HP SIM **Options**→**System Properties**→**Set System Properties**
2. In the task's **Step 1: Select and Verify Target Systems**, select **Remote Support Eligible** from the drop down menu, then click the **Select "Remote Support Eligible" itself** radio button.
3. In **Step 2: Set Properties**, fill out the **Customer Company** and **Customer Contact** information, especially those fields designated by *.
4. Select **Run Now** which will propagate these properties across all devices that are currently discovered in the Remote Support Eligible (RSE) list.

To ensure that these properties are automatically propagated to newly subsequently discovered devices, perform these additional steps:

1. Select the task using HP SIM **Options**→**System Properties**→**Set System Properties**
2. In the task's **Step 1: Select and Verify Target Systems**, select **Remote Support Eligible** from the drop down menu, then click the **Select "Remote Support Eligible" itself** radio button.
3. In **Step 2: Set Properties**, fill out the **Customer Company** and **Customer Contact** information, especially those fields designated by *.
4. Select **Schedule** to move to **Step 3: Schedule Task**.
5. For this example we will use the Task Name provided by HP SIM.
Select *When new systems or events are added to the collection* option under **When would you like this task to run?**
6. Select **Done**. This will create the scheduled task to automatically propagate the properties whenever a new device is discovered in HP SIM and added to the Remote Support Eligible list.

Setting Customer Company and Contact Information Individually

If the customer company or contact information is different among multiple devices, the preferred configuration method is also through the **Set System Properties** or **Edit System Properties** page using the procedures outlined below.

HP SIM 5.1 or greater provides two sections on the **Set System Properties** page under **Contract and Warranty Information**, called **Customer Company Information** and **Customer Contact**. Each section is treated by HP SIM as a unique database record with the first field of each section representing the record's header.

The **Customer Company Information** section uses **Company name** as the header, and **Customer Contact** uses **Contact's first name** and **Contact's last name** as the header. You must be aware, when entering information in these sections, that certain properties are tied to the **Company name** and **Contact's first name / last name** fields. If information is meant to be unique for a particular device or device location, you must ensure that the **Company name** and/or **Contact's first name/last name** are also unique.

Under **Customer Contact**, changing any of the fields **Contact job title** through **Contact other** will change the corresponding properties for *all* of the devices that use the same **Contact's first name/last name**.

For example, if the **Company name** was set globally to *Widgets Inc.* and you require a unique address for an individual device located in Brussels. You can create a **Company name** of *Widgets Inc. – Brussels* to ensure that the unique address information for this system does not overwrite the other system's **Customer Company** information, nor will it be overwritten if changes are made to those devices.



IMPORTANT: Although HP SIM currently does not require you to complete both **Customer Company Information** and **Customer Contact** sections, the Remote Support Pack requires both sections are filled out, especially the fields designated by *.

Setting Customer Company and Contact Information for Complex Deployments

When remotely monitored devices are hosted in several different locations, and service is to be provided at the various locations, it may be useful to customize **Remote Support Eligible** collections and **Set System Properties** tasks.

In this example, the company *Widgets Inc.* has devices located in three locations: **London**, **New York City** and **Brussels**. The Central Management Server (CMS) is located in *London*, which hosts the Remote Support Pack with HP SIM. The other monitored devices are split between the *New York City* and *Brussels* locations.

In the first procedure, new HP SIM collections are created for remote support and devices will be added to each collection.

1. Select **Customize** under **System and Event Collections** in the left navigation panel.
2. From the **Show collections of:** dropdown menu, verify that **Systems** is displayed, then select **New**.
3. Select **Choose members individually** under **New Collection**.
4. Select **Choose members individually** under **New Collection**.
5. In the **Choose from:** dropdown menu, select **Remote Support Eligible**.
6. Find the devices (including the CMS) to be monitored, in the **Available Items** list, and move them to the **Selected Members** list.



NOTE: The added devices will still be part of the original Remote Support Eligible collection.

7. Select **Save As Collection...** and provide a **Collection name**. In this example, a practical name would be *Remote Support Eligible – London*, as it labels a collection of remotely monitored devices located in London.
8. To display the new collection beneath the Remote Support Eligible collection in the left navigation panel, select **Shared** in the **Existing collection:** dropdown menu.
9. Click **OK** to create the new collection *Remote Support Eligible – London*.

Repeat the first procedure to create two additional collections named *Remote Support Eligible – New York City* and *Remote Support Eligible – Brussels*.

In the second procedure, properties are entered and propagated to existing discovered devices.

1. Ensure that properties are propagated to all existing discovered devices in the *Remote Support Eligible – London* collection.
2. Select the task using HP SIM **Options**→**System Properties**→**Set System Properties**.
3. On the **Step 1: Select and Verify Target Systems** page, select the entire *Remote Support Eligible - London* collection.
4. In **Step 2: Set Properties**, fill out the **Customer Company Information** and **Customer Contact** sections, especially those fields designated by *.



NOTE: The added devices will still be part of the original Remote Support Eligible collection, since you will probably require a unique company and contact information. You might want to jot these down for subsequent entry in the third procedure.

5. Select **Run Now**. This will propagate the properties across all devices that are currently discovered in the *Remote Support Eligible – London* collection.

Repeat the second procedure for the *Remote Support Eligible – New York City* and *Remote Support Eligible – Brussels* collections.

The third procedure is to ensure that these properties are automatically propagated to newly, subsequently discovered devices in the *Remote Support Eligible – London* collection, perform these additional steps:

1. Select the task using HP SIM **Options**→**System Properties**→**Set System Properties**.
2. On the **Step 1: Select and Verify Target Systems** page, select the entire *Remote Support Eligible - London* list.
3. In **Step 2: Set Properties**, fill out the **Customer Company Information** and **Customer Contact** sections, especially those fields designated by *. Use the same properties that you used in the second procedure above.
4. Select **Schedule** to move to the **Step 3: Schedule Task** page.
5. Provide a **Task Name**. A practical name would be *Set System Properties - London*.
6. Select **When new systems or events are added to the collection** under **When would you like this task to run?**
7. Select **Done**. This creates the scheduled task to automatically propagate the properties whenever a new device is discovered in HP SIM and added to the *Remote Support Eligible - London* collection.

Repeat the third procedure to create the *Set System Properties – New York City* and *Set System Properties – Brussels* tasks.

A fourth procedure would most likely have to be created manually whenever new systems are added to the **Remote Support Eligible** collection. You must add these devices to one of the three new remote support

locations or create a new collection if it is in a different location. For example, the following is a procedure to add a monitored device to the *London* location.

1. Select **Customize** under **System and Event Collections** in the left navigation panel.
2. From the **Show collections of:** dropdown menu, verify that **Systems** is displayed, and then select the *Remote Support Eligible – London* collection.
3. Click **Edit**.
4. In the **Choose from:** dropdown menu, select *Remote Support Eligible*.



NOTE: The devices will still be part of the Remote Support Eligible collection.

5. Find the new device in the **Available Items** list, and move it to the **Selected Members** list.



NOTE: The device will still be part of the Remote Support Eligible collection.

6. Click **OK** to add the device to the *Remote Support Eligible – London* collection. This will automatically invoke the **Set System Properties – London** task to propagate the existing properties entered with that task.

System information

The information in this section is obtained during *Discovery* and *Identification*. You can update these properties as described below.

- **Identification** This section includes the following information:
 - **Preferred System Name** With this property, you have the capability to specify how the system (including the CMS) appears in the HP Systems Insight Manager (HP SIM) user interface. The **Restore Default Name** button sets the displayed name back to the name originally discovered by HP SIM.



NOTE: If you change the preferred name, a warning message appears stating that any lists referring to this system by name might no longer work, and any subsequent discoveries of a system using the new name cause the system name change to be changed back to the host (DNS) name.

- **Prevent the Discovery process from changing this system name** When checked, this prevents Discovery from overwriting the preferred system name.
- **Serial number** This is the serial number of the system. Any user-entered value will be overwritten by Identification, regardless of the checkbox setting described below. This field is read-only if it is set by Discovery. For Contract and Warranty data collection, if you want to override the serial number obtained by Discovery, enter a number in the **Customer-Entered serial number** field.
- **Product Description** All properties are configurable.
 - **System type.** This is the System type for the system, click the down arrow and select the appropriate System type.
 - **System subtype 1 - 8.** This is the System subtype for the system, click the down arrow and select the appropriate System subtype. You can provide up to eight different system subtypes.
 - **Product model.** This is a free form field and you can enter the system model number here.
 - **Hardware description.** This is a free form field describing the hardware.
 - **Operating system description.** This is the name of operating system running on the system, if any.
 - **Operating system for tool filtering.** This is the operating system for tool filtering, click the down arrow and select the operating system.
 - **Operating system version.** This is a free form field and is the operating system version.
- **Contact Information**

- **Contact** This is a free form field and is the contact user for the system.
- **Location** This is a free form field and is the physical location of the system.
- **Asset Information**
 - **Asset number** This is the asset number of the system and is retrieved through the Data Collection process.
 - **Prevent the Discovery, Identification, and Data Collection processes from changing these system properties** When checked, Discovery, Identification, and Data Collection do not overwrite any of the property values. However, when deselected, the Discovery, Identification, and Data Collection processes might overwrite or clear the properties. One exception to this behavior is with the serial number which is overwritten with any serial number obtained through Identification, regardless of this checkbox setting.



NOTE: If this box is deselected and you click **OK**, HP SIM checks to see if any changes have been made. If so, a warning message appears stating that your changes might be overwritten by the next Discovery. To avoid having Discovery overwrite your changes, you should check this box.

Contract and warranty information

The information in this section is optional.

Asset Information

- **Customer-Entered serial number** The user-entered serial number of the system. When collecting contract and warranty data, this serial number overrides the serial number obtained during Discovery. This serial number must match a serial number that is on record with HP. Entering a serial number here is not required if the serial number was obtained during Discovery.
- **Product number** The user-entered product number of the system. Typically, the product number is the number used to order a system. This number is usually in the format XXXXXX:XXX. HP SIM will try to obtain this number automatically.
- **System Country code** The International Organization for Standardization (ISO) code for your country. The correct country code must be selected for proper reporting of contract and warranty data. See <http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html> for the list of country codes.
- **Entitlement type** This option is required only if you have a service contract with HP. Choose from the following:
 - Customers with service contracts issued by Compaq before HP and Compaq merged should select **Pre-merger Compaq Contract**.
 - Customers with service contracts issued by HP before HP and Compaq merged should select **System Handle**.
 - Customers recently issued a new service contract or migrated from an old pre-merger company contract to a new HP contract should select **SAID** (Service Agreement ID).
 - Customers who purchased an extended warranty at the time the device was purchased should select **Carepack**.
- **Entitlement ID** The ID of the contract, if you entered one. Depending on the selected contract type, the following applies:
 - For Pre-merger Compaq contracts, the contract identifier is on the contract itself.
 - System Handles are on the contract. System Handles are case sensitive and generally use uppercase letters.

- For SAIDs, the documentation provided with the contract explains where to find the SAID. The SAID is a 12-digit number starting with 1. Although it might appear on the contract as a sequence of three four-digit numbers, enter the number as a single 12 digit number without spaces.
- For the HP Carepack, there is a separate support serial number that is different than the serial number for the product itself. Enter the Carepack serial number as the contract identifier.
- **Obligation ID** Platinum, Gold, or Silver pre-merger Compaq contracts provide a red access ID (also called an obligation ID or software access number). Compaq Software Obligation IDs were only issued in North America.

Customer Company Information

This section is for the company's name, address, and time zone. If you enter a company name, any field with an asterisk is also required.



NOTE: When you update the details for an existing company name, HP SIM automatically updates the details for all systems with a matching company name. If you have multiple addresses for a single company, use a unique company name for each one.

- **Company Name** The company name of that the system belongs to.
- **Address 1** The company address first line.
- **Address 2** The company address second line.
- **City** The name of the city that the system is located in.
- **State or province** The name of the state the system is located in. Select state from the dropdown list.
- **Postal Code** The city zip code. This can include the dash with additional four digits.
- **Country** The country name.
- **Time zone** The time zone that the city is located in. Select the appropriate time zone from the dropdown list.

Customer Contact

This section is for information about the contact person responsible for this system. If you enter a first name, a last name is required. The **Contact other** field is for information that does not fit into the previous fields. For example, if this contact person is available from 8:00 a.m. until 7:00 p.m., you could enter that information here.



NOTE: When you update the contact e-mail, phone number, or other information for an existing contact, the HP SIM automatically updates the details for all systems that use the same contact name.

- **Salutation** The salutation of the contact person. Select from the dropdown list.
- **Contact's first name** The first name of a contact that support can use to notify at the customer site.
- **Contact's last name** The last name of a contact that support can use to notify at the customer site.
- **Contact job title** The contact person's job title. This is a free-form field.
- **Contact phone** The phone number of the contact person. Extension can be included by entering `ext.` before the extension number. For example, 555-123-4567 ext. 89.
- **Contact email** The contact person's e-mail address. This field is alphanumeric and can contain only one e-mail address.
- **Contact other** This field is a free-form and can included information such as availability of the contact person, language preference, and so on.

Select **Prevent the Discovery, Identification and Data Collection processes from changing these system properties** to prevent these processes from overwriting the system properties you have set.

Select **Do not gather entitlement data for this system**

Reconfiguring system properties

To reconfigure system properties:

1. From the **System Page**, select the **Tools & Links** tab.
2. Click the **Edit Systems Properties** link to reconfigure the system properties for an individual system. The **Edit System Properties** page appears.
3. Edit any desired fields.
Note: If the serial number field in the **System Information** section was set by discovery, you cannot edit it.
4. Click **OK** to apply the attribute changes or click **Cancel** to cancel all changes. After clicking **OK** or **Cancel**, you are returned to the **Tools & Links** tab.



NOTE: Changing system properties might affect collection results. Changing the **Preferred System Name** of a system affects any system-by-name collections that the user has created. Changing the System type affects any by-system-type collections.

See “Editing system properties for multiple systems” for information about setting system properties for multiple systems.

Related topics

- [System Page](#)
- [Tools & Links tab](#)
- [Editing system properties for multiple systems](#)
- [Viewing contract and warranty information](#)

Editing system properties for multiple systems

This tool enables you to edit system properties for multiple systems at one time. The **Set System Properties** page for multiple systems is similar to the **Edit System Properties** page for a single system, except that a checkbox appears next to each property. The checkboxes enable you to select the properties you want to configure when the tool executes. Only the selected properties are saved as a property for the target systems. If the value of the selected property is blank, that property is not set for the systems **All properties** are optional.



NOTE: This tool does not affect systems that are managed by HP Storage Essentials products.

NOTE: This tool can be used for a single system. However, some of the properties that are available from the **System Page** are not available when selecting this option. For example, the serial number is not available here, whereas it is available from the **System Page**.

NOTE: To complete this procedure, you must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the systems you want to update.

To edit system properties for multiple systems:

1. Select **Options**→**System Properties**→**Set System Properties**. The **Set System Properties** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**.



NOTE: Steps 4-8 apply to the properties in the **System Information** section of the page.

4. Under **Identification**, select **Restore the default system name** to change the name displayed in HP Systems Insight Manager (HP SIM) to the host (DNS) name.

5. Under **Product Description**, select the properties you want to configure. The properties include the following:
 - **System type** The system type for the system, click the down arrow, and then select the appropriate System type.
 - **System subtype 1 - 8** The system subtype for the system, click the down arrow, and then select the appropriate system subtype. You can provide up to eight different system subtypes.
 - **Product model** This free-form field enables you to enter the system model number here.
 - **Hardware description** This free-form field describes the hardware.
 - **Operating system description** The name of operating system running on the system, if any.
 - **Operating system for tool filtering** The operating system for tool filtering, click the down arrow, and then select the operating system.
 - **Operating system version** This free-form field lists the operating system version.
6. Under **Contact Information**, select from the following options:
 - **System contact** This free-form field lists the contact user for the system.
 - **System location** This free-form field lists the physical location of the system.
7. Under **Asset Information**, select the **Asset number** and enter the asset number of the system.
8. Under **System Property Lock**, select from the following options:
 - **Lock - Prevent the Discovery and Identification processes from changing any system properties** The attribute lock setting of the target systems is set, preventing discovery and Identification from overwriting its properties.
 - **Unlock - Allow the Discovery and Identification processes to change system properties** The attribute lock setting of the target systems are cleared, enabling discovery and Identification to overwrite its properties.
 - **Ignore - Do not set the lock property of the target systems** The current attribute lock setting of the target systems remain unchanged.



NOTE: Steps 9-13 apply to the properties in the **Contract and Warranty Information** section of the page.

9. Under **Asset Information**, select the properties you want to configure. The properties include the following:
 - **Product number** The user-entered product number of the system. Typically, the product number is the number used to order a system. This number is usually in the format XXXXXX-XXX. HP SIM will try to obtain this number automatically.
 - **System Country code** The International Organization for Standardization (ISO) code for your country. The correct country code must be selected for proper reporting of contract and warranty data. See <http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html> for the list of country codes.
 - **Entitlement type** This option is required only if you have a service contract with HP. Choose from the following:
 - Customers with service contracts issued by Compaq before HP and Compaq merged should select **Pre-merger Compaq Contract**.
 - Customers with service contracts issued by HP before HP and Compaq merged should select **System Handle**.

- Customers recently issued a new service contract or migrated from an old pre-merger company contract to a new HP contract should select **SAID** (Service Agreement ID).
- Customers who purchased an extended warranty at the time the device was purchased should select **Carepack**.
- **Entitlement ID** The ID of the contract, if you entered one. Depending on the selected contract type, the following applies:
 - For Pre-merger Compaq contracts, the contract identifier is on the contract itself.
 - System Handles are on the contract. System Handles are case sensitive and generally use uppercase letters.
 - For SAIDs, the documentation provided with the contract explains where to find the SAID. The SAID is a 12-digit number starting with 1. Although it might appear on the contract as a sequence of three four-digit numbers, enter the number as a single 12 digit number without spaces.
 - For the HP Carepack, there is a separate support serial number that is different than the serial number for the product itself. Enter the Carepack serial number as the contract identifier.
- **Obligation ID** Platinum, Gold, or Silver pre-merger Compaq contracts provide a red access ID (also called an obligation ID or software access number). Compaq Software Obligation IDs were only issued in North America.

10. Under **Customer Company Information**, select **Set company information** and enter your company details. If you enter a company name, any field with an asterisk is also required.



NOTE: When you update the details for an existing company name, HP SIM automatically updates the details for all systems with a matching company name. If you have multiple addresses for a single company, use a unique company name for each one.

- **Company Name** The company name of that the system belongs to.
- **Address 1** The company address first line.
- **Address 2** The company address second line.
- **City** The name of the city that the system is located in.
- **State or province** The name of the state the system is located in. Select state from the dropdown list.
- **Postal Code** The city zip code. This can include the dash with additional four digits.
- **Country** The country name.
- **Time zone** The time zone that the city is located in. Select the appropriate time zone from the dropdown list.

11. Under **Customer Contact**, select **Set customer contact information** and enter information about the contact person responsible for this system. If you enter a first name, a last name is also required. The **Contact other** field is for additional information that does not fit into the previous fields. For example, if this contact person is available from 8:00 a.m. until 7:00 p.m., you could enter that information here.



NOTE: When you update the contact e-mail, phone number, or other information for an existing contact, the HP SIM automatically updates the details for all systems that use the same contact name.

- **Salutation** The salutation of the contact person. Select from the dropdown list.
- **Contact's first name** The first name of a contact that support can use to notify at the customer site.

- **Contact's last name** The last name of a contact that support can use to notify at the customer site.
- **Contact job title** The contact person's job title. This is a free-form field.
- **Contact phone** The phone number of the contact person. Extension can be included by entering **ext.** before the extension number. For example, 555-123-4567 ext. 89.
- **Contact email** The contact person's e-mail address. This field is alphanumeric and can contain only one e-mail address.
- **Contact other** This field is a free-form and can included information such as availability of the contact person, language preference, and so on.

12. Click **Previous** to select different target systems, click **Schedule** to schedule the task, or click **Run Now** to run the task immediately.

See “Editing system properties for a single system” for information about setting system properties for a single system.

Related topics

- System Page
- Tools & Links tab
- Viewing contract and warranty information
- HP Service Essentials Remote Support Pack

Suspending or resuming system monitoring for a single system

The **Suspend/Resume Monitoring** link enables you to set the timer for suspending monitoring. The Suspend or Resume Monitoring command has no effect on HP Storage Essentials systems.



NOTE: To complete this procedure, you must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the system you want to update.

To suspend or resume system monitoring on a single system:

1. Select **Tools**→**System Information**→**System Page**. The **System Page** appears.
Note: You can also access the **System Page** by selecting a system name in the **System Name** column of the system table view page.
2. Select the target system. See “Creating a task” for more information.
3. Select the **Tools & Links** tab.
4. Click the **Suspend/Resume Monitoring** link. The **Suspend/Resume Monitoring** page appears.
5. Select one of the following options:
 - **Enable monitoring of this system** Select this option if you no longer want the system to be suspended.
 - **Suspend monitoring of this system for** Select this option if you want to suspend a system for a set amount of time. Set the time by clicking the dropdown arrow and selecting an option.
 - **Suspend monitoring of this system indefinitely** Select this option to suspend a system until it is set otherwise.
6. Click **OK** to apply the changes or click **Cancel** to cancel changes. After clicking **OK** or **Cancel** you are returned to the **Tools & Links** tab.

See “Suspending or resuming system monitoring for multiple systems” for information about suspending or resuming monitoring for multiple systems.

Related procedure

- ▲ Editing system properties for multiple systems

Related topics

- System Page
- Suspending or resuming system monitoring for multiple systems

Suspending or resuming system monitoring for multiple systems

The Suspend or Resume Monitoring tool enables you to set the timer for suspending monitoring of multiple systems. The Suspend or Resume Monitoring tool has no effect on HP Storage Essentials systems.



NOTE:

To complete this procedure, you must be authorized to use the **EDIT_SYSTEM_PROPERTIES** tool on the systems you want to update.

To suspend or resume system monitoring for multiple systems:

1. Select **Options**→**System Properties**→**Suspend or Resume Monitoring**. The **Suspend or Resume Monitoring** page appears.
2. Select target systems. See “Creating a task” for more information.
3. Click **Next**. You can click **Add Targets** to add additional systems or select targets and click **Remove Targets** to remove the systems.
4. Select one of the following options:
 - **Enable monitoring of target systems** Select this option if you no longer want the target systems to be suspended.
 - **Suspend monitoring of target systems for** Select this option if you want to suspend target systems for a set amount of time. Set the time by clicking the dropdown arrow and selecting an option.
 - **Suspend monitoring of target systems indefinitely** Select this option to suspend target systems until it is set otherwise.
5. Click **Previous** to select different target systems, click **Schedule** to schedule the task, or click **Run Now** to run the task immediately.

See “Suspending or resuming system monitoring for a single system” for information about suspending or resuming monitoring for a single system.

Related procedure

- ▲ Suspending or resuming system monitoring for a single system

Related topics

- System Page
- System tab
- Tools & Links tab

Version Control Repository



HP Systems Insight Manager (HP SIM) enables you to specify an HP Version Control Repository Manager. The VCRM stores the latest HP ProLiant Support Packs providing the latest software.

To specify a Version Control Repository:

1. Select **Options**→**Version Control Repository**. The **Version Control Repository** page appears.
2. Under **Select the default version control repository**, select a system that has the VCRM installed.

Note: The system that has the VCRM installed must be trusted. See “Trusted certificates” for more information regarding trust relationships. After the trust relationship is established, click **Last Update** to update the **Trusted?** column to **Yes**.

3. Under **Contents of selected version control repository**, click the  icon to drill down and view the contents of the selected Version Control Repository.

Note: To expand the tree to display all contents, click the  icon, located in the upper-right corner of the **Contents of selected version control repository** section. Click the  icon to collapse the listings.

Note: Click any column heading to sort by that column in ascending or descending order.

Note: This section displays systems that are authorized by the current user. If the current user is not authorized to view any systems with the HP Version Control Repository Manager, the system will not be listed in the **Select the default Version Control Repository** section. If there are no *discovered systems* running the VCRM, a message appears, indicating that no repository could be found.

4. Click **OK** to apply your selection. A message appears, indicating if the repository setting was successfully saved.
5. Click **OK** to close the dialog box.

Related topics

- [Version Control](#)
- [About the Version Control Repository Manager](#)
- [About the Version Control Agent](#)

PMP administrative options

Two *HP Performance Management Pack* (PMP) administrative tools are available through HP Systems Insight Manager (HP SIM):

- **Configuration** Enables you to monitor the performance of selected servers, change the monitoring parameters of the monitored servers, and apply licenses to servers and additional licenses to PMP.

To access **Configuration**, select **Options**→**HP Performance Management Pack** **Options**→**Configuration**.

To access help for this option, go to

https://middle_tier:2381/pmp/help/Monitoring_Administration.htm, where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\HP Performance Management Pack\PMP\htm\help\Monitoring_Administration.htm, where *PMP directory* is the PMP directory on the server where PMP is installed.

- **Manual Log Purge** Enables you to delete the unwanted or past logged data from the PMP repository.

To access **Manual Log Purge**, select **Options**→**HP Performance Management Pack** **Options**→**Manual Log Purge**.

To access help for this option, go to

https://middle_tier:2381/pmptools/help/ManualLogPurge.htm, where *middle_tier* is the name or IP address of the server that HP SIM and PMP are installed, or access *PMP directory*\Program Files\HP\HP Performance Management Pack\PMPTools\htm\help\ManualLogPurge.htm, where *PMP directory* is the PMP directory on the server where PMP is installed.

Related topics

- [PMP tools](#)
- [PMP reporting options](#)

Managing SSH keys

The **SSH Keys** feature enables you to view and manage the public *Secure Shell* (SSH) keys, stored in the *known_hosts* file, from the *Central Management Server* (CMS). SSH keys enable the CMS and a managed system to authenticate a secure connection.

HP Systems Insight Manager (HP SIM) provides the following SSH key configuration options:

- **Select secure shell public keys security level** Select **Options**→**Security**→**SSH Host Keys**.
- **Importing SSH keys** Select **Options**→**Security**→**SSH Host Keys**, select the SSH Key to be imported, and then click **Import**.
- **Exporting SSH keys** Select **Options**→**Security**→**SSH Host Keys**, select the SSH Key to be exported, and then click **Export**.
- **Deleting SSH keys** Select **Options**→**Security**→**SSH Host Keys**, select the SSH Key to be deleted, and then click **Delete**.

Related procedures

- Importing an SSH key
- Exporting an SSH key
- Deleting an SSH key
- Configuring SSH key security

Configuring SSH key security

Configuring the *Secure Shell* (SSH) key security level enables you to specify the level of security on the *Central Management Server* (CMS).

To configure the SSH key security level on the CMS:

1. Select **Options**→**Security**→**SSH Host Keys**. The **Managed System SSH Host Keys** page appears.

Under **Select managed systems SSH host key behavior**, the following options are available:

- **The Central Management Server will save the SSH host key the first time an SSH connection is made.**
- **The Central Management Server will accept an SSH connection with any host key, even if not in the list below.**

This option is selected by default.

This option causes all connections to the host to be accepted, even when the SSH key has changed. The `known_hosts` file is disabled and updated to reflect the new key.

Note: This option provides no protection against man-in-middle attacks.

- **The Central Management Server will accept an SSH connection only if the host key is in the list below**

This option requires the SSH key to appear in the **Managed Systems SSH Host Keys** list.

Note: HP recommends this option because it is the most secure.

2. Click **OK**. The setting is saved.

Note: Alternately, you can set the property value for `MX_SSH_ADD_UNKNOWN_HOSTS`, in `mx.properties` file, to either **ALWAYS**, **NEVER**, or **FIRST TIME**. Restart the HP SIM service for the setting to take effect.

Related procedures

- Importing an SSH key
- Exporting an SSH key
- Deleting an SSH key

Related topic

- ▲ Managing SSH keys

Importing an SSH key

Importing a *Secure Shell* (SSH) key list enables the *Central Management Server* (CMS) to authenticate a secure connection and execute commands on managed systems. Multiple SSH keys are imported from one file, and each SSH key appears on a line and is associated with a host system.



NOTE: Only correctly formatted SSH keys can be imported into the Managed Systems SSH public keys list.

See the *Secure Shell (SSH) in HP SIM 5.x* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information about the format of the SSH keys file.

To import an SSH key on the CMS:

1. Select **Options**→**Security**→**SSH Host Keys**. The **Managed System SSH Host Keys** page appears.
2. Click **Import**. The **Import SSH host Keys** section appears under the **Managed System SSH Host Keys** list.
3. Click **Browse** to navigate to the `file` that contains the SSH keys to be imported.
4. Select the file and click **Open** to add the key to the **Managed Systems SSH Public Keys** list, or click **Cancel** to abort the operation.

Related procedures

- Exporting an SSH key
- Deleting an SSH key
- Configuring SSH key security

Related topic

- ▲ Managing SSH keys

Exporting an SSH key

Exporting selected *Secure Shell* (SSH) keys saves the SSH keys to a file. This file can be used to import the SSH keys into the SSH key list on other systems.

To export SSH keys on the *Central Management Server* (CMS) to a file:

1. Select **Options**→**Security**→**SSH Host Keys**. The **Managed System SSH Host Keys** page appears.
2. From the **Managed System SSH Host Keys** list, select the SSH key to be exported. You can select **System** to select all SSH keys in the list.
3. Click **Export**. The **Export SSH host Keys** section appears.
4. Right-click the link provided and select **Save Target As**. The **Save As** dialog box appears.
5. Navigate to the directory where you want to store the file.
6. Click **Save**. The key is exported.
7. Click **OK**.

Related procedures

- Importing an SSH key
- Deleting an SSH key
- Configuring SSH key security

Related topic

- ▲ Managing SSH keys

Deleting an SSH key

Deleting *Secure Shell* (SSH) keys from the **Managed System SSH Host Keys** list enables you to remove SSH trusted keys on the *Central Management Server* (CMS).

To delete an SSH key on the CMS:

1. Select **Options**→**Security**→**SSH Host Keys**. The **Managed System SSH Host Keys** page appears.
2. From the **Managed System SSH Host Keys** list, select the SSH key to be deleted.
3. Click **Delete**. A message appears, indicating you are about to delete SSH keys.
4. Click **OK**. The key is removed from the **Managed Systems SSH Public Keys** list.

Related procedures

- Importing an SSH key
- Exporting an SSH key
- Configuring SSH key security

Related topic

- ▲ Managing SSH keys

Configuring SSH bypass properties

The `globalsettings.props` has many configurable properties. These settings are used to fine-tune the performance of various settings of HP Systems Insight Manager (HP SIM) to adjust to your running environment.

SSH Bypass is used to boost performance by bypassing the overhead of setting up SSH connections for specified users when the *Central Management Server* (CMS) is executing a tool locally on the CMS. This also alleviates potential problems with SSH not being configured properly locally. This applies to tools that run exclusively on the CMS. This feature was introduced with HP SIM 4.2 SP2 – Windows and is also included for HP-UX and Linux with HP SIM 5.0. This feature is enabled by default for the root user on HP-UX and Linux and for the administrator and the installer account on Windows.

To configure SSH bypass properties in `globalsettings.props`:

1. Open the `globalsettings.props` file located at:
 - **On Windows** It is typically located at `C:\Program Files\HP\System Insight Manager\config\globalsettings.props`.
 - **On HP-UX and Linux** It is located at `/etc/opt/mx/config/globalsettings.props`.
2. Edit the following properties:
 - **`mx_dtf_ssh_bypass_user`** Modify this property to add additional user names for the SSH bypass feature. Separate each with a comma. For Windows domain accounts, two backslashes must exist between the domain name and the user name. For example, `mydomain\myname`. Do not add a user name if you do not intend for them to have full administrator privileges on the CMS.
 - **`mx_dtf_enable_ssh_bypass`** Set this property to `True` to bypass use of SSH for most local tools for the users listed in `mx_dtf_ssh_bypass_user`, or set to `False` to always use SSH tools that execute locally. The default setting is set to `True`.

Audit log

HP Systems Insight Manager (HP SIM) logs all *tasks* performed by all HP SIM *users* on all *systems*. The information is stored in the Audit Log file on the *Central Management Server* (CMS). Several features of the HP SIM Audit Log are configurable. For example, you can specify which tools log data and the maximum Audit Log file size. The HP SIM Audit Log is configured through the `log.properties` file, and tool logging is enabled or disabled through the *XML* tool definition files.

Configuring the HP SIM audit log

Configuring the HP SIM Audit log is performed from the *command line interface* (CLI), and you must be signed-in as root or administrator.

See “Configuring the audit log file” for more information.

Configuring the tool definition files

The XML tool definition file provides an option to disable logging of *single-system aware* (SSA) and *multiple-system aware* (MSA) command tools. The log attribute for the command element specifies whether the results of the command are output to the HP SIM log file. Command output is logged by default.

Configuring the log.properties file

You might need to create the file and name it `log.properties` if one does not exist in the directory. HP SIM uses default values when the file does not exist or when a variable is not defined in the file.

See “Configuring the audit log file” for more information.

Related topic

- ▲ Viewing the Audit Log

Viewing the Audit Log

HP Systems Insight Manager (HP SIM) logs all *tasks* performed by all HP SIM *users* on all *systems*. The information is stored in the Audit Log file on the *Central Management Server* (CMS).



NOTE: You must be signed-in as root or administrator (or any user with *administrative rights*) to read the Audit Log file directly.

To view the HP SIM Audit Log for information recorded in the CMS:

1. Select **Tasks & Logs**→**View HP SIM Audit Log**. The **Audit Log** page appears.
2. Select the log entries you want to view by selecting one of the following options:
 - **most recent 40 entries**. Select this to view a selectable number of the most recent log entries. The default is set to view the 40 most recent log entries.
 - **from entry " " to entry " "**. Select this option to view an indexed range of log entries.
3. Click **View Now**. The requested log entries appear.

Log content

The HP SIM Audit Log contains the following information in the order listed, and the log entry key `@!@` precedes all other fields in an audit log entry.

- Time stamp date, time, and time zone
- Category
- Result
- Action
- Object type
- Object type descriptor
- Level
- Session user login string
- (Optional) Session ID
- (Optional) Transaction ID
- (Optional) Session user full user name

These fields are displayed in one line. If messages or additional information about a log entry is present, it appears in the next line.

Example of an HP SIM Audit Log:

```
@!@,2006-07-11 18:21:50 MDT,CONFIG,SUCCESS,ADD,TASK,Default Automatic  
Discovery,SUMMARY,mxadmin,0,11,
```

```
@!@,2006-07-11 18:22:06 MDT,CONFIG,SUCCESS,MODIFY,TASK,Initial Hardware Status  
Polling,SUMMARY,mxadmin,0,12,
```

@!@,2006-07-11 18:51:01

MDT, CONFIG, SUCCESS, ADD, AUTHORI, MX_AUTH, SUMMARY, jsmith, 590, 1186800129,

John Smith Added authorization for user djones with a toolbox of **Monitor Tools** for All Managed Systems.

@!@,2006-02-23 13:15:43 CST, CONFIG, SUCCESS, ADD, AUTHORIZATION, NODE_GROUP, SUMMARY, VIVO\djones, 6866, 351185188, Added automatically updating authorization for user VIVO\djones with a toolbox of Monitor Tools for All Storage Systems 001.

@!@,2006-02-23 13:15:43 CST, CONFIG, SUCCESS, ADD, NODE_GROUP, All Storage Systems 001, SUMMARY, VIVO\djones, 6866, 351185185, Automatic update is true/false.

@!@,2006-02-27 11:05:42 CST, CONFIG, SUCCESS, MODIFY, NODE_GROUP, All Storage Systems 001, SUMMARY, VIVO\djones, 6904, 1029055411, Automatic update is true/false.

@!@,2006-02-27 11:05:42 CST, CONFIG, SUCCESS, MODIFY, NODE_GROUP, All Storage Systems 001, SUMMARY, VIVO\djones, 6904, 1029055411, Automatic update is true/false.

@!@,2006-02-27 11:05:42 CST, CONFIG, SUCCESS, MODIFY, NODE_GROUP, All Storage Systems 001, SUMMARY, VIVO\djones, 6904, 1029055411, Automatic update is true/false. Added EVASAN01. Removed EVASAN99.

Related topic

▲ Audit log

Configuring the audit log file

Configure the Audit Log file to reside in a user specific directory.

To configure the Audit Log:

1. For Windows, create a file named `path.properties` under `C:\Program Files\HP\System Insight Manager\config`.

For Linux and HP-UX, create a file named `path.properties` under `/etc/opt/mx/config`.

2. For Windows, add the following entry in the `path.properties` file: **LOG=**`\\Auditlog\Logs` or `LOG=C:/Auditlog/Logs` .

For HP-UX, add the following entry in the `path.properties` file: **LOG=**`/var/opt/mx/logs` .

Note: `C:\\Auditlog\Log` is listed here as an example for Windows. This path is user defined.

Note: `/var/opt/mx/logs` is listed here as an example for HP-UX. This path is user-defined.

3. For Linux and HP-UX, restart the HP Systems Insight Manager (HP SIM) daemons (`mxstop` and `mxstart`). For Windows, restart the HP SIM service. After restarting the service, a new log file named `mx.log` resides in the directory specified in `path.properties` file.

Five variables can be defined in the `log.properties` file:

- `MX_LOG_FILENAME` for the file name. The default is `"MX_LOG_FILENAME=mx"`.
- `MX_LOG_FILEEXT` for the file extension. The default is `"MX_LOG_FILEEXT=log"`.
- `MX_LOG_FILESIZE` for the maximum file size. The default is `"MX_LOG_FILESIZE=20"`.
- `MX_LOG_ROLLFILEEXT` for the file extension of the roll-over name. The default is `"MX_LOG_ROLLFILEEXT=old"`.
- `MX_LOG_QUEUE_SIZE` for the amount of memory allocated for queuing items to be written to the Audit Log. The default is `"MX_LOG_QUEUE_SIZE=300"`.

The maximum file size is set in megabytes.

When the Audit Log file reaches the maximum file size, the log is renamed with `MX_LOG_ROLLFILEEXT` extension, and a new file is started. If a previous version of the file has already been renamed with the `MX_LOG_ROLLFILEEXT` extension, it is an automatic roll-over of an audit log file. A roll-over occurs after

a task running is completed. However, after one hour exceeding the maximum file size, if the task is not finished, the audit log file rolls over to another file.



CAUTION: Change the queue size only with extreme care. If the queue is set too high, the log manager consumes too much system memory.

Changes made to the `log.properties` file do not take effect until the log manager daemon is restarted. For Windows, restart HP SIM service. For Linux and HP-UX, restart the log manager.



NOTE: By default, for Linux and HP-UX, the path for the log file is set to `/var/opt/mx/logs`. This path can be configured by editing the `LOG` value in the `/etc/opt/mx/config/path.properties` file. If this properties file does not exist, create it. For Windows, the default location is the `logs` subdirectory of the directory where the product was installed.

Related topics

- [Audit log](#)
- [Viewing the Audit Log](#)

Properties for `globalsettings.props` file

The `globalsettings.props` has many configurable properties which control how HP Systems Insight Manager (HP SIM) functions.



WARNING! Changes to these settings should only be done by advanced users that have tested this in a non-production manner in their environment. Many parameters can be changed that could potentially adversely affect the functioning of HP SIM.

HP recommends using the `mxglobalsettings` command to view and modify the `globalsettings.props` property values. This command can display settings or modify their values and reduces the risks of editing the file by hand.

For example, to verify the `ip_ping_timeout` setting, enter the following from the command line interface (CLI):

```
mxglobalsettings -ld ip_ping_timeout
```

The following is displayed:

```
ip_ping_timeout = 3
```

To modify the `ip_ping_timeout` setting, enter the following from the command line interface (CLI):

```
mxglobalsettings -s ip_ping_timeout=4
```



NOTE: Depending on the setting, a restart of HP SIM might be required for changes to take effect.

See the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for additional information on using the `mxglobalsettings` command.

Property	Default	Description
<code>accept_known_check_state</code>	checked	
<code>accept_range_string</code>	*	
<code>accept_unknown_check_state</code>	not	
<code>AllowAltIpForTrap</code>	enabled	
<code>applet_archive_tag</code>	<code>classes/mxclient.jar,classes/XEjgl3.1.0.jar</code>	
<code>applet_archive_tag_appframe</code>	<code>ui/classes/mxclient.jar,ui/classes/XEjgl3.1.0.jar</code>	
<code>applet_versions_tag</code>	3.2.0.0,3.2.0.0,3.2.0.0	
<code>auditSetting</code>	All	

Property	Default	Description
AutomaticSignIn	enabled	Determines if automatic sign-in is enabled so that a Windows user can log on to the desktop and automatically be signed-in to HP SIM.
bypassBrowserCheck	false	
CertificateExpirationCriticalStart	0	
CertificateExpirationMajorStart	10	
CertificateExpirationMinorStart	30	
ClusterCollectorThreadCount	2	This is the number of threads in the pool for CMX data collectors. The default value should be sufficient to support hundreds of clusters. However, you might want to add a thread if you have hundreds of clusters, or many that exhibit slow response characteristics or are often off-line.
ClusterStatusWithThresholds	true	Set to false to have the cluster status be comprised of only the MSCS cluster status.
CMSDeviceKey	2	
CMSLocale		By default, the CMS locale is determined by the environment. If the locale used by the CMS is not the desired locale, change this property to the appropriate locale and override the CMS locale.
compaq.dataCollection.retryInterval	3600	
compaq.OperationalGroup.buildInterval	15	
compaq.SWComponents.PollingInterval	900	
ConstructionQueue	FFIO	DO NOT MODIFY
DataCollectionDetachedMemSize	600	Interval for the data collection task when retrieving data from a system. Tells the task to not get updated information from a system if the last collection time was within this interval.
DataCollectionInitiatorTimeout	60	
DataCollectionMinIntervalMinutes	15	
DataCollectionRetryTimeoutHours	24	
DataCollectionThreadCount	3	
dbType	MSQL	
DC_Abandon_Latency	60	
deleteStatus	0	
Demo_Mode	disabled	Turns off status polling, data collection, and various other internals when using in "demo" fashing.
Detached_DC_Timeout	900	
discard_range_string	\r	
DiscFilterState	disabled	Tells whether discovery filters are turned on or not.
DiscFilterTypes	Server,Switch,Cluster,Printer,MgmtProc,Rack,Enclosure,Complex,Partition,Storage,OnlyMgmt	Lists all applied discovery filters.
discoveryConfigured	yes	
DiscoveryGuidCheck	enabled	DO NOT MODIFY
dmi_check_state	checked	

Property	Default	Description
dmi_register_for_indications	checked	
dmi_retries_default	0	
dmi_timeout_default	1	
DMIStatusPollingThreadCount	5	
download_delay	5	
DTFMaxNoFiles	16	DO NOT MODIFY
DynamicAuthorizations_AutoUpdateDefaultValue	yes	This property controls whether or not the AutoUpdate background process task will actually execute or not. If this property does not reside in <code>globalsettings.props</code> , then by default, the AutoUpdate background task will be enabled.
DynamicAuthorizations_AutoUpdateEnabled	true	This property establishes a default selection for the new radio buttons implemented for Dynamic Authorizations. A value of true forces the Auto Update enabled (tracking on) radio button to be pre-selected, a value of false forces the Auto Update disabled (tracking off) radio button to be pre-selected.
DynamicAuthorizations_AutoUpdateIntervalSeconds	300	This property controls the interval when the background AutoUpdate task runs. The numeric value assigned to this property is in seconds. If this property does not exist in <code>globalsettings.props</code> , then a default value (600 seconds or 10 minutes) as specified in the Dynamic Authorization Auto Update tool XML file will be used as the interval value.
EmailFromAddress	mail@domain.com	
EmailHostName	mail@domain.com	
EmailKeywords	\$Tdesc\#Event Name\:\# \$Dname\#Event originator\:\# \$Tnotsev\#Event Severity\:\# \$Trcvd\#Event received\:\# \$Hdr \$Tdesc\#Event description\:\# \$Hdr See "Configuring e-mail settings" in the "EmailKeywords" section for more information.	
EmailLogin	test	
EmailPrefixUserSubject	false	When set to true, the user defined information from the E-mail Settings page is placed first on the subject line of the e-mail message. If the flag is set to false, the HP SIM defined information is placed first on the subject line of the e-mail message.
EmailRequiresAuth	true	
EnableMyCustomTools	false	
EnableSessionKeepAlive	true	When the timeout option is configured to monitor, the HP SIM session remains alive and is continually refreshed, unless you close the browser or navigate to another site. If you close the browser, the session is closed immediately. If you navigate to another site, HP SIM signs you out after 20 minutes.
EtnaEnabled	false	
exclusion_range_string		
exclusion_range_string_default		
ForwardingIPAddress		

Property	Default	Description
HardwareStatusPollingThreadCount	20	
HasAddedCMSWMIProxy	true	
http_check_state	checked	
http_request_retries	1	
http_request_timeout	15	
http_retries_default	0	
http_timeout_default	1	
IconView_NumberOfColumns	6	DO NOT MODIFY
IdentificationDiscoveryThreadCount	10	DO NOT MODIFY
IdentificationTaskThreadCount	8	DO NOT MODIFY
inclusion_range_string		
inclusion_range_string_default		
instrumentation_locale_language		
ip_check_state	checked	
ip_ping_check_state	checked	
ip_ping_retries	1	
ip_ping_retries_default	1	
ip_ping_timeout	3	
ip_ping_timeout_default	3	
ipx_check_state	NOT	
LockdownModuleInstalled	yes	DO NOT MODIFY
MaxRowsPerCategory	-1	DO NOT MODIFY
MaxRowsPerReport	-1	DO NOT MODIFY
MergeHelpTempRemove	true	DO NOT MODIFY
mx_dtf_enable_ssh_bypass	true	Set this property to <i>True</i> to bypass use of SSH for most local tools for the users listed in <i>mx_dtf_ssh_bypass_user</i> , or set to <i>False</i> to always use SSH tools that execute locally.
mx_dtf_password_expire_time	86400000	DO NOT MODIFY
mx_dtf_ssh_bypass_user		Modify this property to add additional user names for the SSH bypass feature. Separate each with a comma. For Windows domain accounts, two backslashes must exist between the domain name and the user name. For example, <i>mydomain\myname</i> . You should not add a user name if you do not intend for them to have full administrator privileges on the CMS.
mx_dtf_sshconn_expire_time	1 hour	Set this property to set the expiration time for an idle SSH connection.
MxVersionNumber	C.05.00.02.00	
NetworkRetries	1	
NetworkTimeout	5	
NodeReachablePort	80	Used to set the port that is used by automatic discovery, hardware status polling, the ping tool, and any other tool that must verify system availability.

Property	Default	Description
OracleConnectionRetryWaitInSeconds	30	
OracleMaxConnectionRetries	3	
PageSizeThresholdTree	100	DO NOT MODIFY
PageSizeTree=100	100	DO NOT MODIFY
PagingKeywords	\$Dname\#\# \$Tsdsc\#\#	
PagingLineSeparator	,	
PagingLineTerminator	\n	
PagingSizeTable	500	
PagingThresholdTable=500	500	
protocol_debug_data	no	
remoteWakeup_timeout	160	
ReportRefreshCount	20	
ReportRefreshInterval	3	
RetainHistoricalData TimeInDays	90	
rssFeedEnabled	not available	When set to True , this field enables system and event status information to read in RSS newsreaders and applications. If the property is not listed in the <code>globalsettings.props</code> file, it is disabled and must be added to include the True setting (<code>rssFeedEnabled=true</code>). See "Enlarging the System Status panel" for more information.
ServiceComponentExist	yes	
ServiceEnable	no	
ServiceFirstTime	yes	
ServiceProviderName		
ServiceProviderURL		
severity_critical_check_state	checked	
severity_informational_check_state	checked	
severity_major_check_state	checked	
severity_minor_check_state	checked	
showFtw	true	
snmp_check_state	checked	
snmp_retries	1	
snmp_retries_default	1	
snmp_timeout	4	
snmp_timeout_default	4	
SnmpCommunityString	public	
SnmpControlCommunityString	private	
SnmpSaveOrigTrapForForwarding	true	
snmpTrapDisc_enabled_state	NOT	
SnmpTrapPortAddress	162	
SoftwareVersionDataCollectionThreadCount	3	

Property	Default	Description
Storage_DC_Timeout	10800	
suspend_storage_dataCollection	false	
SWDeploymentDownloadTimeoutInMinute	10	
SWDeploymentMaxDownloadDevices	10	
SWDeploymentThreadCount	15	
SWDeploymentTimeoutInMinutes	120	
SWDeploymentWakeDeviceThreadCount	10	
switch_code_wakeup	true	
Systems_List_Table-Cut_Off	22	
TargetCharacterMapEncoding_DefaultLocale	en-US	DO NOT MODIFY
TargetCharacterMapEncoding_en_HPUX	ISO-8859-1	DO NOT MODIFY
TargetCharacterMapEncoding_en_LINUX	UTF-8	DO NOT MODIFY
TargetCharacterMapEncoding_en_SUSELINUX	UTF-8	DO NOT MODIFY
TargetCharacterMapEncoding_en_WINNT	windows-1252	DO NOT MODIFY
TargetCharacterMapEncoding_ja_HPUX	Shift-JIS	DO NOT MODIFY
TargetCharacterMapEncoding_ja_LINUX	x-EUC-JP-LINUX	DO NOT MODIFY
TargetCharacterMapEncoding_ja_SUSELINUX	UTF-8	DO NOT MODIFY
TargetCharacterMapEncoding_ja_WINNT	Shift-JIS	DO NOT MODIFY
TargetCodePage_Cp437_WINNT	437	DO NOT MODIFY
TargetCodePage_ISO-8859-1_WINNT	437	DO NOT MODIFY
TargetCodePage_Shift-JIS_WINNT	932	DO NOT MODIFY
TargetCodePage_windows-1252_WINNT	1252	DO NOT MODIFY
TargetCodePage_windows-31j_WINNT	932	DO NOT MODIFY
TargetLangCountry_en	US	DO NOT MODIFY
TargetLangCountry_ja	JP	DO NOT MODIFY
TargetLangEncoding_EUC-JP_HPUX	eucJP	DO NOT MODIFY
TargetLangEncoding_EUC-JP_LINUX	eucjp	DO NOT MODIFY
TargetLangEncoding_ISO-8859-1_HPUX	iso88591	DO NOT MODIFY
TargetLangEncoding_ISO-8859-1_LINUX	iso885915	DO NOT MODIFY
TargetLangEncoding_Shift-JIS_HPUX	SJIS	DO NOT MODIFY
TargetLangEncoding_Shift-JIS_WINNT	SJIS	DO NOT MODIFY
TargetLangEncoding_UTF-8_HPUX	utf8	DO NOT MODIFY
TargetLangEncoding_UTF-8_LINUX	utf8	DO NOT MODIFY
TargetLangEncoding_windows-1252_WINNT	utf8	DO NOT MODIFY
TargetLangEncoding_x-EUC-JP-LINUX_LINUX	eucjp	DO NOT MODIFY
TrustedCertificateExpirationMinorStart	30 days	Used to determine the days prior to the certificate expiring and sends a Minor event about the trusted certificate's impending expiration.
TrustedCertificateExpirationMajorStart	10 days	Used to determine the days prior to the certificate expiring and sends a Major event about the trusted certificate's impending expiration.

Property	Default	Description
TrustedCertificateExpirationCriticalStart	0 days	Used to determine the days prior to the certificate expiring and sends a Critical event about the trusted certificate's impending expiration.
Using_Collection_Obj	false	DO NOT MODIFY
Using_Customize_Collection_UI	true	DO NOT MODIFY
UXDMI_Register_Timeout	40000	
UXDMI_Unregister_Timeout	40000	
WBEM_Connection_Timeout	1000	
WBEM_Data_Collection_Timeout	300000	
WBEM_Indications_Listener_Port	50004	Used to set the port on which WBEM indications are received.
wbemEnableState	enabled	
WBEMnonSSEnabled	false	
WBEMSLPEnabled	true	
WBEMStatusPollingBypass	Enabled	Used to bypass WBEM hardware status polling
WBEMTimeOut	60	
WebServerThreadCount	10	DO NOT MODIFY
WindowsAdminUserName	Administrator	
WindowsInstallUserName	systemName\\username	
WindowsServiceUserName	systemName\\username	

16 Troubleshooting

Authentication	Automatic event handling	Blade
Browser	Certificates	CIMOM
CLI	Cluster	Collection
Configure or Repair Agents	Custom tools	Database
Discovery	Events	Event/SNMP trap
Firefox	Firmware upgrade	Generic
HP Service Essentials Remote Support Pack	HP SIM	HTTP event
Identification	Integrated Lights-Out (iLO)	Internet Explorer
Installation	IP address	Logs
Menu	OpenSSH	Operating system
Paging notification	Passwords	Ping
Printing	Property pages	Protocol
Replicate Agent Settings	Response	Search
Security	Serviceguard Manager	Sign-in
SMI-S providers	SNMP Agent	Software status
Storage system	Switch	System
System properties	Task	Time zone
Tools	VCRM	Virtual Machine Management Pack
Virtual machine	WBEM Indications	Windows NT event log
WMIMapper		

Authentication

HP Systems Insight Manager (HP SIM) was running fine, but now I receive error messages in the console, such as authentication failure and error accessing *database*, when trying to run HP SIM.

Solution: To resolve this issue, be sure that the *Domain Name Service* (DNS) server correctly associates the network address used by HP SIM with the host name of the CMS. If you are using a DHCP server to assign the Central Management Server (CMS) IP address, statically allocate the IP address. You cannot change the host name of the HP SIM.

Automatic event handling

Some of my Automatic Event Handling messages appear garbled.

Solution: If you are running an old version of the Microsoft Exchange Server (for example, 5.5) and have problems opening an HTML e-mail message sent from the HP SIM event handler, then the Microsoft Exchange Server must be updated to support the CP1252 character set and map CP1252 to US-ASCII. See <http://support.microsoft.com/default.aspx?scid=kb;en-us;184772> for more information.

Blade

A blade enclosure with Cisco Gigabit Ethernet switches does not display in the HP SIM HP BladeSystem Integrated Manager view.

Solution: You must have at least one blade with HP ProLiant Support Pack 7.51 or later in the same enclosure discovered in HP SIM.

For BL25p G1 servers running VMWare ESX 2.5.2 with Insight Management Agent 7.40B, HP SIM displays a Major status in the HS column even though there is no problem with the blades. In addition, when SMH is launched each component has a green status.

Solution: Install Insight Management Agents for VMWare ESX Server 7.4.1A or later.

When using HP SIM to connect to HP BladeSystem Integrated Manager servers, the HP SIM CMS does not display SMH for HP BladeSystem Integrated Manager servers and does not communicate directly with port 2301 or 2381.

Solution: Check the browser security settings or firewall on the systems or switch. If you can use the iLO remote console to view the system's SMH, then access is being prevented.

To configure the firewall on a Windows system:

1. Select **Start**→**Settings Control Panel**.
2. Double-click **Windows Firewall** to configure the firewall settings.
3. Select **Exceptions**.
4. Click **Add Port**.

You must enter the product name and the port number.

Add the following exceptions to the firewall protection:

Product	Port Number
HP SMH Insecure Port:	2301
HP SMH Secure Port:	2381

5. Click **OK** to save your settings and close the **Add a Port** dialog box.
6. Click **OK** to save your settings and close the **Windows Firewall** dialog box.

To configure firewall settings on Linux:

Firewalls are configurable various ways depending on the version of Linux installed.

Red Hat Linux Enterprise 3 and 4

The following list displays an example for iptables firewall rules for Red Hat Enterprise Linux 3 and 4 in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

The following list displays the new value for iptables firewall rules for Red Hat Enterprise Linux 3 that allows access to SMH in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
```



```

*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2301 -j
ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2381 -j
ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT

```

SuSE Linux Enterprise Server

SuSE Linux Enterprise Server 8 and 9 firewalls are configured using the YAST2 utility.

To configure the firewall:

1. Using the YAST2 utility, select **Security & Users**→**Firewall**. The **Firewall Configuration (Step 1 of 4): Basic Settings** window appears.
2. Click **Next**. The **Firewall Configuration (Step 2 of 4): Services** window appears.
3. In the **Additional Services** field, enter 2301:2381 and click **Next**. The **Firewall Configuration (Step 3 of 4): Features** window appears.
4. Click **Next**. The **Firewall Configuration (Step 4 of 4): Logging Options** window appears.
5. Click **Next**. A dialog box displays asking you to confirm your intention to save settings and active firewall.
6. Click **Continue**. The firewall is configured and your settings are saved.

I cannot see a newly booted blade in HP SIM.

Solution: Be sure the blade has the CMS configured as an SNMP trap destination.

To configure the SNMP trap destination on Windows 2000:

1. Select **Start**→**Settings**→**Control Panel**→**Network**→**Services**→**SNMP Service**.
The **SNMP Service Properties** dialog box appears.
2. Click **Traps**.
3. Enter a community name, such as `public`.
4. Click **Add to list**.
5. At the bottom of the dialog box, click **Add**.
The **SNMP Service Configuration** dialog box appears.
6. Enter the host name or IP address of the enterprise management station, and then click **Add**.
The SNMP trap destination is added.
7. Click **OK** to save the changes and close the dialog box.

To configure the SNMP trap destination on HP-UX:

1. Using a text editor, open the following file:
`/etc/snmpd.conf`
2. Insert the following information at the end of the `snmpd.conf` file:
`trap-dest: X.X.X.X`
Replace the `X.X.X.X` with the IP address of the enterprise management station.
3. Save and close the `snmpd.conf` file.
4. Stop the SNMP daemon by entering the following at a shell command prompt:
`ps -ef | grep snmpd`
`kill -9 PID`
Replace `PID` with the process ID returned by the previous command.
5. Restart the SNMP daemon by entering the following at a shell command prompt:
`snmpd`

Browser

My CMS is displaying an error message "Communication with the HP SIM server has been lost".

The HP SIM portal relies on the central management server (CMS) to respond quickly to all requests.

- If the CMS is slow to respond to one request, browser performance may fall significantly during that time.
- If the CMS is slow to respond to two requests, the browser will appear to lock up completely during subsequent interaction; the browser will not send additional requests until there are fewer than two outstanding requests.
- If four sequential ping-like requests each takes more than 30 seconds to complete, due either to request queuing or slow CMS response, the browser will display the message, "Communication with the HP SIM server has been lost", even though the CMS may still be responsive to other browser sessions.

On a LAN, the browser receives a CMS response to most requests within 10-100 milliseconds, which is nearly instantaneous. Requests that involve database queries or secondary network communication may take a few seconds to respond.

There are situations that may result in particularly slow response times. For example:

- Viewing large collections of systems or events.
- Specific/custom database queries taking an unexpectedly long time.
- Many users simultaneously accessing a shared resource, such as the database.

Solution: The maximum number of server connections can be increased in both Internet Explorer and Firefox. The default number of connections is two. Though you can increase this number into the hundreds, it's recommended not to exceed ten. For more information, see:

- Internet Explorer: <http://support.microsoft.com/kb/282402/>
- Firefox: <http://kb.mozillazine.org/Network.http.max-persistent-connections-per-server>

When I try to browse to the System Management Homepage on the same Linux system on which HP SIM is installed, I receive multiple browser warning messages.

Solution:

1. Open a terminal window.
2. At the command prompt, enter:
`cp /etc/opt/hp/sslshare/* /opt/hp/sslshare`
3. Press the Enter key.

4. At the command prompt, enter:

```
service hpsmhd restart
```

5. Press the Enter key.

When browsing into a Linux or HP-UX CMS on which the HP Insight Management Agents are installed, a Security Alert dialog box appears when I click an Insight Management Agent.

Solution: The Management HTTP server certificate has not been overwritten with the HP SIM certificate because OpenSSL is not configured correctly. On Linux, OpenSSL should be installed in the `/usr/bin/` directory. On HP-UX, OpenSSL should be installed in the `/opt/openssl/bin/` directory. Install OpenSSL to the correct directory, and then create a new HP SIM certificate to resolve this issue.

I am receiving security alert dialog boxes on the System Page when I click a system link to the Insight Management Agents that reside on the HP SIM Server that I am logged into.

Solution 1: If the security alert states that the name on the certificate does not match the name of the site, you can change settings in HP SIM so that links to systems use the same format as the names in the system certificate. View the system's certificate to see the name format it is using and complete the following:

1. Select **Options**→**Security**→**System Link Configuration**. The **System Link Configuration** page appears.
2. Select from the following options:
 - **Use the system name.** Select this option to use the system name.
 - **Use the system IP address.** Select this option to use the system IP address. For systems with multiple addresses, multiple links can be entered.
 - **Use the system full DNS name.** Select this option to use the full system *Domain Name Service* (DNS) name.

Note: On an HP-UX or Linux Central Management Server (CMS), the default value is **Use the system full DNS name** on new HP SIM installations. New installations on Windows defaults to **Use the system name** and upgrades maintain the existing setting regardless of the operating system.

Note: During *discovery*, the full system DNS name is used as the primary lookup key (if it is available). Otherwise, the IP address is used.

Note: In the case of systems with multiple network interfaces, selecting the **Use the system name** provides only one link per destination to the system, whereas **Use the system IP address** provides multiple links to the system.

3. To save and apply the changes, click **OK**.

If your system certificates use a name format that does not resolve correctly on your network, then select a link format that does. In this case, you continue to see this name mismatch alert even if you have imported the system certificate into the browser trusted list. This condition can be avoided by disabling the check in Internet Explorer 6.0 SP1. To do this, select **Tools**→**Internet Options**, and then click the **Advanced** tab. Under **Security** settings, clear the **Warn about invalid site certificates** option. However, HP **does not** recommend using this procedure, and it should be considered carefully in accordance with your own security policies and guidelines.

Disabling the **Warn about invalid site certificates** setting in your browser reduces your ability to properly identify the HP SIM server or managed system you are browsing to and any external or internal internet sites having nothing to do with web-based management products.

Solution 2: If the security alert is for another reason, such as an untrusted or invalid certificate, see “Browser” for more information.

When accessing HP SIM after installation is complete, I receive a message stating that the host name in the certificate does not match the URL.

Solution: Create a new certificate after installation with the IP address in the **CN** field. See “Server certificates” in the Creating a Server Certificate section for more information. After the new certificate is created, restart the HP SIM service.

I receive a security alert when accessing a system.

Solution: Be sure that you have the system server certificate imported into your browser and that you browse to the system using the same name as specified in the certificate. For example, having **Browsing to localhost** set in **Internet Options** is most likely the cause for this security alert.

I receive the following error message when browsing to different pages within HP SIM:

This window contains both secure and non-secure items

Solution: Several conditions could cause the browser to display this warning message:

▲ Improper version of Internet Explorer

There is a known problem in Internet Explorer 6.0 that causes this warning message to be erroneously displayed. Pages within HP SIM that are likely to experience the problem include the **Home** page and the **Task Results** page, though this problem is not limited to those pages.

To resolve this problem with the browser, ensure that you have at least version 5.50.4522.1800 by examining the **Version** string in the browser **About** box.



NOTE: Do not rely on the **Update Versions** string provided in the **About** box for Internet Explorer. It does not always correctly indicate the service pack. For example, even if it says SP1 it might not be accurate if the version is 5.50.4134.0600. Instead, ensure you have at least version 5.50.4522.1800.

for more information about the problem with Internet Explorer, see Microsoft Knowledge Base article Q269682. for more information about how to determine which browser version you have installed, see Microsoft Knowledge Base article Q164539.

▲ Navigating to a system that does not support SSL

If you navigate to a HP SIM **System Page** for a system that does not support SSL, system links to the system specify the usage of HTTP, a non-secure protocol, rather than HTTPS. This condition would cause the browser to display both secure items from HP SIM and non-secure items from the system, thus prompting the warning.

There might be newer versions of the HP Insight Management Agent for your system that support SSL. If there are not or you want to view the system now, click **Yes** to display the non-secure items, or you will not be able to view the system. All data between the browser and the managed system continues to be encrypted using SSL, and data between the browser and the system is not encrypted using SSL. The sign-in applet for older HP Insight Management Agent takes special care to separately encode your sign-in credentials so that you can securely sign-in, but all other data is not encrypted.



NOTE: Selecting **Yes** to the warning message removes the lock icon from the browser because portions of the window are not secure. Additionally, the browser might not provide this warning the next time you navigate to a non-secure system until the browser is restarted.

NOTE: Single Login is not supported or attempted on systems that do not support SSL.

▲ An error page displayed in browser

The browser might be attempting to display an error page, in which case it displays this warning message. For more information, see Microsoft Knowledge Base article Q184960.

When browsing to Insight Management Agent on the HP SIM Server itself, multiple security alerts appear while browsing the agent.

Solution: This condition occurs under the following conditions:

- Browsing to Insight Management Agent on the same system as the HP SIM Server. For example, the HP SIM Server is named DAMON, and while browsing to HP SIM, you navigate to the **System Page** for DAMON and select one of the web-based management links such as **System Management Homepage**.

- Both certificates for the Insight Management Agent and HP SIM are not imported into the browser.

Even though HP SIM and the Insight Management Agent are both running on the same system, they are not the same SSL web server and do not have the same certificate.

To stop the security alert windows from displaying, import both certificate for HP SIM and the Web-based Management Agent into the browser. See "Importing a server certificate" for more information. The information provided there can also be applied to importing the Web-based Management Agent certificate as well.

If the security alert is caused by a name mismatch between the name on the certificate and the name on the address, importing the certificates does not resolve the problem. Instead, browse to HP SIM or the Management Agent using the name in the certificate, or browse to one using the certificate name and the other not using

the certificate name. For example, browse to HP SIM using the IP address and to the Management Agent using the system name, or browse to HP SIM using the system name and to the Management Agent using the IP address. Using two different names helps separate the two domains in the browser, preventing confusion with different certificates for the same domain. See remaining security problems for more information.

Starting with HP SIM attempts to synchronize its certificate and private key with the local HTTP server for the Insight Management Agent to alleviate this problem. If synchronization has occurred, the system should be restarted to ensure both HP SIM and the HTTP server restart with the synchronized certificate. See "Synchronizing certificates" for more details.

I am receiving a Page cannot be displayed or <system> not found. Please check the name and try again. error when accessing a managed system.

Solution: The browser message varies based on the browser. Internet Explorer displays page cannot be displayed and Mozilla displays <system> could not be found. Ensure the browser can navigate to the managed system using the name shown in the URL. The URL for the managed system might be only part of what is shown in the browser address bar. To change the format of the name used by HP SIM, modify the **System Link Configuration** setting:

1. From the HP SIM CMS, select **Options**→**Security**→**System Link Configuration**. The **System Link Configuration** page appears.
2. Select one of the following options:
 - **Use the system name** Used to specify the short name
 - **Use the system IP address** Used to specify the IP address
 - **Use the system's full DNS name** Used to specify the full DNS name
3. Click **OK**. Your setting is saved.

I have problems browsing to the CMS from a Windows 2003 system.

Solution: Configure your browser to trust the CMS by performing the following procedure:

1. On the system browsing to the CMS, select **Start**→**Settings**→**Control Panel**→**Internet Options**→**Security**→**Trusted Sites**.
2. Click **Sites**.
3. In the **Add this Web site to the zone** box, enter the CMS, and then click **Add**. Enter the system as **https://<cms name>:50000**.
4. Click **OK**.

When accessing an HP SIM UI page, I receive the following browser error message:

For Firefox:

Warning: Unresponsive script. A script on this page may be busy, or it may have stopped responding. You can stop the script now, or you can continue to see if the script will complete.

For Mozilla:

Script warning. A script on this page is causing Mozilla to run slowly. If it continues to run, your computer may become unresponsive. Do you want to abort the script?

Solution: Pages that run script for more than five seconds in Firefox and Mozilla generate a warning message, enabling you to abort the script. The script run time must be increased to run the HP SIM UI without these script warnings.

1. Enter **about:config** in the browser's Location Bar, and press Enter.
2. Locate the entry for **dom.max_script_run_time** and increase the value to at least 60.

When attempting to browse to HP SIM installed on <server name>, the message HTTP/1.1 400 No Host matches server name <server name> is displayed.

Solution: This error can happen when installing HP SIM into a directory structure created by symbolic links on HP-UX and Linux. For example, using commands such as:

```
# ln -s /hpsim/etc_opt_mx /etc/opt/mx
```

and then installing HP SIM into the /hpsim directory structure will cause this error.

Do not install HP SIM into a directory structure using symbolic links.

I am unable to successfully browse to managed systems from links in HP SIM (for example, you receive browser timeouts or the message, The connection was interrupted)

Solution: The cause could be your browser's proxy settings or the web proxy itself. HP recommends not using a web proxy server if it is optional in your environment.

If you must use a web proxy to access managed systems, the web proxy itself must be able to resolve the system names in URLs generated by HP SIM. By default, HP SIM uses an unqualified system name (for example, no domain is present). If your proxy cannot resolve that style of name, change HP SIM to use IP addresses or full DNS names when creating URL links. To do this, select **Options**→**Security**→**System Link Configuration** in HP SIM.

If you do not need to use a web proxy to access managed systems but you do need a web proxy for other purposes, first try avoiding a proxy to verify that managing systems works properly in HP SIM. Then, reenables the browser's proxy settings and work on a proxy exception list for your managed systems.

In Internet Explorer, the **Bypass proxy server for local addresses** option is usually sufficient for HP SIM's default System Link Configuration. Firefox does not have a setting that is equivalent to the Internet Explorer setting for accessing local systems.

- **Configuring Firefox to accommodate HP SIM** Add your managed systems' names to the proxy exception list, or use a proxy auto-configuration (PAC) file that avoids a proxy for your managed systems.
- **Configuring HP SIM to accommodate Firefox** To help simplify your proxy exception list, configure HP SIM to use full DNS names when creating URL links. To do this, select **Options**→**Security**→**System Link Configuration** in HP SIM

If you reconfigure HP SIM to use IP addresses or full DNS names in URL links, you must also include the addresses or domains of your managed systems in your proxy exception lists for both Internet Explorer and Firefox.



IMPORTANT: A side effect of changing HP SIM's **System Link Configuration** setting is that you might encounter security alerts if the name of the managed system's certificate does not match the name in the link that HP SIM generates.

Certificates

Attempts to import the HP SIM certificate from cert.pem or server_cert.pem into a separate application result in failure.

Solution: This could be caused by an improperly formed certificate file. Backup the certificate file. Then view the file using a text editor, and compare the last two lines before the END CERTIFICATE line. The following is an example of a certificate file with duplication that can cause the failure:

```
O/4Hc19nRz0uZGcdsypjgW5CUDqZyzzEB17DHwnC8qzEC7/D+VpW+5RdRT1hh5c
DzdIjLznRz0uZGcdsypjgW5CUDqZyzzEB17DHwnC8qzEC7/D+VpW+5RdRT1hh5c
-----END CERTIFICATE-----
```

If there is some duplication in the last two lines, manually edit the file to repair it. Be sure you have the file backed up before attempting this. On the last line only, delete the characters, in groups of four, at the end of the line that duplicate the characters from the line above it. All four characters in the group must be identical, including case. Using the same example, the last two lines would look like this after editing:

```
O/4Hc19nRz0uZGcdsypjgW5CUDqZyzzEB17DHwnC8qzEC7/D+VpW+5RdRT1hh5c
DzdIjLzn
-----END CERTIFICATE-----
```

Save the file, then try again to import it into the desired application. Note that some applications are more lenient than others and might work without fixing the certificate file.

I am receiving an error when running the `mxcert -u` command to create a new server certificate.

Solution: The command `mxcert -u` is only used by the HP SIM installation program. HP does not support running this command.

I ran the following command to add systems through the CLI on a Korean system; `mxnode -lf hpdc13as3 > node.xml` where `node.xml` is an `.xml` file listing all available systems. I then ran `mxnode -a -f node.xml` to add the systems. However, I received an `x-windows-949` error message.

Solution: Edit the `.xml` file that you created to add the systems and change the encoding name to UTF-8.

I used `mxreport` to dump the contents of an existing report and report category. For now, I only modified some name fields and reviewed `mxreport(4)` and `mxcategoryitem(4)` to check format for new items to make sure they were set appropriately to create a copy of the report/category I dumped under a new name. I can successfully create my new report using:

```
# mxreport -a -f/home/bvilfer/work/PPUStorageLogicalUnitsReport.xml
Report successfully created.
```

When I try to create a category containing SQL for a new view that I want the report to use, it fails:

```
# mxreport -c -f/home/bvilfer/work/PPUStorageLogicalUnitsCategory.xml
Category failed to create in database.
PPU Storage Logical Units
null
```

Is there a log file somewhere that might give me more information as to what the "null" is referring to?

Solution: You need to create **Category** first, if you want to report new category items that are not in the existing categories, then create the report. To be able to view log files of debug explanations, you need to turn on debug by setting the following properties in the `debugsettings` file:

- `MxCategoryManager`, `MxReportManager` - set them to **true, 30**
- In the `xml` file, you should have created views for three different databases MSSQL, Postgresql and Oracle. If they are the same, then set **dbType=111**.

From the command line, I entered `mxmib -f SHIPPING CFGs not preloaded.txt`, and I received the error The following is an invalid argument value: CFGs.

Solution: The command `mxmib` cannot handle spaces. Place the file name in quotes. For example, enter `mxmib -f "SHIPPING CFGs not preloaded.txt"`.

The command `mxagentconfig -a -n cms_name -u user_name -p password` fails with

```
Unknown hostname: 'cms_name'.
```

Solution: For verification purposes, use `nslookup cms_name` to test the network name resolution on the managed system. To correct the problem, set up a network name resolution properly on the managed system by adding CMS information to the managed system `/etc/hosts` file.

The command `mxnode -a system_name` or `mxnode -r system_name` fails with: Unknown host: 'system_name' System ignored.

Verification: Use `nslookup system_name` to test the network name resolution on the CMS.

Solution: Set up network name resolution properly on the CMS.

I am receiving a message, Another user is currently using `mxmib`, please try again. How do I resolve this?

Solution: This behavior is expected. Run `mxmib -r` to clear the interlock.

MXMIB enables me to compile a MIB with a different file name, but the same internal module name already exists and is a compiled MIB, which is causing inconsistency in the database.

Solution: The module name and file name must be consistent. If the file names do not match, the files might become corrupt.

If attempting to compile a MIB that already exists in the database, the CLI message states that it is importing even though it is actually updating.

I am a member of an existing HP SIM user group, but when I try to run commands from the CLI, I receive an error message, stating There was a problem connecting to the HP SIM server. Be sure that:

1. Your user name has been added to HP SIM. Do this by signing in to the HP SIM GUI at least one time.
2. Your user name and password, if specified, are correctly spelled.
3. HP SIM is running.
4. You used '--' for any long options and double quotes if your username includes a domain. For example, `<commandname> --user "mydomain\myusername" --pass mypassword`.

Solution: Be sure that the HP SIM service is running by using the `ps -ef | grep mx` command. If the managed system is not discovered on the CMS, this message will appear for `mxagentconfig -a -n managed system -u username -p password`. Be sure that the managed system is discovered.

I ran the command `mxnodesecurity -r -p protocol -n <non-full-DNS-name>` and received a message that the system was removed. However, the system still exists in the `mxnodesecurity` list.

Solution: To delete a system from the `mxnodesecurity` list using the command `mxnodesecurity -r -p protocol -n <hostname>`, use the fully qualified domain name in place of `<hostname>`.

I am a *administrative rights* user. However, I receive an exception when trying to run the CLI commands.

Solution for mxnodesecurity: On a Linux system, the command must be executed by the root user.

Solution for all CLI commands:

- If you are a member of an HP SIM user group, sign-in to the HP SIM GUI at least one time. After that, you will be in the list of authorized users and will be able to run commands from the CLI.
- On a Windows system, you must be a member of the Windows Administrators group to execute CLI commands.

When using CLI commands in script files, the commands consume any input data available and when the script is ran, the intended recipient has no data to read.

Solution: When specifying a CLI command in a script, specify `echo "" | command -ln` as the source of standard input data for the CLI command for Windows .bat files and UNIX systems. Specify `command -ln < /dev/null` for HP-UX and Linux systems.

CIMOM

I have a *common information model object manager* (CIMOM) on a discovered network, but I do not receive any information from the port, and the related system is not discovered by HP SIM.

Solution: Try one of the following solutions:

- If the CIMOM is installed and listening on a Secure Sockets Layer (SSL) port other than the default port 5989, the new port number must be specified in the `config/identification/wbemportlist.xml` file. For example:

```
<port id="5991" protocol="https">
  <interopnamespacelist>
    <interopnamespace name="root"/>
    <interopnamespace name="interop"/>
  </interopnamespacelist>
</port>
```


- Verify that the interop namespace for your WBEM provider exists in a port element in the `config/identification/wbemportlist.xml` file. If it does not exist, add it to a port element as an `interopnamespace` element, and restart HP SIM.



NOTE: Adding new ports or interop namespaces causes the discovery process to take longer because HP SIM tries all possible combinations of ports, interop namespaces, and user name and password pairs on each IP address in the discovery range.

NOTE: For information about *storage system* CIMOM problems, see the “SMI-S providers” and “Storage system” sections.

Cluster

A cluster is not identified as a cluster.

Solution: If a cluster is not defined as a cluster or any of its nodes are not identified correctly, be sure all the Cluster Management Agents are installed (if necessary, reinstall) on every cluster node of that cluster.

After manually adding a system as a cluster, the system type does not change, even if the system is not a cluster.

Solution: If you manually add a system as a cluster, the system type might not change even if the system was not a cluster originally. To reset the system type, delete the system and run discovery.

Clusters or cluster nodes are not identified correctly.

Solution: Clusters or cluster nodes might not be found for the following reasons:

- Starting with SmartStart version 6.30, one of the cluster agents is not installed correctly. The executable is installed on the cluster node, but the Windows registry must be updated.
 1. Access the Windows registry (select **Start**→**Run** and enter `regedit.`)
 2. Create the following key:

```
HKEY_LOCAL_MACHINE, "SOFTWARE\Compaq\CompaqCommonClusterAgent\CurrentVersion"  
Value: Pathname, %REG_EXPAND_SZ%, "%SystemRoot%\System32\svrclu.dll"
```

This update is available starting with SmartStart CD 7.4.

- Be sure the IP ranges in automatic discovery are set to include the cluster and cluster nodes (and not exclude them).
- If the name of the cluster or its node has changed, be sure the DNS servers being used by the cluster and HP SIM both have the new name.
- The cluster node might be down.
- The cluster node has Insight Agents older than version 4.22.
- The Insight Agents are not running on the cluster node.
- The SNMP Agents are not running on the cluster node.
- The network traffic is congesting the network for a significant time.
- SNMP community string might not be matching with that of the HP SIM settings.

Verify the following prerequisites are met:

- The Cluster Management Agents must be running on all the cluster nodes.
- The system must be identified as a server or cluster for cluster identification to run against that system during discovery.

The cluster node is not identified properly by discovery.

Solution: The cluster node name for the DHCP server might be different than its Windows NT name. The remedy is to explicitly place the Windows NT computer names into the `LMHOSTS` file on each cluster node and then run discovery again. Also, be sure the registry key for the `svrclu.dll` has been created. See the previous issue for information about the registry key.

A cluster or cluster node is not displayed in the Cluster Monitor cluster or node resource settings.

Solution: This issue can result from specific HP Insight Management Agent for those Cluster Monitor Resources that were not running at the time discovery was run. Ensure that the correct agents are running on the clusters and cluster nodes, and then run discovery again.

Cluster Monitor is not displaying properly.

Solution: Ensure that your browser is configured to use **Small Fonts** as the **Font Size**.

The list boxes under Cluster Monitor within Settings are not working properly.

Solution: It takes a few seconds for the down arrows to appear on the list boxes. If there is more than one list box, select an option from the first box, and wait a few seconds to select an option from the second box and each subsequent box. If you make a selection too soon, the list boxes might not work properly.

The cluster nodes are not discovered when the cluster alias is used as the system in manual discovery.

Solution: In manual discovery, add the cluster alias and each node separately to ensure they are entered into the database. Alternatively, include the cluster alias and the node IP addresses in the IP range.

What should I expect when running HP SIM on a cluster?

Solution: HP SIM is not a cluster-aware application. If each node of the cluster has an instance of HP SIM installed, each node has a different certificate with the name of the node, not the name of the cluster, unless you have created your own certificates using a certificate server or other certification authority. When browsing to the cluster, if your browser is configured to **Warn about invalid site certificates**, the browser should display a security alert, warning you the name you have browsed to does not match the name in the certificate. If you have not imported the certificate into the browser or the certificate has not been issued by a trusted certification authority, the security alert also informs you of the untrusted origin of the certificate. Verify the certificate is correct and continue.

During a failover, one node fails and the other node becomes active. Because HP SIM is not cluster-aware, any browsers open to HP SIM must be closed, and you must browse to the cluster again. You might again be presented with another security alert, using the certificate of the other node as previously described. If so, verify the certificate and continue.

Any managed system that establishes a trust relationship with the HP SIM server (for example, for Single Login support, Replicate Agents, Update Software, and so on) should trust all nodes of the cluster because any node could be active and issue the desired command to the system. See "Setting up trust relationships" for more information about setting up trust relationships.

I am having problems identifying clusters.

Solution: If you notice that the cluster name or cluster member name is the IP address of the system and not the host name, download the new HP Insight Management Agent for Windows 2000/Server 2003 for each cluster member of the cluster.

1. See <http://www.hp.com>, and then click **Support & Drivers**.
2. On the **Support & Drivers** page, under **Or Select a product category**, click **Servers**.
3. Click **ProLiant and Pentium/Xeon servers**.
4. Click **Compaq ProLiant Servers**.
5. Select the appropriate ProLiant series (for example, **Compaq ProSignia 720 server series**).
6. Select the appropriate server (for example, **Compaq ProSignia 720 server 3/350-512**).
7. In the **tasks for your selected products** box, click **download drivers and software**.
8. In the **select operating system** list, select the appropriate operating system (for example, **Microsoft Windows 2000**).
9. In the **select a category** list, select **Software - System Management**.
10. Click **HP Insight Management Agent for Windows 2000/Server 2003**.

The agents are installed.

Collection

While trying to create a duplicate collection name in a Shared or Private section, an error message is generated.

Solution: Duplicate collection names are not allowed in Shared or Private sections. Collection names should be unique even though the collections exist in Private and Shared.

After deleting a system, the product name or Web Agent criteria are not removed.

Solution: After a product name or Web Agent is discovered, that search criteria remains in the database until the database is reinstalled, which enables you to search on criteria that was present once and might be present again in the future (for example, base tasks on a collection with these criteria, and set it to run when new systems or events meet the search criteria).

Machine names that have spaces within their name are truncated at the space character in a collection.

Solution: When HP SIM writes a discovered system to the SQL database, SQL truncates the name if a space occurs in the machine name. Rename the system without a space.

When trying to sort a collection, it sometimes requires multiple clicks for the column to sort.

Solution: Quick mouse movements inhibit the applet from reading mouse clicks. Hold the mouse absolutely still while clicking the column to sort.

When sorting a search by IP address, the addresses are not listed in numerical order.

Solution: The IP addresses are listed in numerical order, which implies an order like 122.22.22.15, 122.22.22.152, 122.22.22.155, 122.22.22.17, 122.22.22.171, 122.22.22.18. HP is investigating the possibility of providing a fix in a later release.

Configure or Repair Agents

After choosing host based authentication for SSH and attempting to run Configure or Repair Agents on an HP-UX or Linux managed system, the following error appears: Failed to configure SSH for host based authentication Configuration failed to complete due to the following exception: Could not access the file or directory <file name> on the target system <target name>. Remote system reported following error message: Permission denied. Check whether the directory or file exists or whether the user has the operating system permission to access it.

Solution: You must provide root user credentials on the target system to configure managed systems for host based SSH authentication.

When running Configure or Repair Agents targeting a Citrix server, it fails due to Citrix drive C: remapping.

Solution: Deploy preconfigured agents through either the Integrity Support Pack or the Install Software and Firmware tools.

Installing SNMP agents (HP Insight Management Agents for Windows server 2003) through Configure or Repair Agents on blade servers, fails with dependency error. The Stdout tab on the Tasks Results page states that HP Smart Update Manager finished, but the installation failed.

Solution: Installation of SNMP agents requires one or more of the following components: HP ProLiant Advanced System Management Controller Driver for Windows, HP ProLiant iLO Advanced and Enhanced System Management Controller Driver for Windows, or HP ProLiant iLO Management Controller Driver for Windows. Be sure that you have the above components installed, and then try installing the SNMP agents again.

I get the following dependency failure message " FAILED, One or more components failed to install, because it depends on another component which is not installed on the system. " What do I do?

Solution: This is because the pre-requisites for the agent you selected to install are not met.

You have two options at this point.

1. Use HP SUM UI to find the dependent component name.
2. Install the whole support pack using Install ProLiant Support Pack Install tool from the HP SIM menu by selecting **Deploy**→**Deploy Drivers, Firmware and Agents**→**Initial ProLiant Support Pack Install**.

An example could be as follows:

When I install HP Version Control Agent for Windows (VCA) through Configure or Repair Agents on Itanium-based servers, it fails with a dependency error. The Stdout tab on the Tasks Results page states that HP Smart Update Manager finished, but the installation failed.

Solution: Installation of HP Version Control Agent on Itanium-based servers requires *HP Integrity Insight Management Agents for Windows Server 2003 on Itanium-based systems*. Make sure that you have the above component(s) installed and then try installing the HP Version Control Agent.

Custom tools

My custom tool fails with the following error:

```
C:\Program Files\OpenSSH\bin\switch.exe: *** ca t create title mutex `Global\cy  
gwin1S3-2003-11-04 16:46.title_mutex.0`, Win32 error 0
```

Solution: The user who is trying to run the custom tool is not in the Administrators group. Add the user to the Administrators group.

I cannot find custom tools that I have created.

Solution: New custom tools are added to the **All Tools** toolbox. You might not have authorization to use that toolbox. To view the tool under **Tools**→**custom tools**, add the tool to your authorized toolbox, which is present under **Command Line Tools**. See “Editing toolboxes” for more information.

Database

When trying to reinstall HP SIM on a Windows system from which I previously uninstalled HP SIM, I receive Unable to Create Database. I receive this error during the database creation process.

Solution: This problem is a result of not deleting or renaming the HP SIM database files from MSDE or Microsoft SQL Server after uninstalling HP SIM. Manually delete or rename the database files, and then run the HP SIM installation again.

Discovery

A system that has had a new IP address assigned to it is discovered as a new system in HP SIM instead of having the existing system in HP SIM updated with the new IP address. The original system shows a Critical status.

Solution: This issue results when DNS is not configured on the network. HP SIM tries to use system names from DNS to match previously discovered systems with new systems of the same name. Be sure that DNS is configured on the HP SIM server, and ensure that the DNS server itself is properly configured for the systems in question. Both forward DNS lookups and reverse lookups must resolve to the same system. On Windows, `nslookup <address or name>` can be used to help diagnose the problem.

There is a mismatch between the system table view and the picture view.

Solution: Delete all the systems that are in the affected rack, which includes all the servers, iLOs, enclosures, and switches in that rack, and run discovery on those deleted systems.



NOTE: Before deleting the servers, iLOs, and switches, note the IP addresses of these systems, then delete the systems, and run discovery.

After upgrading from HP SIM 4.1 to HP SIM 4.2, my ProLiant BL40p server blade to enclosure associations are displayed as "server in iLO" instead of "server in Enclosure."

Solution: Delete the affected server blades from the database and run discovery again. The server blade to enclosure association will now be displayed correctly.

After running discovery, I noticed that a system was discovered but not identified as a WMI/WBEM device. Why was this system not discovered properly?

Solution: A system might not be discovered properly for several possible reasons, including:

- The user credentials were incorrect.
- The provider encounters a problem responding to the WBEM requests.
- The system names can only contain alphabet (A-Z), digits (0-9), minus sign (-), and period (.). However, the system name cannot start with a digit, and the last character must not be a minus sign (-) or period (.).
- On HP-UX or Linux CMS's, no WMIMapper was specified. Therefore, no Windows systems can be identified as WBEM enabled systems.
- There is no provider installed on the target HP-UX or Linux system.

I am trying to see the association of management processor and the HP-UX server, but I do not see the association between the server the management processor.

Solution: Currently, HP SIM cannot make an association of management processor to server if the system is based on PA-RISC.

Events

Unable to clear, delete, assign, or add comments to events.

Solution: The default operator-template, and other authorizations, may not be sufficient to allow event modification.

Ensure the user is authorized for the desired tools against the desired systems. Tools include **Clear Events**, **Delete Events**, **Assign Events**, and **Comment Events** and are included in the default **All Tools** and **Full Rights** toolboxes. You can also create custom toolboxes with these tools, which located are in the **Configuration Tools** category, and use the custom toolboxes to authorize against the desired systems.

Additionally, the user must be authorized for the desired tools, or the **Modify HP SIM Events** tool, against the CMS. If you do not want the user to be able to modify CMS events, use the **Modify HP SIM Events** tool, which is included in the default **All Tools** and **Full Rights** toolboxes. You can also create a custom toolbox with this tool, located in the **HP SIM Tools** category, and use the custom toolbox to authorize against the CMS.

Event/SNMP trap

Why am I not receiving notification when there is a SNMP Authentication trap received?

Solution: The default setting for Enabling Trap Handling in SNMP Extensions is Disabled (Not Processed) because typically, a system can be set up with an incorrect community string or an incorrect community string is set in HP SIM. This error results in an Authentication Failure trap to be sent to the management server each time a request is made to the system, which results in many traps being logged. To change this setting to Processed (Enabled), complete the following steps:

1. Open HP SIM (<http://machinename:280>).
2. Sign-in as a user with *administrative rights*.
3. Select **Options**→**Events**→**SNMP Trap Settings**.
4. In the **Mib Name** field, select **rfc1215.mib**.
5. In the **Trap Name** field, select **authenticationFailure** if it is not already selected.
6. In the **Enable Trap Handling** field, select **Yes**.
7. Click **OK**.

These steps set the **Authentication Failure Trap** to be processed, and you are notified of all failures.

After creating a trap forwarding task, specifying several destination servers, and then running the task, only one destination server receives all of the traps.

Solution: Verify that the server sending the traps is also discovered in HP Systems Insight Manager. If it is not, discover the system and then run the task again. All destination servers should receive traps. This problem can happen on a Windows, HP-UX, or Linux server.

Firefox

When using the Firefox browser while accessing any of the HP SIM menus, the content of the current page disappears temporarily during the menu's usage. After making the menu selection, the requested page appears.

Solution: This is the default behavior for FireFox. If you abort the menu, you can redisplay the current page by clicking the blank area where the page's text should appear. The page is refreshed and the text reappears.

When viewing the Audit Log file on the CMS using Firefox, the text is illegible.

Solution: Increase the font size in Firefox by pressing Ctrl +.

Firmware upgrade

When upgrading my switch firmware, I receive the following error in the log file when I click the succeeded link in the Task Results page:

```
Processed command line: /v 1.1.1 /s /l c:\hpsim_switchfw_logs\
587_11a.wbem.com.log /c /i 170.50.2.3 /f /a swfwupgrade.ini
```

```
Usage: swfwupdate [/c SNMPcommunityString
[/i IPAddr [- IPAddr] ... ]]
[/v FWversion | /b BootVersion] [/m 1 | 2]
[/t TFTPport] [/d] [/l logfile]
[/x IPAddr [IPAddr...]] [/s[ilent]] [/f[orce]]
The /s option requires that /i, /c, and /v also
be specified and implies /f.
The /s option deletes all database entries
prior to discovery.
```

Solution: Verify that the SNMP write community string is set properly for the switch on the **System Protocol Settings** page.

Generic

The keyboard does not always respond the way I expect.

Solution: If you are used to the Windows operating system, you anticipate the behavior of certain keys, such as the **Tab**, **Enter**, or **Alt** keys. However, in Java applets and web applications in general, the Windows style is not necessarily used. Therefore, you might need to use the mouse to return focus to a specific page. For example, if you enter an invalid entry for a system IP address or time, the Criteria or Schedule page is refocused, but the keyboard access might not be restored on the last entry field. This situation typically happens after several attempts. To return the focus, use the mouse to click the page you want to use.

User names are not listed in alphabetical order.

Solution: User names are grouped by authorization level (administrative rights, *operator rights*, and none). Within the groupings, the users are listed in the order they were created.

HP Service Essentials Remote Support Pack

The following error is reported: HP SIM cannot connect to the Remote Support tool.

Solution 1: Verify that the Remote Support tool is installed and running.

Solution 2: Check your firewall settings to see if the Remote Support tool is being blocked.

When I run a warranty-contract report or collect contract and warranty data, the following error appears on the Task Results page: Target does not have a serial number and/or product number.

Solution 1: To collect contract and warranty data for a system, the system's serial number, product ID, and country code must be present in the system properties. In most cases, the serial number and product ID are obtained during HP SIM's identification process. You can enter a serial number and product ID if needed. It is important to specify the correct country code to ensure accurate information. If HP SIM cannot obtain a country code, it defaults to *US*. If you have a support contract, enter an entitlement or obligation identifier and entitlement type if you want to view contract data.

HP SIM

I receive a message regarding memory address violation when I close the browser.

Solution: You might need to reinstall the SNMP Agent after installing Windows NT 4.0 SP3. If you install Windows NT 4.0 SP4, you must install the SNMP hot fix. The SNMP service has a memory leak and consumes your system resources if you do not install the SNMP hot fix.

After creating a user with administrative rights, the user name is shown in the user list generated from the SQL Analyzer. However, after editing the UserID file, exiting HP SIM, and restarting HP SIM, the user is not listed when selecting Options→Security→Users and Authorizations→Users, although the user name is listed in the database.

Solution: Any attempt to manually modify the UserID file or any user information hash file causes the user account to be removed from HP SIM. Therefore, the user can no longer access HP SIM.

Database connection is lost while using the MIB installer tool, command line MIB Manager, or command line System Type Manager, but the tools indicate successful completion.

Solution: If you lose accessibility to the database when running these command line tools outside HP SIM, you can potentially corrupt the operation you were performing, and predictable results and recovery are not guaranteed.

The Home and Sign Out links are missing in the banner area.

Solution: Click the **Refresh** button at the top of the browser window.

I am receiving an HTTP 404 error when launching the Partition Manager through HP SIM.

Solution: If you have reconfigured the secure port for HP SIM, the port must be modified in the `/var/opt/mx/tools/parmgr-web-tools.xml` file. To do this:

1. Edit `/var/opt/mx/tools/parmgr-web-tools.xml`.
2. Modify the port from 50000 to whatever you have configured the secure port to be.
3. Run `/opt/bin/mxtool -m -f /var/opt/mx/tools/parmgr-web-tools.xml` from the command line.

The HP SIM service fails to start on a Windows-based operating system. Failures are shown in the NT application log but do not state an explicit error.

Solution: Search the root directory for a folder or file named `Program`. If this file exists, delete it. If this folder exists, rename it or delete it if the folder is empty.

After signing in to HP SIM, no systems, events, or tools are displayed in the console. In some cases, HP SIM might not start correctly or display the sign-in page.

Solution: To resolve this issue, run the database integrity check command (`mxconfigrepo`) from the CLI to verify that dependent items in HP SIM are properly defined in the database.

```
mxconfigrepo -c (for checking errors)
```

If errors are reported after running this command:

1. Stop the HP SIM service.
2. From the CLI, run `mxconfigrepo -f`.

Caution: If the HP SIM dependent items are not properly defined, running this command (`mxconfigrepo -f`) deletes errant records, which can cause minimal data loss.

3. Start the HP SIM service.

If no errors are reported, call the HP support center.

HP SIM will not start.

Solution: Set the **SNMP Trap Service** to **Manual** instead of **Disabled**.

1. In Windows, select **Start**→**Control Panel**→**Administrative Tools**→**Services**→**SNMP Trap Services**.
2. Under the **General** tab, change **Startup type** to **Manual**.
3. Click **OK**.

HP SIM does not start on an HP-UX system.

Solution: If HP SIM does not start on an HP-UX system, the `vps_pagesize` may be too large.

To resolve this issue, run the following commands:

1. `chattr +pd 4K /opt/mx/lbin/mxdomainmgr`
2. `chattr +pd 4K /opt/mx/bin/mxinitconfig`
3. `/sbin/init.d/hpsim start`

This limits the virtual memory page size used for the data segment to 4K for each of these processes.

WARNING: Changing the tunable kernel parameters may impact HP SIM and other applications. Be sure to review the applicable manpages before making such changes.

HTTP event

After creating a new HTTP category, it is not listed in the criteria box on the Advanced Search page when searching for new event types.

Solution: To search for new event types generated by HTTP events, select events by Event Category Selection, and then select the event type from the **and type is** list.

Identification

After running discovery and Identification, the serial number is missing for ProLiant BL p-Class and e-Class switches on the System Page→Identity tab and in the Data Collection report.

Solution: To obtain the serial number for these switches requires support in the firmware of the switches. At this time, this firmware is not available. However, this support is being planned in future versions of the ProLiant BL p-Class switches. There currently is no firmware upgrades being planned for existing switches.

HP SIM fails to identify a valid iLO 2 WS-Management credential using the list of global default WBEM credentials configured in HP SIM.

Solution: Specify a system-specific WBEM credential that grants access to the iLO 2 on port 443. Use either the `mxnodesecurity` command or set the WBEM credential for a specified system and port on the **System Protocol Settings** page.

Integrated Lights-Out (iLO)

How do I associate an iLO with a server?

Solution: To associate an iLO with a server, **The Level of Data Returned** must be set to **Enabled** on the iLO itself. See “System license information reporting” for more information.

Internet Explorer

Hot keys or other keys, such as Tab and Enter, might not work as expected in the browser.

Solution: Use the mouse to ensure expected results.

During the installation, the system reboots, and then the installation launches the browser. Internet Explorer displays a message saying that it could not establish a connection with the local host. The browser is being launched before the service has had time to start.

Solution: Try to access the URL again by placing the cursor in the URL field and pressing the Enter key. Keep trying until the application loads in the browser.

Sometimes the browser Back button does not take me back to a previous window.

Solution: In Internet Explorer, when the framesets are changed, the browser history is lost. Navigate back through the HP SIM header that is present at all times.

Clicking the browser Back button while viewing a collection returns me to the appropriate system or event overview page.

Solution: This functionality is correct. The browser history is not being updated because of frameset updates. Click the system or event collection to navigate back to the table view page.

I cannot drill down on a collection or an agent link on the System Page.

Solution: When two browsers are open on the same system and they are each pointed to a different HP SIM Management server, unexpected results can occur. Some inconsistencies include not being able to open a collection or not being able to drill down on an agent (for example, Configuration History Reports (Survey Utility)).

I cannot access HP SIM on the local system at `http://localhost:280/`.

Solution 1: Verify proxy server configuration in Internet Explorer. An invalid proxy server address prevents Internet Explorer from browsing to any addresses, including the local system.

Solution 2: Some systems might not be able to resolve the name `localhost`. If this is the case, use `http://127.0.0.1:280/` or `http://machine_name:280`, where `machine_name` is the system on which HP SIM is installed.

When the All Systems window sits idle for an extended period and I launch a new browser window, the All Systems window turns white and Internet Explorer hangs. I am forced to end the task. How can I avoid hanging up in Internet Explorer?

Solution: Avoid leaving Internet Explorer open for extended periods with the **All Systems** collection displayed. Sign out of HP SIM before leaving your monitor to prevent this situation and for security reasons.

I am experiencing unexpected or odd behavior while browsing HP SIM using Internet Explorer.

Solution: This behavior can be caused by a third-party browser extension. Disable these extensions to verify that it alleviates the problem. In the Internet Explorer menu, select **Tools**→**Internet Options**→**Advanced**, disable **Enable third-party browser extensions**, and restart all running copies of Internet Explorer.

A blank page is displayed when clicking a Microsoft Virtual Server or VMWare link, such as VMWare Management Interface.

Solution: Internet Explorer may need to enable both **Active scripting** and **Allow META REFRESH** to allow these pages to properly redirect.

1. In Internet Explorer, select **Tools**→**Internet Options**.
2. Select the **Security** tab and select the appropriate zone (Internet, Local intranet, and so on).
3. Click **Custom Level**.
4. Under **Miscellaneous**, enable **Allow META REFRESH**.
5. Under **Scripting**, enable **Active scripting**.
6. Click **OK**.
7. Click **OK**.

If you are using an Internet Explorer proxy server to access your network, be sure exceptions include the IP range and FQDN of the CMS and target system.

Solution: If your browser is configured to use a proxy server, you can configure it to bypass the proxy server for specific systems, which removes those systems from the browser **Internet Zone**.

1. From the browser menu, select **Tools**→**Internet Options**.
2. Click the **Connections** tab.
3. Click **LAN Settings**.
4. Click **Advanced**.
5. Enter the address of the CMS in the Exceptions list, and then click **OK**.



NOTE: You might also need to add the addresses of your managed systems. To enter multiple systems in the same domain, you can use a wildcard. For example: ***.scr.mt.com**.

Addresses in the Exceptions list are no longer in the Internet Zone, and are not affected by the privacy settings policy.

6. Click **OK** to close the Local Area Network (LAN) Settings window.
7. Click the **Security** tab.
8. Click the **Local intranet** icon, and then the **Sites** button.
9. Ensure the options for **Include all local (intranet) sites not listed in other zones** and **Include all sites that bypass the proxy server** are enabled.
10. Click **OK** twice to close both windows.

Alternatively, browsing to systems by IP address or fully-qualified domain name causes the browser to consider those systems to be in the Internet Zone. Instead, browse by name. To configure HP SIM to use system names when creating links, select **Options**→**Security**→**System Link Configuration**, and choose **Use the system name**.

Installation

During the HP SIM installation on Windows Vista using a user who is member of the administrators group, after is installed, when I click Next, an error displays indicating there are insufficient rights to the database.

Solution: To resolve:

Disable the **User Account Control** (UAC) for the user and continue the installation.

During the HP SIM installation, the Port values on the Database configuration page are grayed out for Oracle.

Solution: To resolve, select **Use SQL/SQL Express** and then select **Use Oracle**. The port values are enabled.

The HP Virtual Server Environment (VSE) Standalone Servers collection displays the same result as the All Servers collection after the database initialization during the HP SIM installation.

Solution: To resolve, restart the HP SIM server if collections return unexpected results after the HP SIM installation.

After installing HP SIM on a system, mxstop and mxstart commands do not work.

Solution: This issue is caused by a firewall. To resolve, make sure your firewall allows the HP Systems Insight Manager service to run.

When attempting to install HP SIM with a named instance using , I receive the error "Unable to get information from the specified database server".

Solution: By default, the **SQL Browser** option is not selected during the installation of with a named instance. This option is also disabled by default in the Services Manager.

To resolve, from the installation screen, select **SQL Browser** when installing or manually starting the service after the installation.

I am unable to install HP SIM on with the default security settings.

Solution:

1. Click **Start**→**All Programs**→**Administrative Tools**→**Server Manager** or go to **Control Panel**→**Administrator Tools**→**Server Manager**.
2. From the right panel, scroll down to **Security Information**→**Configure IE ESC** and set **Internet Explorer Enhanced Security Configuration (IE ESC)** to **Off** for **Administrator** and **Users**.
3. Click **OK** and restart the HP SIM installation.

After installing HP SIM using a domain account on Windows Vista, the HP SIM icon on the desktop is not executable if signed in using the domain account.

Solution: Sign into HP SIM using the Administrator account and the icon is executable.

After installing HP SIM on Windows Vista and , the command window opens, by default, as a non-administrator even if the user is an administrator if UAC (User Access Control) is turned on.

Solution: UAC is turned on by default. Since the HP SIM install folders are protected by providing access only to users with administrator rights, a command window opened by a non-administrator user does not have access to contents in the HP SIM install folder and thus the commands fail.

To resolve, right-click on the command window short-cut and select **run as Administrator** or disable UAC in the system.

Windows Vista has been identified as Unmanaged after I used a standard account which is a member of the Administrator group.

Solution: You must use the local Administrator account on the Windows Vista system. To be identified as Desktop in HP SIM, you must turn off user account control (UAC).

The Service Account Credentials page displays the user name as "undefined" after upgrading Windows XP to Windows Vista and then upgrading HP SIM.

Solution:

1. Go to **Manage**→**User and Groups**→**Enable Administrator account**
2. From the **Service Account Credentials** page, change the **Username** field to **Administrator** and enter the associated password.
3. Restart the HP SIM service.

I cannot load HP SIM on Windows NT 3.51 or Windows NT 4.0.

Solution: Windows NT 3.51 and Windows NT 4.0 are not supported platforms.

During a Windows install at the database credentials screen, the installer fails with an invalid credentials error, and I am unable to enter my password.

Solution: A user name and password cannot contain a space followed by a double quote. An Oracle user name cannot contain a backslash (\) or a forward slash (/).

If you use these characters in your user name or password, you will receive an "Invalid character" error and not be allowed to sign in.

I receive the error "Database Connection Error" during the Java-based database installation portion of HP SIM installation.

Solution: Verify that the target Microsoft SQL Server service (MSSQL) is running (select **Control Panel**→**Services**→**MSSQLSERVER**). For SQL Server 2005, servicename will be "SQLServer."

When installing HP SIM on Microsoft SQL Server 2005 Express Edition Service Pack 1 the following error message appears "TCP/IP protocol is not enabled. Run SVRNETCN.exe to enable TCP/IP."

Solution: TCP/IP is disabled in SQL 2005 by default. To enable TCP/IP:

1. Click **Start**>**Microsoft SQL Server 2005** >**Configuration Tools**> **SQL Server Configuration Manager**. The **SQL Server Configuration Manager** window appears.
2. Select **SQL Server 2005 Network Configuration** from the left pane. The protocols will be displayed on the right frame.
3. Right click **TCP/IP** and select **Enable**.
4. Restart SQL server to reflect the changes.

During the installation, the system reboots, and then the installation launches the browser. Internet Explorer displays a message saying that it could not establish a connection with the local host. The browser is being launched before the service has had time to start.

Solution: Try to access the URL again by placing the cursor in the URL field and pressing the Enter key. Keep trying until the application loads in the browser.

I cannot load HP SIM on Windows NT 3.51 or Windows NT 4.0.

Solution: Windows NT 3.51 and Windows NT 4.0 are not supported platforms.

I receive the error Database Connection Error during the Java-based database installation portion of HP SIM installation.

Solution: Verify that the target Microsoft SQL Server service (MSSQL) is running (Select **Control Panel**→**Services**→**MSSQLSERVER**). For SQL Server 2005, servicename will be **SQLServer**

When installing HP SIM on Microsoft SQL Server 2005 Express Edition Service Pack 1 the following error message appears "TCP/IP protocol is not enabled. Run SVRNETCN.exe to enable TCP/IP."

Solution: TCP/IP is disabled in SQL 2005 by default. To enable TCP/IP:

1. Click **Start**>**Microsoft SQL Server 2005** >**Configuration Tools**> **SQL Server Configuration Manager**. The **SQL Server Configuration Manager** window appears.
2. Select **SQL Server 2005 Network Configuration** from the left pane. The protocols will be displayed on the right frame.
3. Right click **TCP/IP** and select **Enable**.
4. Restart SQL server to reflect the changes.

Global Unique Identifiers are the same for all systems when using Disk Imaging software on servers.

Solution 1: If the disk image has not been taken, perform the following:

1. Uninstall all Insight Management Agents from one of the systems.
2. Use the Disk Imaging software to copy the configuration from the system without the Insight Management Agent installed.
3. Use the disk image from step 2 to copy to the target systems.
4. Reinstall the HP Insight Management Agents on all the systems.

Solution 2: If the disk image has already been deployed, perform the following to remove the image from each target system. The following information is divided by network operating systems.

▲ In NetWare:

The Globally Unique Identifier information is stored in a 16-byte file on the `sys:\system` subdirectory of the NetWare server. This file is created and populated with the Globally Unique Identifier when HP SIM performs an SNMP SET command to the NetWare server.

To remove the permanence of the Globally Unique Identifier, delete the file `\system\cpqbssa.cfg` in the NetWare SYS volume.

After the file is deleted, restart the Insight Management Agent and a new Globally Unique Identifier is assigned by HP SIM when the system is discovered.

▲ In Windows NT:

The Management Agents create the Globally Unique Identifier information in an entry in the Windows NT registry.

To remove permanence of the Globally Unique Identifier, remove the entry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Compaq Insight Agent\hostGUID`

After the entry is removed, restart the Insight Management Agent services. A new Globally Unique Identifier is automatically generated.

▲ In UnixWare:

The Globally Unique Identifier information is stored in a file that is created and populated with the Globally Unique Identifier when HP SIM performs an SNMP `SET` command to the UnixWare server.

To remove the permanence of the Globally Unique Identifier, delete the following file from the UnixWare system.

`/var/spool/Compaq/foundation/registry/cpqhoguid.dat`

After this file has been deleted, restart the Management Agents. A new Globally Unique Identifier is assigned by HP SIM when the system is discovered.

On a Windows XP SP2 machine, I receive an error message and the installation does not complete.

Solution: If Simple File Sharing is enabled, it must be disabled.

1. Go to **Start**→**My Computer**→**Tools**→**Folder Options**→**View**.
2. Scroll to the bottom of the list of advanced settings, and deselect **Use Simple File Sharing (Recommended)**.
3. Click **OK**.

On an HP-UX system, the `mxinitconfig -a` command fails at step 8, and the following error appears in the `/var/opt/mx/logs/initconfig.logfile`: ...8. Database Configuration Connecting to database...- Failed HP Systems Insight Manager shutting down: Lost connection to database. org.postgresql.util.PSQLException: Connection refused. Check that the host name and port are correct and that the postmaster is accepting TCP/IP connections. for db loaded from database.props

Solution: Try the following solutions:

- Ensure that the `semnmi` and `semnms` kernel parameters are set to the minimum values (1024 for `semnmi` and 2048 for `semnms`.)
- The subdirectory `/var/opt/iexpress/postgresql` exists because the PostgreSQL product is not installed or was installed and uninstalled incorrectly. Uninstall PostgreSQL if it is installed, delete the `/var/opt/iexpress/postgresql` directory, and then reinstall PostgreSQL.

After installing HP SIM, a CMS that is setup on a desktop is shown as a server.

Solution: Identification identifies a system as a server if SMH is found on the system. Re-identify the CMS with WBEM credentials. The system will be identified as Desktop with the correct system information.

IP address

When systems change IP addresses on the network, the information in the database becomes unreliable. For example, the system name comes from one system, and the description comes from the new system that took that address.

Solution: After systems have been discovered, they can never be "un-discovered." Systems that are no longer reachable must be deleted through a collection (signed-in with administrative rights). Systems that HP SIM can no longer communicate with change to Critical status. Systems can be deleted by selecting systems in the collection and clicking **Delete**.

Logs

Null pointer exceptions seen on HP-UX 11.23 during a upgrade from 4.2 when debugging is turned on.

Solution: SQL duplicate errors occur when you perform an upgrade or replace a MIB that already exists because the code does an insert without searching the database, therefore, generating an SQL exception. The exception handler, upon fielding this exception, updates the MIB information in the data.

Menu

Internet Explorer can exhibit poor or erratic behavior, such as repainting excessively, not fully displaying sub-menu options, not keeping up with mouse movement, and sometimes showing menu cascades with scroll bars and other unusual formatting.

Solution: Internet Explorer has several settings that alleviate or eradicate these issues:

- Solution 1:
 1. Select **Start**→**Settings**→**Control Panel**→**Internet Options**→**Security**→**Trusted sites** and click **Sites**.
 2. In the **Add this Web site to the zone** field, enter the HP SIM system as `https://<system name>:50000` and click **Add**.
 3. Click **OK**.

Note: This solution is specifically (and only) for the problem described as not fully displaying sub-menu options.

- Solution 2:
 1. Select **Tools**→**Internet Options**→**General**→**Temporary Internet Files**→**Settings**→**Check for newer versions of stored pages**.
 2. Select the Microsoft default of **Automatically**. The setting of **Every visit to the page** causes the problem.
 3. Click **OK**.
- Solution 3:
 1. Select **Tools**→**Internet Options**→**Advanced**→**Security**→**Do not save encrypted pages to disk**.
 2. Use the Microsoft default of **unselected**. Selecting this option causes the problem. HP SIM already marks all encrypted pages to not be stored by the browser. HP SIM does allow caching of images and style sheets; selecting this setting disables caching of those resources as well, which degrades performance.

I ran discovery, but when I go to the Tools menu, the command line tools are not present.

Solution: In HP SIM, menus are refreshed only after accessing a new URL or clicking the browser refresh button.

After upgrading HP SIM, there are two menu options for License Manager.

Solution: This could happen if Virtual Machine Management Pack is using License Manager in an unsupported mode and the version of Virtual Machine Management Pack in use is a legacy version.

OpenSSH

After installing OpenSSH on a managed system, I cannot find the .ssh directory.

Solution: The `.ssh` directory is not created by the SSH installer. Run `mxagentconfig` on the CMS, and enter the target system name (such as, `hpsystem`) and credentials.

I am receiving errors when running OpenSSH, such as %1 is not a valid Win32 application.

Solution: Search the root directory for a folder or file named `Program`. If this file exists, delete it. If this folder exists, rename it or delete it if the folder is empty.

When deploying OpenSSH, the installation times-out or ends in an error.

Solution: The problem might be that the domain that the target systems are in is too large. The `mkgroup` command, which runs as part of the OpenSSH install, is finding a large number of defined Domain Groups

within the domain (perhaps from Backup Domain Controllers (BDC), trust relationships with other domains, or from all of the systems that are a member of the domain) and adding them to the group file created in the `\etc` directory of the OpenSSH installation. This occurs for about 10 to 15 minutes before the OpenSSH install either times-out or simply crashes. To verify if this issue is occurring, verify if the size of the `\etc\group` file is greater than 50 KB.

HP suggests manually installing OpenSSH on the system using the `openssh.exe` program located in the `C:\Program Files\OpenSSH` directory on the installation media, and then running Configure and Repair Agents against the system if you are experiencing this issue.

Operating system

When the operating system changes on a system and system discovery restarts, HP SIM still discovers an instance of the system running the old operating system with no items in the system links section. HP SIM also discovers the system with the new operating system and with the correct system links.

Solution: After systems have been discovered, they can never be "un-discovered." Systems that are no longer active (the management server can communicate with the system) change to Critical status and can be deleted.

My Evo Workstation 6000 system does not show the correct operating system when it is running Windows XP.

Solution: The root problem is that the SNMP Agent does not correctly recognize this version of Windows. Stop the SNMP service, set it to a manual startup, and run Data Collection from HP SIM again to get the correct information.

Paging notification

On an upgraded version of HP SIM, which has a paging user upgrade, I am receiving an error, indicating that the user does not exist!, but I can see the user on the Users page. Why do I get this message?

Solution: A user with administrative rights must delete the existing paging user and create a new paging user with the same details as the original paging user.

To resolve:

1. Select **Options**→**Security**→**Users and Authorizations**→**Users**.
2. Find the paging user in the **Pager Configured** column. **Yes** appears if the user is a paging user.
3. Select the user account to delete.
4. Click **New**.
5. Create a new paging user account.
6. Click **OK**.

Passwords

The password for the service account used by the HP SIM Windows service is changing. What do I need to change?

Solution:

1. Stop HP SIM.
2. Access the **Services** control panel and edit the service credentials to provide the new password for the HP Systems Insight Manager service.
3. Run `mxcpassword -g` and modify the following password:
`MxHPSIMServicePassword`
4. Restart HP SIM.

The password for the database account used by the HP SIM Windows service is changing. What do I need to change?

Solution:

1. Stop HP SIM.
2. Run `mypassword -g` and modify the following password to the new account password:
MxDBUserPassword
MxPMPPassword
3. Restart HP SIM.

Ping

I am not able to ping discovered systems.

Solution: If you manage more than 1,000 systems in HP SIM, tune the kernel parameters by adding the following entries to the `/etc/sysctl.conf` file:

```
net.ipv4.neigh.default.gc_thresh3 = 4096
```

```
net.ipv6.neigh.default.gc_thresh3 = 4096
```

After adding the entries, reboot the system.

Printing

When printing a container view page that includes a Rack Display, the display does not print correctly.

Solution: In Internet Explorer, select **Tools**→**Internet Options**, then select the **Advanced** tab. Select **Printing**→**Print background colors and images**. The system Details page should now print the Rack Display correctly, showing all details of the rack.

When trying to print in Internet Explorer, I am receiving a message, stating that my printer is not configured. In Mozilla, the print dialog box appears to print to a file.

Solution: The printer must be installed before trying to print in both Internet Explorer and Mozilla.

When printing lists or reports in HP SIM, selecting Landscape as the paper orientation is not changing the printout to landscape.

Solution: From **Control Panel**→**Printers**, set the orientation to **Landscape**.

Property pages

When I click the FC HBA link on the Property Pages Status tab, I receive an error message.

Solution: Even though FC control is not present on the system the FC HBA hot link might be displayed on the **Status** tab. For an FC HBA, HP SIM cannot anticipate if there will be instances present and might display this link. If there are instances present, the CIM Client connection might have timed out.

The following error messages can be received on the Property pages:

error message	meaning
Property pages are unavailable because this system acts as a WBEM storage proxy.	The target system contains a WBEM installation (CIMOM) that is a storage proxy CIMOM. There is not a WBEM CIMOM that models the target system. Therefore, the Property pages do not have an agent that collects system-specific information. Install a server WBEM CIMOM to enable WBEM manageability for the target system.
Communication has been lost. Close the window and relaunch Properties for this system.	The Property pages are subject to the web server default time-out (20 minutes). If the Property pages time out, this message appears. Close the window, and relaunch the Property pages against the target system.
Unknown WBEM error.	An unanticipated WBEM error has occurred. Contact HP Support.
Error: Cannot connect to target system using WBEM. Check WBEM protocol settings for this system under Options Protocol Settings Global Protocol Settings .	The target system has been identified as WBEM enabled, but the credentials are failing for the target system. Verify the credentials, and identify the target system again.
Target system is unavailable.	The target system is not able to create a WBEM connection.
No WBEM data is available.	The WBEM connection to the target system is successful but the system is not returning data for specific WBEM classes.

Requests to retrieve information from the CPU Instance Provider, Memory Instance Provider, and the Environmental Provider might time out on some platforms since providers are slow in gathering inventory information. Also, providers do not inform the client that the inventory information is being gathered. This results in periodic failures or missing data entries when populating the HP SIM Property Pages or Inventory data.

Solution: This issue is fixed in the System Fault Management (SFM) product delivered with 0603OEUR. Providers no longer time out. Instead, a message is displayed on the managed system, stating `Inventory is being build currently`. Please try after some time. After the inventory information is gathered, providers respond with the requested information to the client as subsequent requests are made.



NOTE: After installation of the SFM product, the first request to any provider for information related to various systems is slow. Subsequently, requests are quick (event after a reboot).

Protocol

When adding a client to the CMS, the WBEM protocol is not displayed under management protocols, and none of the WBEM properties are listed on the System Page for the client.

Solution: The password might be incorrect on the **System Protocol Settings** page (**Options**→**Protocol Settings**→**System Protocol Settings**).

I receive the error message <<<CANNOT BE BLANK, and the Schedule and Run Now buttons are disabled.

Solution: If a field is left blank on the **System Protocol Settings** page, this message appears. Fill in the blank fields, and the buttons will be enabled.

Replicate Agent Settings

When running a Replicate Agent Settings task with the Wake target systems from low power mode before configuring option selected, I receive the following error on the Task Results page in the Task Details section:

Failed to power up system.

Solution:

1. Release and renew the IP address of the system.
 - a. Select **Start**→**Settings**→**Network and Dial-up Connections**.
 - b. Double-click **Local Area Connection Status**. The **Local Area Connection Status** window appears.
 - c. Click **Properties**. The **Local Area Connection Properties** window appears.
 - d. Select **Internet Protocol (TCP/IP)**, and then click **Properties**. The **Internet Protocol (TCP/IP) Properties** window appears.
 - e. Update the IP address accordingly.
2. Delete the system from the database, and rediscover the system. See “Configuring automatic discovery” for more information about running discovery.
3. Run the Replicate Agents Settings task. See “Creating a Replicate Agent Settings task” for more information.

When running a Replicate Agent Settings task, I receive the following error on the Task Results page in the Task Details section: `No is not true: Wrong compaq.cimom.supported.`

Solution: This message indicates that the system does not have any Web Agent that supports being configured by way of Replicate Agent Settings. It is possible that the Replicate Agent Settings, such as System Management Homepage, were not running during discovery or were not installed on the target system. Verify that there is a System Management Homepage link on the system page in HP SIM. If there is no System Management Homepage link, try to deploy one by using the Initial HP ProLiant Support Pack installation.

Response

It takes five minutes or more to load when https:// is entered in the URL address.

Solution: The URL address should be entered `http://`, without the “s.” When `https://` is entered in the URL, an SSL message is sent to the server, causing delay.

When browsing to the Web Agents or to System Management Homepage on a remote system from HP SIM, the browser displays Page Note Found.

Solution: There are several possible solutions:

- It might be that the Web Agents or the System Management Homepage is no longer running on the remote system. They must be started to be accessible.
- It might be that the remote system is not reachable from your browser. If the HP SIM server is managing systems on two networks and your browser client is only on one network and the remote system is on the other network, then it will be unreachable.
- It might be that the address of the target system is not correctly resolving to the proper IP address. There might be a problem in the DNS configuration of your network. If so, and it is beyond your realm of control, you can alleviate the problem by adding the remote system name and its real IP address to the hosts file on the HP SIM server, the browser system, or both. Another solution is to modify the **Options→Security→System Link Configuration** settings in HP SIM, and then select **Use the system IP address**.

Search

When searching for systems on which the operating system is the single version of HP-UX 11.11, two criteria are displayed in the operating system collection. If I select HP/HP-UX 11.11, the CMS appears. If I select HP-UX/HP-UX B.11.11 U, all of the HP-UX systems are displayed except the CMS.

Solution: Instead of selecting **is** in the comparison selection box, select **contains**, and then enter **HP-UX 11.11**.

Security

Security Alerts are appearing on the client browser indicating secure and unsecure mixture of data on the page. Pressing ok to these alerts causes me to be logged out of HP SIM.

Solution: If Security Alerts are appearing on the client browser indicating secure and unsecure mixtures of data on the page, and/or the CMS performance seems poor, it may be due to a low memory condition. Check the memory usage of the Mxdomainmgr.exe service on the CMS. If it appears to be high (700MB usage or greater) and HP SIM is installed on a system with only the minimum recommended memory (see *HP Systems Insight Manager 5.2 Installation and Configuration Guide for Microsoft Windows* for requirements), you may want to consider upgrading the memory on the CMS. Alternately, if you are running HP SIM with the database installed locally on the CMS, installing a remote database may also help to improve performance.

Executing a tool on a managed system results in the error: Authentication failure: The Central Management Server (CMS) and managed system time clocks might not be synchronized, or a communication time limit might have been exceeded.

Solution: The CMS and managed systems must be time-synchronized to prevent authentication failures. The communication time limit is 20 minutes, and exceeding this limit causes authentication failures. Use the command `xntpdate(1m)` to configure the time synchronization.

I am unable to Single Login or set the trust status to Linux agents.

Solution: To resolve this issue, configure the System Link Configuration setting to IP address or full DNS name.

To configure the System Link Configuration setting from the HP SIM CMS:

1. Select **Options→Security→System Link Configuration**. The **System Link Configuration** page appears.
2. Select from the following options:
 - **Use the system name**. Select this option to use the system name.
 - **Use the system IP address**. Select this option to use the system IP address. For systems with multiple addresses, multiple links can be entered.
 - **Use the system full DNS name**. Select this option to use the full system *Domain Name Service* (DNS) name.

Note: On an HP-UX or Linux Central Management Server (CMS), the default value is **Use the system full DNS name** on new HP SIM installations. New installations on Windows defaults to **Use the system name** and upgrades maintain the existing setting regardless of the operating system.

Note: During *discovery*, the full system DNS name is used as the primary lookup key (if it is available). Otherwise, the IP address is used.

Note: In the case of systems with multiple network interfaces, selecting the **Use the system name** provides only one link per destination to the system, whereas **Use the system IP address** provides multiple links to the system.

3. To save and apply the changes, click **OK**.

Serviceguard Manager

When upgrading from SCM 3.0 with Serviceguard Manager installed to HP SIM 4.1, Serviceguard Manager no longer runs.

Solution: When HP SIM is upgraded, some of the files that Serviceguard Manager installs are replaced so that it appears that Serviceguard Manager is not installed. Reinstall Serviceguard Manager.

When I launch Serviceguard Manager, I am asked to download a `.jnlp` file. The following scenarios might appear when installing Serviceguard Manager.

Scenario 1: Java Web start not installed.

Solution: Download and Install Java Web start.

Scenario 2: Java Web start is installed, but you are still being asked to download the `.jnlp` file. See one of the operating systems in the following list for the solution.

Windows 2003 IE Browser Solution:

1. Download the `.jnlp` file.
2. Right-click the `.jnlp` file.
3. Select **Open with...and Choose Program**.
4. Click **Browse**.
5. Navigate to and open `C:\Program Files\Java Web Start\javaws.exe`.
6. Select **Always use this program to open these files**.
7. Click **OK**.

Linux Mozilla Browser Solution:

1. Click **Launch Serviceguard Manager**.
2. Select **Open with...and Choose Program**.
3. Click **Choose**.
4. Navigate to `/usr/java/j2re1.4.2/javaws/javaws`.
5. Select **Always perform this action**.
6. Click **OK**.

HP-UX Mozilla Browser Solution:

1. Click **Launch Serviceguard Manager**.
2. Select **Open with...and Choose Program**.
3. Click **Choose**.
4. Navigate to `/opt/java1.4/jre/javaws/javaws`.



NOTE: If this path is not present, install the T1456AA with Java Web start.

5. Select **Always perform this action**.
6. Click **OK**.

I received an HTTP 404 error when I tried to launch Serviceguard Manager.

Solution: After installing HP SIM, Serviceguard Manager must be installed on the CMS platform (Windows, Linux, HP-UX). At this time, SGM is registered with HP SIM. If, at a later time, you uninstall Serviceguard Manager, you will receive an HTTP 404 error if you try to launch it. Because the Serviceguard Manager uninstall application deletes the directory `sgmgr` under the HP SIM webapps directory, which is located at `/opt/hpwebadmin/webapps` on HP-UX and Linux and at `\Program Files\HP\System Insight Manager\hpwebadmin\webapps` on Windows.

To avoid the HTTP 404 error in the future, remove the tool from HP SIM using the following command:

```
mxtool -r -f sgmw-web-tools.xml
```

If Serviceguard Manager is reinstalled in the future, add the tool to HP SIM again, using the following command:

```
mxtool -a -f sgmw-web-tools.xml
```

Sign-in

I cannot sign-in to HP SIM on Windows XP using a blank password.

Solution 1: Use a non-blank password, which provides better security. Have an administrator reconfigure the Windows User Accounts to specify a non-blank password.

Solution 2: If you must use a blank password, disable the following **Security Policy** on the Windows XP machine: **Accounts: Limit local account use of blank passwords to console login only**.



NOTE: Disabling this policy allows remote logins over the network using accounts that have no passwords.

On a Windows system, to limit local account use of blank passwords to console sign-in only, complete the following procedure:

1. Open Local Security Settings MMC Application by selecting **Programs**→**Administrative Tools**→**Local Security Policy**.
2. Open the **Local Security Policies** folder, and then open the **Security Options** subfolder.
3. Disable the policy.

I cannot sign-in to HP SIM on Windows XP.

Solution: If using a blank password, see the preceding problem. Otherwise, change the following Local Security Policy on the Windows XP machine: **Network Access: Sharing and security model for local accounts** from Guest Only to Classic.



NOTE: This setting does not affect remote sign ins using domain accounts. Modifying this policy allows remote sign ins over the network using any local account configured to do so, not just the Guest account. Ensure all local accounts have appropriate passwords.

To change the setting:

1. Open Local Security Settings MMC Application by selecting **Programs**→**Administrative Tools**→**Local Security Policy**.
2. Open the **Local Security Policies** folder, and then open the **Security Options** subfolder.
3. Change the setting from Guest Only to **Classic**.

If Guest Only is the preferred policy setting, perform the preceding steps, sign-in to HP SIM, and then add domain accounts (not local accounts) or the local Guest account as accounts to HP SIM. Restore the local policy setting back to Guest when done.

Single Login fails on cluster systems.

Solution: Single Login does not work on a virtual cluster system. It works on the physical systems that comprise the cluster.

By using a proxy server, you might inadvertently or intentionally bypass IP address login restrictions configured for the user.

Solution: A proxy server can be used to bypass specific IP exclusions, if the proxy server IP address is not included in the IP exclusion ranges on the **Login IP Address Restrictions** page. Likewise, the possibility that a valid proxy server is included in the IP exclusion ranges would prevent a valid user from signing in through that particular proxy server.

Ensure valid proxy servers are within a valid Inclusion ranges, and make the Inclusion ranges as small as possible. Using IP inclusion ranges is more effective than using IP exclusion ranges because Inclusion ranges exclude all addresses not specified in the IP inclusion range.

I cannot sign-in to HP SIM using Internet Explorer 6.0.

Solution: If your HP SIM server has an underscore in the name, use the IP address of the HP SIM server instead of the name in the Internet Explorer address field. Internet Explorer has a problem with underscores in system names, which prevents the authentication cookie from working properly.

I cannot sign-in to HP SIM or to managed systems browsing from HP SIM using Internet Explorer 6.0.

Reason 1: Internet Explorer has a problem with underscores in system names, which prevents the authentication cookie from working properly.

Solution: If the names of the systems have an underscore, use the IP address of the system. Configure HP SIM to create links to the system using the IP address instead of the name:

1. Browse and sign-in to HP SIM.
2. Select **Options**→**Security**→**System Link Configuration**. The System Link Configuration page appears.
3. Select Use the system IP address.
4. Click **OK**.

Note: By using IP addresses instead of names, you might encounter security alerts, if the name in the managed system certificate does not match the name in the link. The default certificate for managed systems uses the system name, not the IP address.

Reason 2: For managed systems, the privacy policy setting in Internet Explorer 6.0 is blocking the authentication cookies from the managed systems.

Solution 2A: (Recommended) Remove the systems from the Internet Zone. The privacy policy only affects systems in the browser **Internet Zone**. Therefore, by removing systems from that zone, you prevent the privacy policy from affecting those systems. To change the browser privacy policy setting, select **Tools**→**Internet Options**, and then click the **Privacy** tab from the Internet Explorer browser menu. Modify the privacy setting in **one** of the following ways:

- ▲ Browsing to systems by IP address instead of by name can cause the browser to consider those systems to be in the **Internet Zone**. Instead, browse by name. You can configure HP SIM to use system names when creating links to systems by selecting **Options**→**Security**→**System Link Configuration** and selecting **Use the system name**.
- ▲ If your browser is configured to use a proxy server, you can configure your browser to bypass the proxy server for specific systems, which removes those systems from the browser **Internet Zone**. From the browser menu, select **Tools**→**Internet Options**, and then click the **Connections** tab. Click **LAN Settings**, and if you are configured to use a proxy server, click **Advanced**. In the **Exceptions** list, you can specify a list of addresses that should bypass the proxy server. These addresses are no longer in the **Internet Zone** and are not affected by the privacy settings policy.
 1. From the browser menu, select **Tools**→**Internet Options**.
 2. Click the **Connections** tab.
 3. Click **LAN Settings**.
 4. Click **Advanced**.
 5. Enter the address of the CMS in the Exceptions list, and then click **OK**.



NOTE: You might also need to add the addresses of your managed systems. To enter multiple systems in the same domain, you can use a wildcard. For example: **https://*.scr.mt.com**.

Addresses in the Exceptions list are no longer in the Internet Zone, and are not affected by the privacy settings policy.

6. Click **OK** to close the Local Area Network (LAN) Settings window.
7. Click the **Security** tab.
8. Click the **Local intranet** icon, and then the **Sites** button.

9. Ensure the options for **Include all local (intranet) sites not listed in other zones** and **Include all sites that bypass the proxy server** are enabled.
10. Click **OK** twice to close both windows.

Solution 2B: (Not Recommended) Change the browser privacy security policy setting. From the Internet Explorer browser menu, select **Tools**→**Internet Options**, and then click the **Privacy** tab. The privacy setting can be modified in one of the following ways:

- Set the privacy setting to **Accept all Cookies** by sliding the slider bar to the bottom. This setting allows a browser to accept all cookies for both first-party and third-party sites. When browsing to HP SIM or directly to a managed system, it is considered a first-party site. When navigating to a managed system through HP SIM, the system is considered a third-party site.
- Customize the handling of cookies by clicking **Advanced** and enabling **Override automatic cookie handling**. Then select the appropriate radio buttons for first-party and third-party cookies to **Accept** or **Prompt**. If you select **Prompt**, the browser prompts you on how to handle a cookie each time a cookie is received. You can choose to block or allow the cookie each time, or for all times. Enabling **Always allow session cookies** does not resolve the problem because the Web Agents do not use session cookies.
- Individually specify the handling of cookies for each system. Click **Edit** in the **websites** section and add the address of the system in the specified field. Click **Allow** to always allow cookies to that system. Repeat this for all systems.

Selecting a link that opens a new browser window requires another sign-in.

Solution: If you are browsing using the Internet Explorer link from within Windows Explorer, you must instead start Internet Explorer as a separate process. Start Internet Explorer by selecting it from the Windows Start menu or using the desktop icon.

I cannot sign-in to the HP SIM server from Windows NT, Windows 2000, or Windows XP.

Solution: The Windows accounts used to access HP SIM must have the **access this computer from the network** right selected.

In Windows NT 4, open the User Manager by selecting **Start**→**Programs**→**Administrative Tools**. In the **Policies** menu, select **User Rights**. In the **Rights** dropdown list, select **access this computer from network**, and ensure the HP SIM users are granted administrative rights.

In Windows 2000 and Windows XP, open the Local Security Policy by selecting **Start**→**Programs**→**Administrative Tools**. Expand the Local Policies tree, and then select **User Rights Assignment**. Ensure the HP SIM users have the **access this computer from the network** right and that they do not have the **Deny access to this computer from the network** right selected.

I am receiving the exception org.apache.jasper.JasperException while signing in to HP SIM.

Solution: Delete all the files in the work directory, and sign-in again.

- On HP-UX and Linux: /opt/mx/jboss/server/hpsim/work
- On Windows: \jboss\server\hpsim\work

I am being asked for my sign-in credentials when accessing a trusted system.

Solution: Verify that you have a valid trust relationship set up between HP SIM and the managed system. Also, verify that you are authorized for an appropriate tool on the desired system. Tools that enable Single Login to System Management Homepage include System Management Homepage as Administrator, System Management Homepage as Operator, System Management Homepage as User, Replicate Agent Settings, and Install Software and Firmware. For Single Login to Onboard Administrator, tools include Onboard Administrator as Administrator, Onboard Administrator as Operator, and Onboard Administrator as User. For Single Login to HP StorageWorks Command View EVA, tools include Command View EVA as Administrator, Command View EVA as Operator, and Command View EVA as User. See “Setting up trust relationships” for more information about setting up trust relationships.

I am prompted for sign-in credentials when accessing a trusted StorageWorks Command View system.

Solution: If the Command View system is configured to trust HP SIM for Single Login, it is possible that HP SIM is attempting to access the Command View system using a host name that does not resolve on the CMS. Examine the URL being used to access Command View to determine the host name being used, either from the Command View link, or the browser address bar on the Command View sign-in page. Ensure that name

can be resolved and is reachable from the CMS; you might need to reconfigure network or name service settings on the CMS.

After installing the Microsoft MS04-025: Cumulative Security Update for Internet Explorer (867801), I can no longer access HP SIM and System Management Homepage.

Solution: This issue affects any system running Windows XP Service Pack 2 and any version of HP SIM and System Management Homepage or any system running Windows XP Service Pack 2 and browsing to HP SIM running on any supported operating system. To resolve:

- Configure Windows XP Service Pack 2 firewall to allow access to System Management Homepage.
 1. On the Windows XP system, select **Start**→**Control Panel**→**Windows Firewall** to configure the firewall settings.
 2. Click the **Exceptions** tab, and then click **Add Port**.
 3. Add the following exceptions to the firewall protection. Enter the product name and the port number for each.

Description	Port	Protocol
HP SMH Web Server*	2301	HTTP
HP SMH Secure Web Server*	2381	HTTPS
WBEM/WMI Mapper	5988	HTTP
WBEM/WMI Mapper Secure Port	5989	HTTPS
SSH port	22	SSH
SNMP Agent	161	SNMP
Ping Discovery (ICMP)**	***	ICMP
Ping Discovery (TCP)**	80	HTTP

* If the system is not being managed from HP SIM, only ports 2301 and 2381 should be configured to enable browser access to System Management Homepage.

** Usage is configurable in HP SIM.

*** This setting is under the **Advanced** tab of the **Windows Firewall** window. Select **ICMP Setting**→**allow incoming echo request**.

4. In the **Add a Port** window, click **OK**.
5. In the **Windows Firewall** window, click **OK**.

This configuration leaves the Windows XP Service Pack 2 security enhancements intact and allows traffic over the ports listed in the previous table.

Note: HP SIM discovers Web servers on other ports

- Enable file and print sharing and Remote Administration Exception.
 1. Enable file and print sharing:
 - a. Select **Start**→**Control Panel**.
 - b. Click **Windows Firewall** to configure the firewall settings.
 - c. Click the **Exceptions** tab.
 - d. Select the **File and Print sharing** checkbox.
 - e. Click **OK**.
 2. Enable Remote Administration Exception:
 - a. In the **Control Panel**, open the **Group Policy** editor.
 - b. Select **Computer Configuration**.
 - c. Select **Administrative Templates**.
 - d. Select **Network**.
 - e. Select **Network Connections**.
 - f. Select **Windows Firewall**.

- g. Select **Domain profile**.
 - h. Select **Enable the Windows Firewall: Allow Remote Administration Exception**.
- Configure Windows XP Service Pack 2 to allow access to HP SIM on the system running Windows XP Service Pack 2 and HP SIM.
 1. On the Windows XP system, select **Start**→**Control Panel**→**Windows Firewall** to configure the firewall settings.
 2. Click the **Exceptions** tab, and then click **Add Port**.
 3. Add the following exceptions to the firewall protection. Enter the product name and the port number for each.

Product	Port	Protocol
SNMP Trap Listener	162	SNMP Trap (UDP)
HP SIM web Server	280	HTTP
RMI registry	2367	RMI
JBoss RMI/JRMP Invoker**	4444	TCP
JBoss Pooled Invoker**	4445	TCP
JBoss Web Service port**	8083	TCP
HP SIM Secure Web Server	50000	HTTPS
HP SIM SOAP *	50001	HTTPS
HP SIM SOAP with client certificate authentication*	50002	HTTPS
HP SIM SOAP*	50003	HTTPS
HP SIM WBEM Event Receiver*	50004	HTTPS/HTTP*
WBEM Events	50005	TCP
PostgreSQL	50006	TCP
JBoss Naming Service RMI port**	50008	TCP
JBoss Naming Service port**	50009	TCP
HP SIM VMM Essentials v 1.1.2.0	50010	TCP
Web services RMI class loader	50013	TCP
JRMP invoker	50014	TCP
Pooled invoker	50015	TCP

* Configurable in HP SIM

** Configurable in the `SIM/jboss/server/hpim/conf/jboss-service.xml` descriptor

4. In the **Add a Port** window, click **OK**.
5. In the **Windows Firewall** window, click **OK**.

This configuration leaves the Windows XP Service Pack 2 security enhancements intact and allows traffic over the ports listed in the table.

After installing HP SIM, I changed the Windows administrator password and can no longer sign-in to HP SIM.

Solution: If you have SQL Server installed locally, verify that it is running. If it is not running verify the logon credentials. The service login credentials could have changed. The HP SIM service is registered to run under the credentials used during installation. To resolve this issue:

1. Change the MSSQL service password:
 - a. In Windows, open **Services (Start**→**Control Panel**→**Services)**.
 - b. Locate the MSSQL service (SQLserver service for SQL2005) and select **Properties**.

- c. Select the **Logon** tab, and change the password.
 - d. Restart the MSSQL (or SQLserver) service.
2. Change the HP SIM service password:
 - a. In Windows, open **Services (Start→Control Panel→Services)**.
 - b. Locate the HP SIM service, and then select **Properties**.
 - c. Select the **Logon** tab, and change the password.
 - d. Restart the HP SIM service.
3. If you are using OpenSSH on Windows Server 2000 or 2003, change the OpenSSH Server service password:
 - a. In Windows, open **Services (Start→Control Panel→Services)**.
 - b. Locate the OpenSSH Server service, and then select **Properties**.
 - c. Select the **Logon** tab, and change the password.
 - d. Restart the OpenSSH and HP SIM service.

Signing in from a dial-up connection takes a long time.

Solution: Your connection depends on many factors that are beyond your control. You might have a slow modem, the server you are connecting to might not be operating at peak efficiency, or you might have a bad phone line.

I cannot sign-in to HP SIM.

Solution: This condition can result from any of the following reasons:

- If the **IP Address Restriction** field (on the **New User Group, Edit User, New User, or the Edit User Group** pages) is configured, ensure that it includes all IP addresses of the CMS. If browsing to *localhost* ensure that the loopback address 127.0.0.1 is also included.
- You are not entering the information correctly. Passwords are case-sensitive.
- The account you are entering is not a valid account for HP SIM.
- The account you are entering has been deleted, disabled, or locked out.
- The password for the account must be changed.
- You are attempting to sign-in from an IP address that is not valid for the specified account.
- You do not have cookies enabled in your browser or you are using a cookie blocker.

I cannot sign-in to my Windows HP SIM.

Solution: If you are attempting to sign-in with a Windows user account created on the CMS (as opposed to a domain account) and the CMS host name is longer than 15 characters, then you must enter the first 15 characters of the CMS name in the domain field to sign-in. For example, if your Windows CMS is named "SIMwin2003withsp2" and you have a local account "bob," then sign-in with username = "bob" and domain = "SIMwin2003withsp2." Any new local user account created cannot sign-in, unless they were created using only the first 15 characters of the system name entered in domain name field and signed-in using the same.

SMI-S providers

HP SIM relies on CIM/WBEM servers and providers that conform to the *Storage Management Initiative (SMI-S)*. Before HP SIM can manage and report on a *storage system*, the appropriate SMI-S provider must be installed and configured.

Testing SMI-S provider installations

Complete the following procedure to test an SMI-S provider installation.

1. Open a DOS window on the CMS.
2. Set the current directory to `./Program Files/HP/Systems Insight Manager/.`
3. For each installed provider, type: `wbemdisco <host> <port> <interopnamespace> <user> <password>`.

See the following table for more information about each command option.

<code><host></code>	The IP address or DNS name of the SMA or PC on which the SMI-S provider is installed.
---------------------------	---

<port>	The port on which the SMI-S provider is running.
<namespace>	The "interoperability" namespace of the provider.
<user>	The user name giving access to the data available from the provider.
<password>	The corresponding password giving access to the data available from the provider.

4. The output should be similar to the following:

```
HOST    = coresma2
PORT    = 5989
NAMESP  = root
USER    = administrator
PASSWD  = ***** Connect to coresma2 in namespace root
with SSL=true
```

```
Enumerating instances of CIM_Registered Profile...
```

```
Profile.RegisteredName=Array
  Profile.RegisteredVersion=1.0.2
  ProviderVersion=4.0
  Profile.HPVersion=EVA4.0.0-Dev25
    SubProfile.RegisteredName=SNIA:Software
    SubProfile.RegisteredName=SNIA:Pool Manipulation
Capabilities and Settings
  SubProfile.RegisteredName=SNIA:Backend Ports
  SubProfile.RegisteredName=SNIA:LUN Mapping and
  Masking
  SubProfile.RegisteredName=SNIA:LUN Creation
  SubProfile.RegisteredName=SNIA:Copy Services
  SubProfile.RegisteredName=SNIA:Access Point
  SubProfile.RegisteredName=SNIA:Location
  SubProfile.RegisteredName=SNIA:Cluster
HPEVA_StorageSystem.CreationClassName=
"HPEVA_StorageSystem",Name="50001FE150014420"
  Namespace = root/eva
  Vendor=HP
  Name=HSV100
  IdentifyingNumber=50001FE150014420
```

This example shows one EVA array being reported on by the provider.

Troubleshooting SMI-S provider installations

If the output from `wbemdisco` is not similar to the previous example, check for the following errors:

Error connecting with `SSL=true` - Connection refused: connect (CIMCLIENT_ERR_CONNECTION_FAILED)

- Cause: The *CIMOM* is not running on the specified host .
Possible solutions:
 - Make sure the *CIMOM* is installed on the specified host, or try again with the correct host.
 - Verify that the *CIMOM* is running. See the *CIMOM* documentation for instructions. If the *CIMOM* is not running, start it and run `wbemdisco` again.
- Cause: The *CIMOM* is listening on a different port than the one specified. The default port for all *CIMOMs* communicating via `SSL` is `5989`.
Possible solution:
 - Check the port number on which the *CIMOM* is listening. If necessary, change the port number, and run `wbemdisco` again. See the *CIMOM* documentation for instructions on checking and changing the port number.

Error connecting with `SSL=true` - (CIM_ERR_ACCESS_DENIED)

Cause: The user name or password is incorrect.

Possible solutions:

- Make sure you enter a user name and password that allow at least read access to all data in the CIMOM.
- See the CIMOM documentation for instructions on determining the appropriate user name, and how to determine (or change) the password.
- For most HP SMI-S providers the default is user name: *administrator* and password: *administrator*. Use the `.\Program Files\Hewlett-Packard\SMI-S\cimom\UserAccountsManager.bat` utility to change the password. If you run the utility without input, it displays its syntax.
- For Command View EVA 5.0, the default user name is *administrator*. The password is created during the provider installation. You can change the password with the `cimuser` utility, which is installed during the provider installation.
- For Command View XP Advanced Edition 1.1 and later, the default user name is *system* and the default password is *manager*. You can add Users and change passwords through the Command View XP Advanced Edition user interface (you must log in with a username/password that is in the *Admin* group). Click the **User Management** branch, and then select **Users**. The user chosen for CIMOM access must be in the *Admin* or *StorageAdmin* group.
- For Windows HBAs (Emulex OEM), the default user name is *cimadmin* and the default password is *pwd580*. You can change the user name and password during the provider installation, or with the `cimuser` utility.

Error connecting with SSL=true - (CIM_ERR_INVALID_NAMESPACE)

Cause: The namespace is incorrect.

Possible solution:

Make sure you enter the correct namespace for the affected device.

Device	Default namespace
HP arrays	The default for most HP arrays is <code>root</code> , with the following exceptions: <ul style="list-style-type: none">• If you are running Command View EVA 5.0, the default namespace is <code>root/pg_interop</code>.• If you are running Command View XP Advanced Edition 5.0, the namespace is <code>root/hitachi/dm50</code>.• If you are running Command View XP Advanced Edition 5.1, the namespace is <code>root/hitachi/dm51</code>.
Emulex HBAs	<code>root/emulex</code>
HP-UX HBAs	<code>root/cimv2</code>
QLogic HBAs	<code>root/qlogic</code>
Brocade switches	<code>interop</code>
Cisco switches	<code>root/cimv2</code>
HP switches	<code>interop</code> or <code>root/cimv2</code> depending on the switch model
McData switches	<code>interop</code>

The output from `wbemdisco` lists information about the CIMOM and provider, but no storage devices are listed

Cause: Most storage device CIMOMs require additional management software. This error usually means the management software is not configured to manage any storage devices.

Possible solutions: Consult the documentation for the management software that includes the SMI-S provider. Complete the steps required to configure the software to manage the appropriate storage devices, and then run `wbemdisc` again.

- HP EVA arrays use the Command View EVA management software. In Command View EVA, click **Discover** to discover all EVAs on the SAN that are visible to the computer running Command View EVA. By default, Command View EVA will try to manage all of the discovered arrays.



NOTE: The same EVA cannot be managed by more than one copy of Command View EVA.

- HP XP arrays use Command View XP or Command View XP Advanced Edition. Run the Command View XP/XP Advanced Edition software and specify the XP arrays to manage.
- HP VA arrays use Command View SDM. Command View SDM typically discovers any VA array visible on the SAN, and begins to manage it. If this is not the case, for example, if SAN connectivity is created after the installation of the software, run the batch command `armdiscover` to discover your VA arrays.
- HP MSA arrays do not require additional management software. The standard management software is called ACU, but it is not required for the SMI CIMOM/provider to work. For MSA arrays, the provider automatically reports on any MSA visible to the host on which it is running. No configuration is needed.
- HP EMA/ESA/MA arrays with HSG80 controllers use HSG Element Manager. The software should automatically discover any HSG80-based arrays visible on the SAN. No configuration is needed.

SNMP Agent

How do I enable or disable the Restart Agents option that is available for the SNMP Agents when using the HP SIM Replicate Agent Settings Task?

Solution: The option must be changed from inside the HP SIM Replicate Agent Settings Task.

1. Select **Configure**→**Replicate Agent Settings**.
2. Select a target system, and then click **Next**. See “Creating a task” for more information about selecting the target system.



NOTE: The source system must have a trust relationship with the HP SIM Server. See “Requiring trusted certificates” for more information.

3. Select the **configure** link related to system.
4. On the **Insight Management Agent** page, under the **Restart Agents** option, select the **Enable** or **Disable** radio button.
5. Click **Apply**, and close the **SNMP Configuration** page.
6. Return to HP SIM, and then click **Refresh**. The updated configuration appears in the Replicate Agent Settings Task
7. Complete the Replicate Agent Settings Task setup by clicking **Next**, defining a task name, selecting a collection, and defining a schedule for the task. Click **Save** to complete the setup and return to the **Tasks Results** page.



NOTE: Restart the agent on the source system after finishing the Replicate Agent Settings Task to cause the changes to take effect.

Software status

The SW Status column displays Unknown. How do I determine why the status is Unknown?

Solution: There are several reasons why the **SW** Status displays Unknown. To assist in determining why a status is unknown, position the cursor over the **SW** Status column that displays Unknown. A tool tip appears and displays a hint indicating what is unknown. Any of the following can display:

- HP Version Control Repository Manager not found
Solution: Configure the VCA on the target system to point to VCRM.
- Possible VCA trust issue
Solution: Configure SMH of the target system to trust the CMS
- Software Status Polling task not run on system
Solution: From **+Options**→**Status Polling**→**Software Status Polling**, and run the task on the managed system.

If the status cannot be determined, then the tool tip displays `Click for Details`.

Storage system

Sections of a storage system's System tab are missing or say No data available.

Solution: Data has not been collected, or the data collection task was not successful. Try the following solutions:



NOTE: HP SIM displays data supplied by a storage system's *SMI-S provider*. If the SMI-S provider does not supply all of the data that HP SIM can display, the table containing that data will say `No data available`, even though data collection was successful.

- Verify that HP SIM is configured to discover and collect data from storage systems. See “Configuring HP SIM with storage systems” for more information.
- Create and run a new data collection task for the affected systems. See “Creating a data collection task” for instructions.
- Restart the SMI-S provider. See the SMI-S provider's documentation for instructions.

One or more storage systems is missing from the Storage Systems collections in HP SIM.

Solution: There might be a configuration problem with the *SMI CIMOM* or the *SMI-S provider*. Perform the following:

- Verify that HP SIM is configured to discover storage systems. See “Configuring HP SIM with storage systems” or for more information.
- Verify that your SMI-S provider is installed and configured with SSL enabled. See the *HP SIM Installation and User Guide* for more information about obtaining and installing SMI-S providers.
- Verify that the WBEM SSL port is accessible on the network. On the CMS, open a command window, and enter `telnet providerIPAddress 5989`.
 - If the port is accessible, a blank line appears, and no error such as `Connect failed` or `Connection refused` appears. Press **Control-]**, and enter `quit` to disconnect and close Telnet.
 - If the port is unreachable and the SMI-S provider is correctly installed and configured, verify that there is a firewall between the CMS and the system hosting the SMI-S provider. If there is a firewall, configure it to allow traffic through the port the provider is running on (usually 5989).
- If the CIMOM is installed and listening on a Secure Sockets Layer (SSL) port other than the default port 5989, the new port number must be specified in the `config/identification/wbemportlist.xml` file. For example:

```
<port id="5991" protocol="https">
  <interopnamespace name="root" />
  <interopnamespace name="interop" />
```

</port>

- Verify that the interop namespace for your WBM provider exists in a port element in the config/identification/wbemportlist.xml file. If it does not exist, add it to a port element as an interopnamespace element, and restart HP SIM.

When running a Data Collection task, I receive the following error on the Task Results page in the Target Details section for a storage system: The CIMOM for this device did not respond.

Possible causes

- The CIMOM was stopped.
- The system running the CIMOM is down.
- There are problems with the network between the CMS and the system running the CIMOM.
- The CIMOM was moved to a different system or port.
- The CIMOM or the underlying management software on which it depends is no longer managing this storage system.

Solution

Ensure that the CIMOM is running on the expected system and port, is managing the storage system, and is accessible to the CMS. See “Configuring HP SIM with storage systems” or “SMI-S providers” for more information.

When running a Data Collection task, I receive the following error on the Task Results page in the Target Details section for a storage system: An unexpected error was encountered in the middle of communication with the CIMOM.

Possible causes

- The CIMOM was stopped.
- The system running the CIMOM is down.
- There are problems with the network between the CMS and the system running the CIMOM.
- An unexpected error occurred within the CIMOM.

Solution

Verify that the CIMOM is running and responding to requests from the CMS.

When running a Data Collection task, I receive the following error on the Task Results page in the Target Details section for a storage system: The CIMOM for this device rejected the credentials supplied.

Possible causes

- The username and password have been changed in the CIMOM, and the new values have not been entered into HP SIM, or were entered incorrectly.
- The CIMOM is configured to require a client certificate that matches one in its keystore, and the certificate is no longer there.

Solution

- ▲ Enter the correct username and password in HP SIM. See “Configuring HP SIM with storage systems” or “SMI-S providers” for more information.

When running a Data Collection task, I receive the following error on the Task Results page in the Target Details section for a storage system: The CIMOM is no longer managing this device.

Possible causes

- The device was removed from the list of devices managed by the CIMOM from which it was originally discovered.
- The CIMOM has lost connectivity to the device, and is no longer able to report on it.

Solutions

- Ensure that the CIMOM has this device in its list of devices to manage, and that it is able to connect to the device and gather data for it.
- Choose a different CIMOM to manage the device, and then:
 1. Enter the IP address and credentials for that CIMOM in HP SIM. See “Configuring HP SIM with storage systems” for instructions.
 2. Delete the device from HP SIM and run a discovery task to discover the device through the new CIMOM.

When running a Data Collection task, I receive the following error on the Task Results page in the Target Details section for a storage system: An unexpected error was returned while writing to the database.

Possible causes

- The database and/or LUN on which it resides is full.
- Some unanticipated data from the CIMOM could not be handled by the persistence layer or the database.
- An unknown problem occurred in the persistence layer of the database.

Solution

- ▲ Make sure that the database has adequate space to insert new data.

Switch

After discovering and identifying an HP ProCurve Switch, the switch management page is not displayed when I click the HP ProCurve switch link under the System Page, Link tab.

Solution: Change the **System Link Configuration** settings for the system.

1. Select **Options**→**Security**→**System Link Configuration**. The **System Link Configuration** page appears.
2. Select **Use the system full DNS name** to use the full system DNS name instead of the system name.
3. Click **OK** to save and apply the changes.

Return to the **System Page** for the HP ProCurve Switch, and the link will now open correctly.

System

Systems displaying on the system table view page with Critical status do not display IP/IPX address and have no system link.

Solution: HP SIM has assigned this system address to another node. The following scenarios can cause this issue to occur:

- The system is temporarily removed from the network. When it returns, the system returns to a managed state. This situation can happen when a laptop computer is removed from the network for an extended period and its previous address has been reused by DHCP.
- The system could have changed names. However, this change was not discovered by HP SIM. HP SIM continues to look for a system by that name.

Re-run discovery on the sub-net to resolve the above problems.

My SNMP parameters are not saved when I add a system with a host file. I created a file that did not exist on the network. For example:

```
#$IMXE: Type="Server"  
#$IMXE: SNMP_RET=4 SNMP_TIM=10 SNMP_MON=HP SNMP_CON=HP  
1.1.1.1 myserver
```

How can I save the SNMP parameters?

Solution: This problem only exists when a system is not online yet. However, HP recommends the following workaround:

```
#$IMXE_DEFAULT: Type = Server SNMP_RET=4 SNMP_TIM=10 SNMP_MON=HP SNMP_CON=HP  
1.1.1.1 myserver
```

When the All Systems window sits idle for a few minutes and I launch a new browser window, the All Systems window turns white and Internet Explorer hangs. I am forced to end the task. How can I avoid hanging up in Internet Explorer?

Solution: For security reasons, always sign out of HP SIM before closing Internet Explorer. Signing out before closing Internet Explorer resolves this issue.

When I use the command `mxnode -r -f` to delete systems, the container systems (for example, clusters, enclosures, and racks) are not deleted.

Solution: Containers must be deleted individually.

How do I change a credential for a system that is currently using the global defaults?

Solution:

1. Run the `mxnodesecurity` command to change or add the credentials.
2. Run `mxnode` from the CLI to generate an XML file for a particular system and redirect the output to an external file:

```
mxnode -lf nodename >somefilename.xml
```

where *somefilename.xml* is the name of the external file in which the output is directed.

The following is an example of a partial `mxnode` XML file:

```
<?xml version="1.0" encoding="UTF-8"?>  
<node-list>  
<node name="abc" guid="..." host-name="abc.mycompany.com">  
<hw-attribute name="DeviceType">Workstation</hw-attribute>  
<hw-attribute name="DeviceSubType">HP9000</hw-attribute>  
<hw-attribute name="Model">9000/785</hw-attribute>  
<hw-attribute name="ProcessorFamily">pa-risc</hw-attribute>  
<sw-attribute name="OSName">HPUX</sw-attribute>  
<sw-attribute name="OSVendor">HP</sw-attribute>  
<sw-attribute name="OSRevision">11.00</sw-attribute>  
<sw-attribute name="IPAddress">192.1.2.3</sw-attribute>  
<sw-attribute name="ProtocolSupport">SNMP:1.0</sw-attribute>  
<sw-attribute name="Description">HP-UX phoenix</sw-attribute>  
<sw-attribute name="SystemName">abc.mycompany.com</sw-attribute>  
<sw-attribute name="DefaultProtoSettings">>true</sw-attribute>  
<sw-attribute name="DefaultAttributeSettings">>true</sw-attribute>  
<sw-attribute name="DefaultSystemName">>true</sw-attribute>  
</node>  
</node-list>
```

3. The last three *sw-attribute* elements represent the current *default* settings (true or false).
4. Edit the file and change all three values to false, and save the file.
5. Use the `mxnode` command to modify the same system, using the modified XML file as input:

```
mxnode -m -f somefilename.xml
```

The system should now use the new settings.

System Page

After accessing the System tab for a blade system and clicking Refresh from the browser, the timestamp in the System Status panel does not match the time shown in the Rack View.

Solution: The System Status panel automatically refreshes at a slightly different interval than the System tab and when the browser Refresh is used, it causes a difference in the timestamps.

On the System Page, when I click the Management Processor link, I receive an HTTP 1.1 dependency error and there is no status icon for the Management Processor.

Solution: The iLO and proxy server (if being used) must be configured to use HTTP 1.1.

- **To configure Internet Explorer to use HTTP 1.1:**
 1. In Internet Explorer, select **Tools**→**Internet Options**→**Advanced**.
 2. Under **HTTP 1.1 Settings**, select **Use HTTP 1.1**.
 3. Click **OK**.
- **To configure Mozilla to use HTTP 1.1:**
 1. Select **Edit**→**Preferences**→**Advanced**→**HTTP Networking**.
 2. In the **Direct Connection Options**, select **Use HTTP 1.1** and select **Enable Keep-Alive**.
 3. Click **OK**.
- **If you are communicating to an iLO through a proxy server:**
 1. In Internet Explorer, select **Tools**→**Internet Options**→**Advanced**.
 2. Under **HTTP 1.1 Settings**, select **Use HTTP 1.1 through proxy connections**.
 3. Click **OK**.

Links on the System Page that participate in HTTP communication do not get updated when an agent is stopped.

Solution: When browsing to a particular system that has a Web Agent (`http://machinename:2301`), the first link/GIF on the window (usually Insight Manager Web Agents) is the proxy agent that sends all HTTP commands. If a Web Agent is stopped that is not the proxy agent, then the appropriate HTTP command is not sent to HP SIM, allowing the link to the Web Agent to be updated. To verify that you have the correct links for a system, execute discovery or the Daily Identification Task, which verifies all Web Agents running on a particular system.

When drilling down on links on the System Page, time-outs occur.

Solution: This error often happens when the HP SIM Management server can see multiple subnets. However, the system that the user is browsing from cannot. When drilling down on some links (like Management Agents), HP SIM connects to `http://systemIPaddress:2301` with added URL information. This link connects directly to the agent running on that system. The machine that the user is browsing from must be able to speak to the system in question through TCP/IP (for example, be able to ping the system).

When drilling down on a Critical system, the System Page still displays all links that were present before HP SIM could not talk to the system.

Solution: This behavior is expected. Links remain in case the system in question is in a reboot state or some other state of flux. If the system is actually down, the links time out when connecting to any agent or web server.

System properties

After updating system properties, I cannot see the updates on the other pages in HP SIM.

Solution: Changes are not reflected instantaneously. To see changes right away, click the refresh button in your browser.

Task

The HP ProLiant Support Pack task runs for more than two hours.

Solution: The HP SUM might have hung on the target system. Therefore, on the **Task Results** page, click **Stop** to stop the task.

Go to the target system and from Task manager kill `HPSumServerW32.exe`, which is running on the target.

To kill `HPSumServerW32.exe`

1. Right click on the Windows task bar and select **Task Manager**. The **Task Manager** window appears.
2. Select the **Processes** tab.
3. Select **HPSumServerW32.exe** and click **End Process**.

When creating a task, I cannot use the Backspace key to delete text in any of the text boxes. How can I edit my entry?

Solution: When creating a task, use your mouse to select the text to be corrected, or use the Delete key to delete text from the text box. Enter the updated information.

When executing a task, the message Unknown OS appears.

Solution:

1. If the system that you are trying to execute a task against is a Windows system, verify that it was rebooted after installation of SSH. A reboot is required to complete the installation.
2. Enable DMI, WBEM, or SNMP on the system so the type of operating system can be determined, and then run identification and data collection to update the HP SIM database.
3. Verify that the commands to determine the operating system are working.

For Windows `ver`

For HP-UX and Linux `uname`

When running the Initial ProLiant Support Pack Install task, it fails.

Solution: When running the Initial ProLiant Support Pack Install task on a Windows 2000 or Windows 2003 system, be sure to enter the domain in the **Domain** field. If the system is not part of the domain, enter the target system name instead.

When running an SSH task on Windows, such as the Initial ProLiant Support Pack task, Install Open SSH or Configure or Repair Agents, I receive an error indicating I cannot connect to the remote system.

Solution: Perform the following:

1. Click **Tools**→**command line tools**→**windows**→**dir**.
2. From the `c:\` prompt on the target system, enter `dir`. If you get the partition output, then SSH is functioning correctly.
3. If SSH is not functioning correctly, see the *Secure Shell (SSH) in HP SIM 5.x* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

On an HP-UX system, when an administrative rights user edits a task, changes the owner to a operator rights user, and then views the task, the original owner is still shown as the owner. If an administrative rights user opens another browser and views the task, the correct owner appears.

Solution: This is a sporadic error with no known solution.

After executing the Install Software/Firmware task on a Windows 2000 Advanced Server system, the status does not update in the Task Results section. The status continues to report In Progress, and the Install Software/Firmware task finally times out after two hours.

Solution: The Linux VCA target system cannot resolve the address of the CMS. Ensure whether the name resolution is configured properly, and if it is not working, the Linux system that has the VCA installed must be configured to include the CMS name in the host file.

To configure the host file on the Linux system:

1. Edit the host's file in `\etc` directory.

Note: You can use a text editor or `vi` to edit this file.

Add an entry in the host file:

- `<ipaddress of server> <fully qualified DNS name of server> <name of server>`

For example, an HP SIM system with IP address `170.50.1.201`, fully qualified domain name `perf760g2.wbem.com`, and name `perf760g2` displays the following entry in the host file of the managed system on the Linux VCA system:

```
170.50.1.201 perf760g2.wbem.com perf760g2
```

2. Save the file.

All automatic event handling tasks fail with the following error on the Tasks Results page: Send failed.
class Could not connect to SMTP host: ipaddress, port
25;java.net.SocketException: Software caused connection abort:connect.

Solution: If you have antivirus software installed and it is configured to block port 25, configure the antivirus software to unblock port 25 or disable it for the automatic event handling tasks (e-mail) to run correctly.

When deploying the Software and Firmware task on HP-UX or Linux, the task might fail with an error unable to contact system. To successfully execute the task, change the System Link Configuration to use the system IP address and then execute the task.

Solution: Select **Options**→**Security**→**System Link Configuration**. The **System Link Configuration** page appears. Select **Use the system IP Address**.

Time zone

HP SIM might not correctly reflect Daylight Saving Time for Antarctica, Australia, Caicos, Haiti, Honduras, Turks, Syria, and New Zealand when Daylight Saving Time begins in the New Zealand time zone on September 30.

Solution: Download Sun Java SE TZupdater Tool 1.2.2 (or later) from http://java.sun.com/javase/tzupdater_README.html.

After the updater tool is downloaded, expand the tzupdater-1_2_2-2007g.zip file. This includes the tzupdater.jar file.

For Microsoft Windows CMS

1. sign-in to HP SIM with an administrative level account.
2. Stop HP SIM by running the `mxstop` command from the CLI.
3. Point to the HP SIM JRE: `Set JAVA_HOME=<install_dir>\j2re`.
4. Navigate to the folder where tzupdater was expanded.
5. Run the update:

```
%JAVA_HOME%\bin\java -jar tzupdater.jar -u
```
6. Start HP SIM by running the `mxstart` command from the CLI.

For HP-UX or Linux CMS

1. sign-in to HP SIM with an administrative level account.
2. Stop HP SIM by running the `mxstop` command from the CLI.
3. Point to the HP SIM JRE: `export JAVA_HOME=/opt/mx/j2re`.
4. Navigate to the folder where tzupdater was expanded.
5. Run the update:

```
:%JAVA_HOME%/bin/java -jar tzupdater.jar -u
```
6. Start HP SIM by running the `mxstart` command from the CLI.

After the updater tool runs, HP SIM properly utilizes the Daylight Saving Time change in Antarctica, Australia, Caicos, Haiti, Honduras, Turks, Syria, and New Zealand.

Tools

I am receiving the HTTP - 404 error when trying to launch a tool.

Solution: This error is received when you try to access any tool that you are not authorized to use.

An mxauthenticationexception is generated when a tool is run from the GUI or the CLI.

Solution:

1. Be sure that you have privileges to run the tool on the system. See “Users and authorizations” to verify and grant privileges.
2. Be sure that the SSH daemon is accessible on the target system.
 - a. Try to log in as an administrative user to a Windows system and as root to an HP-UX or Linux system.
 - b. From an HP-UX or Linux CMS, enter:


```
ssh root@<HP-UX/Linux node>
```

 or


```
ssh Administrator@<Windows node>
```

 From a Windows CMS:


```
<OpenSSH directory>\bin\ssh root@<HP-UX/Linux node>
```

```
<OpenSSH directory>\bin\ssh Administrator@<Windows node>
```

If you are prompted to accept a host key or enter a password, then the SSH daemon is accessible.

3. Run `mxagentconfig` again to verify that the keys are transferred:


```
mxagentconfig -a -n <node name or ipaddress> -u <user> -p <password>
```
4. On the system you are attempting to run tools on, verify the permissions of some directories. Verify the permission on the home directory of the user name you are using.
 - The home directory should have permissions: `drwxr-xr-x (755)`
 - The `.ssh` directory within the home directory should have permissions: `drwxr-xr-x (755)`
 - The `authorized_keys2` file in the `.ssh` directory should have permissions: `-rw-r--r- or -rwxr-xr-x (644 or 755)`
 - a. To verify these permissions:
 - On Windows:


```
Run <OpenSSH Install Directory>\bin\ls -ld <File or directory name>
```
 - On HP-UX or Linux:


```
Run ls -ld <File or directory name>
```
 - b. To change permissions:
 - On Windows:


```
Run <OpenSSH Install Directory>\bin\chmod <Permission number><File or directory name>
```
 - On HP-UX or Linux:


```
Run chmod <Permission number> <File or directory name>
```

 (Permission number is the number above, for example, 644/755)

Note: If the target system is a Windows system, then run the Configure and Repair Agents tool from the HP SIM GUI to verify steps 3 and 4.
5. When the command is run, the Execute-as user is listed in the status, which is the user for which you have to run `mxagentconfig`.

6. If execution has worked in the past and is now failing, verify that SSH has been reinstalled on the target system. Reinstalling SSH causes the system to have a different host key. Therefore, SSH can verify that it is the system that it is trying to contact.
 - a. Run `mxagentconfig -r -n system name`
or
Go to the GUI and remove the system host key.
 - b. Remove the lines that see the system on which to execute. Remove all references to the system (for example, `systemname` and `systemname.hp.com`)
 - c. Alternately, you can also remove the entire `known_hosts` file, which means that SSH registers the keys of every system again the next time it contacts them. This behavior could be a security problem until each system has been contacted.
7. Remove the `.ssh` directory from the home directory of the user on the managed system to ensure that there are no old keys or old permissions that could cause `mxagentconfig` to fail.
8. Run `mxagentconfig` again.

Mxagentconfig fails when trying to authorize a user on a Windows managed system that OpenSSH was not installed by HP SIM.

Solution:

1. Run:
`sshuser -u <username> -d <domain name> >> "c:\Progra~1\OpenSSH\etc\passwd"`
2. Run `mxagentconfig` again.

If `mxagentconfig` still fails, be sure SSH is running by following the steps outlined in step 1.

1. Remove the `.ssh` directory from the home directory of the user on the managed system to ensure that there are no old keys or old permissions that could cause `mxagentconfig` to fail.
2. If none of these work, then manually copy the key. Transfer the file `.dtfSshKey.pub` to the managed system. The file can be found at `/etc/opt/mx/config/sshtools/` on Windows and at `<HP SIM Install Directory>\config\sshtools` on HP-UX and Linux.
 - On Windows:
Enter `<location of .pub file> >> <user home directory>\.ssh\authorized_keys2`.
Or enter `hpsimssh` if user's home directory did not exist before running `sshuser`.
 - On HP-UX or Linux:
Enter `.cat <location of .pub file> >> ~/.ssh/authorized_keys2`.

After installing HP SIM on a Windows system, I cannot run any of the command line tools. I receiving the following error: %1 is not a valid Win32 application.

Solution: Search the root directory for a folder or file named `Program`. If this file exists, delete it. If this folder exists, rename it or delete it if the folder is empty.

When I use the `mxnodesecurity` command on an HP-UX system to add a system from a different domain, the command does not work properly. For example, if I enter `mxnodesecurity -a -p wbem -c openview\wmi:wmi -n testnode10`, the single backslash between `openview` and `wmi` is missing.

Solution: The UNIX shell environment recognizes the single backslash as an escape character. If you want to add a system from a different domain, add another backslash for it to be recognized. For example, `mxnodesecurity -a -p wbem -c openview\\wmi:wmi -n testnode10`.

When I try to run tools, they fail. This error happens with any tool selected.

Solution: This problem happens if HP SIM is installed on a system without a C drive.

When a tool opens a new window and I click the browser Refresh button, the window closes.

Solution: All windows close if they are manually refreshed using the browser Refresh button because the Refresh operation is indistinguishable from a close operation.

I am an administrative rights user on a Linux or HP-UX system. However, I am receive an exception when I try to run the `mxnodesecurity` command.

Solution: The command must be executed by the root user and the user should exist on HP SIM with authorizations to execute CLI commands.

When trying to run tools from the command line, I receive an error, stating that SSH authentication failed.

Solution 1: If you have renamed the administrator account, edit the TDEF files for each tool, and change the Execute-as user. For example:

1. Navigate to `/System Insight Manager/tools`, and open `mx-tool.xml`.
2. Change the `<execute-as-user>Administrator</execute-as-user>` to the new administrator account name.
3. Save the file.
4. At the DOS prompt, run **command:** `mxtool -m -f mx-tool.xml -x force`. The tool will now run.
5. Run the `mxagentconfig` command to push key against the target system with the changed administrator name.

You must do this for all of the command line tools.

Solution 2: If the target system is running Windows, complete the following on the CMS:

The value for the attribute `WindowsAdminUserName` in the `C:\Program Files\HP\System Insight Manager\config\globalsettings.props` file should be updated with the new administrator account name by running `mxnodesecurity -a -p ssh -c username:password -n target IP address`, where `username` is the new administrator account name and `password` is the password for the new user name.

In the above two solutions, an SSH public/private pair should be present for the new administrator account and the SSH key should be pushed from the CMS using the `mxagentconfig` command.

After creating a new command line tool and then upgrading HP SIM, there are two copies of the tool listed under Tools→Command Line Tools.

Solution: Remove one of the tools by using the `mxtool` command. See the manpage at [mxtool\(1M, 8\)](#) or [mxtool\(4\)](#).

After exporting a command line tool from a previous version of HP SIM and importing the command into HP SIM 5.1, there are two copies of the tool listed under Tools→Command Line Tools.

Solution: Remove one of the tools by using the `mxtool` command. See the manpage at [mxtool\(1M, 8\)](#) or [mxtool\(4\)](#). Or, you can edit the tool definition and remove the `guid="numerical value"` attribute, and modify the tool by using the `mxtool` command

I am unable to run SSA tools on the target system on which key is pushed before upgrade.

Solution: Run `mxagentconfig` on all target systems.

Command Line Tool created against a target system before upgrade fails to run after upgrade with error message of SSH authentication failure.

Solution: Run `mxagentconfig` on all target systems.

VCRM

After upgrading from HP SIM 4.0 to 5.1, the VCRM setting is lost.

Solution: To resolve this issue, go to **Options→VCRM** and reselect the VCRM.

I cannot find a desired software component in HP SIM in its listing of a HP Version Control Repository Manager software catalog. I know it exists in the selected VCRM, but I cannot find it in the displayed list.

Solution: It might be listed as a revision of another component with a slightly different name if the component name has changed since a previous revision. If you still cannot find the component, you might want to browse to the HP Version Control Agent on each individual system and install the component from there.

During the HP Systems Insight Manager (HP SIM) installation, the VCRM fails to install.

Solution:

Use the following method to uninstall the VCRM. Simply reinstalling the VCRM over the existing VCRM might continue to produce the error.

1. Select **Start→Control Panel**.
2. Double-click **Add or Remove Programs**. The **Add or Remove Programs** dialog box appears.

3. Scroll down and select the current **HP Version Control Repository Manager**.
4. Click **Remove** to uninstall the VCRM.

Virtual machine

JVM is shutting down.

Solution: This could happen if you have physically disconnected the Central Management Server from your network. Restart HP SIM and the problem should correct itself.

Virtual Machine Management Pack

The HP ProLiant Essentials Virtual Machine Management Pack (HP ProLiant Essentials Virtual Machine Management Pack) functions are not working in HP SIM.

Solution: Attempts to log in to the Virtual Machine Management Pack plug-in for HP SIM 4.x will not succeed if the user name contains a character that is not alphanumeric, which prevents the Virtual Machine Management Pack functions from being used within HP SIM.

WBEM Indications

When you get a FAILED to create indication subscription" message when Subscribing for WBEM Events on HP-UX .

Solution: Be sure that the requirements are met and all of the software required to support indications is installed.

On the managed system:

For HP-UX 11.11 and 11.23:

- WBEMServices A.02.00.09 at a minimum.
Note: Patch is required for both HP-UX 11.11 and 11.23 with WBEM Services A.02.00.09 for HP SIM to manage correctly.
- PHSS_34428 - 11.11 HP WBEM Services A.02.00.09
- PHSS_34429 - 11.23 HP WBEM Services A.02.00.09
- SFM provider module.
 1. Run `#cimprovider -ls`.
 2. Verify that the SFMProviderModule is listed.
 3. The following must be installed on the system:
 - SysMgmtWeb version A.2.2.2 (HP-UX Web Based System Management User Interface)
 - OpenSSL A.00.09.07e.012 or later
 - WBEMServices A.02.00.09
 - WBEM Services CORE Product OnlineDiag B.11.11.16.xx
 - EMS Version A.04.20
 - STM Version A.49.10

Note: The SFM providers are not available as part of the core operating system on an old HP-UX 11.11 installation will not work.

On HP SIM:

Confirm the target system has the correct software installed to support indication subscription and delivery.

1. Navigate to the **System Page** for the target system.
2. Select the **System** tab.

3. Expand the **Product Description** section and verify that WBEM is listed as one of the discovered management protocols.

If WBEM is not listed, confirm the target system has the correct WBEM credentials assigned to the managed system.

- a. Navigate to the **System Page** for the target system.
- b. Select the **Tools & Links** tab.
- c. Select **System Protocol Settings**.
- d. Under **WBEM Settings**, verify the correct credential has been assigned to this system. If it does not have the correct credentials, manually add them and re-identify the system.

If WBEM is discovered, check the following:

- From the CMS, run `mxwbemsub -l -n target name` . See the *HP SIM 5.2 Command Line Interface Reference Guide* at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for examples of using this command.

Additionally, you can use a CIM instance browsing tool to search for the instances created in the CIMOM that represent the subscription.

- A. Enumerate instances of `CIM_IndicationSubscription` on the managed system.
- B. View all instances of `CIM_IndicationListenerCIMXML` and look at their destination URLs to see who subscribed and where they are asking for them to be delivered.

If no subscriptions are found, subscribe to WBEM events for this managed system. If you are still not receiving indications in HP SIM from this managed system after successfully subscribing, continue with step 4. See “Subscribing to WBEM indications” for information about subscribing to WBEM indications.

4. If subscriptions are found, verify the HP SIM CMS is reachable from the target system.
 - a. From the HP SIM CMS, run `mxwbemsub -l -n target name` .
 - b. Review the output received to find the CMS host name string that is used in the **Destination** property.
 - c. Use the CMS host name (exactly as it appears) to ping (or run `nslookup`) from the managed system by running `ping Central Management Server host name used in Destination` from the command line on the managed system. If this command fails, there is a disconnect in network connectivity or name resolution between the managed system and the CMS.
 - d. If ping fails, edit the `/etc/hosts` file and add the CMS per the destination string in the subscription. Ideally, all systems should be in DNS, but this is not always the case.
 - e. After ping is successful, telnet from the managed system to `telnet CMS host name used in Destination 50004`. To exit telnet, execute `CTRL +]` and enter `quit`.

Note: If telnet fails, the following error message is displayed `Connecting To localhost...Could not open connection to the host, on port 50004: Connect failed.`

Ensure that indications are generated by the managed system

After you confirm that connectivity and name resolution are not an issue and you have confirmed that you have a valid subscription from the CMS, generate a test indication to verify that the HP-UX managed system can send indication.

HP-UX 11.11 and 11.23

1. From the HP-UX managed system, run `/etc/opt/resmon/sbin/send_test_event monitor name` . For example, `/etc/opt/resmon/sbin/send_test_event disk_em`.

Possible monitor names:

- `dm_memory`
- `lpmc_em`
- `disk_em`
- `dm_chassis`
- `dm_core_hw`

- ia64_corehw
 - fpl_em
2. Confirm that the test indication is shown in the HP SIM event table view after you trigger it.
 3. Additionally, on the HP-UX managed system, you can run `/opt/sfm/bin/evweb eventviewer -L` to verify that indications are generated and received on the local system. This command lists all of the WBEM events that have been generated on the system.



NOTE: If all of the above troubleshooting tips for WBEM indications on an HP-UX system fail, try to restart the CIMOM using the following solution and retry subscribing to the WBEM indication and following the troubleshooting tips again.

Solution: Stop the HP-UX CIMOM by running `/opt/wbem/sbin/cimserver -s`, and then restart the HP-UX CIMOM by running `/opt/wbem/sbin/cimserver`.

Windows NT event log

If you receive the error message DCOM was unable to communicate with computer<system> using any of the configured protocols, in the Windows NT Event Log, disable logging the WMI errors. These error messages are not generated by WMIMapper. Rather, they are generated by the Microsoft Windows Management Instrumentation (WMI) service when it cannot communicate with the target system to get the WMI information. Usually, the target system is a non-Windows system.

Solution: To disable logging the WMI errors to the Windows NT Event Log, perform the following procedure on the system where WMIMapper is installed.

1. In Windows NT, select **Control Panel**→**Administrative Tools**→**Services**, and stop the **Pegasus WMI Mapper** service.
2. Right-click **My Computer**.
3. Select **Manage**. The **Computer Management** page appears.
4. Expand **Services and Applications**.
5. Right-click **WMI Control**. The **WMI Control Properties** page appears.
6. Select the **Logging** tab.
7. Select **Disabled** from the **Logging level** section, and then click **OK** to close this page.
8. From the **Computer Management** window, double-click **Services**, and then select **Windows Management Instrumentation** service. Stop and restart the service.
9. Start the **Pegasus WMI Mapper** service from the **Services** page.

WMIMapper

The WBEM protocol is not listed on the System Page for the system, and the data from WBEM is not displayed.

Solution: By default, when the CMS is installed on a Windows platform, the WMIMapper service is installed at `c:\Program Files\The Open Group\WMIMapper`. The WMIMapper installation also creates a directory named `c:\hp` (lowercase) with a subfolder containing the certificates used by the system. If you previously created a directory called `c:\HP` (uppercase) the certificates are installed under that directory. When the WBEM and WMIMapper try to communicate, WMIMapper looks for a directory named `c:\hp` (lowercase) and cannot find the certificates. This same problem applies wherever the Windows platform the WMIMapper is installed. To solve this problem, delete the `c:\HP` (uppercase) directory before installing the CMS or WMIMapper on a Windows platform. Be sure to reroute any application using data in that directory to the new directory.

On a Linux or HP-UX CMS WMI mapper proxy, select **Options**→**Protocol Settings**→**WMI mapper proxy** to get WBEM data from a Windows managed system.

On a Windows CMS, WMI mapper proxy is installed with HP SIM. The mapper running on the local system is set as WMI mapper proxy as default.

I cannot access WMI information from a client system.

Solution: WMI is configured to allow remote access to accounts in the *administrators* group. If the privileges are reduced to *guest* on the remote system, no WMI connection can be obtained from the remote system. Therefore, the local security policy on the client system might be the problem. Modify the setting.

1. Select **Start**→**Control Panel**→**Administrative Tools**→**Local Security Policy**→**Local Policies**→**Security Options**, and then select **Network Access: Sharing and security model for local accounts**.
2. Select **Classic - local users authenticate as themselves**.

17 Reference information

HP Systems Insight Manager (HP SIM) uses a Microsoft SQL Server 2000 Service Pack 3, MSDE or Microsoft SQL Server 2005 Express Edition (Windows Install), or PostgreSQL SQL 7.4.x (HP-UX or Linux install) database to store collected event and system data. The *database* can be on the same system as the management application or on a different system that has network access to the database server. However, configuration of HP SIM database tables cannot be performed on a remote system. HP SIM uses the *Java DataBase Connectivity* (JDBC) and the Open DataBase Connectivity (ODBC) on Windows systems to communicate with the database.

During installation, the necessary database systems and transaction log systems are created before creating and populating the database.



CAUTION: Only the HP SIM application should add or delete from these tables. Any other modifications to these tables cause cache coherency problems for the application.

The database contains:

- Events
- Discovered systems
- System status
- User preferences
- Detailed system information
- Language text (English only)



IMPORTANT: Back up the database on a regular basis and monitor the size of the database to expand it as necessary. See *Backing up and restoring data files for HP SIM data files in a Windows environment* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> and *Backing up and restoring data files for HP SIM data files in an HP-UX and Linux environment* white paper at <http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html> for more information.

Reports can be created in Microsoft Access, Excel, Crystal Reports, or any standard reporting tool that can access the database. The database schema is published to make creating the reports easier.

Predefined views

Several predefined views are shipped with HP SIM. These views can be used to search the database for different information such as data collection information, event data and license data.

Notices_view. This view can be used to list events in the system along with their descriptions. It does not contain the specifics of an event, but it can be useful for some simple reports. It returns the system name, event severity, cleared status, received time, cleared time and event description.

View_deviceAssociations. This view is used in building searches, mainly used internally.

licenseCounts. This view is used to show license count data in the license report.

deviceTypesEnum. This view links the devices_table productType field with an (English) string representing the system type.

deviceSubTypesEnum. This view links the nodeSubTypesEnum table enumOrd field with an (English) string representing the system subtype.



NOTE: The database and views are not deleted when you uninstall HP SIM.

See "Reporting views" to see the available Reporting Views.

Database tables

The following sections provide the contents of the database. The tables describe the information collected by HP SIM and the database table structures that store the information. The following tables are available:

AuthenticationMethods_values table	CIM_ActiveConnection table	CIM_Chassis table
CIM_ComponentCS table	CIM_ComputerSystemPackage table	CIM_ComputerSystem table
CIM_ControlledBy table	CIM_DeviceSAPImplementation table	CIM_DeviceSoftwareIdentity table
CIM_ElementCapabilities table	CIM_HostedStoragePool table	CIM_Fan table
CIM_IPProtocolEndpoint table	CIM_IPRoute table	CIM_iSCSICapabilities table
CIM_iSCSIConn_TCPProtoEnd table	CIM_iSCSIConnection table	CIM_iSCSISession table
CIM_LogicalDevice table	CIM_LogicalDisk table	CIM_LogicalPortGroup table
CIM_MediaAccessDevice table	CIM_MemberOfCollection table	CIM_NetworkPipeComposition table
CIM_NetworkPort table	CIM_NetworkAdapter table	CIM_OperatingSystem table
CIM_PhysicalElement table	CIM_PhysicalMedia table	CIM_PhysicalMemory table
CIM_PhysicalPackage table	CIM_PortController table	CIM_PowerSupply table
CIM_Process table	CIM_Processor table	CIM_Product table
CIM_ProtoControlAccessesUnit table	CIM_ProtocolControllerForPort table	CIM_ProtocolControllerForUnit table
CIM_ProtocolEndpoint table	CIM_Rack table	CIM_Realizes table
CIM_RemoteServiceAccessPoint table	CIM_SCSIProtocolController table	CIM_SCSIProtocolEndpoint table
CIM_Sensor table	CIM_SoftwareElement table	CIM_SoftwareIdentity table
CIM_StoragePool table	CIM_StorageVolume table	CIM_TCPProtocolEndpoint table
Classifications_values table	ComputerSys_HAP table	ComputerSys_LogicalPortGroup table
ComputerSys_NetworkPort table	ComputerSys_PortController table	ComputerSys_SAP table
ComputerSys_SCSIProtoCont table	ComputerSys_SCSIProtoEndp table	ComputerSys_SoftwareIdent table
ComputerSys_StorageVol table	DB_DeviceInfo table	DB_DeviceInfoEx table
DC_Enclosure table	DC_ProliantHost table	Dedicated_values table
DeviceNames table	Device Extended Attributes database table	Devices table
DeviceProtocolInfo table	ExtentStatus_values table	DeviceSnmSettings table
HP_Cluster table	HP_Node table	HP_NParCabinet table
HP_NParCell table	HP_NParIOChassis table	HP_NParIOChassisSlot table
HP_NparPartition table	HP_NParComplex table	HPUX_BaseKernelParameter table
HPUX_Bundle table	HPUX_DNSService table	HPUX_Fileset table
HPUX_HFS table	HPUX_LogicalVolume table	HPUX_NISServerService table
HPUX_NTSPService table	HPUX_PhysicalVolume table	HPUX_Product table
HPUX_VolumeGroup table	HPVM_Guest table	HPVM_Host table
IPAddress table	IPProtocolEnd_NetworkPort table	IPXAddress table
NetworkAddresses_values table	NodeSnapshot table	NodeTypesEnum table
NodeSubTypesEnum table	Notices table	NoticeType table
OperationalStatus_CSvalues table	OperationalStatus_NPvalues table	operationalStatus_PCvalues table
OperationalStatus_SVvalues table	PhysicalPackage_Product table	SCSIProtoCont_SCSIProtoEnd table
SCSIProtocolCont_SoftwareId table	SCSIProtoEnd_SCSIProtoEnd table	SCSIProtoEnd_iSCSISession table
SCSIProtoEnd_NetworkPort table	Snapshot table	SPAllocatedFromStoragePool table
SVAllocatedFromStoragePool table	TCPProtoEnd_IPProtoEnd table	

AuthenticationMethods_values table

Column Name	Data Type	Description
AuthenticationMethodsId	BIGINT	Uniquely defines this row
AuthenticationMethodsValue	SMALLINT	Used for reporting purposes
AuthenticationMethodsPos	SMALLINT	Used for reporting purposes

CIM_ActiveConnection table

Column Name	Data Type	Description
Antecedent	BIGINT	A ServiceAccessPoint that is configured to communicate and/or is actively communicating with the Dependent SAP. In a unidirectional connection, this is the SAP that is transmitting.
Dependent	BIGINT	A second ServiceAccessPoint that can communicate with the Antecedent SAP. In a unidirectional connection, this is the SAP that is receiving the communication.

CIM_Chassis table

Column Name	Data Type	Description
Chassis_LUID	BIGINT	LUID uniquely defines this row
ModelID	BIGINT	Partly identifies CIM_Chassis
SnapshotID	BIGINT	Partly identifies CIM_Chassis
CreationClassName	NVARCHAR(256)	Partly identifies CIM_Chassis and equates to CIM_Chassis
Tag	NVARCHAR(256)	An arbitrary string that uniquely identifies the Physical Element, serves as the Element key and can contain information such as asset tag or serial number data
dc_ProductID	NVARCHAR(64)	The product ID string of the enclosure and is empty if the enclosure does not report the productID string
dc_SystemCreationClassName	NVARCHAR(256)	If the chassis is part of a rack, then this attribute is CIM_Rack; otherwise, it is CIM_ComputerSystem
dc_SystemName	NVARCHAR(256)	If the chassis is part of a rack, then this attribute is the value of CIM_Rack.Name; otherwise, it is the value of the owning CIM_ComputerSystem.Name
Name	NVARCHAR(256)	A label by which the object is known
ElementName	NVARCHAR(256)	A user-friendly name for the object
Width	real	Inherited from CIM_PhysicalPackage.Width and is the width of the Physical Package in inches
Height	real	Inherited from CIM_PhysicalPackage.Height and is the height of the Physical Package in inches
Depth	real	Inherited from CIM_PhysicalPackage.Depth and is the depth of the Physical Package in inches
SerialNumber	NVARCHAR(64)	Inherited from CIM_PhysicalElement.SerialNumber and is a manufacturer-allocated number used to identify the Physical Element
PartNumber	NVARCHAR(256)	Inherited from CIM_PhysicalElement.PartNumber and is the part number assigned by the organization responsible for producing or manufacturing the Physical Element
SKU	NVARCHAR(64)	Inherited from CIM_PhysicalElement.SKU and is the stock keeping unit number for this Physical Element
Model	NVARCHAR(64)	Inherited from CIM_PhysicalElement.Model and is the name by which the Physical Element is generally known
Manufacturer	NVARCHAR(256)	Name of the manufacturer of the component
ChassisTypes	SMALLINT	An enumeration of CIM_ChassisTypes. (1 = Other, 2 = Unknown, 3 = Desktop, 4 = Low Profile Desktop, 5 = Pizza Box, 6 = Mini Tower, 7 = Tower, 8 = Portable, 9 = Laptop, 10 = Notebook, 11 = Hand Held, 12 = Docking Station, 13 = All in One, 14 = Sub Notebook, 15 = Space Saving, 16 = Lunch Box, 17 = Main System Chassis, 18 = Expansion Chassis, 19 = SubChassis, 20 = Bus Expansion Chassis, 21 = Peripheral Chassis, 22 = Storage Chassis, 23 = Rack Mount Chassis, 24 = Sealed-Case PC)

Column Name	Data Type	Description
TypeDescriptions	NVARCHAR(512)	Additional information about the CIM_Chassis.ChassisTypes
Version	NVARCHAR(64)	Inherited from CIM_PhysicalElement.Version and is a string indicating the version of the Physical Element
OtherIdentifyingInfo	NVARCHAR(512)	Inherited from CIM_PhysicalElement.OtherIdentifyingInfo. Captures additional data, beyond that of Tag information, that could be used to identify a Physical Element (One example is bar code data associated with an Element that also has an asset tag. If only bar code data is available and is uniqueable to be used as an Element key, this property would be NULL and the bar code data used as the class key, in the Tag property)
R_Model	NVARCHAR(256)	A field used by reporting

CIM_ComponentCS table

Column Name	Data Type	Description
GroupComponent	BIGINT	The ComputerSystem that contains and/or aggregates other systems
PartComponent	BIGINT	The contained (Sub)ComputerSystem

CIM_ComputerSystemPackage table

Column Name	Data Type	Description
Antecedent	BIGINT	A field used by reporting
Dependent	BIGINT	A field used by reporting

CIM_ComputerSystem table

Column Name	Data Type	Description
ComputerSystem_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_ComputerSystem
SnapshotID	BIGINT	Partly identifies CIM_ComputerSystem
Name	NVARCHAR(256)	The inherited Name serves as key of a System instance in an enterprise environment
CreationClassName	NVARCHAR(256)	CreationClassName indicates the name of the class or the subclass used in the creation of an instance (When used with the other key properties of this class, this property allows all instances of this class and its subclasses to be uniquely identified.)
Description	NVARCHAR(512)	The Description property provides a textual description of the object
Caption	NVARCHAR(64)	The Caption property is a short textual description (one-line string) of the object
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status and is a string indicating the current status of the object
PrimaryOwnerContact	NVARCHAR(256)	A string that provides information on how the primary system owner can be reached
PrimaryOwnerName	NVARCHAR(64)	The name of the primary system owner
dc_PrimaryOwnerPager	NVARCHAR(32)	Not standard, based on CIM_Person.Pager and includes pager information for the primary owner
dc_SystemLocation	NVARCHAR(256)	Not standard and includes information describing the physical location of this system

Column Name	Data Type	Description
dc_HardwareCapability	NVARCHAR(64)	Not standard and is the hardware capability (32 and 64 bits) of the system
R_OverallStatus	NVARCHAR(50)	A field used by reporting
R_ProductType	NVARCHAR(256)	A field used by reporting
Domain	NVARCHAR(256)	Domain of this system
Elementname	NVARCHAR(256)	A user friendly name for this element
NameFormat	NVARCHAR(64)	Defines how the Name is generated
ReleaseDate	NVARCHAR(256)	For Non-Stop systems, date of system release
R_OperationalStatus	NVARCHAR(256)	A field used by Reporting
R_PortCount	INT	A field used by Reporting
R_PortUtilized	INT	A field used by Reporting

CIM_ControlledBy table

Column Name	Data Type	Description
Dependent	BIGINT	The controlled Device
Antecedent	BIGINT	The controller

CIM_DeviceSAPImplementation table

Column Name	Data Type	Description
deviceSAPImplementation_LUID	BIGINT	Used for reporting purposes
NodeID	BIGINT	Partly identifies CIM_DeviceSAPImplementation
SnapshotID	BIGINT	Partly identifies CIM_DeviceSAPImplementation
Dependent	BIGINT	The ServiceAccessPoint implemented using the LogicalDevice
Antecedent	BIGINT	The LogicalDevice
dc_PermanentAddress	NVARCHAR(256)	Used for reporting purposes

CIM_DeviceSoftwareIdentity table

Column Name	Data Type	Description
System	BIGINT	Used for reporting purposes
InstalledSoftware	BIGINT	Used for reporting purposes

CIM_ElementCapabilities table

Column Name	Data Type	Description
Dependent	BIGINT	The managed element
Antecedent	BIGINT	The Capabilities object associated with the element

CIM_Fan table

Column Name	Data Type	Description
Fan_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_Fan

Column Name	Data Type	Description
SnapshotID	BIGINT	Partly identifies CIM_Fan
Description	NVCHAR(255)	Provides a textual description of the object
SystemCreationClassName	NVCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVCHAR(256)	The value of CIM_ComputerSystem Name with equal NodeID
CreationClassName	NVCHAR(256)	Equates to CIM_Fan
DeviceID	NVCHAR(256)	An address or other identifying information to uniquely name the LogicalDevice
ActiveCooling	BIT	ActiveCooling is a boolean indicating that the Cooling Device provides active (as opposed to passive) cooling
FanType	SMALLINT	An enumeration describing the cooling device type (0 = Unknown , 1 = Other , 2 = Cabinet Blower , 3 = Compute Cabinet I/O Fans , 4 = I/O Expansion Cabinet Utility Chassis Fan , 5 = I/O Expansion Cabinet I/O Fan , 6 = Processor Fan)
Location	NVCHAR(255)	Physical location of a cooling device.
Manufacturer	NVCHAR(255)	Currently a placeholder. When implemented, this will reflect the manufacturer of the fan.
PhysicalPosition	NVCHAR(255)	Position is a free-form string indicating the placement of a PhysicalElement. It can specify slot information on a HostingBoard, mounting site in a Cabinet, or latitude and longitude information, for example, from a GPS. It is part of the key of the Location object.
Tag	NVCHAR(255)	Partly identifies CIM_Fan
SerialNumber	NVCHAR(255)	Currently a placeholder. When implemented will reflect the serial number of the fan.
Version	NVCHAR(255)	Currently a placeholder. When implemented will reflect the version number of the fan.
Name	NVCHAR(255)	A label by which the object is known
R_PhysicalPosition	Smallint	New column added to hold fan physical position

CIM_HostedStoragePool table

Column Name	Data Type	Description
GroupComponent	BIGINT	The parent system in the Association
PartComponent	BIGINT	The StoragePool that is a component of a system

CIM_IPProtocolEndpoint table

Column Name	Data Type	Description
IPProtocolEndpoint _LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_IPProtocolEndpoint
SnapshotID	BIGINT	Partly identifies CIM_IPProtocolEndpoint
Name	NVARCHAR(1024)	A label by which the object is known
ServiceCreationClassName	NVARCHAR(256)	For future use
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
IPv4Address	NVARCHAR(255)	The IPv4 address that this ProtocolEndpoint represents

CIM_IPRoute table

Column Name	Data Type	Description
IPRoute_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_IPRoute
SnapshotID	BIGINT	Partly identifies CIM_IPRoute
CreationClassName	NVARCHAR(256)	Equates to CIM_IPRoute
ServiceCreationClassName	NVARCHAR(256)	For future use
ServiceName	NVARCHAR(256)	For future use
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
IPDestinationAddress	NVARCHAR(256)	
IPDestinationMask	NVARCHAR(256)	The IP address that serves as the destination of the traffic, formatted according to the appropriate convention as defined in the AddressType property of this class (This property has the same semantics as DestinationAddress inherited from the NextHopRouting superclass but uses a different property name because this property and class were defined before NextHopRouting and are Key properties. They cannot be removed. ModelCorrespondence indicates that they should be set to equivalent values for consistency and ease of searching.)
AddressType	SMALLINT	An enumeration that describes the format of the address property (Addresses that can be formatted in IPv4 format must be formatted that way to ensure mixed IPv4/IPv6 support. AddressType is part of the key so that an IPv4 and an IPv6 route to IP subnets with the same network number but different versions (v4/v6) can coexist. (0, Unknown; 2, IPv4; 2 IPv6))
IsStatic	bit	True indicates that this is a static route and False indicates a dynamically-learned route
NextHop	NVARCHAR(256)	Contains the address of the next-hop router or the interface used to reach the destination
	NVARCHAR(32)	Not standard and is the gateway to the route destination (Unknown, Local, Remote)
dc_RouteArgument	NVARCHAR(1024)	Not standard and is the argument list for the /usr/sbin/route command

CIM_iSCSICapabilities table

Column Name	Data Type	Description
iSCSICapabilities_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Used to partially identify CIM_iSCSICapabilities
SnapshotID	BIGINT	Used to partially identify CIM_iSCSICapabilities
Elementname	NVARCHAR(255)	Used for reporting purposes
InstanceID	NVARCHAR(255)	Used for reporting purposes
MinimumSpecificationVersionS	BIT	Used for reporting purposes
MaximumSpecificationVersionS	BIT	Used for reporting purposes

CIM_iSCSIConn_TCPProtoEnd table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_iSCSIConnection table

Column Name	Data Type	Description
ISCSIConnection_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_iSCSIConnection
SnapshotID	BIGINT	Partly identifies CIM_iSCSISession
ElementName	NVARCHAR(255)	Used for reporting purposes
InstanceID	NVARCHAR(255)	Used for reporting purposes
ConnectionID	INT	Used for reporting purposes
HeaderDigestMethod	SMALLINT	Used for reporting purposes
OtherheaderDigestMethod	NVARCHAR(255)	Used for reporting purposes
DataDigestMethod	SMALLINT	Used for reporting purposes
OtherDataDigestMethod	NVARCHAR	Used for reporting purposes
ActiveiSCSIVersion	BIT	Used for reporting purposes

CIM_iSCSISession table

Column Name	Data Type	Description
ISCSISession_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_iSCSISession
SnapshotID	BIGINT	Partly identifies CIM_iSCSISession
InstanceID	NVARCHAR(255)	Used for reporting purposes
SessionType	SMALLINT	Used for reporting purposes
TSIH	INT	Used for reporting purposes
EndPointName	NVARCHAR(255)	Used for reporting purposes
CurrentConnections	INT	Used for reporting purposes
ErrorRecoveryLevel	INT	

SCSIProtoEnd_iSCSISession table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

SCSIProtoEnd_NetworkPort table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_LogicalDevice table

Column Name	Data Type	Description
LogicalDevice_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_LogicalDevice
SnapshotID	BIGINT	Partly identifies CIM_LogicalDevice
DeviceID	NVARCHAR(64)	An address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_LogicalDevice and equates to CIM_LogicalDevice
ServiceCreationClassName	NVARCHAR(256)	SystemCreationClassName partly identifies CIM_LogicalDevice and equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	SystemName partly identifies CIM_LogicalDevice and is the value of CIM_ComputerSystem.Name with equal NodeID
Name	NVARCHAR(256)	A label by which the object is known
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption and is a short textual description (one line string) of the object
Description	NVARCHAR(512)	A textual description of the object
Availability	SMALLINT	The primary availability and status of the system and is an enumeration. (1 = Other, 2 = Unknown, 3 = Running/Full Power, 4 = Warning, 5 = In Test, 6 = Not Applicable, 7 = Power Off, 8 = Off Line, 9 = Off Duty, 10 = Degraded, 11 = Not Installed, 12 = Install Error, 13 = Power Save, Unknown, 14 = Power Save, Low Power Mode, 15 = Power Save, Standby, 16 = Power Cycle, 17 = Power Save, Warning, 18 = Paused, 19 = Not Ready, 20 = Not Configured, 21 = Quiesced)
LastErrorCode	INT	Captures the last error code reported by the Logical Device
dc_HardwareType	NVARCHAR(64)	Not standard and is the hardware type for this system
OtherIdentifyingInfo	NVARCHAR(256)	Captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice. One example would be to hold the Operating System user friendly name for the Device in this property.
dc_AssociatedDriver	NVARCHAR(64)	Not standard and the associated driver for this system
HardwarePath	NVARCHAR(64)	A numerical string of hardware components, notated sequentially from the bus address to the device address. For example, 0/2/0/0 .

CIM_LogicalDisk table

Column Name	Data Type	Description
LogicalDisk_LUID	BIGINT	LUID uniquely defining this table row
NodeID	INT	Partly identifies CIM_LogicalDisk
Snapshot	INT	Partly identifies CIM_LogicalDisk
DeviceID	NVARCHAR(256)	Inherited from CIM_LogicalDevice.DeviceID and is an address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	Equates to CIM_LogicalDisk
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
Win32_FreeSpace	BIGINT	Derived from Win32_LogicalDisk and is the total amount of free space in bytes

Column Name	Data Type	Description
Win32_Size	BIGINT	Derived from Win32_LogicalDisk and is the total size in bytes; if unknown, enter 0. Units (bytes)
Description	NVARCHAR(512)	A textual description of the object
R_SizeMB	NVARCHAR(256)	A field used by reporting
R_UsedMB	NVARCHAR(256)	A field used by reporting
R_UsedPercent	NVARCHAR(256)	A field used by reporting
dc_SpaceUsed	BIGINT	Not standard and is the file system space currently in use in bytes
dc_PercentSpaceUsed	INT	Not standard and is the percent of file system space currently in use
BlockSize	BIGINT	Size in bytes of a block on the logical disk.
NumberOfBlocks	BIGINT	Number of storage block in the logical disk; size in bytes can be calculated from BlockSize * NumberOfBlocks.

CIM_LogicalPortGroup table

Column Name	Data Type	Description
LogicalPortGroup_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_LogicalPortGroup
Snapshot	BIGINT	Partly identifies CIM_LogicalPortGroup
InstanceID	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(256)	A label by which the object is known
NameFormat	NVARCHAR(64)	Used for reporting purposes
ElementName	NVARCHAR(255)	Used for reporting purposes

CIM_MediaAccessDevice table

Column Name	Data Type	Description
MediaAccessDevice_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_MediaAccessDevice
SnapshotID	BIGINT	Partly identifies CIM_MediaAccessDevice
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID and is an address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	Equates to CIM_MediaAccessDevice
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name for this NodeID
Name	NVARCHAR(256)	A label by which the object is known
Description	NVARCHAR(512)	A textual description of the object
MaxMediaSize	BIGINT	Maximum size, in KB, of media supported by this system. (KB is interpreted as the number of bytes X 1000 not bytes X 1024)
UnitsUsed	BIGINT	An unsigned integer indicating the currently used units of the AccessDevice, helpful to describe when the system might require cleaning (The property UnitsDescription, defines how units should be interpreted)
DefaultBlockSize	BIGINT	Default block size, in bytes

Column Name	Data Type	Description
OtherIdentifyingInfo	NVARCHAR(256)	Inherited from CIM_LogicalDevice.OtherIdentifyingInfo (Captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice. One example would be to hold the Operating System user-friendly name for the Device in this property.)
TotalPowerOnHours	BIGINT	Inherited from CIM_LogicalDevice.TotalPowerOnHours and is the total number of hours that this Device has been powered
UnitsDescription	NVARCHAR(256)	Defines units relative to its use in the property, MaxUnitsBeforeCleaning; describes the criteria used to determine when the MediaAccessDevice should be cleaned
NeedsCleaning	BIT	Indicates the MediaAccessDevice needs cleaning
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status; a string indicating the current status of the object
MAStatInf_UnrecoverableWriteOp	INT	Corresponds to MediaAccessStatInfo_UnrecoverableWriteOperations. CIM_MediaAccessStatInfo.UnrecoverableWriteOperations; the number of unrecoverable write operations
MAStatInf_UnrecoverableReadOp	INT	Corresponds to MediaAccessStatInfo_UnrecoverableReadOperations. CIM_MediaAccessStatInfo.UnrecoverableReadOperations; the number of unrecoverable read operations
dc_RaidLevel	NVARCHAR(64)	Holds the fault-tolerant RAID setting for a logical drive on a RAID controller (Possible statuses include Not enabled, RAID Level 0, RAID Level 1, RAID Level 0 + 1, Mirroring, Data Guard, Distributed Data Guard (RAID 5), Advanced Data Guarding, RAID Level 4, RAID Level 5)
dc_Type	NVARCHAR(64)	Not standard; a string describing the type of media used to access the system
dc_TransferMode	NVARCHAR(64)	Not standard. Compaq ATA Disk Transfer Mode (othe, pioMode0, pioMode1, pioMode2, pioMode3, pioMode4, dmaMode0, dmaMode1, dmaMode2, ultraDmaMode0, ultraDmaMode1, ultraDmaMode2, ultraDmaMode3, ultraDmaMode4, ultraDmaMode5)
R_DrivePort	NVARCHAR(256)	A field used by reporting
R_Type	NVARCHAR(64)	A field used by reporting

CIM_NetworkAdapter table

Column Name	Data Type	Description
NetworkAdapter_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_NetworkAdapter
SnapshotID	BIGINT	Partly identifies CIM_NetworkAdapter
CreationClassName	NVARCHAR(256)	Equates to CIM_NetworkAdapter
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID; (an address or other identifying information to uniquely name the Logical Device)
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name for this NodeID
Name	NVARCHAR(256)	A label by which the object is known
NetworkAddress	NVARCHAR(64)	An array of strings indicating the network addresses for an adapte; represented by a comma separated list

Column Name	Data Type	Description
StatusInfo	SMALLINT	Inherited from CIM_LogicalDevice.StatusInfo (The StatusInfo property indicates whether the Logical Device is in an enabled (value = 3), disabled (value = 4), other (value = 1), or unknown (value = 2) state. If this property does not apply to the LogicalDevice, the value 5 (Not Applicable), should be used. If a Device is Enabled (value=3), it has been powered up and is configured and operational. The system might not be functionally active, depending on whether its Availability (or AdditionalAvailability) indicates that it is Running/Full Power (value=3) or Off line (value=8). In an enabled but offline mode, a system might be performing out-of-band requests, such as running Diagnostics. If (\\"Disabled\\") StatusInfo value=4), a device can only be \\"enabled\\" or powered off. In a personal computer environment, (\\"Disabled\\") means that the system's driver is not viable in the stack. In other environments, a system can be disabled by removing its configuration file. A disabled device is physically present in a system and consuming resources but cannot be communicated with until a load of a driver, a load of a configuration file, or some other \\"enabling\\" activity has occurred. CIM_LogicalDevice.StatusInfo Enumeration. (1 = Other, 2 = Unknown, 3 = Enabled, 4 = Disabled, 5 = Not Applicable)
PermanentAddress	NVARCHAR(64)	PermanentAddress defines the network address hardcoded into an adapter (This hardcoded address can be changed through firmware upgrade or software configuration. If so, this field should be updated when the change is made. PermanentAddress should be left blank if no hardcoded address exists for the NetworkAdapter.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description (one line string) of the object
EthernetAdp_InternalMACRcvErr	INT	A count of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error (A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the FrameTooLong property, the AlignmentErrors property, or the FCSErrors property. The precise meaning of the count represented by and instance of this object is implementation-specific. In particular, an instance of this object can represent a count of receive errors on a particular interface that are not otherwise counted.)
EthernetAdp_InternalMACTranErr	INT	A count of frames for which reception on a particular interface fails because of an internal MAC sublayer receive error (A frame is only counted by an instance of this object if it is not counted by the corresponding instance of the LateCollisions property, the Excessive Collisions property, or the CarrierSenseErrors property. The precise meaning of the count represented by and instance of this object is implementation-specific. In particular, an instance of this object can represent a count of transmission errors on a particular interface that are not otherwise counted.)
FullDuplex	BIT	Boolean indicating that the adapter is operating in full duplex mode
OctetsTransmitted	BIGINT	The total number of octets transmitted, including framing characters
OctetsReceived	BIGINT	The total number of octets received, including framing characters
MaxSpeed	BIGINT	The maximum speed, in bits per second, for the Network Adapter
IPProtocolEndpoint_SubnetMask	NVARCHAR(64)	Derived from CIM_IPProtocolEndpoint.SubnetMask; the mask for the IP address of this ProtocolEndpoint, formatted according to the appropriate convention as defined in the AddressType property of this class
dc_AdminStatus	NVARCHAR(32)	Holds the administrative status of the adapter (For example, Up, Down, Testing, Dormant, Some component missing)

Column Name	Data Type	Description
dc_BroadcastAddress	NVARCHAR(64)	Not standard. This attribute is the broadcast address assigned to this interface in dot notation format.
dc_DHCPEnabled	NVARCHAR(32)	Not standard; this attribute indicates whether DHCP enabled or not
dc_OperStatus	NVARCHAR(32)	Holds the operational status for the adapter (For example, Up, Down, Testing)
R_InputErrors	NVARCHAR(256)	A field used by reporting
R_OutputErrors	NVARCHAR(256)	A field used by reporting
R_Duplex	NVARCHAR(25)	A field used by reporting
R_MacAddress	NVARCHAR(64)	A field used by reporting
LANEndpoint_ProtocolType	SMALLINT	Integer indicating protocol active on port: ValueMap { "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15", "16", "17", "18", "19", "20", "21", "22", "23", "24", "25", "26", "27" }, Values {"Unknown", "Other", "IPv4", "IPv6", "IPX", "AppleTalk", "DECnet", "SNA", "CONP", "CLNP", "VINES", "XNS", "ATM", "Frame Relay", "Ethernet", "TokenRing", "FDDI", "Infiniband", "Fibre Channel", "ISDN BRI Endpoint", "ISDN B Channel Endpoint", "ISDN D Channel Endpoint", "IPv4/v6", "BGP", "OSPF", "MPLS", "UDP", "TCP" }
LANEndpoint_OperationalStatus	nvarchar(255)	Operational status values for this port
EthernetPort_PortType	SMALLINT	Integer code for port type if Ethernet: ValueMap {"0", "1", "50", "51", "52", "53", "16000..65535"}, Values {"Unknown", "Other", "10BaseT", "10-100BaseT", "100BaseT", "1000BaseT", "Vendor Reserved" }
EthernetPort_MaxDataSize	INT	Max data size of Ethernet packets

CIM_MemberOfCollection table

Column Name	Data Type	Description
Collection	BIGINT	Used for reporting purposes
Member	BIGINT	Used for reporting purposes

CIM_NetworkPipeComposition table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_NetworkPort table

Column Name	Data Type	Description
NetworkPort_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_NetworkPort
SnapshotID	BIGINT	Partly identifies CIM_NetworkPort
ElementName	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes

Column Name	Data Type	Description
DeviceID	BIGINT	Used for reporting purposes
Speed	BIGINT	Used for reporting purposes
MaxSpeed	BIGINT	Used for reporting purposes
UsageRestriction	SmallInt	Used for reporting purposes
PortType	SMALLINT	Used for reporting purposes
OtherPortType	NVARCHAR(255)	Used for reporting purposes
LinkTechnology	SMALLINT	Used for reporting purposes
OtherLinkTechnology	NVARCHAR(255)	Used for reporting purposes
PermanentAddress	NVARCHAR(64)	Used for reporting purposes
PortNumber	SMALLINT	Used for reporting purposes
R_OperationalStatus	NVARCHAR(256)	Used for reporting purposes
R_ParentName	NVARCHAR(256)	Used for reporting purposes
R_PortType	NVARCHAR(256)	Used for reporting purposes

CIM_OperatingSystem table

Column Name	Data Type	Description
OperatingSystem_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies CIM_OperatingSystem
SnapshotID	BIGINT	Partly identifies CIM_OperatingSystem
CSCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem.
CSName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name for this NodeID
CreationClassName	NVARCHAR(256)	Equates to CIM_OperatingSystem.
Name	NVARCHAR(256)	The inherited Name serves as key of an operating system instance within a computer system
LastBootupTime	BIGINT	Time when the OperatingSystem was last booted
LocalDateTime	BIGINT	OperatingSystem notion of the local date and time of day
Version	NVARCHAR(64)	A string describing the OperatingSystem version number (The format of the version information is as follows: <Major Number>.<Minor Number>.<Revision> or <Major Number>.<Minor Number>.<Revision Letter>)
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object

Column Name	Data Type	Description
OSType	SMALLINT	An integer indicating the type of Operating System (CIM_OSType enumeration. (0 = Unknown, 1 = Other, 2 = MACOS, 3 = ATTUNIX, 4 = DGUX, 5 = DECNT, 6 = Digital Unix, 7 = OpenVMS, 8 = HPUX, 9 = AIX, 10 = MVS, 11 = OS400, 12 = OS/2; 13 = JavaVM, 14 = MSDOS, 15 = WIN3x, 16 = WIN95, 17 = WIN98, 18 = WINNT, 19 = WINCE, 20 = NCR3000, 21 = NetWare, 22 = OSF, 23 = DC/OS, 24 = Reliant UNIX, 25 = SCO UnixWare, 26 = SCO OpenServer, 27 = Sequent, 28 = IRIX, 29 = Solaris, 30 = SunOS, 31 = U6000, 32 = ASERIES, 33 = TandemNSK, 34 = TandemNT, 35 = BS2000, 36 = LINUX, 37 = Lynx, 38 = XENIX, 39 = VM/ESA, 40 = Interactive UNIX, 41 = BSDUNIX, 42 = FreeBSD, 43 = NetBSD, 44 = GNU Hurd, 45 = OS9, 46 = MACH Kernel, 47 = Inferno, 48 = QNX, 49 = EPOC, 50 = lxWorks, 51 = VxWorks, 52 = MiNT, 53 = BeOS, 54 = HP MPE, 55 = NextStep, 56 = PalmPilot, 57 = Rhapsody, 58 = Windows 2000, 59 = Dedicated, 60 = OS/390, 61 = VSE, 62 = TPF, 63 = Windows (R) Me, 64 = Caldera Open UNIX, 65 = OpendBSD, 66 = Not Applicable)
NumberOfUsers	INT	Number of user sessions for which the operating system is currently storing state information
NumberOfProcesses	INT	Number of process contexts currently loaded or running on the operating system
MaxNumberOfProcesses	INT	Max number of process contexts the operating system can support; if no fixed value, then 0
CurrentTimeZone	SMALLINT	Indicates the number of minutes the operating system is offset from GMT; the number is +, -, or 0
TotalVisibleMemorySize	BIGINT	Amount of physical memory in KB available to operating system; not necessarily true amount of physical memory but what is reported to the operating system as available
TotalSwapSpaceSize	BIGINT	Total swap space in Kb; can be null if swap space is not distinguished from page files
OtherTypeDescription	NVARCHAR(64)	A string describing the manufacturer and operating system type; used when the OperatingSystem property, OSType, is set to 1 or 59 (Other or Dedicated) (The format of the string inserted in OtherTypeDescription should be similar in format to the Values strings defined for OSType. OtherTypeDescription should be set to null when OSType is any value other than 1 or 59.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description (one line string) of the object
dc_OperatingSystemCapability	NVARCHAR(64)	Not Standard; the capability (32 and 64 bits) of this operating system
dc_OSType	NVARCHAR(256)	Not standard; a string describing the operating system type (This can involve interpretation and not strictly reflect the value of OSType.)
dc_PrimaryOS	bit	Not standard; derived from CIM_InstalledOSBoolean indicating that the OS is the default for the Computer System
Win32_CSDVersion	NVARCHAR(256)	Not standard; CSD version/Service Pack level of OS from Windows systems
dc_SwapSpaceName	NVARCHAR(256)	Not standard. Name identifying the swap space.
dc_SwapType	NVARCHAR(64)	Not standard; type description of swap space
dc_SwapSpaceMinimumSize	BIGINT	Not standard. Minimum size of swap space
dc_SwapSpaceMaximumSize	BIGINT	Not standard; maximum size of swap space
dc_SwapSpaceReservedSize	BIGINT	Not standard; reserved size of swap space

CIM_PhysicalElement table

Column Name	Data Type	Description
PhysicalElement_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PhysicalElement
SnapshotID	BIGINT	Snapshot partly identifies CIM_PhysicalElement
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_PhysicalElement; equates to CIM_PhysicalElement
Tag	NVARCHAR(256)	Tag partly identifies CIM_PhysicalElement; an arbitrary string that uniquely identifies the Physical Element and serves as the Element's key and can contain information such as asset tag or serial number data
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description (one line string) of the object
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object
Name	NVARCHAR(256)	The label by which this object is known
InstallDateTime	BIGINT	Inherited from CIM_ManagedSystemElement.InstallDate; a datetime value indicating when the object was installed; a lack of a value does not indicate that the object is not installed
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status; a string indicating the current status of the object
ManufactureDate	BIGINT	Date this physical element was manufactured
Manufacturer	NVARCHAR(256)	The name of the organization responsible for producing the Physical Element (This can be the entity from which the element is purchased, but this is not necessarily true. The latter information is contained in the Vendor property of CIM_Product.)
Model	NVARCHAR(64)	The name by which the Physical Element is generally known
OtherIdentifyingInfo	NVARCHAR(512)	Captures additional data, beyond that of Tag information, that could be used to identify a Physical Element (One example is bar code data associated with an Element that also has an asset tag. Note that if only bar code data is available and is unique or able to be used as an Element key, this property would be null and the bar code data used as the class key in the Tag property.)
PartNumber	NVARCHAR(256)	The part number assigned by the organization responsible for producing or manufacturing the Physical Element
PoweredOn	bit	Boolean value indicating that the Physical Element is powered on (true), or is currently off (false)
SerialNumber	NVARCHAR(64)	A manufacturer-allocated number used to identify the Physical Element
SKU	NVARCHAR(64)	The stock keeping unit number for this Physical Element
Version	NVARCHAR(64)	A string indicating the version of the Physical Element
Slot_Number	SMALLINT	The Number property indicates the physical slot number, which can be used as an index into a system slot table, whether that slot is physically occupied
dc_Location	NVARCHAR(64)	Not standard; a string describing the location of the physical element
dc_Condition	NVARCHAR(64)	Not standard; a string describing the condition of the physical element such as OK, Degraded, or Failed
dc_FirmwareRevision	NVARCHAR(64)	Not standard; a firmware revision associated with the physical element
dc_HWLocation	NVARCHAR(256)	Not standard; a text description of the hardware location, on complex multi-SBB hardware only, for the element

Column Name	Data Type	Description
dc_ProductID	NVARCHAR(64)	The product ID string of the server blade

CIM_PhysicalMedia table

Column Name	Data Type	Description
PhysicalMedia_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PhysicalMedia
SnapshotID	BIGINT	Snapshot partly identifies CIM_PhysicalMedia
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_PhysicalMedia; equates to CIM_PhysicalMedia
Tag	NVARCHAR(256)	Inherited from CIM_PhysicalElement.Tag; an arbitrary string that uniquely identifies the Physical Element and serves as the Element's key, can contain information such as asset tag or serial number data
MediaType	SMALLINT	Specifies the type of the PhysicalMedia, as an enumerated integer (The MediaDescription property is used to provide more explicit definition of the Media type, whether it is pre-formatted, compatibility features and so on. CIM_PhysicalMedia.MediaType enumeration. 0 = Unknown, 1 = Other, 2 = Tape, 3 = QIC Cartridge, 4 = AIT Cartridge, 5 = DTF Cartridge, 6 = DAT Cartridge, 7 = 8mm Tape Cartridge, 8 = 19mm Tape Cartridge, 9 = DLT Cartridge, 10 = Half-Inch Magnetic Tape Cartridge, 11 = Cartridge Disk, 12 = JAZ Disk, 13 = ZIP Disk, 14 = SyQuest Disk, 15 = Winchester Removable Disk, 16 = CD_ROM, 17 = CD_ROM/XA, 18 = CD-I; 19, 19 = Recordable, 20 = WORM, 21 = Magneto-Optical, 22 = DVD, 23 = DVD-RW+, 24 = DVD-RAM, 25 = DVD-ROM, 26 = DVD-Video, 27 = Divx, 28 = Floppy/Diskette, 29 = Hard Disk, 30 = Memory Card, 31 = Hard Copy, 32 = Klik Disk, 33 = CD-RW, 34 = CD-DA, 35 = CD+, 36 = DVD Recordable, 37 = DVD-RW, 38 = DVD-Audio, 39 = DVD-5, 40 = DVD-9, 41 = DVD-10, 42 = DVD-18, 43 = Magneto-Optical Rewriteable, 44 = Magneto-Optical Write Once, 45 = Magneto-Optical Rewriteable (LIMDOWN), 46 = Phase Change Write Once, 47 = Phase Change Rewriteable, 48 = Phase Change Dual Rewriteable, 49 = Ablative Write Once, 50 = Near Field Recording, 51 = MiniQic, 52 = Travan, 53 = 8mm Metal Particle, 54 = 8mm Advanced Metal Evaporate, 55 = NCTP, 56 = LTO Ultrium, 57 = LTO Accelis, 58 = 9 Track Tape, 59 = 18 Track Tape, 60 = 36 Track Tape, 61 = Magstar 3590, 62 = Magstar MP, 63 = D2 Tape, 64 = Tape, DST Small , 65 = Tape, DST Medium, 66 = Tape, DST Large)
Capacity	BIGINT	The number of bytes that can be read from or written to a Media (This property is not applicable to \"Hard Copy\" (documentation) or cleaner Media. Data compression should not be assumed because it would increase the value in this property. For tapes, it should be assumed that no filemarks or blank space areas are recorded on the Media.)
Removable	bit	Inherited from CIM_PhysicalComponent.Removable (A PhysicalComponent is Removable if it is designed to be taken in and out of the physical container in which it is normally found, without impairing the function of the overall packaging. A component can still be Removable if power must be off to perform the removal. If power can be on and the component removed, then the element is both Removable and HotSwappable. For example, an upgradeable processor chip is removable.)
OtherIdentifyingInfo	NVARCHAR(512)	Captures additional data, beyond that of Tag information, that could be used to identify a Physical Element (One example is bar code data associated with an Element that also has an asset tag. Note that if only bar code data is available and is unique or able to be used as an Element key, this property would be null and the bar code data used as the class key in the Tag property.)

Column Name	Data Type	Description
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object
Name	NVARCHAR(256)	The label by which this object is known
HotSwappable	bit	Inherited from CIM_PhysicalComponent.HotSwappable; (Is HotSwappable if it is possible to replace the Element with a physically different but equivalent one while the containing package has power applied to it (for example, is on))
Manufacturer	NVARCHAR(256)	The name of the organization responsible for producing the Physical Element (This can be the entity from whom the element is purchased, but this is not necessarily true. The latter information is contained in the Vendor property of CIM_Product.)
Model	NVARCHAR(64)	The name by which the Physical Element is generally known
SerialNumber	NVARCHAR(64)	A manufacturer-allocated number used to identify the Physical Element
Version	NVARCHAR(256)	A string indicating the version of the Physical Element

CIM_PhysicalMemory table

Column Name	Data Type	Description
PhysicalMemory_LUID	BIGINT	LUID uniquely defining this table row
ModelID	BIGINT	
SnapshotID	BIGINT	
CreationClassName	NVARCHAR(256)	CreationClassName identifies CIM_PhysicalMemory; equates to CIM_PhysicalMemory
Tag	NVARCHAR(256)	Tag partly identifies CIM_PhysicalMemory; inherited from CIM_PhysicalElement.Tag; an arbitrary string that uniquely identifies the Physical Element and serves as the Element's key and can contain information such as asset tag or serial number data
MemoryType	SMALLINT	The type of physical memory (CIM_PhysicalMemory.MemoryType Enumeration. 0 = Unknown, 1 = Other, 2 = DRAM, 3 = Synchronous DRAM, 4 = Cache DRAM, 5 = EDO, 6 = EDRAM, 7 = VRAM, 8 = SRAM, 9 = RAM, 10 = ROM, 11 = Flash, 12 = EEPROM, 13 = FEPRAM, 14 = EPROM, 15 = CDRAM, 16 = 3DRAM, 17 = SDRAM, 18 = SGRAM, 19 = RDRAM, 20 = DDR)
Capacity	BIGINT	The total capacity of this PhysicalMemory in bytes
R_MemoryType	NVARCHAR(256)	A field used by reporting
R_MemoryTech	NVARCHAR(256)	A field used by reporting
FormFactor	SMALLINT	Derived from CIM_Chip (The implementation form factor for the Chip. CIM_PhysicalMemory.FormFactor enumeration. 0 = Unknown, 1 = Other, 2 = SIP, 3 = DIP, 4 = ZIP, 5 = SOJ, 6 = Proprietary, 7 = SIMM, 8 = DIMM, 9 = TSOP, 10 = PGA, 11 = RIMM, 12 = SODIMM, 13 = SRIMM, 14 = SMD, 15 = SSMP, 16 = QFP, 17 = TQFP, 18 = SOIC, 19 = LCC, 20 = PLCC, 21 = BGA, 22 = FPBGA, 23 = LGA)
PartNumber	NVARCHAR(256)	The part number assigned by the organization responsible for producing or manufacturing the Physical Element
SerialNumber	NVARCHAR(64)	A manufacturer-allocated number used to identify the Physical Element
dc_ErrorMethodology	NVARCHAR(512)	Not standard; the main error correction scheme supported by this memory component

Column Name	Data Type	Description
dc_HWLocation	NVARCHAR(256)	Not standard; a text description of the hardware location, on complex multi-SBB hardware only, for the memory element
R_Slot	SMALLINT	A field used by reporting
Description	NVARCHAR(64)	Description of the element
BankLabel	nvarchar(64)	Memory bank designator
MemLoc_LocationIdentifiers	nvarchar(255)	Location identifiers for memory on boards

CIM_PhysicalPackage table

Column Name	Data Type	Description
PhysicalPackage_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	System partly identifies CIM_PhysicalPackage
SnapshotID	BIGINT	Snapshot partly identifies CIM_PortController
ElementName	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known
Tag	NVARCHAR(256)	Used for reporting purposes
CreationClassName	NVARCHAR(256)	Used for reporting purposes
Manufacturer	NVARCHAR(64)	Used for reporting purposes
Model	NVARCHAR(256)	Used for reporting purposes
PartNumber	NVARCHAR(256)	Used for reporting purposes

CIM_PortController table

Column Name	Data Type	Description
PortController_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PortController
SnapshotID	BIGINT	Snapshot partly identifies CIM_PortController
ElementName	NVARCHAR(255)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
DeviceID	NVARCHAR(64)	Used for reporting purposes
ProtocolSupported	SMALLINT	Used for reporting purposes
R_OperationalStatus	NVARCHAR(256)	Used for reporting purposes
R_PortCount	INT	INT
R_PortUtilized	INT	Used for reporting purposes
R_Condition	NVARCHAR(256)	A field used by reporting
R_MaxCapacity	NVARCHAR(256)	A field used by reporting
dc_RedundancyState	NVARCHAR(512)	Not standard; The redundancy state of the power supply
dc_CurrentOutputPower	INT	Not standard; capacity and or output power of the power supply in watts

CIM_PowerSupply table

Column Name	Data Type	Description
PowerSupply_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_PowerSupply
SnapshotID	BIGINT	Snapshot partly identifies CIM_PowerSupply
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_PowerSupply; equates to CIM_PowerSupply
DeviceID	NVARCHAR(64)	DeviceID partly identifies CIM_PowerSupply; inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device
SystemCreationClassName	NVARCHAR(256)	SystemCreationClassName partly identifies CIM_PowerSupply (When related data is in CIM_PhysicalElement, this field equates to CIM_PhysicalElement. Otherwise, CIM_ComputerSystem.)
SystemName	NVARCHAR(256)	The value of CIM_PhysicalElement.Name or CIM_ComputerSystem.Name where NodeID is equal.
Name	NVARCHAR(256)	A label by which the object is known
Availability	SMALLINT	The primary availability and status of the System (Additional status information can be specified using the AdditionalAvailability array property. For example, the Availability property indicates that the System is running and has full power (value=3) or is in a warning (value = 4), test (value = 5), degraded (value = 10), or power save state (values 13-15 and 17). Regarding the Power Save states, these are defined as follows: Value 13 (\ "Power Save - Unknown\ ") indicates that the system is known to be in a power save mode, but its exact status in this mode is unknown; value 14 (\ "Power Save - Low Power Mode\ ") indicates that the system is in a power save state but still functioning and might exhibit degraded performance; value 15 (\ "Power Save - Standby\ ") describes that the system is not functioning but could be brought to full power quickly; and value 17 (\ "Power Save - Warning\ ") indicates that the system is in a warning state, though also in a power save mode. CIM_LogicalDevice.Availability enumeration. 1 = Other, 2 = Unknown, 3 = Running/Full Power, 4 = Warning, 5 = In Test, 6 = Not Applicable, 7 = Power Off, 8 = off Line, 9 = Off Duty, 10 = Degraded, 11 = Not Installed, 12 = Install Error, 13 = Power Save - Unknown, 14 = Power Save - Low Power Mode, 15 = Power Save - Standby, 16 = Power Cycle, 17 = Power Save - Warning, 18 = Paused, 19 = Not Ready, 20 = Not Configured, 21 = Quiesced)
AdditionalAvailability	SMALLINT	Additional availability and status of the device, beyond that specified in the Availability property (The property denotes the primary status and availability of the device. In some cases, this is not sufficient to denote the complete status of the device. In those cases, the AdditionalAvailability property can be used to provide further information. For example, a device primary Availability might be \ "Off line\ " (value=8), but it might also be in a low power state (AdditionalAvailability value=14), or the device could be running Diagnostics (AdditionalAvailability value=5, \ "In Test\ "). See CIM_PowerSupply.Availability enumeration.)
TotalOutputPower	INT	Represents the total output power of the PowerSupply in milliWatts; 0 denotes Unknown units (milliWatts)
OtherIdentifyingInfo	NVARCHAR(256)	Additional information that can identify the power supply
R_Status	NVARCHAR(256)	A field used by reporting
R_Condition	NVARCHAR(256)	A field used by reporting
R_MaxCapacity	NVARCHAR(256)	A field used by reporting

Column Name	Data Type	Description
dc_PowerSupplyPresent	NVARCHAR(32)	Not standard; indicates whether the power supply is present in the chassis
dc_PowerSupplyStatus	NVARCHAR(64)	The status of the power supply (noError (1), generalFailure (2), bistFailure (3), fanFailure (4), tempFailure (5), interlockOpen (6), epromFailed (7), vrefFailed (8), dacFailed (9), ramTestFailed (10), voltageChannelFailed (11), orringdiodeFailed (12), brownOut (13), giveupOnStartup (14), nvramInvalid (15), calibrationTableInvalid (16))
dc_PowerSupplyState	NVARCHAR(32)	Not standard; the redundancy state of the power supply
dc_CurrentOutputInfo	INT	Not standard; capacity and or output power of the power supply in watts
OtherIdentifyingInfo	NVARCHAR(256)	OtherIdentifyingInfo captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice
Type	SMALLINT	Indication of the type the power supply device including: "0" = Unknown "1" = Other "2" = Compute Cabinet Bulk Power Supply "3" = Compute Cabinet System Backplane Power Supply "4" = Compute Cabinet I/O chassis enclosure Power Supply "5" = Compute Cabinet AC Input Line "6" = I/O Expansion Cabinet Bulk Power Supply "7" = I/O Expansion Cabinet System Backplane Power Supply "8" = I/O Expansion Cabinet I/O chassis enclosure Power Supply "9" = I/O Expansion Cabinet AC Input Line
Location	NVARCHAR(64)	Position is a free-form string indicating the placement of a PhysicalElement. It can specify slot information on a HostingBoard, mounting site in a Cabinet, or latitude and longitude information, for example, from a GPS. It is part of the key of the Location object.
PhysicalPosition	NVARCHAR(64)	Position is a free-form string indicating the placement of a PhysicalElement. It can specify slot information on a HostingBoard, mounting site in a Cabinet, or latitude and longitude information, for example, from a GPS. It is part of the key of the Location object.
Caption	NVARCHAR(64)	The Caption value can be one of the following, depending on the device type: <ul style="list-style-type: none"> • Compute Cabinet Bulk Power Supply • Compute Cabinet Backplane Power Supply • Compute Cabinet I/O Chassis Enclosure Power Supply • Compute Cabinet AC Input Line • I/O Expansion Cabinet Bulk Power Supply • I/O Expansion Cabinet Backplane Power Supply • I/O Expansion Cabinet I/O Chassis Enclosure Power Supply • I/O Expansion Cabinet AC Input Line • Cooling Device Slot • Power Device Slot Note: This property may not be available when the cell is powered off.
Manufacturer	NVARCHAR(64)	Displays manufacturer Hewlett-Packard

Column Name	Data Type	Description
Tag	NVARCHAR(64)	Unique value including the Physical Location of the power supply device

CIM_Process table

Column Name	Data Type	Description
Process_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Process
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProcessM/para
CSCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
CSName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name where NodeID is equal
OSCreationClassName	NVARCHAR(256)	OSCreationClassName partly identifies CIM_Process. Equates to CIM_OperatingSystem
OSName	NVARCHAR(256)	OSName partly identifies CIM_Process; the value of CIM_OperatingSystem.Name where NodeID is equal
Handle	NVARCHAR(256)	Handle partly identifies CIM_Process; a string used to identify the Process. A Process ID is a kind of Process Handle
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Process; equates to CIM_Process
Name	NVARCHAR(256)	Name partly identifies CIM_Process; the name of the process
ExecutionState	SMALLINT	Indicates the current operating condition of the Process; CIM_Process.ExecutionState enumeration (0 = Unknown, 1 = Other, 2 = Ready, 3 = Running, 4 = Suspended Blocked, 6 = Suspended Ready, 7 = Terminated, 8 = Stopped, 9 = Growing)
Priority	INT	Priority indicates the urgency or importance of execution of a Process
UnixProcess_ParentProcessID	NVARCHAR(256)	Derived from CIM_UnixProcess.ParentProcessID; the parent process ID of this executing process
UnixProcess_ProcessGroupID	BIGINT	Derived from CIM_UnixProcess.ProcessGroupID; the group ID of the currently executing process
UnixProcess_RealUserID	BIGINT	Derived from CIM_UnixProcess.RealUserID; the real user id of the currently executing process
UnixProcess_ProcessTTY	NVARCHAR(32)	Derived from CIM_UnixProcess.ProcessTTY; the TTY currently associated with this process
UnixProcess_ModulePath	NVARCHAR(512)	Derived from CIM_UnixProcess.ModulePath; the file path to the executing module for the process
OtherExecutionDescription	NVARCHAR(512)	Derived from CIM_UnixProcess.ModulePath; the executing process command path
UnixProcess_Parameters	NVARCHAR(512)	A string describing the state - used when the instance's ExecutionState property is set to Other; else this field is null
UnixProcess_ProcessNiceValue	INT	Derived from CIM_UnixProcess.Parameters; the operating system parameters provided to the executing process
UxPrStatInf_RealStack	BIGINT	Derived from CIM_UnixProcess.ProcessNiceValue; the process nice value; used to compute its priority
UxPrStatInf_VirText	BIGINT	UnixProcessStatisticalInformation_RealStack; derived from CIM_UnixProcessStatisticalInformation.RealStack; the number of KB of real stack space used by the process

Column Name	Data Type	Description
UxPrStatInf_VirData	BIGINT	UnixProcessStatisticalInformation_VirtualText; derived from CIM_UnixProcessStatisticalInformation.VirtualText; The number of KB of virtual text space used by the process
UxPrStatInf_VirStack	BIGINT	UnixProcessStatisticalInformation_VirtualData; derived from CIM_UnixProcessStatisticalInformation.VirtualData; the number of KB of virtual data space used by the process
UxPrStatInf_VirSharedMem	BIGINT	UnixProcessStatisticalInformation_VirtualStack; derived from CIM_UnixProcessStatisticalInformation.VirtualStack; the number of KBs of virtual stack space used by the process
UxPrStatInf_VirSharedMem	BIGINT	UnixProcessStatisticalInformation_VirtualSharedMemory; derived from CIM_UnixProcessStatisticalInformation.VirtualSharedMemory; the number of KB of shared memory used by the process
UxPrStatInf_VirMemMapFileSize	BIGINT	UnixProcessStatisticalInformation_VirtualMemoryMappedFileSize; derived from CIM_UnixProcessStatisticalInformation.VirtualMemoryMappedFileSize; the number of KB of virtual space used for memory mapped files by the process.

CIM_Processor table

Column Name	Data Type	Description
Processor_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Processor
SnapshotID	BIGINT	Snapshot partly identifies CIM_Processor
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Processor; equates to CIM_Processor
DeviceID	NVARCHAR(64)	DeviceID partly identifies CIM_Processor; inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device
Name	NVARCHAR(256)	Name partly identifies CIM_Processor; a label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem.
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name where NodeID is equal

Column Name	Data Type	Description
Family	SMALLINT	The Processor Family Type. CIM_Processor.Family enumeration (1 = Other, 2 = Unknown, 3 = 8086, 4 = 80286, 5 = 80386, 6 = 80486, 7 = 8087, 8 = 80287, 9 = 80387, 10 = 80487, 11 = Intel® Pentium® brand, 12 = Pentium® Pro, 13 = Pentium® II, 14 = Pentium® processor with MMX™ technology, 15 = Celeron®, 16 = Pentium® II Xeon™, 17 = Pentium® III, 18 = M1 Family, 19 = M2 Family, 24 = K5 Family, 25 = K6 Family, 26 = K6-2, 27 = K6-3, 28 = AMD Athlon Processor Family, 29 = AMD Duron Processor, 30 = AMD29000 Family, 31 = K6-2+, 32 = Power PC Family, 33 = Power PC 601, 34 = Power PC 603, 35 = Power PC 603+, 36 = Power PC 604, 37 = Power PC 620, 38 = Power PC X704, 39 = Power PC 750, 48 = Alpha Family, 49 = Alpha 21064, 50 = Alpha 21066, 51 = Alpha 21164, 52 = Alpha 21164PC, 53 = Alpha 21164a, 54 = Alpha 21264, 55 = Alpha 21364, 64 = MIPS Family, 65 = MIPS R4000, 66 = MIPS R4200, 67 = MIPS R4400, 68 = MIPS R4600, 69 = MIPS R10000, 80 = SPARC Family, 81 = SuperSPARC, 82 = microSPARC, 83 = microSPARC IIep, 84 = UltraSPARC, 85 = UltraSPARC II, 86 = UltraSPARC Ili, 87 = UltraSPARC Ilii, 88 = UltraSPARC Ilii, 96 = 68040, 97 = 68xxx Family, 98 = 68000, 99 = 68010, 100 = 68020, 101 = 68030, 112 = Hobbit Family, 120 = Crusoe TM5000 Family, 121 = Crusoe TM3000 Family, 128 = Weitek, 130 = Intel® Itanium® Processor, 144 = PA-RISC Family, 145 = PA-RISC 8500, 146 = PA-RISC 8000, 147 = PA-RISC 7300LC, 148 = PA-RISC 7200, 149 = PA-RISC 7100LC, 150 = PA-RISC 7100, 160 = V30 Family, 176 = Pentium® III Xeon™, 177 = Pentium® III Processor with Intel® SpeedStep Technology, 178 = Pentium® 4, 179 = Intel® Xeon™, 180 = AS400 Family, 181 = Intel Xeon processor MP, 190 = K7, 200 = Intel® Xeon™ processor MP, 201 = G4, 202 = G5, 250 = i860, 251 = i960, 260 = SH-3, 261 = SH-4, 280 = ARM, 281 = StrongARM, 300 = 6x86, 301 = MediaGX, 302 = MII, 320 = WinChip, 350 = DSP, 500 = Video Processor)
CurrentClockSpeed	INT	The current speed (in MHz) of this Processor
UniqueID	NVARCHAR(256)	A globally unique identifier for the processor (This identifier might only be unique within a processor family.)
LoadPercentage	SMALLINT	Loading of this processor, averaged over the last minute in percent
CPUStatus	SMALLINT	The CPUStatus property indicates the current status of the processor (For example, it might be disabled by the user through BIOS (value=2), or disabled because of a POST error (value=3). Information in this property can be obtained from SMBIOS, the Type 4 structure, the Status attribute. CIM_Processor.CPUStatus Enumeration. (0 = Unknown, 1 = CPU, 2 = CPU disabled by user through BIOS setup, 3 = CPU disabled by BIOS (POST error), CPU Is Idle, Other)
OtherIdentifyingInfo	NVARCHAR(64)	Inherited from CIM_LogicalDevice.OtherIdentifyingInfo.OtherIdentifyingInfo captures additional data, beyond DeviceID information, that could be used to identify a LogicalDevice (One example would be the socket and slot information for this processor.)
R_CPUType	NVARCHAR(256)	A field used by reporting
R_CPUSpeed	NVARCHAR(256)	A field used by reporting
R_CPUStatus	NVARCHAR(256)	A field used by reporting
dc_HWLocation	NVARCHAR(256)	Not standard; a text description of the hardware location, on complex multi-SBB hardware only for the processor
ArchitectureRevision	SMALLINT	Architecture revision of the processor
FirmwareRevision	NVARCHAR(255)	Firmware revision of the processor
DataWidth	SMALLINT	Width of the processor datapath in bits

Column Name	Data Type	Description
ProcessorLocation_CellNumber	NVARCHAR(255)	Cell in the complex containing this processor (Cellular systems only)

CIM_Product table

Column Name	Data Type	Description
Product_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Product
SnapshotID	BIGINT	Snapshot partly identifies CIM_Product
Elementname	NVARCHAR(255)	Used for reporting purposes
Name	NVARCHAR(256)	A label by which the object is known
IdentifyingNumber	NVARCHAR(64)	Product identification
Vendor	NVARCHAR(256)	The name of the Product's supplier or entity selling the product
Version	NVARCHAR(64)	Product version information; corresponds to the Version property in the Product object in the DMTF Solution Exchange Standard

CIM_RemoteServiceAccessPoint table

Column Name	Data Type	Description
RemoteServiceAccessPoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_RemoteServiceAccessPoint
SnapshotID	BIGINT	Snapshot partly identifies CIM_RemoteServiceAccessPoint
ElementName	NVARCHAR(255)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
AccessInfo	NVARCHAR(255)	Used for reporting purposes
CreationClassName	NVARCHAR(256)	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known

CIM_SCSIProtocolController table

Column Name	Data Type	Description
SCSIProtocolController_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_SCSIProtocolController
SnapshotID	BIGINT	Snapshot partly identifies CIM_SCSIProtocolController
ElementName	NVARCHAR(255)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
DeviceID	NVARCHAR(256)	Used for reporting purposes
MaxUnitsControlled	INT	Used for reporting purposes

CIM_SCSIProtocolEndpoint table

Column Name	Data Type	Description
SCSIProtocolEndpoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_SCSIProtocolEndpoint
SnapshotID	BIGINT	Snapshot partly identifies CIM_SCSIProtocolEndpoint
Name	NVARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
ConnectionType	SMALLINT	Used for reporting purposes

CIM_ProtoControlAccessesUnit table

Column Name	Data Type	Description
ProtoControlAccessUnit_LUID	BIGINT	Used for reporting purposes
ProtoControlAccessUnit_LUID	BIGINT	Used for reporting purposes

CIM_ProtocolControllerForPort table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
NodeID	BIGINT	Node partly identifies CIM_ProtocolControllerForUnit
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProtocolControllerForUnit
DeviceNumber	NVARCHAR(255)	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes
Name	NVARCHAR(255)	A label by which the object is known

CIM_ProtocolControllerForUnit table

Column Name	Data Type	Description
ProtocolControllerForUnit_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_ProtocolControllerForUnit
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProtocolControllerForUnit
DeviceNumber	NVARCHAR(255)	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

CIM_ProtocolEndpoint table

Column Name	Data Type	Description
protocolEndpoint_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_ProtocolEndpoint
SnapshotID	BIGINT	Snapshot partly identifies CIM_ProtocolEndpoint

Column Name	Data Type	Description
Name	NVARCHAR(1024)	Used for reporting purposes
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
ProtocolIFType	NVARCHAR(256)	Used for reporting purposes

CIM_Rack table

Column Name	Data Type	Description
Rack_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Rack
SnapshotID	BIGINT	Snapshot partly identifies CIM_Rack
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Rack; equates to CIM_Rack
Tag	NVARCHAR(256)	Tag partly identifies CIM_Rack; inherited from CIM_PhysicalElement.Tag; an arbitrary string that uniquely identifies the Physical Element and serves as the Element key and can contain information such as asset tag or serial number data
SerialNumber	NVARCHAR(64)	Inherited from CIM_PhysicalElement.SerialNumber; a manufacturer-allocated number used to identify the Physical Element
Name	NVARCHAR(256)	A label by which the object is known

CIM_Realizes table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

CIM_Sensor table

Column Name	Data Type	Description
Sensor_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_Sensor
SnapshotID	BIGINT	Snapshot partly identifies CIM_Sensor
DeviceID	NVARCHAR(64)	DeviceID partly identifies CIM_Sensor; inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device
CreationClassName	NVARCHAR(256)	CreationClassName partly identifies CIM_Sensor; Equates to CIM_Sensor
SystemCreationClassName	NVARCHAR(256)	SystemCreationClassName partly identifies CIM_Sensor (If the sensor is owned by a chassis, then this field equates to CIM_Chassis; otherwise it is set to CIM_ComputerSystem.)
SystemName	NVARCHAR(256)	Equates to CIM_Sensor.Name or CIM_ComputerSystem.Name where NodeID is equal
Name	NVARCHAR(256)	Name partly identifies CIM_Sensor; a label by which the object is known
Status	NVARCHAR(10)	Inherited from CIM_ManagedSystemElement.Status; a string indicating the current status of the object

Column Name	Data Type	Description
CurrentState	NVARCHAR(128)	The current state indicated by the Sensor (This is always one of the Possible States property.)
PossibleStates	NVARCHAR(512)	Possible States enumerates the string outputs of the Sensor (For example, a switch sensor can output the states On or Off. Another implementation of the Switch can output the states Open and Close. Another example is a NumericSensor supporting thresholds. This Sensor can report the states like Normal, Upper Fatal, Lower non-critical and so on. A Numeric Sensor that does not publish readings and threshold but stores this data internally can still report its states.)
CurrentReading	INT	The current air temperature at the exhaust of the power supply in degrees Celsius
dc_OtherCurrentReading	INT	The current air temperature at the intake of the power supply in degrees Celsius
BaseUnit	INT	Code for the units used by the readings (pull from CIM_NumericSensor)
SensorType	SMALLINT	Type of sensor: ValueMap { "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12" }, Values { "Unknown", "Other", "Temperature", "Voltage", "Current", "Tachometer", "Counter", "Switch", "Lock", "Humidity", "Smoke Detection", "Presence", "Air Flow" }

CIM_SoftwareElement table

Column Name	Data Type	Description
SoftwareElement_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies CIM_SoftwareElement
SnapshotID	BIGINT	Snapshot partly identifies CIM_SoftwareElement
SoftwareElementID	NVARCHAR(256)	SoftwareElementID partly identifies CIM_SoftwareElement (This is an identifier for the Software Element and is designed to be used in conjunction with other keys to create a unique representation of the element.)
SoftwareElementState	SMALLINT	SoftwareElementState partly identifies CIM_SoftwareElement (The SoftwareElementState is defined in this model to identify various states of a SoftwareElement life cycle. A SoftwareElement in the deployable state describes the details necessary to successfully distribute it and the details (checks and actions) required to move it to the installable state (for example, the next state). A SoftwareElement in the installable state describes the details necessary to successfully install it and the details (checks and actions) required to create an element in the executable state (for example, the next state). A SoftwareElement in the executable state describes the details necessary to successfully start it and the details (checks and actions) required to move it to the running state for example, the next state). A SoftwareElement in the running state describes the details necessary to manage the started element. CIM_SoftwareElement.SoftwareElementState enumeration 0 = Deployable, 1 = Installable, 2 = Executable, 3 = Running)
Version	NVARCHAR(64)	Version partly identifies CIM_SoftwareElement; Software Version should be in the form <Major>.<Minor>.<Revision> or <Major>.<Minor><letter><revision>
Name	NVARCHAR(256)	Name partly identifies CIM_SoftwareElement; the name used to identify this software element

Column Name	Data Type	Description
TargetOperatingSystem	SMALLINT	TargetOperatingSystem partly identifies CIM_SoftwareElement (The TargetOperatingSystem property specifies the Element operating system environment. The value of this property does not ensure that it is binary executable. Two other pieces of information are needed. First, the version of the operating system must be specified using the class, CIM_OSVersionCheck. The second piece of information is the architecture that the operating system runs on. This information is verified using CIM_ArchitectureCheck. The combination of these constructs clearly identifies the level of operating system required for a particular SoftwareElement. See CIM_OperatingSystem.OSType Enumeration.)
InstallDate	BIGINT	Inherited from CIM_ManagedSystemElement.InstallDate; the datetime value indicating when the object was installed
R_Date	NVARCHAR(256)	A field used by reporting
R_Status	NVARCHAR(256)	A field used by reporting
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; a textual description of an object
DeviceSW_Purpose	SMALLINT	DeviceSoftware_Purpose; an enumerated integer to indicate the role this software plays in regards to its associated Device; CIM_DeviceSoftware.Purpose enumeration (0 = Unknown, 1 = Other, 2 = Driver, 3 = Configuration Software, 4 = Application Software, 5 = Instrumentation, 6 = Firmware, 7 = BIOS, 8 = Boot ROM)
DeviceSW_PurposeDescription	NVARCHAR(512)	A free-form string to provide more information for the DeviceSW Purpose property
swd_VersionWeight	INT	swd_VersionWeight is of CIM_SoftwareElement; a field used by Software Version Polling
dc_OtherVersionInfo	NVARCHAR(64)	Not standard. A string that specifies the version of this item
R_Type	NVARCHAR(64)	A field used by reporting.

CIM_SoftwareIdentity table

Column Name	Data Type	Description
SoftwareIdentity_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Used to partially identify CIM_SoftwareIdentity
SnapShotID	BIGINT	Used to partially identify CIM_SoftwareIdentity

Column Name	Data Type	Description
InstanceID	NVARCHAR(255)	InstanceID opaquely and uniquely identifies an instance of this class. To ensure uniqueness within the NameSpace, the value of InstanceID SHOULD be constructed using the following 'preferred' algorithm: " <orgid>:<localid> "="" <localid>="" <orgid>="" ':'="" <b="" a="" and="" are="" by="" colon="" separated="" where="">must include a copyrighted, trademarked, or otherwise unique name that is owned by the business entity creating/defining the InstanceID or is a registered ID that is assigned to the business entity by a recognized global authority. (This is similar to the <Schema Name>_<Class Name> structure of Schema class names.) In addition, to ensure uniqueness <OrgID> must note contain a colon (":"). When using this algorithm, the first colon to appear in InstanceID must appear between <OrgID> and <LocalID>. <LocalID> is chosen by the business entity and should not be re-used to identify different underlying (real-world) elements. If the above 'preferred' algorithm is not used, the defining entity must assure that the resultant InstanceID is not re-used across any InstanceIDs produced by this or other providers for this instance's NameSpace. For DMTF defined instances, the preferred algorithm must be used with the <OrgID> set to <i>CIM</i>. An example might be "HEWLETT-PACKARD:HPCPQASM.EXE:7.15.19.0"</orgid>:<localid>>
VersionString	NVARCHAR(255)	A string representing the complete software version information (Because varying semantics and representations might not allow simple calculation and comparison, both numeric and string representations are provided. See MajorVersion, MinorVersion, RevisionNumber and BuildNumber for the numeric components.)
Manufacturer	NVARCHAR(255)	Manufacturer of this software
Description	NVARCHAR(512)	Description of this element
MajorVersion	SMALLINT	Major version number of this element
MinorVersion	SMALLINT	Minor version number of this element
RevisionNumber	SMALLINT	Revision number of this element
BuildNumber	SMALLINT	Build number of this element
Classification	SMALLINT	An enumerated integer to indicate the role this software plays in regards to its associated Device; CIM_DeviceSoftware.Purpose enumeration (0 = Unknown, 1 = Other, 2 = Driver, 3 = Configuration Software, 4 = Application Software, 5 = Instrumentation, 6 = Firmware, 7 = BIOS, 8 = Boot ROM)
IdentifyInfoValue	NVARCHAR(256)	Key file name.; an application-specific invariant identifier that is consistent between versions of a SoftwareIdentity (It is consistent across more major changes to the Software Identity naming structure. The purpose of the parameter is to allow Software Identities to be selected by a client that are compatible with a specific SoftwareInstallationService. A client uses this parameter to select candidate Software Identities by comparing TargetType with the contents of the SupportedTargetTypes parameter in SoftwareInstallationServiceCapabilities.)
TargetOperatingSystem	SMALLINT	The TargetOperatingSystem property specifies the Element operating system environment (The value of this property does not ensure that it is binary executable. Two other pieces of information are needed. First, the version of the operating system must be specified using the class, CIM_OSVersionCheck. The second piece of information is the architecture on which the operating system runs. This information is verified using CIM_ArchitectureCheck. The combination of these constructs clearly identifies the level of operating system required for a particular SoftwareElement. See CIM_OperatingSystem.OSType Enumeration.)

Column Name	Data Type	Description
InstallDate	NVARCHAR(256)	Installation date of this element in CIM date-time format
swd_VersionWeight	INT	swd_VersionWeight is of CIM_SoftwareElement; a field used by Software Status Polling
dc_OtherVersionInfo	NVARCHAR(64)	Not standard; a string that specifies the version of this item
OperationalStatus	SMALLINT	Used for reporting purposes
ClassificationDescription	NVARCHAR(512)	A free-form string to provide more information for the DeviceSW_Purpose property
Description	NVARCHAR(256)	The HP Smart Array SAS/SATA Event Notification Service provides event notification to the Windows 2000/Windows Server 2003 system event log and the HP ProLiant Integrated Management Log for systems using the HP Smart Array SAS/SATA controller driver.
IdentityInfoValue	NVARCHAR(256)	[C:\Program Files\hp\cissesrv, HPQ:cissesrv.exe] Software/firmware Key file name
IdentityInfoType	NVARCHAR(256)	[HPQ: SoftwarePath, CIM:SoftwareFamily Software Family Path
FirmwareCategory	NVARCHAR(256)	Firmware Category
R_Type	NVARCHAR(64)	A field used by reporting
R_Date	NVARCHAR(256)	A field used by reporting
R_Status	NVARCHAR(256)	A field used by reporting
LatestVersion	NVARCHAR(100)	Stores the latest version of each software with a matching component in the repository
SWFWBaselineVersion	NVARCHAR(100)	Stores the version of software available in the VCRM's sw fw baseline

CIM_StoragePool table

Column Name	Data Type	Description
StoragePool_LUID	BIGINT	Used to uniquely identify CIM_StorageVolume
NodeID	BIGINT	Used to partially identify CIM_StorageVolume
SnapShotID	BIGINT	Used to partially identify CIM_StorageVolume
ElementName	NVARCHAR(255)	Used for reporting purposes
InstanceID	NVARCHAR(255)	Used for reporting purposes
PoolID	NVARCHAR(255)	Used for reporting purposes
Primordial	BIT	Used for reporting purposes
TotalManagedSpace	BIGINT	Used for reporting purposes
RemainingManagedSpace	BIGINT	Used for reporting purposes

CIM_StorageVolume table

Column Name	Data Type	Description
StorageVolume_LUID	BIGINT	Used to uniquely identify CIM_StorageVolume
NodeID	BIGINT	Used to partially identify CIM_StorageVolume
SnapShotID	BIGINT	Used to partially identify CIM_StorageVolume
DataRedundancy	SMALLINT	Used for reporting purposes
ElementName	NVARCHAR(255)	Used for reporting purposes
NameFormat	SMALLINT	Used for reporting purposes

Column Name	Data Type	Description
NoSinglePointOfFailure	BIT	Used for reporting purposes
PackageRedundancy	SMALLINT	Used for reporting purposes
Name	NARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NARCHAR(256)	Used for reporting purposes
SystemName	NARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NARCHAR(256)	Used for reporting purposes
DeviceID	NARCHAR(64)	Used for reporting purposes
Availability	SMALLINT	Used for reporting purposes
BlockSize	BIGINT	Used for reporting purposes
NumberOfBlocks	BIGINT	Used for reporting purposes
ConsumableBlocks	BIGINT	Used for reporting purposes
IsBasedOnUnderlyingRedundanc	BIT	Used for reporting purposes
SequentialAccess	BIT	Used for reporting purposes
R_OperationalStatus	NARCHAR(256)	Used for reporting purposes
R_ExtentStatus	NARCHAR(256)	Used for reporting purposes
R_RaidLevel	NARCHAR(256)	Used for reporting purposes

CIM_TCPProtocolEndpoint table

Column Name	Data Type	Description
TCPProtocolEndpoint_LUID	BIGINT	Used for reporting purposes
NodeID	BIGINT	Used for reporting purposes
SnapshotID	BIGINT	Used for reporting purposes
Name	NVARCHAR(1024)	A label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Used for reporting purposes
SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name with equal NodeID
CreationClassName	NVARCHAR(256)	Used for reporting purposes
ProtocolIFType	SMALLINT	Used for reporting purposes
PortNumber	NVARCHAR(256)	Used for reporting purposes

Classifications_values table

Column Name	Data Type	Description
ClassificationsId	BIGINT	Used for reporting purposes
ClassificationsValue	SMALLINT	Used for reporting purposes
ClassificationsPos	INT	Used for reporting purposes

ComputerSys_HAP table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

ComputerSys_LogicalPortGroup table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes

ComputerSys_NetworkPort table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

ComputerSys_PortController table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

ComputerSys_SAP table

Column Name	Data Type	Description
AvailableSAP	BIGINT	Used for reporting purposes
ManagedElement	BIGINT	Used for reporting purposes

ComputerSys_SCSIProtoCont table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

ComputerSys_SCSIProtoEndp table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

ComputerSys_SoftwareIdent table

Column Name	Data Type	Description
System	BIGINT	Used for reporting purposes
InstalledSoftware	BIGINT	Used for reporting purposes

ComputerSys_StorageVol table

Column Name	Data Type	Description
GroupComponent	BIGINT	Used for reporting purposes
PartComponent	BIGINT	Used for reporting purposes

DB_DeviceInfo table

The DB_DeviceInfo table contains general system information. Any system that supports SNMP has information in this table. The DB_DeviceInfo fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	
UpdateTime	DATETIME	Date and time the database record was last updated
Description	CHAR (200)	System description.
Location	CHAR (200)	Physical location (must be filled in at the system)
Contact	CHAR (200)	The contact for this system (must be filled in at the system)



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

DB_DeviceInfoEx table

The DB_DeviceInfoEx table contains basic information for systems that are running the HP SIM agent or a standard Desktop Management Interface (DMI) service layer. The DB_DeviceInfoEX fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	The DeviceKey associates a system with its collected set of data; system information is linked to the device table using the DeviceKey
UpdateTime	DATETIME	Date and time the database record was last updated
TotalMemory	INT	Total amount of system memory
ROMVersion	CHAR (80)	System ROM version
SerialNumber	CHAR (80)	System serial number
AssetTag	CHAR (100)	System asset tag (must be filled in at the system)
OSName	CHAR (100)	Operating system name. <i>Note:</i> This is not the same OSName from the tool definitions files; this is the OSNameStr value from mxnode
OSType	CHAR(100)	The OSType identifier that is used for tool definitions OSName field; this is a value like WINNT, HPUX, or LINUX
OSVersion	CHAR (100)	Operating system version
OSVendor	CHAR(64)	Vendor name of the operating system
ClusterName	CHAR (100)	If present, the name of the cluster to which this system belongs
OSDescription	CHAR(100)	The description of the host operating system
TrustStatus	Int	System trust state for HP web enabled agents



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

DC_Enclosure table

Column Name	Data Type	Description
Enclosure_LUID	BIGINT	LUID uniquely defining this table row

Column Name	Data Type	Description
NodeID	BIGINT	Node partly identifies dc_Enclosure
SnapshotID	BIGINT	Snapshot partly identifies dc_Enclosure
Tag	NVARCHAR(256)	Tag partly identifies dc_Enclosure and is an arbitrary string that uniquely identifies the enclosure and serves as the Element key
dc_Address	INT	The unique address of the enclosure within the rack
dc_EnclosureMaxNumBladesX	INT	The maximum number of server blades the enclosure can contain
dc_EnclosureMaxNumBladesY	INT	The maximum number of server blades the enclosure can contain
dc_FusePresent	NVARCHAR(32)	Specifies if the fuse described is present in the system: Other (1), Absent (2) and Present (3)
dc_FuseCondition	NVARCHAR(32)	The condition of the fuse (Other (1), Fuse status detection is not supported, OK (2), Fuse is operating properly, Failed (4), Fuse has been tripped or is not operating properly)

DC_ProliantHost table

Column Name	Data Type	Description
ProliantHost_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Identifies the system ID for this row
SnapshotID	BIGINT	Identifies the snapshot ID for this row
dc_SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
dc_SystemName	NVARCHAR(256)	The value of CIM_ComputerSystem.Name where NodeID is equal.
OverallCondition	NVARCHAR(16)	This object represents the overall status of the server host system represented by this MIB
MIBStatusArray	NVARCHAR(512)	An array of MIB status structures (Each structure is made up of 4 octets. The first octet is the MIB presence. The second octet is MIB condition. The third octet is MIB major revision. The fourth octet is MIB minor revision. These blocks of 4 octets each are index by the mib identifier just after the HP enterprise (for example, in 1.3.6.1.232.11 mib, the index is 11). The 4 octets in the first block (block 0) are reserved for systems management and serve as an aggregate of their MIBs.)
GUID	NVARCHAR(64)	The globally unique identifier of this server (If the operating system cannot determine a unique ID, it defaults the variable to contain all 0's. The management station can then perform a SET to this variable to provide the unique ID.)
WebManagementPort	INT	This item indicates the port used by the HP Insight Management Agent
ASRStatus	NVARCHAR(16)	The Automatic Server Recovery (ASR) feature status (If this object is currently Other (1) or Not Available (2), all set operations fail. Any attempt to set this object to Other (1) or Not Available (2) by a management station fails. Setting this object to Disabled (3) or Enabled (4) disables or enables the ASR feature.)
SystemID	INT	The HP System ID; this value indicates the HP system ID of the system board in this system (This ID replaces the product ID used in older machines (cpqSiProductId). A value of 7EH for the cpqSiProductId indicates that the cpqSiSystemId should be used to identify the HP system. A value of zero (0) indicates that the system ID function is not supported on this machine. In this case, the cpqSiProductId should be used to identify the system.)

Column Name	Data Type	Description
ServerRole	NVARCHAR(64)	The system role; this is a settable free form text field intended to be assigned by a remote console briefly describing the system's function
ServerRoleDetail	NVARCHAR(512)	The system detailed description; this is a settable free form text field intended to be assigned by a remote console describing the system function in detail
ConfigChangeDate	BIGINT	The date and time when the agents were last loaded
SystemUptime	BIGINT	The total time (in minutes) the system has been in full operation (while the server health supporting software was running)

Dedicated_values table

Column Name	Data Type	Description
DedicatedId	BIGINT	Used to uniquely identify this row
DedicatedValue	SMALLINT	Used for reporting purposes
DedicatedPos	INT	Used for reporting purposes



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table; where multiple fields in the same table show an asterisk, the primary key connects to each

DeviceNames table

The DeviceNames table contains the names for devices as determined by the various protocols that this device supports. The DeviceNames fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	The deviceKey associates a system with its collected set of data (System information is linked to a system using the DeviceKey from the devices table)
nameSNMP	CHAR (60)	The name for this system obtained through SNMP
nameIPX	CHAR (60)	The name for this system obtained through a name service (such as WINS or DNS) or the hosts file
nameDMI	CHAR (60)	The name for this system obtained through DMI
NameFullDNS	CHAR (90)	This is the fully qualified DNS name (if available)
nameActiveDisc	CHAR (60)	This field is no longer an active field



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

Device Extended Attributes database table

The Device Extended Attributes fields are defined in the following table.

Column Name	Data Type	Description
snoozeTimeMin	INT	The value in minutes a system will be disabled starting with the time marked by snoozeStartTime
snoozeStartTimeMs	Long	The initial timestamp from when a system was placed in a disabled state

Devices table

The Devices table contains discovered system information. This is the primary table used to define system related data. The Devices fields are defined in the following table.

Column Name	Data Type	Description
DeviceKey	INT	The DeviceKey associates a system with its collected set of data (System information is linked to the device table using the DeviceKey)
Name	VARCHAR (255)	The name of the system
GUID	VARCHAR (128)	Globally Unique Identifier, a unique key used to identify this system on the network in the event that it changes its network address (This requires that a system support retrieval of this value in order for it to be stored here.)
Discovered	BIGINT	The date and time that the system was discovered represented as the number of milliseconds since 1970 UTC
ProductType	INT	The product type for this item (See the nodeTypesEnum table, which is best viewed using the deviceSubTypesEnum view, for additional information.)
ProductTypeStr	VARCHAR(32)	A string representation of the product type (See the nodeTypesEnum table, which is best viewed using the deviceTypesEnum view, for additional information.)
ProductSubType	VARCHAR(32)	The subtype, if any (See the NodeSubTypesEnum table, which is best viewed using the deviceSubTypesEnum view, for additional mapping information)
ProductName	NVARCHAR (100)	Product name (such as Proliant 1500)
OverallStatus	INT	Indicates the overall status of the system (0 = Unknown, 1 = Normal, 2 = Warning, 3 = Minor, 4 = Major, 5 = Critical, 10 = No Status (occurs for new systems or on startup before polling))
LockFlags	INT	Indicates whether product type, name, or both are locked so that discovery cannot change them ▲ 0 = Nothing is locked.
Timestamp	BIGINT	RESERVED (The last time some system information was updated, in the database, not just in this table.)
FullDNSName	VARCHAR(90)	The full DNS name of the system
MxGUID	VARCHAR(32)	The HP SIM uniquely assigned identifier for this system
DiscoveredName	NVARCHAR(32)	
DurableName	NVARCHAR(32)	If the system was found by an SMI-S agent, this will be equal to the name field of the top-level CIM_ComputerSystem that represents the system.
WWName	NVARCHAR(32)	
NodeLUID	INT	
UniqueIdentifier	VARCHAR(32)	Used to uniquely identify the system

DeviceProtocolInfo table

The Device Protocol Information fields are defined in the following table.

Column Name	Data Type	Description
DeviceKey	INT	The DeviceKey associates this table with the system in the devices table.
IPAddressable	INT	Flag indicating if this system is addressable through TCP/IP

Column Name	Data Type	Description
IPXAddressable	INT	Flag indicating if this system is addressable through IPX
SNMP	INT	Flag indicating if this system, supports SNMP-based management; a value of -1 indicates the system was not identified yet; a value of 0 indicates SNMP was not found on the system; a value of 1 to 5 indicates that SNMP was found on the system
SNMPverStr	NVARCHAR(32)	A string indicating what version of SNMP was detected (Currently HP Systems Insight Manager only supports "1.0")
HTTP	INT	Flag indicating if this system supports HTTP-based management; a value of -1 indicates the system was not yet identified; a value of 0 indicates HTTP was not found on the system a value of 1 indicates that HTTP was found on the system
DMI	INT	Flag indicating if this system supports DMI-based management; a value of -1 indicates the system was not yet identified; a value of 0 indicates DMI was not found on the system; a value of 1 indicates DMI was found on the system
DMIVerStr	NCHAR(32)	Always 2.0.
WBEM	INT	If WBEM is detected on the system, then this is set to 1; otherwise, it is set to 0
WBEMverStr	NCHAR(32)	The version of WBEM that HP SIM found on the system
SSH	INT	If SSH was detected on the system this is set to 1; otherwise, it is set to 0
SSHverStr	NCHAR(64)	The System ID returned from the SSH request
PrimaryAddress	nchar(32)	For future expansion.
WMIProxyID	INT	The device key of the system that is used for the WMI proxy for the system for this record (In other words HP SIM uses the system with same device key as the WMIProxyID for making WBEM to requests through the WMI Mapper running on that other system.)

ExtentStatus_values table

Column Name	Data Type	Description
ExtentStatusId	BIGINT	Used for reporting purposes
ExtentStatusValue	SMALLINT	Used for reporting purposes
ExtentStatusPos	INT	Used for reporting purposes

DeviceSnmpSettings table

The DeviceSnmpSettings table contains the SNMP settings currently configured for the systems. The DeviceSnmpSettings fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	Associates a system with its collected set of data (This system information is linked using the DeviceKey from the devices table.)
networkTimeout	INT	The network timeout value in seconds
networkRetries	INT	The number of retries to be used for SNMP requests
icmpTimeout	INT	ICMP ping timeout value in seconds
icmpRetries	INT	The number of ICMP ping retries to perform

Column Name	Data Type	Description
defaultProtoMask	INT	Defines if this system uses defaults (Global protocol settings) for some or all protocols or its individual settings (This is a bitmask field where the different bits define what defaults are to be used. The values are logically ordered together: 1 = use the default SNMP read community, 2 = use the default SNMP write community, 4 = use the default SNMP timeout, 8 = use the default SNMP retries, 16 = use the default icmp timeout, 32 = use the default ICMP retries, 64 = use the default WBEM user name, 128 = use the default WBEM password)



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

HP_Cluster table

Column Name	Data Type	Description
HPCluster_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParCell
SnapshotID	BIGINT	Snapshot partly identifies HP_NParCell
MembershipIncarnation	BIGINT	An integer value used to uniquely identify the cluster membership (A change in the membership of the cluster results in an increase in the MembershipIncarnation. Thus, a higher value of this property indicates a more recent set of cluster members (found by following the HP_ParticipatingCS associations.)
Name	NVARCHAR(256)	A label by which the object is known
Interconnect	NVARCHAR(256)	A free-form string that describes the interconnection mechanism for the cluster
dc_Types	NVARCHAR(256)	The cluster types (This specifies whether the cluster is for failover (value=2), performance (3), and so on. The values which can be specified are not mutually exclusive. ValueMap { "0", "1", "2", "3", "4", "5", "6" } Values { "Unknown", "Other", "Failover", "Performance", "Distributed OS", "Node Grouping", "SysPlex" })

HP_Node table

Column Name	Data Type	Description
HPNode_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_Node
SnapshotID	BIGINT	Snapshot partly identifies HP_Node
Name	NVARCHAR(256)	A label by which the object is known
Membername	NVARCHAR(256)	Describes the name for this member in the generic HP cluster (The inherited Name value must be fully qualified and unique within the enterprise, while the MemberName value can be an abbreviated version unique within the cluster.)
MemberID	INT	An integer value uniquely identifying this cluster member in the generic HP Cluster; assigned when the system is first added to the cluster and remains unchanged until the system is removed from the cluster (when this instance is deleted) (If the member is re-added later to the cluster, a new instance is created, with a different MemberID value.)

HP_NParCabinet table

Column Name	Data Type	Description
NParCabinet_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParCell
SnapshotID	BIGINT	Snapshot partly identifies HP_NParCell
CabinetType	INT	Values are: Unknown(0), Other(1), 8-cell full height cabinet(2), 4-cell full height cabinet(3), 4-cell half-height cabinet(4), 2-cell cabinet(5), I/O expansion cabinet(6). Examples of these cabinet types: 8-cell full height cabinet (SD-32000), 4-cell full-height cabinet (SD-16000), 4-cell half-height cabinet (rp8620), 2-cell cabinet (rx7620)
Label	NVARCHAR(256)	Display string containing the cabinet number, for example <i>cab0</i>
ServiceProcessorCount	NVARCHAR(256)	Number of service processors in this cabinet
ServiceProcessorLocation	NVARCHAR(1024)	Array of long display names for the location of service processors in this cabinet (On cabinets where the service processor is location on a core I/O card, it will include a specification of which card, for example <i>cab0, coreio0</i>)
ServiceProcessorStatus	NVARCHAR(256)	Array of status of any service processors in this cabinet, in the same order as ServiceProcessorLocation; values are: Unknown(0), Other(1), Active(2), Backup(3)

HP_NParCell table

Column Name	Data Type	Description
NParCell_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParCell
SnapshotID	BIGINT	Snapshot partly identifies HP_NParCell
SlotID	INT	The ID of the slot the NPar Cell resides in
TotalMemoryInstalled	BIGINT	Total memory (MB) installed in the cell
MaxCPUCount	INT	Maximum CPU count
MaxCPUCount	INT	The maximum number of processors supported on this cell, accounting for both the number of processor module slots and the maximum number of processors per module supported by this platform (The value might not reflect the maximum number of processors in this cell given the number of processor per module actually installed. The maximum number of processors per module supported by this system can be computed by dividing this value by CPUModuleSlotCount.)
CPUCount	SMALLINT	The actual number of processors on this cell
CPU Speed	INT	The clock speed in megahertz of the processors on the cell
FirmwareRevision	NVARCHAR(256)	Displayable firmware revision string
DIMMSlotPopulated	NVARCHAR(256)	Array, indexed by DIMM slot number, indicating whether the slot contains a DIMM (Note: This property might not be available when the cell is powered off.)
CPUSlotPopulated	NVARCHAR(256)	Array, indexed by processor slot number; true when the processor slot is populated (Note that the processor slot number divided by the CPUCountPerModule gives the processor module slot number. All processor slots where that value is equal are in the same processor module.)
ConnectedToIOChassis	BIT	True if this cell is connected to an IO chassis
ConnectedIOChassisId	INT	I/O Chassis ID of the chassis to which the cell is connected (The property is not present if ConnectedToIOChassis is false.)

Column Name	Data Type	Description
CellArchitecture	SMALLINT	The architecture of the processors on this cell; values are Unknown(0), Other(1), PA-RISC(2) and Itanium®-based(3)
ComponentStatus	SMALLINT	Status of this component; values are: Unknown(0), Other(1), Powered Off(2), Powering On(3), Inactive(4), Active(5) (A component is powering on when power has been turned on, but it is still performing power-on self-tests (POST). A component is Inactive if it has completed POST, but has not joined its nPartition. This might be because the component is not assigned to a nPartition, if it is assigned to a nPartition and the nPartition is not active, if the component failed during nPartition boot, if the component was assigned to an active nPartition and no reboot or shut down for reconfiguration of the nPartition has been done, or the component has been configured to remain inactive when the nPartition boots. A component is active when it has joined a nPartition during boot. Note that the status of the component does not imply anything about the state of the operating system on the nPartition. The component will be active, for example, while the operating system is still in the boot process. The status is Unknown if a failure occurred while getting the data for this component.)
CPUCountOK	SMALLINT	The number of installed processors that are configured for use. Processors may be deconfigured by the OS or by system firmware. Note: This property may not be available when the cell is powered off.
TotalMemoryOK	BIGINT	Amount of functional memory installed on the cell, in megabytes. Note: This property may not be available when the cell is powered off.
CellType	SMALLINT	Identifies the type of each cell. Possible values are Unknown (0), Other (1), Floating (2), Base(3), and Free(4). User settable.
dc_PartitionID	INT	Partition ID of the nPartition in to which this cell is assigned.
R_SlotInCab	NVARCHAR(255)	
R_SlotID	NVARCHAR(255)	
R_SlotInCab	NVARCHAR(255)	

HP_NParComplex table

Column Name	Data Type	Description
NParComplex_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParComplex
SnapshotID	BIGINT	Snapshot partly identifies HP_NParComplex
ProfileID	INT	Profile ID of the NPar Complex
dc_ComputeCabCount	INT	Number of compute cabinets in the complex
dc_IOXCabCount	INT	Number of IOX cabinets in the complex
ComplexName	NVARCHAR(256)	Name of the NPar Complex
RevisionString	NVARCHAR(256)	Displayable revision string
MaxPartitionsSupported	SMALLINT	The maximum number of nPartitions that this complex can support (For example, an rp7410 system can support no more than 2 nPartitions.)
CreatorSerialNumber	NVARCHAR(256)	The serial number of the complex as assigned by the original manufacturer

Column Name	Data Type	Description
CreatorProductName	NVARCHAR(256)	The name of the product as assigned by the OEM manufacturer (This property is supported only on Itanium®-based platforms but might not be present on all of those.)
OEMSerialNumber	NVARCHAR(256)	The name of the product as assigned by the OEM manufacturer (This property is supported only on Itanium®-based platforms but might not be present on all of those.)
OEMSerialNumber	NVARCHAR(256)	The serial number of the complex as assigned by an OEM manufacturer (This property might not be supported on all platforms.)
OEMProductName	NVARCHAR(256)	The name of the product as assigned by the OEM manufacturer (This property is supported only on Itanium®-based platforms but might not be present on all of those.)
OriginalProductOrderNumber	NVARCHAR(256)	The product order number for this complex as originally delivered, for example, AxxxxxA (If the complex has been upgraded, this is the product order number before the upgrade.)
CurrentProductOrderNumber	NVARCHAR(256)	The product order number for this complex as it current exists (If the complex has been upgraded, this is the product order number after the upgrade.)
UUID	NVARCHAR(128)	A 16-byte value used for software licensing (This property might not be supported on all platforms.)
CellAssignments	NVARCHAR(256)	Array of values, indexed by cell ID; provides the nPartition ID of the nPartition in to which this cell is assigned or 255 if the cell has type equal to Free, user settable (On iCOD systems, requires iCOD software approval to modify.)
ProductName	NVARCHAR(256)	Product Name of the System. For example, 9000/800/SD32A
dc_InactiveCells	INT	Number of Inactive Cells in this Complex
dc_CellSlots	INT	Cell slots
cellUsageRights	INT	Cell Usage Rights, which represents authorized cells
coreUsageRights	INT	Core Usage Rights, which represents authorized cores
cellsWithoutUsageRights	INT	Cells Without Usage Right, which represents iCAP cells
coresWithoutUsageRights	INT	Cores without Usage Rights, which represents iCAP cores/entry
iCAPCompliant	Nvarchar(5)	iCAPCompliant column value is derived from cellCompliant and cpuCompliant properties. iCAPCompliant = cellCompliant && cpuCompliant
dc_AvailableCellSlots	INT	Available cell slots

HP_NParIOChassis table

Column Name	Data Type	Description
NParIOChassis _LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParIOChassis
SnapshotID	BIGINT	Snapshot partly identifies HP_NParIOChassis
ConnectedCellID	INT	ID of the cell
PopulatedPCISlotCount	SMALLINT	Number of occupied PCI slots in this chassis.

HP_NParIOChassisSlot table

Column Name	Data Type	Description
NParIOChassisSlot_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParChassisIOSlot
SnapshotID	BIGINT	Snapshot partly identifies HP_NParChassisIOSlot
ID	INT	ID of the NPar I/O Chassis Slot
CabinetID	INT	ID of the cabinet in which the I/O Chassis belongs
IOBayNumber	INT	Bay number in the cabinet where the I/O Chassis resides
Number	INT	The I/O Chassis number that is unique across the bay

HP_NparPartition table

Column Name	Data Type	Description
NParPartition_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HP_NParPartition
SnapshotID	BIGINT	Snapshot partly identifies HP_NParPartition
PartitionID	INT	ID of the NPar Partition
dc_TotalCPU	INT	Total CPUs in the NPar Partition
dc_InstalledCells	INT	Number of installed cells in the NPar Partition
dc_PoweredOnCells	INT	Number of powered on cells of the NPar Partition
PartitionName	NVARCHAR(256)	Name of the NPar Partition
dc_CoreCell	INT	Core cell Index in the NPar Partition
dc_CoreCellCabinet	INT	Core cell Index in the Cabinet of the NPar Partition
dc_HasInterleaveMem	INT	Flag to indicate if the NPar Partition has Interleave Memory configured (1 = yes)
R_dc_HasInterleaveMemory	NVARCHAR(256)	A field used by reporting
PartitionNameLabel	NVARCHAR(256)	Concatenation of the nPartition name and its label, for example, "MyPartition (par2)"
PartitionType	SMALLINT	Type of cells in this nPartition; values are Unknown(0), Other(1), PA-RISC(2) and Itanium®-based(3)
PartitionsDefined	BOOLEAN	True if this partition currently exists (has been configured in the complex), otherwise false
CoreCellID	INT	The cell ID of the core cell for this nPartition, or 255 if the nPartition is not booted
PrimaryBootPath	NVARCHAR(256)	The primary boot path for this nPartition; present and settable when BootPathsAreAvailable is true, user-settable
AlternateBootPath	NVARCHAR(256)	The alternate boot path for this nPartition; present and settable for all nPartitions on PA-RISC platforms, but is present and settable only for the nPartition on which the provider is running on Itanium®-based platforms, user-settable
HAAlternateBootPath	NVARCHAR(256)	The HA alternate boot path for this nPartition; present and settable when BootPathsAreAvailable is true, user-settable
R_CoreCellCabinet	NVARCHAR(256)	Cabinet number associated with the core cell
dc_ActiveCells	INT	Number of active cells in this partition
R_CoreCellCabinet	NVARCHAR(255)	Used for reporting to display the core cell cabinet

HPUX_BaseKernelParameter table

Column Name	Data Type	Description
BaseKernelParameter_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_BaseKernelParameter
SnapshotID	BIGINT	Snapshot partly identifies HPUX_BaseKernelParameter
BaseKernelParameterID	INT	BaseKernelParameterID partly identifies HPUX_BaseKernelParameter. Index of Kernel Configure Group
settingID	NVARCHAR(256)	Name of the kernel configure parameter
CurrentValue	NVARCHAR(256)	Value of the kernel configure parameter

HPUX_Bundle table

Column Name	Data Type	Description
Bundle_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_Bundle
SnapshotID	BIGINT	Snapshot partly identifies HPUX_Bundle
IdentifyingNumber	NVARCHAR(64)	Inherited from CIM_Product.IdentifyingNumber; product identification such as a serial number in software, a die number on a hardware chip, or a project number
Version	NVARCHAR(64)	Inherited from CIM_Product.Version; product version information; corresponds to the Version property in the Product object in the DMTF Solution Exchange Standard
Vendor	NVARCHAR(256)	Inherited from CIM_Product.Vendor; the name of the Product's supplier, or entity selling the Product (the manufacturer, reseller, OEM); corresponds to the Vendor property in the Product object in the DMTF Solution Exchange Standard
Name	NVARCHAR(256)	Inherited from CIM_Product.Name; commonly used product name
Architecture	NVARCHAR(64)	Local to HPUX_Bundle; a vendor-defined string used to distinguish variations of a product (It is used for presentation purposes and for resolving software specifications. If a product with the same value of the Revision and Vendor Tag attributes has different versions of software for different target architectures or any other variation (such as supportedlocale), then the value of the architecture attribute is different for each version. No additional semantics are assumed for its value.)
Location	NVARCHAR(256)	Location is of HPUX_Bundle; local to HPUX_Bundle; used for resolving software specifications for installed software. A specific product location refers to all filesets of that product that are installed at that location (This is the path beneath which the relocatable files of that product are stored.)
QualifierID	NVARCHAR(64)	Local to HPUX_Bundle; specified by a user when installing software and used for identifying a product (or set of product versions) using a logical name
CreateTime	BIGINT	Local to HPUX_Bundle; a value set by the implementation to be the time that the catalog information for this object was first written; stored as MS since the Epoch
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; the Description property provides a textual description of the object
ModificationTime	BIGINT	Local to HPUX_Bundle; a value set by the implementation to be the time that the catalog information for this object was last written; stored in MS since the Epoch

Column Name	Data Type	Description
Size	NVARCHAR(32)	Local to HPUX_Bundle; the sum of the sizes in bytes of all files and control files contained within the software object (For objects other than filesets, the value is computed dynamically as required.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; the Caption property is a short textual description of the object
Copyright	NVARCHAR(256)	Local to HPUX_Bundle; the copyright notice for the bundle
Directory	NVARCHAR(256)	Local to HPUX_Bundle; the vendor-defined directory commonly associated with the product (Generally, this is the directory in or below which all (or mostly all) files within the product are installed. For a product that has filesets with the Is Locatable attribute equal to true, all files that contain this directory as the first part of their path can be relocated to the Location Directory during installation by replacing the product.directory portion with the product.location.)
InstanceIdentifier	NVARCHAR(16)	Local to HPUX_Bundle; a single attribute that distinguishes versions of products (and bundles) with the same Tag (It is a simple form of the version distinguishing attributes, valid only within the context of an exported catalog.)
IsLocatable	bit	Local to HPUX_Bundle; a Boolean value indicating whether any of the filesets in the product have the Is Locatable attribute set to true
LayoutVersion	NVARCHAR(64)	Local to HPUX_Bundle; this attribute and its value, are included for future use
MachineType	NVARCHAR(64)	Local to HPUX_Bundle; a software pattern matching string describing valid machine members of the uname structure as defined by POSIX.1 (2) section 4.4.1 (It is used for determining compatibility.)
SKUNumber	NVARCHAR(64)	Inherited from CIM_Product.SKUNumber; product SKU information
OperatingSystemName	NVARCHAR(256)	Local to HPUX_Bundle; a software pattern matching string describing valid sysname members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemRelease	NVARCHAR(256)	Local to HPUX_Bundle a software pattern matching string describing valid release members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemVersion	NVARCHAR(64)	Local to HPUX_Bundle; a software pattern matching string describing valid version members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
ISPatch	bit	Local to HPUX_Bundle; a Boolean value indicating whether this software object is a patch
InstallSource	NVARCHAR(256)	Local to HPUX_Bundle; location of source from where software was installed
DataModelRevision	Nvarchar(64)	Local to HPUX_Bundle; supplies information on version of POSIX compatibility and corresponds to the operating system release that packaged or installed the software
InstallDate	BIGINT	Local to HPUX_Bundle; date timestamp of day, month, year and time when the software was installed on the system; stored as MS since the Epoch
Contents	NVARCHAR(256)	Local to HPUX_Bundle; the Fileset Software Specification of the bundle's content

HPUX_DNSService table

Column Name	Data Type	Description
DNSService_LUID	BIGINT	LUID uniquely defining this table row

Column Name	Data Type	Description
NodeID	BIGINT	Node partly identifies HPUX_DNSService
SnapshotID	BIGINT	Snapshot partly identifies HPUX_DNSService
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	Equates to CIM_ComputerSystem.Name were NodeID is equal
Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; the Name property defines the label by which the object is known
SearchList	NVARCHAR(512)	The search list for host-name lookup; this attribute and Domain Name attribute are mutually exclusive
Addresses	NVARCHAR(512)	Specifies the IP addresses in dot notation format of the name server that the resolver should search (It can list up to 9 name servers. These names are space delimited.)

HPUX_Fileset table

Column Name	Data Type	Description
Fileset_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_Fileset
SnapshotID	BIGINT	Snapshot partly identifies HPUX_Fileset
SoftwareElementID	BIGINT	Inherited from CIM_SoftwareElement.SoftwareElementID; this is an identifier for the SoftwareElement and is designed to be used in conjunction with other keys to create a unique representation of the element
Name	NVARCHAR(256)	Inherited from CIM_SoftwareElement.Name; the name used to identify this software element
Version	NVARCHAR(64)	Inherited from CIM_SoftwareElement.Version; Software Version should be in the form <Major>.<Minor>.<Revision> or <Major>.<Minor><letter><revision>
TargetOperatingSystemName	SMALLINT	Inherited from CIM_SoftwareElement.TargetOperatingSystemName (Uses CIM_OperatingSystem.OSType enumeration: 0 = Unknown, 1 = Other, 2 = MACOS, 3 = ATTUNIX, 4 = DGUX, 5 = DECNT, 6 = Digital Unix, 7 = OpenVMS, 8 = HPUX, 9 = AIX, 10 = MVS, 11 = OS400, 12 = OS/2, 13 = JavaVM, 14 = MSDOS, 15 = WIN3x, 16 = WIN95, 17 = WIN98, 18 = WINNT, 19 = WINCE, 20 = NCR3000, 21 = NetWare, 22 = OSF, 23 = DC/OS, 24 = Reliant UNIX, 25 = SCO UnixWare, 26 = SCO OpenServer, 27 = Sequent, 28 = IRIX, 29 = Solaris, 30 = SunOS, 31 = U6000, 32 = ASERIES, 33 = TandemNSK, 34 = TandemNT, 35 = BS2000, 36 = LINUX, 37 = Lynx, 38 = XENIX, 39 = VM/ESA, 40 = Interactive UNIX, 41 = BSDUNIX, 42 = FreeBSD, 43 = NetBSD, 44 = GNU Hurd, 45 = OS9, 46 = MACH Kernel, 47 = Inferno, 48 = QNX, 49 = EPOC, 50 = IxWorks, 51 = VxWorks, 52 = MiNT, 53 = BeOS, 54 = HP MPE, 55 = NextStep, 56 = PalmPilot, 57 = Rhapsody, 58 = Windows 2000, 59 = Dedicated, 60 = OS/390, 61 = VSE, 62 = TPF, 63 = Windows Me, 64 = Caldera Open UNIX, 65 = OpendBSD, 66 = Not Applicable)
CreateTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was first written.; stored as MS since the Epoch
Description	NVARCHAR(32)	Inherited from CIM_ManagedElement.Description; this property provides a textual description of the object
ModificationTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was last written; stored as MS since the Epoch

Column Name	Data Type	Description
Size	NVARCHAR(32)	The sum of the sizes in bytes of all files and control files contained within the software object (For objects other than filesets, the value is computed dynamically as required.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description of the object
ControlDirectory	NVARCHAR(256)	The name of the fileset control directory below which the control files for the fileset are stored within an exported catalog
ISKernel	bit	A boolean value indicating the fileset requires a kernel rebuild
ISLocatable	bit	A boolean value indicating whether the fileset can be relocated during installation
ISReboot	bit	A boolean value indicating the host on which the fileset is configured should be re-booted
Location	NVARCHAR(256)	Specifies the location below which relocatable files are stored (This attribute is only valid for filesets in installed software. It differs from the product.directory attribute only if relocation was specified during installation.)
MediaSequenceNumber	NVARCHAR(256)	A list of values which identify the medium on which the files for this fileset is found
SoftwareElementState	SMALLINT	An enumeration: 0 = Deployable, 1 = Installable, 2 = Executable, 3 = Running
DataModelRevision	NVARCHAR(64)	Supplies information on version of POSIX compatibility and corresponds to the operating system release that packaged or installed the software
InstancelIdentifier	NVARCHAR(16)	A single attribute that distinguishes versions of products (and bundles and filesets) with the same Tag (It is a simple form of the version distinguishing attributes, valid only within the context of an exported catalog.)
InstallDate	BIGINT	Date timestamp of day, month, year and time when the software was installed on the system; stored as MS since the Epoch
Architecture	NVARCHAR(64)	A vendor-defined string used to distinguish variations of a product; used for presentation purposes and for resolving software specifications (If a product with the same value of the Revision and Vendor Tag attributes has different versions of software for different target architectures or any other variation (such as supported locale), then the value of the architecture attribute shall be different for each version. No additional semantics are assumed for its value.)
MachineType	NVARCHAR(64)	A software pattern matching string describing valid machine members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemName	NVARCHAR(64)	A software pattern matching string describing valid sysname members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemRelease	NVARCHAR(256)	A software pattern matching string describing valid release members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
OperatingSystemVersion	NVARCHAR(64)	A software pattern matching string describing valid version members of the uname structure as defined by POSIX.1 (2)Use t section 4.4.1 (It is used for determining compatibility.)
InstallSource	NVARCHAR(128)	Location of source from where software was installed
ISPatch	bit	A Boolean value indicating whether this software object is a patch

Column Name	Data Type	Description
ISSparse	bit	Denotes a fileset that is not complete, but one that has been qualified as an update (as opposed to a patch) (One outcome of updating through a sparse fileset is that the catalog information from the old fileset is merged into the new fileset and the old fileset is then removed, leaving the system in the same state as it would be after an update of a full fileset. This option should be used in conjunction with an ancestor attribute showing exactly which versions of software this sparse fileset can update. Filesets that are sparse are only useful when installed along with those versions or when those versions are already installed.)
PatchState	NVARCHAR(16)	Only applied to installed patches; characterizes the current state of an installed patch
AppliedPatches	NVARCHAR(256)	Only applicable to installed patches; specifies the software on which this patch fileset has been applied
SupersededBy	NVARCHAR(256)	Lists what patch superseded this patch
SavedFileDirectory	NVARCHAR(256)	Used by swinstall during the installation of this patch fileset to save the patched files if patch_save_files was set to true at that time (When rolling back or committing this patch, this attribute is used to determine the directory to access those saved files.)



NOTE: WBEM providers is only collected under the Desktop Management Interface (DMI).

HPUX_HFS table

Column Name	Data Type	Description
HFS_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	
SnapshotID	BIGINT	
Name	NVARCHAR(256)	Inherited from CIM_FileSystem.Name; the inherited Name serves as key of a FileSystem instance within a ComputerSystem
CreationClassName	NVARCHAR(256)	Equates to HPUX_HFS
CSCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
CSName	NVARCHAR(256)	Equates to CIM_ComputerSystem.Name where NodeID is equal
Root	NVARCHAR(256)	Inherited from CIM_FileSystem.Root; path name or other information defining the root of the FileSystem
ReadOnly	bit	Inherited from CIM_FileSystem.ReadOnly; indicates that the FileSystem is designated as read only
FileSystemType	NVARCHAR(256)	Inherited from CIM_FileSystem.FileSystemType; string describing the type of FileSystem and its conventions (For example, \\\"NTFS\\\" or \\\"S5\\\" can be as well as any additional information on the FileSystem implementation. Because various flavors of FileSystems (like S5) exist, this property is defined as a string.)
FileSystemSize	BIGINT	Inherited from CIM_FileSystem.FileSystemSize; the total size of the File System in bytes (If unknown, enter 0.)
BlockSize	BIGINT	Inherited from CIM_FileSystem.BlockSize.The FileSystem's block size for data storage and retrieval
AvailableSpace	BIGINT	Inherited from CIM_FileSystem.AvailableSpace; the total amount of free space for the FileSystem, in bytes
RemoteFileSystem_Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; a label by which an object is known

Column Name	Data Type	Description
Freelnodes	BIGINT	Inherited from CIM_UnixLocalFileSystem.FreelNodes; the number of free inodes present in the file system
Totalnodes	BIGINT	Inherited from CIM_UnixLocalFileSystem.TotalNodes; the total number of inodes available in the file system. 0 indicates this file system does not have a preset limit
FSReservedCapacity	BIGINT	Inherited from CIM_UnixLocalFileSystem.FSReservedCapacity; the reserve data capacity of the file system in bytes
Bootable	bit	Indicates whether a file system is a bootable
LargeFileSupported	bit	Indicates that this file system supports large files
MinimumFreespace	bit	Indicates the minimum percentage of free disk spaces allowed
FragmentSize	INT	Specifies the fragment block size of this file system
InodeSize	INT	Specifies the density of Inodes in this file system
SectorsPerTrack	INT	The number of sectors per track on the disk
TracksPerCylinder	INT	Specifies the number of tracks per cylinder on the disk
DiskCylindersPerCylinderGroup	INT	Specifies the number of disk cylinders per cylinder group
DiskRevolutionsPerSecond	INT	Specifies the number of disk revolutions per second
RotationalDelay	INT	Specifies the expected time in MS to service a transfer completion interrupt and initiate a new transfer on the same disk
dc_MountedFileSystems	INT	The total number of currently mounted file systems

HPUX_LogicalVolume table

Column Name	Data Type	Description
LogicalVolume_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_LogicalVolume
SnapshotID	BIGINT	Snapshot partly identifies HPUX_LogicalVolume
Name	NVARCHAR(256)	Name of Logical Volume in the System
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the Logical Device
Access	SMALLINT	Inherited from CIM_StorageExtent.Access; describes whether the media is readable, writeable, or both (An enumeration: 0 = Unknown, 1 = Readable, 2 = Writeable, 3 = Read/Write Supported, 4 = Write Once)
LogicalExtentSize	BIGINT	Computed by multiplying HPUX_LogicalVolume.BlockSize by HPUX_LogicalVolume.NumberOfBlocks
Capacity	BIGINT	Capacity of logical volume in number of logical extent
MirrorCopyNumber	INT	Number of the mirrored Copy for the logical volume
ConsistencyRecovery	NVARCHAR(64)	Consistency Recovery Method for the mirrored logical volume. No value for NOT mirrored Logical Volume (MWC, NOMWC, NONE)
SchedulePolicy	NVARCHAR(64)	Access Scheduling Policy of the logical volume; might have values such as (Striped, Sequential, Parallel)
NumberOfStripes	INT	Number of stripes for the logical volume
StripeSize	INT	Size of stripes for logical volume; value in KB
BadBlockRelocation	BIT	Switch of Bad Block Relocation feature; true if it is on, false otherwise

Column Name	Data Type	Description
AllocationPolicy	NVARCHAR(64)	Allocation Policy of the logical volume; might contain values such as (Non-Strict, Non-Strict/Contiguous, Strict, Strict/Contiguous, PVG-Strict, PVG-Strict/Contiguous, PVG-Strict/Distributed, Unknown)
StaledLogicalExtent	INT	Counter of staled Logical Extent in the logical volume; valid only the logical volume is mirrored
NumberReadAccesses	INT	Number of read accesses to the logical volume
NumberWriteAccesses	INT	Number of write accesses to the logical volume
Status	NVARCHAR(64)	Availability status of Logical Volume; might contain values such as (Available/State, Available/Syncd, Available, Unavailable)

HPUX_NISServerService table

Column Name	Data Type	Description
NISServerService_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_NISServerService
SnapshotID	BIGINT	Snapshot partly identifies HPUX_NISServerService
Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; the Name property defines the label by which the object is known
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	Equates to CIM_ComputerSystem.Name where NodeID is equal
CreationClassName	NVARCHAR(256)	Equates to HPUX_NISServerService
ServerWaitFlag	SMALLINT	The NIS Server Wait Flag; makes the host wait for a response for the NIS server (An enumeration: 0 = Unknown, 1 = Other, 2 = Wait, 3 = No Wait)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description of the object
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; provides a textual description of the object
ServerType	SMALLINT	Returns what type of NIS Server the managed system is; if the system is not a NIS server, returns None (An enumeration: 0 = Unknown, 1 = Other, 2 = None, 3 = NIS Master, 4 = NIS Slave)

HPUX_NTPTService table

Column Name	Data Type	Description
NTPTService_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_NTPTService
SnapshotID	BIGINT	Snapshot partly identifies HPUX_NTPTService
SystemCreationClassName	NVARCHAR(256)	Equates to CIM_ComputerSystem
SystemName	NVARCHAR(256)	Equates to the value of CIM_ComputerSystem.Name where NodeID is equal
CreationClassName	NVARCHAR(256)	Equates to HPUX_NTPTService
Name	NVARCHAR(256)	Inherited from CIM_ManagedSystemElement.Name; the Name property defines the label by which the object is known
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; a short textual description of the object

Column Name	Data Type	Description
ServerAddress	NVARCHAR(512)	This attribute is specified by host name that appears in the file <code>/etc/hosts</code> , or it is an IP Address in dot notation format (Multiple servers are specified as comma delimited names.)
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; provides a textual description of the object

HPUX_PhysicalVolume table

Column Name	Data Type	Description
PhysicalVolume_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_PhysicalVolume
SnapshotID	BIGINT	Partly identifies HPUX_PhysicalVolume
Name	NVARCHAR(256)	Name of Physical Volume in the System
DeviceID	NVARCHAR(64)	Inherited from CIM_LogicalDevice.DeviceID; an address or other identifying information to uniquely name the LogicalDevice (Might return the name of the physical volume. For example, <code>/dev/dsk/c0t0d0</code> .)
AlternatePVName	NVARCHAR(256)	Can return alternate physical volume path name (For example, <code>/dev/rdisk/c0t0d0</code> ; returns the same as DeviceID replacing "dsk" for "rdsk")
Status	NVARCHAR(32)	Availability status of Physical Volume. Returns (Available; Unavailable).
PhysicalExtentSize	BIGINT	Size in bytes; calculated by multiplying HPUX_PhysicalVolume.BlockSize by the HPUX_PhysicalVolume.NumberOfBlocks
Capacity	BIGINT	Capacity of the whole Physical Volume in number of Physical Extent
Allocated	INT	Size of the allocated Physical Volume in number of Physical Extent
Free	INT	Size of the free Physical Volume space in number of Physical Extent
NumberStaledPEs	INT	Counter of Staled Physical Extent in the Physical Volume

HPUX_Product table

Column Name	Data Type	Description
Product_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_Product
SnapshotID	BIGINT	Snapshot partly identifies HPUX_Product
IdentifyingNumber	NVARCHAR(64)	Inherited from CIM_Product.IdentifyingNumber; product identification such as a serial number on software, a die number on a hardware chip, or a project number
Name	NVARCHAR(256)	Inherited from CIM_Product.Name; commonly used Product name
Version	NVARCHAR(64)	Inherited from CIM_Product.Version; a vendor-defined string describing the revision of the product
Vendor	NVARCHAR(256)	Inherited from CIM_Product.Vendor; the name of the product supplier or entity selling the product (the manufacturer, reseller, or OEM)

Column Name	Data Type	Description
Architecture	NVARCHAR(64)	A vendor-defined string used to distinguish variations of a product (It is used for presentation purposes and for resolving software specifications. If a product with the same value of the revision and Vendor Tag attributes has different versions of software for different target architectures or any other variation (such as supported locale), then the value of the architecture attribute is different for each version. No additional semantics are assumed for its value.)
Location	NVARCHAR(256)	Used for resolving software specifications for installed software (A specific product location refers to all filesets of that product that are installed at that location. This is the path beneath which the relocatable files of that product are stored.)
QualifierID	NVARCHAR(64)	Specified by a user when installing software and used for identifying a product (or set of product versions) using a logical name
CreateTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was first written; stored as MS since the Epoch
Description	NVARCHAR(512)	Inherited from CIM_ManagedElement.Description; the Description property provides a textual description of the object
ModificationTime	BIGINT	A value set by the implementation to be the time that the catalog information for this object was last written; stored as MS since the Epoch
Size	NVARCHAR(32)	The sum of the sizes in bytes of all files and control files contained within the software object (For objects other than filesets, the value is computed dynamically as required.)
Caption	NVARCHAR(64)	Inherited from CIM_ManagedElement.Caption; is a short textual description of the object
AllFileSets	NVARCHAR(256)	Contains the actual filesets that make up a product (This is a list of all filesets defined for the product, as opposed to what is currently installed, described by the filesets attribute. The all_filesets attribute is used to determine completeness of this product when another software object has a dependency on this product. In checking a product prerequisite or corequisite, the existence of a fileset.tag in all_filesets that is not actually installed or available indicates that the dependency is not satisfied. This does not affect prerequisites because they test whether any of the contents of the dependency specification are present instead of all of the contents tested for prerequisites or corequisites.)
ControlDirectory	NVARCHAR(256)	The name of the product control directory below which the control files for the product are stored within an exported catalog
Copyright	NVARCHAR(256)	The copyright notice for the product
Directory	NVARCHAR(256)	The vendor-defined directory commonly associated with the product (Generally, this will be the directory in or below that all (or mostly all) files within the product are installed. For a product which has filesets with the Is Locatable attribute equal to true, all files which contain this directory as the first part of their path can be relocated to the Location Directory during installation by replacing the product.directory portion with the product.location.)
InstanceIdentifier	NVARCHAR(16)	A single attribute that distinguishes versions of products (and bundles) with the same Tag (It is a simple form of the version distinguishing attributes, valid only within the context of an exported catalog.)
ISLocatable	bit	A boolean value indicating whether any of the filesets in the product have the Is Locatable attribute set to true

Column Name	Data Type	Description
PostKernelPath	NVARCHAR(256)	The path to the script that is run after the kernel filesets have been installed. Any product containing kernel filesets should include this path (If this attribute is supplied, the corresponding script is executed if it exists relative to the root directory of the installed software. If this attribute is not supplied, then the implementation defined path (the default value for the attribute) is used if it exists relative to the root directory of the installed software. Note that the use of an alternative root directory might mean that the default path does not exist relative to the root directory of the installed software.)
LayoutVersion	NVARCHAR(64)	This attribute and its value, are included for future use
MachineType	NVARCHAR(64)	A software pattern matching string describing valid machine members of the uname structure as defined by POSIX.1 (2), section 4.4.1 (It is used for determining compatibility.)
SKUNumber	NVARCHAR(64)	The semantics associated with the values of this attribute are undefined; can be used to store such vendor-defined values as part number, order number, or serial number
OperatingSystemName	NVARCHAR(256)	A software pattern matching string describing valid sysname members of the uname structure as defined by POSIX.1 (2), section 4.4.1; used for determining compatibility
OperatingSystemRelease	NVARCHAR(256)	A software pattern matching string describing valid release members of the uname structure as defined by POSIX.1 (2), section 4.4.1; used for determining compatibility
OperatingSystemVersion	NVARCHAR(64)	A software pattern matching string describing valid version members of the uname structure as defined by POSIX.1 (2), section 4.4.1; used for determining compatibility
ISPatch	bit)	A Boolean value indicating whether this software object is a patch
InstallSource	NVARCHAR(128)	Location of source from where software was installed
DataModelRevision	NVARCHAR(8)	Supplies information on version of POSIX compatibility and corresponds to the operating system release that packaged or installed the software
InstallDate	BIGINT	Date timestamp of day, month, year and time when the software was installed on the system; stored as MS since the Epoch

HPUX_VolumeGroup table

Column Name	Data Type	Description
VolumeGroup_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Node partly identifies HPUX_VolumeGroup
SnapshotID	BIGINT	Snapshot partly identifies HPUX_VolumeGroup
CollectionID	NVARCHAR(64)	Inherited from CIM_DiskGroup.CollectionID; the identification of the Collection object
Name	NVARCHAR(256)	Name of Volume Group in the System
AccessPermission	NVARCHAR(64)	Access Permission of Volume Group in the System; can be one of the following (Read-Only; Read-Write)
Status	NVARCHAR(32)	Availability status of Volume Group in the System; can be one of the following values (Available; Unavailable)
PhysicalExtentSize	INT	The size of the fundamental physical extent size in bytes
Capacity	INT	Capacity of whole Volume Group in number of Physical Extent
Allocated	INT	Allocated space in the volume group in number of Physical Extent

Column Name	Data Type	Description
FreeSpace	INT	Number of free Physical Extents in the volume group
MaxNumberOfPVs	INT	Max number of definable physical volume in the volume group
NumberOfDefinedPVs	INT	Number of max allocatable Physical Extent from physical volume
NumberOfActivePVs	INT	Number of current defined physical volume in the volume group
MaxNumberOfLVs	INT	Max number of definable logical volume in the volume group
NumberOfDefinedLVs	INT	Number of current defined logical volume in the volume group
NumberOfActiveLVs	INT	Number of current active logical volume in the volume group
NumberOfPVGroups	INT	Total number of physical volume group in this volume group

HPVM_Guest table

Column Name	Data Type	Description
HPVM_Guest_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies HPVM_Guest
SnapshotID	BIGINT	Partly identifies HPVM_Guest
Name	NVARCHAR(256)	Displays the name of the host
GuestID	SMALLINT	Displays the Guest ID
HostUUID	NVARCHAR(255)	The UUID of the VM Host
ExpectedOperatingSystemType	SMALLINT	Displays the expected OS type
ProcessorCount	SMALLINT	Displays the number of virtual processors
ElementName	NVARCHAR(256)	Displays a user-defined name for this guest
MemorySize	BIGINT	The amount of memory assigned to this guest in units defined by MemorySizeUnits. The value cannot exceed the amount of memory installed on the host system.
MemorySizeUnits	SMALLINT	The units used for the MemorySize property.
r_MemorySize	BIGINT	Used by Reporting to display the memory size
ProcessorEntitlement	REAL	The amount of physical processor resources to which each virtual processor in this guest is entitled in units defined by ProcessorEntitlementUnits
ProcessorSpeed	REAL	The effective speed of the physical processors used by this guest in MegaHertz. The following relationship is always true: $ProcessorSpeed * ProcessorEntitlement (in percent) / 100 = ProcessorEntitlement (in MegaHertz)$.
ProcessorEntitlementUnits	SMALLINT	The units for the ProcessorEntitlement property. If <i>Percent</i> , then the entitlement is the percentage of a single physical processor that each virtual processor in this guest. If <i>Cycles</i> , then the value is the number of host processor cycles per second allocated to each virtual processor in this guest.
ProcessorEntitlementSubUnits	SMALLINT	Displays the SubUnits
r_CPUEntitlement	NVARCHAR(256)	Used by Reporting to display CPU Entitlement

HPVM_Host table

Column Name	Data Type	Description
HPVM_Host_LUID	BIGINT	LUID uniquely defining this table row
NodeID	BIGINT	Partly identifies HPVM_Host
SnapshotID	BIGINT	Partly identifies HPVM_Host
Name	NVARCHAR(256)	Displays the name of the host
HPVMVersion	NVARCHAR(256)	Displays the HPVM version
UUID	NVARCHAR(256)	The UUID for this system. If the Role is "Guest", then this value can be used to correlate the system on which this provider is running to an instance of an instance of HPVM_Guest from the Integrity Virtual Machine (HPVM) provider on a host system. Note that the identity of the host system is not directly known to the guest.
VMHostUUID	NVARCHAR(256)	Displays the UUID of the VM host
VMHostIPAddress	NVARCHAR(256)	Displays the Ip address of the VM host

IPAddress table

The IPAddress table contains the known IP addresses for the devices. The IPAddress fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	Associates a system, with its collected set of data; system information is linked to the device table using the DeviceKey
*ipindex	INT	The addresses index for the system, for example, 0 is the first IP address. 1 is the second and and so on
*IPAddress	CHAR (16)	TCP/IP address (x.x.x.x)
IPAddressNumber	bigint	A numeric representation of the IP address
MACaddr	CHAR (12)	The MAC address of the system network card (without and delimiter, such as ":" or "-")
IPsubnetMask	CHAR (16)	The TCP/IP subnet mask (x.x.x.x)
IFType	IFType	The interface type



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

IPProtocolEnd_NetworkPort table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

IPXAddress table

The IPXAddress table contains the known IPX addresses for the systems. The IPXAddress fields are defined in the following table.

Column Name	Data Type	Description
*DeviceKey	INT	Associates a system with its collected set of data; system information is linked to the devices table using the DeviceKe
*IpxIndex	INT	A unique IPX index for the system used mainly when 2 or more IPX addresses exist for a system
*IPXAddress	CHAR (25)	IPX address for this system



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

OperationalStatus_SVvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	BIGINT	Used for reporting purposes

PhysicalPackage_Product table

Column Name	Data Type	Description
PartComponent	BIGINT	Used for reporting purposes
GroupComponent	BIGINT	Used for reporting purposes

SCSIProtoCont_SCSIProtoEnd table

Column Name	Data Type	Description
AvailableSAP	BIGINT	Used for reporting purposes
MangedElement	BIGINT	Used for reporting purposes

SCSIProtocolCont_SoftwareId table

Column Name	Data Type	Description
System	BIGINT	Used for reporting purposes
InstalledSoftware	BIGINT	Used for reporting purposes

SCSIProtoEnd_SCSIProtoEnd table

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes

NetworkAddresses_values table

Column Name	Data Type	Description
NetworkAddressesId	BIGINT	Uniquely identifies this row
NetworkAddressesValue	NVARCHAR(64)	Used for reporting purposes
NetworkAddressesPos	INT	Used for reporting purposes

NodeSnapshot table

Column Name	Data Type	Description
Snapshot_LUID	BIGINT	Snapshot partly identifies NodeSnapshot
NodeID	BIGINT	Node partly identifies NodeSnapshot
Tag	NVARCHAR(256)	Contains the user-defined tag
Description	NVARCHAR(512)	Description of the user-defined tag
CollectionDateTime	BIGINT	Stored as MS since the Epoch
DetailedInformation	NVARCHAR(512)	Additional collection status information
ReturnCode	SMALLINT	Binary status information. Zero indicates no error
Status	NVARCHAR(256)	Status of the snapshot for the system; used by different reports
DataAvailable	INT	Currently unused, reserved
FilterID	BIGINT	Currently unused, reserved for collection filter ID

NodeTypesEnum table

Column Name	Data Type	Description
enumOrd	INT	The enumeration identifier for this entry (This can be used when linking in the deviceTypesEnum view. This should also match the productType value in the devices table.)
enumLabel	char(64)	Unique (non displayable) string used for identifying a product type (This is the only value guaranteed to be unique across any installation.)

NodeSubTypesEnum table

Column Name	Data Type	Description
enumOrd	INT	The enumeration identifier for this entry (This can be used when linking in the deviceSubTypesEnum view.)
enumLabel	char(64)	This is a unique (non displayable) string used for identifying a product subtype (This is the only value guaranteed to be unique across any installation. This can be linked to the devices tables productSubType field.)

Notices table

The Notices table contains all the events received or generated, such as Discovered Device events, SNMP traps and so on. The Notices fields are defined in the following table.

Column Name	Data Type	Description
*NoticeId	INT	Unique identifier for this notice instance
State	INT	<ul style="list-style-type: none"> 1=In Progress 2=Not Cleared (active) 5=Cleared
NoticeType	INT	Index into the noticeType table
NoticeSeverity	INT	1 = Normal, 2 = Warning, 3 = Minor, 4 = Major, 5 = Critical, 100 = Informational
NoticePriority	INT	RESERVED
DeviceKey	INT	Index into the devices table

Column Name	Data Type	Description
Generated	bigint	Date/time notice was generated or received represented as the number of milliseconds since 1970 UTC
Cleared	bigint	Date/time notice was cleared represented as the number of milliseconds since 1970 UTC
Completed	bigint	RESERVED
LastChecked	bigint	RESERVED
LastModified	bigint	Date/time notice was cleared represented as the number of milliseconds since 1970 UTC
JobID	char(128)	If this notice is related to some job, this is the job ID for that job
Timestamp	bigint	RESERVED
AssignedTo	VARCHAR(255)	User names to which an event is assigned
Comments	VARCHAR(1000)	User input comments for one or more events



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

NoticeType table

The NoticeType table defines all of the event types that can be processed. The NoticeType fields are defined in the following table.

Column Name	Data Type	Description
*NoticeType	INT	System assigned identifier.
GUID	Char(32)	Unique system assigned identifier
TypeIdStr	CHAR (255)	A unique String Identification for the event
dispHandler	CHAR (255)	Internal handler for the display of the event
rxHandler	Char(255)	Internal handler for event reception, usually blank.
defaultSeverity	Int	A default severity to use for the event
Privilege	Int	The internal privilege level a user must have to view the event details
ServiceEnable	INT	Used when the CRSM is installed
ServiceEnable	INT	Used when the CRSM is installed
ProviderID	INT	Used when the CRSM is installed



NOTE: An asterisk (*) indicates that the field is part of the primary key of the table. Where multiple fields in the same table show an asterisk, the primary key connects to each.

OperationalStatus_CSvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	SMALLINT	Used for reporting purposes
OperationalStatusPos	INT	Used for reporting purposes

OperationalStatus_NPvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	SMALLINT	Used for reporting purposes
OperationalStatusPos	INT	Used for reporting purposes

operationalStatus_PCvalues table

Column Name	Data Type	Description
OperationalStatusId	BIGINT	Used for reporting purposes
OperationalStatusValue	SMALLINT	Used for reporting purposes
OperationalStatusPos	INT	Used for reporting purposes

Snapshot table

Column Name	Data Type	Description
SnapshotID	BIGINT	LUID uniquely defining the snapshot
OverallStatus	NVARCHAR(256)	OverallStatus of the Snapshot: Code indicating if the snapshot was successful
SnapshotTag	NVARCHAR(256)	Contains the user-defined tag
CollectionDateTime	BIGINT	Stored as MS since the Epoch

SPAllocatedFromStoragePool table

Column Name	Data Type	Description
SPAllocFromStoragePool_LUID	BIGINT	LUID uniquely defining the SPAllocFromStoragePool
NodeID	BIGINT	Used for reporting purposes
SnapshotID	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes
SpaceConsumed	BIGINT	Used for reporting purposes

SVAllocatedFromStoragePool table

Column Name	Data Type	Description
SVAllocFromStoragePool_LUID	BIGINT	LUID uniquely defining the SVAllocFromStoragePool
NodeID	BIGINT	Used for reporting purposes
SnapshotID	BIGINT	Used for reporting purposes
Antecedent	BIGINT	Used for reporting purposes
Dependent	BIGINT	Used for reporting purposes
SpaceConsumed	BIGINT	Used for reporting purposes

TCPProtoEnd_IPProtoEnd table

Column Name	Data Type	Description
Antecedent	BIGINT	Used for reporting purposes

Column Name	Data Type	Description
Dependent	BIGINT	Used for reporting purposes

Windows event log

Windows NT/2000 events

HP Systems Insight Manager (HP SIM) can write the following events to the NT Event Log during normal operation.

Event ID	Event Type
1	Error
2	Warning
3	Informational

Windows NT/2000 event log error messages

Message	Description
HP SIM error: NNNN StartServiceCtrlDispatcher failed	An attempt was made to start the HP SIM service with an invalid cmdline argument.
HP SIM error: NNNN SetServiceStatus failed	An error was returned when attempting to acquire status from HP SIM.
HP SIM Application Stopped Abnormally	The HP SIM application has performed an abnormal termination.
SNMP and Snmptrap services required by HP SIM are not installed or not running	The HP SIM service program has detected that SNMP services are not installed or not running and, thus, will not make an attempt to start the HP SIM application. The service program will automatically terminate.
Failed to set SQL Server 'show advanced options' to 1	HP SIM could not configure the database server.
Failed to set SQL Server 'min server memory' to MemorySizeHere MB	HP SIM could not configure the database server.
The SQL Server 'min server memory' is set to MemorySizeHere MB, which is less than the recommended MemorySizeHere MB	HP SIM configured database server memory usage as specified by user.
Failed to set SQL Server 'show advanced options' back to 0	HP SIM could not configure database server.
NoticeDescriptionHere	HP SIM received a security notice.
Modified SQL Server 'min server memory' from 0 to MemorySizeHere MB	HP SIM configured database server memory usage as specified by user.
Attempting to Restart HP SIM Application	The Auto-restart feature of the HP SIM service program is making an attempt to restart the HP SIM application.
HP SIM Application Started	The HP SIM application has been started by the HP SIM service program.
HP SIM Application Stopped	The HP SIM application has performed a normal termination.
HP SIM Application stopped Abnormally	The HP SIM application has performed an abnormal termination.
HP SIM Installation Complete	The HP SIM program has been successfully created and installation of HP SIM is complete.
HP SIM Service Removed	The HP SIM service program has been successfully stopped and removed.
HP SIM Service Started	The HP SIM service program has successfully started.
HP SIM Service Stopped	The HP SIM service program has successfully terminated.

Message	Description
CPU Cluster Monitor Resource	Connectivity problems exist or definable thresholds for CPU utilization have been exceeded.
Disk Cluster Monitor Resource	Connectivity problems exist or definable thresholds for disk capacity have been exceeded.
System Cluster Monitor Resource	Connectivity problems for receiving system information exist.
SNMP and SNMP trap services required by HP SIM are not installed or not running	The HP SIM service program has detected that SNMP services are not installed or not running and, thus, will not make an attempt to start the HP SIM application. The service program will then terminate normally.
DCOM was unable to communicate with computer<system> using any of the configured protocols	Disable logging the WMI errors. See "WMI Mapper Proxy" for more information.

Service and support

Service and support

Support for HP Systems Insight Manager (HP SIM) is provided as an adjunct to support of the underlying hardware. The purpose of the HP Support page is to provide you with a variety of product, service, and support related resources. In particular, you can use this page to:

- Access <http://www.hp.com/servers/manage>. This website is devoted to systems management products. You will find a wealth of product and service related information on this portal.
- Access the links to HP support home page and World Wide Web locator for phone numbers, online tools, and information.
- Contact the HP Support Forum to get answers to your questions about HP products. The HP Support Forum can be found at <http://forums.itrc.hp.com/>.

Keeping good records of your configuration can significantly speed up the troubleshooting process. Consult the following list when you obtain assistance from your HP service provider:

- Management server make, model, and serial number information
- Operating system information, including version number, a list of all service packs that have been applied, the Compaq SSD version, and Insight Agent names and versions that have been applied
- Hardware configuration information:
 - Survey Utility output or Inspect printout
 - System Configuration Utility printout
 - Description of any third-party equipment that is not shown on the Inspect or System Configuration printout

glossary

A

administrative rights user	A user who is authorized for the All Tools toolbox on all systems, including the Central Management Server. This type of user has been given special privileges to administer the HP SIM software.
agent	A program that regularly gathers information or performs some other service without the user's immediate presence. HP Systems Insight Manager (HP SIM) agents provide in-depth hardware and software information and subsystem status to HP SIM and numerous third-party management applications. <i>See also</i> management agent.
alarm	A user-configurable notification displayed in the System Status panel of HP SIM when certain events occur. For instance, if a monitored item changes, an alarm notifies the user that a change has occurred. <i>See also</i> trap, event.
all events collection	Displays all events that have occurred for all systems.
All Tools toolbox	A default toolbox that provides complete access to all tools for the authorized system or system group.
attribute	A single characteristic of a manageable product or component, as in an attribute of a Management Information Format (MIF) file. A set of related attributes constitutes a group. For example, the clock speed of a processor chip is an attribute of a group that describes that chip. <i>See also</i> Management Information Format.
authentication	The process of identifying an individual, based on a user name and password. Authentication is distinct from authorizations and ensures that the individual is who they claim to be.
authorizations	A mapping of a relationship between a user, a toolbox, and a system or system group.
automatic discovery	The process that HP SIM uses to find and identify systems on your network and populate the database with that information. A system must first be discovered to collect data and track system health status. The primary source for automatic discovery is ping sweeps configured in the automatic discovery tasks page. Other sources might include receiving events from unknown systems or from a management processor that has information about a server. Identification automatically runs on discovered systems.
available software	A listing of the software components available in the repository to which the HP Version Control Agent (VCA) has been configured to point. When browsing directly into a VCA, these additional components can be selected for installation.

B

banner	The section of the GUI at the top of the screen that includes the user name and links to the Home page and sign out functions.
---------------	---

C

caution	A note to indicate that failure to follow directions could result in damage to equipment or loss of information.
Central Management Server (CMS)	A system in the management domain that executes the HP SIM software. All central operations within HP SIM are initiated from this system.
central processing unit polling rate	The rate for how often the Cluster Monitor CPU Resource checks CPU utilization as reported by HP Insight Management Agent on monitored systems.
certificate	An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together. <i>See also</i> certificate authority.

certificate authority (CA)	A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual they claim to be.
certificate key	A value used alone or with an encryption decoder (corresponding public or private key) for cryptography. In traditional private key cryptography, the communicators share a key or cipher so that each can encrypt and decrypt messages. The risk in this system is that if any party loses the key, the system is broken. In public key cryptography, the private key is associated with a public key, so each person in the system has a personal private key that is never shared.
cleared status	A status condition that indicates an event is cleared.
clearing events	Changing the event status from uncleared to cleared.
clients	HP desktop, portable, and workstation systems.
cluster	A parallel or distributed computing system made up of many discrete systems that form a single, unified computing resource. Clusters vary in their features, complexity, and the purposes for which they are best suited.
cluster IP address	The IP address of the cluster.
cluster monitor	A core component of HP SIM. Cluster Monitor adds the ability to monitor and manage multi-node clusters. Cluster Monitor also manages multiple cluster platforms in a heterogeneous environment.
cluster monitor resource	A program that provides a monitoring or management function for clustered nodes in a cluster.
cluster system identification	Information about cluster systems. This information is stored in the database.
collections	The method for grouping system or event.
command line interface (CLI)	A text-based application that can be executed from a command shell such as sh, csh, ksh or the Microsoft Windows CMD shell.
common information model (CIM)	An object-oriented schema defined by the Desktop Management Task Force (DMTF). CIM is an information model guide that describes and shares management information enterprise-wide. CIM is designed for extending each management environment in which it is used.
common information model object manager (CIMOM)	A CIMOM acts as the interface for communication between web-based enterprise management (WBEM) providers and management applications such as HP Systems Insight Manager. A CIMOM that provides an interface for an <i>SMI-S provider</i> is called an SMI CIMOM.
communications protocol	See management protocol.
complex	Computer systems that support multiple hardware partitions are referred to as a complex. For example, the HP Integrity Superdome systems support multiple hardware partitions within a single complex.
component	A component is a single, self-describing, installable (interactive or silent) binary file containing a single piece of software, such as firmware image, driver, agent, or utility, that is supported by the management and update tools.
configuration history report	The Survey Utility that contains reports that show configuration details for server and compares configuration history files for differences.
Configure or Repair Agents	An HP SIM feature that enables you to repair credentials for SNMP settings and trust relationships that exist between HP SIM and target systems. You can also update Web Agent passwords on target systems that have 7.1 agents or earlier installed.
control tasks	Sequences of instructions that are associated with a search, event, or both, such as Delete Events, Remove Disk Thresholds, Set Disk Threshold, and Set Device Access community strings.
critical status	A state generated when HP SIM can no longer communicate with a managed system.

- custom tools** Custom tools are tools that can be created by the user to run on the Central Management Server or on target systems. For example:
- **Remote tool** A tool that runs on selected target systems. It might copy files to the target systems or run specific X-Window applications on the target systems. This tool can be scheduled.
 - **CMS tool** A tool that runs on the CMS. It is usually a script or batch file and can pass in environment variables. Using Automatic Event Handling, this tool can optionally be configured to run when events are received. This tool can be scheduled.
 - **Web page tool** A tool that launches a web URL. The URL is launched in a separate browser window on the Central Management Server. This tool cannot be scheduled.

D

- data collection reports** Data collection reports include information about discovered systems in a single instance or a historical trend analysis report. HP SIM supports **Overwrite existing data set (for detailed analysis)**, formerly known as Single Instance Data Collection task in Insight Manager 7, and **Append new data set (for historical trend analysis)**. With **Overwrite existing data set (for detailed analysis)**, data is collected from a system at a single instance. With **Append new data set (for historical trend analysis)**, data detailing the system history is collected.
- data collection tasks** Procedure that involves gathering information from a group of managed systems and storing that information in the database. HP SIM uses Hardware Status Polling and Data Collection Tasks to implement data collection.
- Desktop Management Interface (DMI)** An industry-standard protocol, primarily used in client management, established by the Desktop Management Task Force (DMTF). DMI provides an efficient means of reporting client system problems. DMI-compliant computers can send status information to a central management system over a network.
- Desktop Management Task Force (DMTF)** An industry standard body that defines DMI and WBEM standards for the industry. HP is an active sponsor and participant in the DMTF body.
- digital signatures** A technology used to validate the sender of a transaction. This technology uses private keys to digitally sign the data and public keys to verify the sender.
- discovery** A feature within a management application that finds and identifies network objects. In HP management applications, discovery finds and identifies all the HP systems within a specified network range.
- discovery filters** Enables users with to prevent or allow certain system types from ever being added to the database.
- discovery template** Files that can be used by automatic discovery in lieu of typing the addresses directly in to the **Ping inclusion ranges** or **Exclusion ranges** fields on the **Automatic Discovery - General Settings** page and are designed to be used as a quick way to change the scope of automatic discovery.
- Distributed Component Object Model (DCOM)** An extension of the Component Object Model (COM) that enables COM components to communicate between clients and servers on the same network.
- Distributed Task Facility (DTF)** A management application that manages the remote execution of tasks on managed systems.
- DMI** See Desktop Management Interface.
- Domain Name Service (DNS)** A service that translates domain names into IP addresses.

E

- e-mail notification** One of the notification tasks in HP SIM that sends notifications through e-mail.
- edit collection** To modify existing collections to add or remove search criteria.

enclosure	A physical container for a set of server blades. It consists of a backplane that routes power and communication signals and additional hardware for cabling and thermal issues. It also hosts the CPU or server power supplies.
event	Information sent to certain users that something in the managed environment has changed. Events are generated from SNMP traps. HP SIM receives a trap when an important event occurs. Events are defined as: <ul style="list-style-type: none"> • Warning. Events of this type indicate a state that might become a problem. • Informational. Events of this type require no attention and are provided as useful information. • Normal. Events of this type indicate that this event is not a problem. • Minor. Events of this type indicate a warning condition that can escalate into a more serious problem. • Major. Events of this type indicate an impending failure. • Critical. Events of this type indicate a failure and signal the need for immediate attention.
event overview	A chart that summarizes the events by product type.
external sites	Third-party application URLs.
G	
graphical user interface (GUI)	A program interface that takes advantage of the graphics capabilities of the computer to make the program easier to use. The HP SIM GUI runs in a web browser.
H	
health status	Health status is an aggregate status all of the status sources (which can be SNMP, WBEM, DMI, and HTTP) with the most critical status being displayed. <i>See also</i> system health status.
hosts files	A file that follows the UNIX, Linux, or Windows host file format, which is an IP address followed by a name and each system is listed on a separate line in this file. This file is used by manual discovery to manually add multiple systems to the HP SIM database,
HP BladeSystem Integrated Manager	HP BladeSystem Integrated Manager is an HP Systems Insight Manager (HP SIM) plugin that enables you to manage blade systems from HP SIM for Windows, HP-UX and Linux. HP BladeSystem Integrated Manager is composed of blade computer systems, integrated connectivity to data and storage networks, and shared power subsystems. The HP BladeSystem Integrated Manager enables you to quickly navigate your HP blade environments including server blades and desktops, enclosure infrastructures, racks, and integrated switches, through hierarchical tree views. Users are able to conveniently configure, deploy, and manage individual or groups of blade systems.
HP Insight Management Agent	A program that regularly gathers information or performs some other service without the user's immediate presence.
HP Insight Power Manager	An integrated power monitoring and management application that provides centralized control of server power consumption and thermal output at the datacenter level. It extends the capacity of datacenters by enabling the user to control the amount of power and cooling required for ProLiant servers. Built on ProLiant Power Regulator Technology, it extends new server energy instrumentation levers into HP SIM for greater Unified Infrastructure Management.
HP ProLiant Essentials Virtual Machine Management Pack (Virtual Machine Management Pack)	Provides central management and control of Virtual Machines on Microsoft Virtual server, Vmware's GSX and ESX. Integrated with HP SIM, Virtual Machine Management Pack provides unified management of HP ProLiant host servers and virtual machines.

HP ProLiant Essentials Vulnerability and Patch Management Pack	The all-in-one vulnerability assessment and patch management tool integrated into HP SIM, simplifying and consolidating the proactive identification and resolution of issues that can impact server availability into one central console.
HP Systems Insight Manager	System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables. HP SIM combines the strengths of Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms. HP SIM can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins for rapid deployment, performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets.
HP Systems Insight Manager database (database)	The database that stores vital information about HP SIM, including users, systems, and toolboxes.
HP Version Control Agent (VCA)	An agent that is installed on a server to enable you to see the HP software installed on that server. The VCA can be configured to point to HP Version Control Repository Manager, enabling easy version comparison and software update from the repository.
HP Version Control Repository Manager (VCRM)	An HP agent that enables a customer to manage HP provided software stored in a user-defined repository.
HyperText Transfer Protocol (HTTP)	The underlying protocol used by the World Wide Web.
I	
identification	While discovery finds systems, identification attempts to determine what the system type is. In addition, it determines what management protocol a system supports, using credentials from the Global Protocol Settings page, and attempts to determine the operating system and version loaded, along with other basic attributes about the system. Finally, it determines if the system is associated with another system. For example, a management processor in a server.
installed version	A particular HP software component that is installed on the server.
Internet Protocol (IP)	Specifies the format of datagrams (packets) and the addressing scheme on a network. Most networks combine IP with Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source.
IP range	Systems with an IP address that falls in the specified range.
J	
Java database connectivity (JDBC)	Similar to Open DataBase Connectivity (ODBC), this set of application program interfaces (APIs) provides a standard mechanism to allow Java applets access to a database.
Java Remote Method Invocation (RMI)	A set of protocols that enable Java objects to communicate remotely with other Java objects.
K	
keystore	A database that maintains a list of keys. The keystore can contain a subject's own private key. A keystore can also contain a list of public keys, as published in certificates.
M	
Major status	Status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken immediately.

managed systems	Any system managed by HP SIM, such as servers, desktops, storage systems, and Remote Insight Boards (RIBs).
management agent	A daemon or process running on a managed system. It receives and executes requests from the Central Management Server on the managed system.
management domain	A collection of resources called managed systems that have been placed under the control of HP SIM. Each Central Management Server is responsible for a management domain. The managed systems can belong to more than one management domain.
Management HTTP Server	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software. This version is available in the ProLiant Support Pack 7.10 or earlier.
Management Information Base (MIB)	The data specification for passing information using the SNMP protocol. An MIB is also a database of managed objects accessed by network management protocols.
Management Information Format (MIF)	An ASCII text file in the DMI architecture that describes the manageable features and attributes of a product. The DMI maintains this information in a MIF database and makes it available to operating systems and management applications. The DMTF has specified MIF formats for a variety of system types and peripheral systems.
management instrumentation	Agents running on systems that provide management information for HTTP, DMI, or SNMP protocols.
management LAN	A LAN dedicated to the communications necessary for managing systems. It is typically a moderate bandwidth (10/100 BaseT) and secured through limited access.
management protocol	A set of protocols, such as WBEM, HTTP, SNMP, or DMI, used to establish communication with discovered systems.
management scope	A set of systems within the set of all discovered systems that HP SIM manages.
management services	A core set of capabilities such as automatic discovery, data collection, a central repository for system and event information, event management, basic notification, and secure access. These functions are used by add-ins from HP, a Management Solutions Partner, and HP SIM users.
management tasks	Procedures you set up to search systems or events.
manual discovery	Similar to automatic discovery, but rather than ping sweeps and events being used to find systems, you manually add systems, either by IP address or name, using template of hosts files. Identification runs on these systems. Manual discovery can be used to set a system type. However, if identification determines the target is something different, the <i>found</i> type is used.
manual discovery techniques	Processes that enable you to bypass a full discovery for the following tasks: <ul style="list-style-type: none"> • Adding a single system • Editing the system • Creating or importing an HP SIM database hosts file • Creating or importing generic hosts files
Microsoft Clustering Service status page	A page that summarizes cluster status as defined by Microsoft Cluster Server and lists the status and values of MSCS-defined cluster attributes. The Cluster Monitor uses color to display status based on MSCS condition values (Normal, Degraded, Failed, and Other).
Minor status	Status information collected from the system that indicates one or more of the monitored subsystems are not operating properly which is impacting the system. Action should be taken as soon as possible to prevent further failure.
Monitor Tools toolbox	A default toolbox that contains tools that display the state of managed systems but not tools that change the state of managed systems.
multiple-system aware (MSA)	A run type that supports multi-system operations. Tools with this run type operate on the target systems using their own internal mechanisms instead of using the Distributed Task Facility. The MSA run type uses the Distributed Task Facility to launch the tool on a single system before the tool interacting with the other managed systems.

N

network clients Any computer system connected to your network with a compatible browser used to connect to the HP SIM GUI.

O

Onboard Administrator The Onboard Administrator is the central point for controlling an entire c-Class rack. It offers configuration, power, and administrative control over the rack, and its associated blades (Compute Servers), blade management processors (iLOs), network switches (depending on the models of switches used) and storage components (such as SAN or SATA). The Onboard Administrator is a single management processor, with shared resources to an optional backup twin processor for failover.

Open Service Event Manager (OSEM) Enables you to collect, filter, and send problem reports for supported systems (ProLiant and Integrity) running Insight Management Agents. In addition, OSEM automatically sends service event notifications to HP SIM when a problem is detected on the system.

OpenSSH A set of network connectivity tools providing encrypted communication sessions over a computer network using SSH. It was created as an open source alternative to the proprietary SSH software suite offered by SSH Communications Security.

operator rights user A user who has limited capability to configure the Central Management Server. operator rights users have permission to create, modify, and delete all reports and their own tools.

overall software status This section indicates whether the software on the server that the HP Version Control Agent is installed on has any updates available within the repository in which it has been configured to monitor.

P

HP Performance Management Pack (PMP) A software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers. PMP tools consist of Online Analysis, Offline Analysis, Comma Separated Value (CSV) File Generator Report, System Summary Report, Status Analysis Report, Configuration, Licensing, and Manual Log Purge.

HP ProLiant and Integrity Support Pack An HP ProLiant and Integrity Support Pack is a set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An HP ProLiant and Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.

HP ProLiant Support Pack A set of HP software components that have been bundled together by HP and verified to work with a particular operating system. A HP ProLiant Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.

ProLiant Essentials license key The contractual permissions granted by HP to the customer in the form of a coded embodiment of a license that represents a specific instance of a license. A single license can be represented by a single key or by a collection of keys.

R

rack A set of components cabled together to communicate between themselves. A rack is a container for an enclosure.

Red Hat Package Manager (RPM) The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.

Reference Support Pack A baseline bundle of HP software components that the HP Version Control Agent can be configured to point to in the repository. This setting enables users to indicate that they want to keep all of their software up to a certain Support Pack level.

remote wakeup Sometimes referred to as Wake-On-LAN (WOL). The remote powering up of a system through its resident WOL network card, provided that the system has been enabled to be so awakened using the ROM or F10 Setup.

This is a capability on which HP SIM relies to turn on the systems for scheduled Software Updates or Replicate Agent Settings.

remove all disk thresholds	A task provided by HP SIM to remove disk thresholds for systems in an associated collection. This task only removes disk thresholds that were set by HP SIM or by browsing directly to the Web Agent. Any thresholds set by HP SIM for Windows 32, including disk thresholds, are not removed by this task.
Replicate Agent Settings repository	A tool that can be used to copy web-based agent settings to a group of systems. A directory containing HP ProLiant Support Pack or Integrity Support Packs and Smart Components.
Resource Partition	A subset of the resources owned by an operating system instance. The use of those resources is controlled through technologies such as the Fair Share Scheduler, pSets, and Memory Resource Groups. A resource partition also has a set of processes associated with it, and only those processes can use the resources within the resource partition. Policies established by tools such as Process Resource Manager (PRM), Workload Manager (WLM), or Global Workload Manager (gWLM) control how resources are allocated to the set of resource partitions within an operating system instance.
role	See toolbox.
rule set	Conditions, policies, or criteria applied to system information to determine what it is.
S	
HP Service Essentials Remote Support Pack	The HP HP Service Essentials Remote Support Pack provides proactive remote monitoring, diagnostics, and troubleshooting to help improve the availability of HP-supported servers and storage devices in your data center. The Remote Support Pack reduces cost and complexity in support of systems and devices. The Remote Support Pack securely communicates incident information through your firewall and/or Web proxy to the HP Support Center for reactive support. Additionally, based on your support agreement, system information can be collected for proactive analysis and services.
search criteria	A set of variables (information) used to define a requested subset of information from the HP SIM database.
Secure HTTP (HTTPS)	An extension to the HTTP protocol that supports sending data securely over the web.
Secure Shell (SSH)	A program to log in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.
Secure Sockets Layer (SSL)	A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common usage of SSL is to provide authentication of the server, so clients can be assured they are communicating with the server it claims to be. It is application protocol independent.
secure task execution (STE)	A feature of HP SIM that securely executes a task from a managed system. STE ensures that the user requesting the task has the appropriate rights to perform the task, and encrypts the request to protect data from snooping.
security roles	A feature that enables administrators to restrict system access and manage access on a per-user or per-group basis. This capability enables systems administrators to delegate tasks to junior staff without providing access to advanced or dangerous features. It also enables systems administrators to delegate management of systems to specific organizations or customers without providing access to systems owned by other organizations or customers.
self-signed certificate	A certificate that is its own Certificate Authority (CA), such that the subject and the CA are the same. <i>See also</i> certificate, certificate authority.
server blade	Typically a very dense server system containing microprocessors, memory, and network connections that can be easily inserted into a rack-mountable enclosure to share power supplies, fans, switches, and other components with other server blades. Server blades tend to be more cost-efficient, faster to deploy, and easier to adapt to growth and change than traditional rack-mounted or tower servers. <i>See also</i> enclosure.

server blade visual locator	A feature designed to provide visual representation of ProLiant BL e-Class, p-Class and c-Class servers within their respective enclosures and racks. <i>See also</i> enclosure.
Service Advertising Protocol (SAP)	A NetWare protocol used to identify the services and addresses of servers attached to the network.
set disk thresholds	A task provided by HP SIM to set a disk threshold for systems in an associated collection. This threshold is set on all disk volumes on the target systems.
Shared Resource Domain (SRD)	A collection of compartments—all of the same type—that share system resources. The compartments can be nPartitions, virtual partitions, processor sets (pSets), or Fair Share Scheduler (FSS) groups. A server containing nPartitions can be an SRD—as long as nPartition requirements are met. A server or an nPartition divided into virtual partitions can be an SRD for its virtual partition compartments. Similarly, a server, an nPartition, or a virtual partition containing pSets can be an SRD for its pset compartments. Lastly, a Server, an nPartition, or a virtual partition containing FSS groups can be an SRD for its FSS group compartments. A complex with nPartitions can hold multiple SRDs. For example, if the complex is divided into nPartitions, named Par1 and Par2, Par1's compartments could be virtual partitions, while Par2's compartments are pSets. Each compartment holds a workload. gWLM manages the workload by adjusting the compartment's resource allocation.
Short Message Service (SMS)	A convenient way to send brief text messages directly to a wireless phone. There is a maximum message length of 140 characters.
Simple Network Management Protocol (SNMP)	One of the management protocols supported by HP SIM. Traditional management protocol used extensively by networking systems and most servers. Management Information Base for Network Management of TCP/IP-based internets (MIB-II) is the standard information available consistently across all vendors.
Simple Object Access Protocol (SOAP)	A lightweight protocol for exchange of information in a decentralized, distributed environment.
Single Login	Permission granted to an authenticated user browsing to HP SIM to browse to any of the managed systems from within HP SIM without re-authenticating to the managed system. HP SIM is the initial point of authentication, and browsing to another managed system must be from within HP SIM.
single-system aware (SSA)	A run type that does not support multi-system operations. Tools with this run type are only aware of the system on which they are running.
SMI CIMOM	<i>See</i> common information model object manager.
SMI-S provider	An industry-standard WBEM provider that implements a well defined interface for storage management. The manufacturers of host bus adapters (HBAs), switches, tape libraries, and storage arrays can integrate SMI-S providers with their systems, or provide them as separate software packages. <i>See also</i> Web-Based Enterprise Management.
SNMP communication setting	Default SNMP community string used when communicating with systems supporting SNMP communications.
SNMP trap	Asynchronous event generated by an SNMP agent that the system uses to communicate a fault.
Software Distributor	The HP-UX administration tool set used to deliver and maintain HP-UX operating systems and layered software applications.
software inventory	A listing of the HP software installed on the system where the HP Version Control Agent is installed.
software update	A task to remotely update software and firmware.
spoofing	The act of a website posing as another site to gather confidential or sensitive information, alter data transactions, or present false or misleading data.
standard error (stderr)	The default place where the system writes error messages. The default is the terminal display.

standard output (stdout)	The default place to which a program writes its output. The default is the terminal display.
status message list	A list created by Cluster Management Resources to collect entries found in the bottom left area of the Cluster Monitor page to bring your attention to cluster attributes that are in an abnormal state.
status message summary header	The list header summary of the total number of status messages in the list and, in parentheses, the number of status messages that have not been examined.
status type	The classification of status messages (for example, Critical, Major, Minor, Normal, Warning, and Unknown).
Storage Management Initiative Specification (SMI-S)	A standard management interface developed by the Storage Networking Industry Association (SNIA). SMI-S provides a common interface and facilitates the management of storage devices from multiple vendors. SMI-S uses industry-standard <i>common information model</i> and <i>Web-Based Enterprise Management</i> technology.
storage systems	SAN-attached Fibre Channel disk arrays, switches, tape libraries, or hosts (with Fibre Channel host bus adapters).
subnet	On TCP/IP networks, subnets are all systems whose IP addresses have the same prefix. For example, all systems with IP addresses that start with 10.10.10. would be part of the same subnet.
Survey Utility	An agent (or online service tool) that gathers and delivers hardware and operating system configuration information. This information is gathered while the server is online.
symmetric key	A common key that both the server and receiver of a message share and use to encrypt and decrypt a message.
system	Systems on the network that communicate through TCP/IP. To manage a system, some type of management protocol (for example, SNMP, DMI, or WBEM) must be present on the system. Examples of systems include servers, workstations, desktops, portables, routers, switches, hubs, and gateways.
system group	A group of systems based on a system collection; a static snapshot of the source collection at the time the system group was created. Used for authorizations.
system health status	This is aggregate status all of the status sources (which can be SNMP, WBEM, DMI, and HTTP) that are supported on a target system, with the most critical status being displayed. The following are the different system health statuses that can be displayed: <ul style="list-style-type: none"> • Critical HP SIM can no longer communicate with the system. The system was previously discovered but cannot be pinged. The system might be down, powered off, or no longer accessible on the network because of network problems. • Major A major problem exists with this system. It should be addressed immediately. For systems running an HP Insight Management Agent, some component has failed. The system might no longer be properly functioning, and data loss can occur. • Minor A minor problem exists with this system. For systems running Insight Management Agent, some component has failed but the system is still functioning. • Warning The system has a potential problem or is in a state that might become a problem. • Normal The system is functioning correctly. • Disabled The system is disabled from monitoring but is not necessarily turned off. • Unknown HP SIM cannot obtain management information about the system. • Informational The system might be in a transitional or non-error state.
system identification	Identifying information about systems. This information is stored in the database. The following information is identified: <ul style="list-style-type: none"> • Type of management protocol on the system (SNMP, DMI, WBEM, HTTP, and SSH) • Type of HP system (server, client, switch, router, and so on) • Network name of system

system information	Information that is provided on the System Page under the System tab. The system information includes: <ul style="list-style-type: none"> • Network address • Network name • Description • Contact • Location • System links
system information using DMI	Agents that conform to the DMI V2 standard and have passed testing. The list of compliant DMI V2 agents can be found on http://www.dmtf.org .
system information using SNMP	Agents that conform to SNMP MIB-2 standards.
system links	A summary information page for a specific system that has a management agent.
System Management Homepage (SMH)	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.
system overview report	A report indicating the state of systems that is available at the time that HP SIM is first opened. A system search result contains the number of systems that are registered with the HP SIM databases. Systems are grouped by their status conditions. Each number in a column is a hyperlink to a more detailed list of systems, which displays the systems that correspond to the number in the overview.
system properties	properties can be set for a single system or for multiple systems at the same time and include options such as system name, system type, system sub-type, operating system version, asset number, contact information, and whether or not the system properties can be changed or updated by the discovery process.
system search	Logical grouping of systems into a collection based on information in the HP SIM database. After a search is defined, you can display the results from the system view page or associate it with a management task.
system search results	The result of a system search.
system status panel	The section of the GUI on the left of the screen that displays status information and system or event alarms.
system type	One of 12 supplied types. You can add your own based on one of these types. For example, use Server type to create MyServer type. It is still a server and is reported on in the same way, but it has your designation.
System Type Manager (STM)	A utility that enables you to modify the default behavior of the discovery and identification of objects classified as Unknown or as another category of systems are discovered and identified precisely as you require. HP SIM discovers and identifies the system and applies the new information when an Unknown system matches a rule set that you specify as the primary rule set. Furthermore, creating the new system type provides a System Link page for viewing the information returned from the system agent or from the communication protocol of SNMP or DMI.

T

task	An executed instance of an HP SIM tool, on one or more systems, with a specific set of arguments.
task scheduling	A master scheduling tool for the scheduling of polling, control, and notification tasks.
template files	Template files are a concept that was used before HP SIM had multiple automatic discovery tasks. Template files should no longer be used. However, a template file enables you to create the same data range (IP ranges, and so on) that would be entered in a discover IP inclusion range. The automatic discovery task can have as input one or more template files. However, template files cannot be nested.
threshold	A preset limit that produces an event when the limit is reached or exceeded.

Tomcat	An open source implementation of Java Servlet and JavaServer Pages technologies that is used by HP SIM as a web server.
tool	An application, command, or script that can be executed by HP SIM on one or more systems to perform a task.
toolbox	A defined set of tools that a user might need for a particular task, such as database administration or software management. Each HP SIM toolbox is associated with a set of tools and authorizations.
trap	An unsolicited message generated by a management agent that indicates that an event has occurred. For example, a monitored item has exceeded a set threshold or changed status. Previously called alarm. <i>See also</i> event.
trap categories	Event collection systems found by event type. SNMP traps categorized by HP SIM into logical groups according to their functions.
trap forwarding address	The IP address of a system that has been specified to receive trap notifications forwarded by the HP SIM systems.
type	The classification of a system, which identifies it as a standard system type. The system types are client, cluster, portable, printer, remote access device, repeater, router, server, switch, unknown, workstation, and other.

U

uncleared event status	Events that have a Critical, Major, Minor, Normal, or Informational severity and have not been cleared or deleted from the database. Events can be cleared without being deleted from the database by using the Clear events menu option. <ul style="list-style-type: none"> • Critical. A failure has occurred, and immediate attention is required. • Major. A failure is impending. • Minor. A warning condition exists that can escalate into a more serious problem. • Normal. These events are not a problem. • Informational. No attention required. This status is provided as useful information
unknown status	HP SIM cannot obtain management information about the system using SNMP or DMI. Although no management instrumentation information is available, the system can be pinged. It might have an invalid community string or security setting.
user	A network user with a valid login on the Central Management Server that has been added to HP SIM.
user accounts	Accounts used to sign-in to HP SIM. These accounts associate a local Windows user account or a domain account with privilege levels and paging attributes inside HP SIM.
user group	A group of users defined on the Central Management Server operating system that has been added to HP SIM. Members of the user group in the operating system can sign-in to HP SIM.
user rights user	A user who cannot configure the Central Management Server. However, the user can view and run predefined reports on the Central Management Server and all managed systems.

V

VCA log	A listing of all the software maintenance tasks completed by the HP Version Control Agent and reports resulting from those tasks.
version control	Referred to as the HP Version Control Repository Manager installed on a Windows system for Windows and Linux ProLiant systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software Distributor can be launched from an HP SIM Central Management Server against one or more installed HP-UX systems.

Virtual Server Environment (VSE) An integrated server virtualization offering for HP-UX, Linux, and Windows servers that provides a flexible computing environment maximizing usage of server resources. VSE consists of a pool of dynamically sizeable virtual servers; each can grow and shrink based on service level objectives and business priorities. For more information, see <http://hp.com/go/vse>.

W

WBEM Services HP WBEM Services for HP-UX is an HP product that uses WBEM and DMTF standards to manage HP-UX system resources.

Web-Based Enterprise Management (WBEM) An Industry initiative to provide management of systems, networks, users, and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM client applications.

Web-Based Enterprise Services (WEBES) A tool suite that is aimed at preventing or reducing the downtime of a system.

Web-launch aware (WLA) A run type for tools that are launched in a web browser using a web server. WLA tools can be designed to deal with multiple systems.

Windows Management Instrumentation (WMI) An API in the Windows operating system that enables systems in a network, typically enterprise networks, to be managed and controlled.

workspace The section of the GUI where tools are displayed.

X

X client An application or tool that appears on an X server. X clients can also be called X applications.

X server A local application that accepts X client requests and acts on them.

X Window System A cross-platform windowing system that uses the client/server model to distribute services across a network. It enables applications or tools to run on a remote computer.

XML document A collection of data represented in XML.

Index

A

- about, 456–457
 - default polling tasks, 277
 - licenses, 358
 - searches, 246
 - sign-in, 162
 - single login, 162
 - storage solutions (SNMP), 272–273
 - System License Information Reporting, 368
 - trust relationships, 181, 393
 - version control agent, 455
- accessing, 458–459
 - automatic event handling, 540
 - discovery filters, 111
 - Event Monitoring Service, 483
 - HP Array Configuration Utility, 492
 - HP BladeSystem Integrated Manager in HP Systems Insight Manager, 492
 - HP Client Manager, 493
 - HP Insight Power Manager, 488
 - HP OpenView Storage Data Protector, 487
 - HP OpenView Storage Management Appliance, 488
 - HP Performance Management Pack, 416
 - HP Server Migration Pack - Universal Edition, 422
 - HP Serviceguard Manager, 485
 - HP Storage Essentials, 494
 - HP StorageWorks Command View EVA, 495
 - HP StorageWorks Command View SDM, 495
 - HP StorageWorks Command View TL, 495
 - HP StorageWorks Command View XP, 496
 - HP StorageWorks Command View XP Advanced Edition, 496
 - HP StorageWorks Modular Smart Array 1000, 496
 - HP Web Jetadmin, 493
 - Ignite-UX, 484
 - Integrated Lights-Out, 484
 - Partition Manager, 485
 - PMP, 597
 - PRM, 489
 - property pages, 473
 - Replicate Agent Settings, 417
 - RPM tools, 419
 - SMP Universal, 421
 - System Fault Management, 474
 - System Management Homepage, 422
 - VPM, 493
 - VSE, 490
 - WBEM Providers for Linux, 474
 - Webmin, 486
- add systems
 - CLI, 121
- adding
 - DMI rules, 132
 - hosts files to database, 119
 - individual keys, 364
 - keys from file, 365
 - SMP Universal license, 421
 - SNMP rules, 132
 - STM rules, 126
 - systems, 114
 - systems to database, 116
 - WMI Mapper Proxy, 571–572
- administering
 - events, 538, 540
 - software, 535
 - user groups, 137
 - users, 137
 - WMI Mapper Proxy, 571
- administration
 - adding user groups, 139
 - authorizations, 135
 - authorizations overview, 148
 - cluster resource settings, 299
 - creating authorization, 150
 - creating toolbox, 145
 - creating users, 138
 - deleting authorizations, 154
 - deleting toolboxes, 147
 - deleting user groups, 142
 - deleting users, 142
 - node resource settings, 299
 - overview, 535
 - report authorizations, 154
 - toolboxes overview, 145
 - updating authorization, 153
 - user overview, 137
 - version control repository, 596
- administrator-template, 144
- agents, 58, 61, 69
- aggregate event status, 423, 428
- alarm, 80
- all scheduled tasks, 286, 290, 585
 - task results list, 277
 - viewing, 286
- always accept
 - trusted certificates, 391
- antivirus software, 611
- application
 - launching, 322
- application storage management, 477
- applying
 - time filters, 283, 544, 564, 567
- assigning licenses, 366
- assistance, 41
- attributes
 - cluster monitor, 302
- audit log, 166, 337, 600–601, 611
 - configuring, 602
 - viewing, 601
- authentication, 33, 611
 - problems, 611

- authorization
 - users, 161
- authorizations, 148, 155
 - adding user groups, 139
 - automatically updating, 150
 - creating, 148, 150
 - creating toolbox, 145
 - creating users, 138
 - delete authorizations, 154
 - deleting, 148, 154
 - deleting toolboxes, 147
 - deleting user groups, 142
 - deleting users, 142
 - editing toolboxes, 146
 - editing user groups, 141
 - editing users, 141
 - overview, 135, 148
 - printing report, 148
 - reports, 154
 - toolbox report, 148
 - updating, 148, 153
 - user group report, 143
 - user report, 143
 - users, 76, 137
 - viewing report, 148
- automatic
 - discovery, 98
- automatic discovery, 33, 50–52, 76, 97, 100, 111–112, 124, 226, 244, 573–574
 - configuring, 109
- automatic event handling, 33, 54, 76
 - accessing, 540
 - creating new task, 540
 - e-mail settings, 54, 540, 550
 - managing tasks, 540
 - modem settings, 540, 552
 - problems, 611
- automatic event handling task
 - creating, 567
 - with specific event, 567
 - with specified attributes, 544
- automatic event handling tasks, 538
 - copying, 542
 - creating, 538, 542, 544
 - deleting, 538, 542
 - disabling, 542, 549
 - e-mail settings, 538
 - editing, 542
 - enabling, 542, 549
 - examples, 542
 - managing, 538, 542
 - modem settings, 538
 - task results, 542
 - viewing definition, 542
- Availability Manager, 477
- B**
- Backup Manager, 477
- banner, 78
- basic search, 247
- bdf, 337
- biweekly data collection, 583
- blade, 33, 102, 109, 208, 219, 223, 235, 463, 611, 663
 - creating a rack, 220
 - editing a rack, 222
- browser
 - problems, 611
- browsing
 - CMS, 44
- C**
- capacity
 - storage arrays, 270
- Capacity Advisor, 477
- cat, 337
- Central Management Server, 33, 611
 - browsing to, 44
 - overview, 40
 - setting language, 82
 - setting locale, 82
 - setting up trust relationship, 44
- Central Management Server tool, 326
- certificate, 611
 - error messages, 177
 - problems, 611
 - trusted, 611
- certificate signing request
 - creating, 173
 - importing, 174
 - submitting, 173
- certificates, 167, 169–175, 178–181
 - server, 161, 167
 - setting trust relationships, 181, 393
 - WBEM, 161, 394
- changing
 - SSL port, 167
- Chargeback Manager, 477
- cim_ip.dat, 120
- CIMOM, 611
- Class Scheduler, 477
- clear events task
 - running, 552
 - scheduling, 552
- clearing
 - events, 241, 538, 552, 565
- CLI, 611
 - batch add systems, 121
- CLI problems, 611
- cluster, 102, 124, 611
 - HP Serviceguard, 229, 485
 - identification, 569
 - problems, 611
 - searching, 245
 - System tab, 440
- cluster collections, 298
 - copying, 197
 - creating, 192

- customizing, 191–192, 229
- deleting, 198
- editing, 194
- managing, 229
- moving, 197
- overview, 189
- printing, 229, 234
- report, 234
- setting properties, 199
- cluster monitor, 298, 300–301
 - attributes, 302
 - cluster resource settings, 299
 - cluster tab, 300
 - CPU polling rate, 303
 - Disk polling rate, 303
 - MSCS polling rate, 303
 - network tab, 300
 - node resource settings, 299
 - nodes tab, 300
 - polling rates, 303
 - resources, 302
 - resources tab, 301
 - system status polling rate, 303
 - viewing CPU utilization, 303
- cluster monitor resource
 - configure node settings, 299
 - configure settings, 299
 - CPU, 303
 - CPU polling rate, 299
 - CPU thresholds, 299
 - Disk polling rate, 299
 - Disk thresholds, 299
 - MSCS polling rate, 299
 - overview, 302
 - thresholds, 304
- cluster search results
 - printing, 253
- cluster table view
 - printing results, 229
- cluster table view page, 298
 - adding columns, 233
 - customizing, 229, 233
 - deleting columns, 233
 - navigating, 229
 - overview, 229
 - printing, 234
 - sorting, 233
- clusters, 97
 - deleting, 229, 233
 - deleting from search, 253
 - monitoring, 187
 - MSCS, 298, 300
 - searching, 252
 - Serviceguard Manager, 33
- CMS (see Central Management Server)
 - communications, 377
- CMS security configuration rights
 - users, 138
- CMS tool
 - editing, 331
- collecting
 - license information, 357
 - license keys, 359
- collections, 155, 611
 - by attribute, 187
 - by member, 187
 - cluster, 189
 - combination, 187, 191
 - deleting, 198
 - event, 187, 189, 565–566
 - naming conventions, 263
 - private, 189
 - problems, 611
 - saving, 196, 565
 - shared, 189, 258
 - storage systems, 265, 268
 - system, 187, 189
- combination collections, 187, 191
- command line
 - interface, 33, 85
- command line tools, 293, 304
 - parameters, 336
- Command View
 - discovery, 274
- commands
 - , 85
 - bdf, 304
 - cat, 304
 - cp, 304
 - df, 304
 - find, 304
 - ls, 304
 - mv, 304
 - ps, 304
 - rm, 304
- common tasks, 89
 - Setting up managed systems, 89
- communications
 - events tab, 381
 - identification, 381
 - printing table, 386
 - quick repair, 380, 383
 - run tools tab, 382
 - updating, 385
 - version control tab, 382
- community strings, 51, 93, 226, 574
- comparing snapshots, 531
- compiling
 - Compiling and customizing SNMP MIBs with HP SIM, 89
 - MIB, 408
- complex, 33, 102
 - System tab, 441
- configuration management, 477
- configuration rights, 135
- Configure or Repair Agents, 317–318, 321, 389, 394, 401
 - configuring, 305–306, 312

- repairing, 305–306, 312
- updating, 306, 312
- configuring
 - audit log, 600, 602
 - automatic discovery, 109
 - Configure or Repair Agents, 305–306, 312
 - Configuring or Repairing Agents, 89
 - directory groups, 158
 - directory service, 157
 - DMI access, 293, 354
 - e-mail settings, 54, 76, 550
 - event filters, 553
 - events, 555, 558
 - firewalls, 386
 - first time wizard, 48, 54
 - HP SIM, 48, 54
 - HP Version Control Repository Manager, 596
 - iLO, 368
 - managed systems, 48, 53
 - modem settings, 552
 - pager settings, 76, 138
 - PAM on HP-UX, 162
 - Pluggable Authentication Modules, 162
 - PMP, 597
 - protocol settings, 76
 - protocols, 576–577
 - sign-in events, 166
 - SNMP access, 293, 354
 - SNMP traps, 554
 - SSH bypass properties, 600
 - storage system discovery, 268
 - system link, 165
 - timeout options, 166
 - tool definition files, 600
 - VCA, 322
 - WBEM, 320
 - WMI, 320
- contacting
 - support, 41
- containers
 - deleting, 225
- contract and warranty, 280
 - data collection, resume multiple systems, 503
 - data collection, resume single system, 502
 - data collection, suspend multiple systems, 503
 - data collection, suspend single system, 502
 - default tasks, 277
 - HP Service Essentials Remote Support Pack, 496
 - search, 253
 - status, 208, 423, 428, 498, 500–501
 - system properties, 586, 592
- controlling
 - HP 9000 iLO, 375
 - HP Integrity iLO, 375
- Copy Depot Software, 475
- copying
 - automatic event handling tasks, 542
 - cluster collections, 197
 - event collections, 205
 - reports, 511
 - system collections, 197
 - tasks, 548
 - time filters, 283
- copyright, 29
- cp, 337
- CPU resource, 302, 304
- CPU thresholds, 299
- CPU utilization, 304
 - cluster monitor, 303
- Create or Modify Recovery Archive, 475
- Create or Modify Tape Recovery Archive, 475
- creating
 - authorizations, 148
 - automatic event handling task, 540, 567
 - automatic event handling tasks, 538, 542, 544
 - cluster collections, 192
 - CSR, 173
 - custom tools, 322, 324, 326
 - data collection task, 585
 - discovery hosts files, 116
 - discovery task, 97–98
 - discovery templates, 111–112
 - event collection, 565–566
 - event collections, 202
 - hosts files, 116–117
 - HP 9000 iLO user, 372
 - HP Integrity user, 372
 - racks, 220
 - replicate agent settings task, 418
 - reports, 507
 - server certificates, 167, 169
 - STM rules, 129
 - system collections, 192
 - tasks, 277, 280
 - time filters, 283
 - toolboxes, 145
 - users, 76, 138
 - web page tool, 328
- CSR (see certificate signing request)
- custom tool
 - problems, 611
- custom tools, 293
 - CMS, 326
 - deleting, 329, 333
 - editing, 329
 - environment variables, 322, 334
 - managing, 322, 329
 - naming conventions, 324, 326
 - remote, 324
 - removing, 322
 - running, 329
 - scheduling, 329
 - valid characters, 324, 326
 - web page tool, 322
- customizing
 - cluster collections, 191–192
 - cluster table view, 229
 - cluster table view page, 233

- event collections, 200
- event table view, 235
- event table view page, 240
- System and Event Collections panel, 189
- system collections, 191–192
- system status panel, 80
- system table view, 208
- system table view page, 224

D

- data collection, 33, 583
 - append new data set, 583
 - biweekly, 583
 - detailed analysis, 583
 - initial, 583
 - overwrite existing data set, 583
 - search criteria, 583
 - storage systems, 268
- data collection task
 - creating, 585
 - running, 585
 - scheduling, 583, 585
 - viewing results, 585
- data migration tool, 33
- database, 124, 611
 - adding systems, 116
 - administration, 233, 241–242
 - assigning events, 242
 - deleting clusters, 233
 - deleting events, 241
 - deleting system, 225
 - systems, 722
 - views, 513
- database account
 - password, 611
- default tasks
 - bi weekly data collection, 277
 - daily device identification, 277
 - delete events older than 90 days, 277
 - hardware status polling for non servers, 277
 - hardware status polling for servers, 277
 - hardware status polling for systems no longer disabled, 277
 - Initial contract and warranty collection, 277
 - initial data collection, 277
 - initial hardware status polling, 277
 - Monthly contract and warranty collection , 277
 - software version status polling, 277
 - software version status polling for systems no longer disabled, 277
- deleting
 - authorizations, 148, 154
 - automatic event handling tasks, 542
 - clusters, 229, 233
 - collections, 198
 - containers, 225
 - custom tools, 329, 333
 - discovery task, 97, 101
 - discovery templates, 111, 113
 - disk thresholds, 356
 - event collections, 207
 - events, 241, 538, 553, 565–566
 - hosts files, 116, 119
 - HP 9000 iLO user, 373
 - HP Integrity user, 373
 - management proxy host systems, 225
 - reports, 512
 - SSH keys, 597, 599
 - STM rule, 132
 - STM rules, 126
 - systems, 208, 225
 - task instance, 288
 - task results, 289
 - tasks, 277, 286, 290
 - time filters, 283
 - toolboxes, 147
 - trusted certificates, 177, 180
 - user groups, 142
 - users, 142
 - WMI Mapper Proxy, 225, 571, 573
- Deploy SSH Public Key, 475
- deploying
 - Deploying HP SIM on MSCS Clusters , 89
 - HP 9000 iLO SSH public key, 375
 - HP Integrity SSH public key, 375
- desktop, 102
- df, 135
- DHCP server, 611
- directory groups, 157
 - configuring, 158
- directory service, 157
 - configuring, 157
- disabling
 - automatic event handling tasks, 542, 549
 - discovery filters, 111
 - discovery task, 52, 97, 100
- discovery, 48, 54, 58, 61, 69, 124
 - automatic, 33, 50–52, 76, 93, 97–98, 100, 109, 111–112, 124, 226, 244, 270, 535, 573–574
 - Command View, 274
 - creating hosts files, 116
 - creating templates, 111
 - deleting hosts files, 116
 - editing hosts files, 116
 - event based automatic discovery, 93
 - first, 93
 - general settings, 109
 - IP ranges, 124
 - manual, 76, 93, 114, 535
 - storage solutions (SNMP), 273
 - storage systems, 268
 - systems that can be discovered, 104
 - templates, 93
- discovery command, 611
- discovery filters, 33, 109, 124
 - accessing, 111
 - disabling, 111
 - editing, 111

- discovery task
 - creating, 97–98
 - deleting, 97, 101
 - disabling, 52, 97, 100
 - editing, 97, 100
 - enabling, 52, 97, 100
 - general settings, 97
 - running, 97, 101
 - scheduling, 98
 - stopping, 97, 101
 - system automatic discovery, 52
- discovery templates, 93
 - creating, 111–112
 - deleting, 111, 113
 - editing, 111, 113
 - managing, 97
- disk capacity, 304
- disk resource, 302, 304
- disk thresholds, 299
 - example, 356
 - overview, 355
 - removing, 355
 - setting, 355–356
- Distributed Task Facility, 337
- DML, 58, 61, 69, 109, 124, 389, 423, 428, 570, 574, 583
 - adding rules, 132
 - configuring access, 354
 - deleting rules, 126
 - identification, 132
 - setting global defaults, 574
 - status polling, 569
- DML access
 - configuring, 293
- document type definition
 - mxtool, 337
- DTD (see document type definition)
- DTF (see Distributed Task Facility)
- DTMF
 - , 579
- E**
- e-mail
 - encoding, 544
 - html, 544
 - message format, 544
 - pager/SMS, 544
- e-mail paging
 - examples, 559
- e-mail settings, 48, 54, 538, 540
 - automatic event handling tasks, 538
 - CMS, 54, 550
 - configuring, 54, 76, 550
 - SMTP host, 54, 550
- edit
 - rack, 222
- editing
 - authorizations, 148
 - automatic event handling tasks, 542
 - cluster collections, 194
 - CMS tool, 331
 - custom tools, 329
 - discovery filters, 111
 - discovery task, 97, 100
 - discovery templates, 111, 113
 - event collections, 203
 - hosts files, 116, 118
 - HP 9000 iLO user, 372
 - HP Integrity user, 372
 - MIB, 408
 - remote tool, 330
 - reports, 510
 - server certificates, 167, 170
 - STM rules, 131
 - system collections, 194
 - system properties, 33
 - tasks, 277, 285, 290, 547
 - time filters, 283
 - toolboxes, 146
 - user groups, 141
 - users, 141
 - web page tool, 332
 - WMI Mapper Proxy, 571–572
- enabling
 - automatic event handling tasks, 542, 549
 - discovery task, 52, 97, 100
 - system monitoring, 33
- enclosure, 102, 109, 124, 208, 219, 223, 235, 244
- enclosure view, 219
- English, 82
- environment variables
 - custom tools, 322, 334
- environmental monitor, 102
- error messages
 - certificate, 177
- Essentials tab, 454
- event
 - problems, 611
- event collections
 - copying, 205
 - creating, 202, 565–566
 - customizing, 200, 234
 - deleting, 207
 - editing, 203
 - HP Storage Essentials, 270
 - managing, 234
 - moving, 205
 - overview, 189
 - printing, 234, 243
 - report, 243
 - setting properties, 207
 - shared, 258
- event filters
 - adding to tasks, 280
 - modifying, 280
- Event Monitoring Service
 - accessing, 483
 - overview, 483

- event search results
 - printing, 251
- event status, 80
- event table view
 - printing results, 235
- event table view page, 189, 241–242, 244, 253, 423
 - adding columns, 240
 - customizing, 235, 240
 - deleting columns, 240
 - navigating, 235
 - overview, 234
 - printing, 243
 - sorting, 240
- event tasks
 - examples, 564
- event type, 244
- event/SNMP trap, 611
- events
 - adding comments, 234, 242
 - administering, 538, 540
 - assignee, 244
 - assigning, 234, 242
 - associated system, 244
 - change details, 244
 - cleared status, 244
 - clearing, 234, 241, 538, 552, 565
 - comments, 244
 - configuring, 166, 555, 558
 - configuring filters, 553
 - creating tasks, 544
 - deleting, 234, 241, 251, 538, 540, 553, 565–566
 - description, 244
 - details, 235, 244
 - filter settings, 538
 - filtering settings, 540
 - filters, 553
 - HP Storage Essentials, 270
 - managing tasks, 542
 - modem settings, 552
 - monitoring, 187
 - print details, 244
 - problems, 611
 - rules, 540
 - searching, 245, 250
 - server, clearing, 565
 - service, 258
 - service notifications, 560
 - severity, 235, 243–244
 - SNMP trap settings, 538
 - SNMP traps, 554
 - source, 244
 - status, 235, 555
 - status change, 555
 - storage (SNMP), 272
 - storage solutions (SNMP), 275
 - time, 235, 244
 - type, 235
 - view details, 244
- events collections
 - printing, 234
- events tab
 - communications, 381
- events task
 - running, 565
 - scheduling, 565
- example
 - automatic event handling tasks, 542
- examples, 58, 61, 69, 175
 - clearing server events, 565
 - command line tool parameters, 336
 - delete cleared events, 564
 - delete informational events, 564
 - deleting disk thresholds, 356
 - e-mail paging, 559
 - send e-mail, 564
 - web launch tool parameters, 336
- Exchange Viewer, 477
- execute-as user, 58, 61, 69, 611
- exporting
 - server certificates, 172
 - SSH keys, 597, 599
 - trusted certificates, 177, 179
- F
- fault management, 33
- File System Viewer , 477
- filter settings
 - events, 538
- filtering
 - event settings, 540
- filters
 - configuring, 553
- Firefox, 611
- firewalls
 - configuring, 386
- firmware
 - ROM firmware updates, 465
 - upgrade, 611
 - upgrade problems, 611
- First Time Wizard
 - managed environment, 49, 56
- first time wizard, 33, 44, 48, 54
 - finishing, 55
 - SNMP settings, 51
 - system automatic discovery, 52
 - WBEM settings, 50
- G
- generic, 611
 - problems, 611
- getting started, 43
- GlancePlus Pak
 - overview, 484
- global protocol settings, 50–51, 97, 573–574
 - setting, 109, 583
 - storage systems, 268
- Global Reporter, 477
- Global Workload Manager, 477

- globalsettings.props, 81–82, 150, 166, 229, 550, 556, 570, 574, 600, 603
 - SnmpTrapPortAddress, 579
- graphical user interface, 33
 - banner, 78
 - customize Home page, 79
 - customizing system status panel, 80
 - Home page, 78
 - overview, 78
- groups, 148
- GUI (see graphical user interface)
- H
- handheld, 102
- hardware status, 208
- hardware status polling, 570, 574
 - running, 570
 - scheduling, 570
- hardware status polling for non servers, 569
- hardware status polling for servers, 569
- health lifecycle indications
 - subscribing, 558
 - unsubscribing, 558
- health status, 80, 93, 189, 199, 277, 423, 428, 569–570
 - types, 226
- health status section, 78
- help, 41
- Home page, 78
 - customize, 79
 - overview, 78
- hosts files
 - , 93
 - add system, 93
 - adding systems, 116
 - adding to database, 119
 - creating, 116–117
 - deleting, 116, 119
 - editing, 116, 118
 - extensions, 121
 - importing, 120
 - valid format, 117
- HP 9000 iLO, 370
 - controlling iLO, 375
 - creating user, 372
 - deleting user, 373
 - deploying SSH public key, 375
 - editing user, 372
 - LAN access, 374
 - LDAP settings, 374
 - system locator, 371
 - system power, 371
 - upgrading firmware, 375
- HP Array Configuration Utility
 - accessing, 492
 - overview, 492
- HP BladeSystem Integrated Manager, 477
- HP BladeSystem Integrated Manager in HP Systems Insight Manager, 33
 - accessing, 492
 - overview, 492
- HP Client Manager, 477
 - accessing, 493
 - overview, 493
- HP Configure or Repair Agents, 33, 305–306, 312
- HP HP Performance Management Pack, 33, 293, 597
 - accessing, 597
 - configuring, 597
 - licensing, 597
 - manual log purge, 597
- HP Insight Management Agent, 611
- HP Insight Management WBEM Providers for Windows Server 2003/2008, 394
- HP Insight Power Manager, 33
 - accessing, 488
 - overview, 488
- HP Instant Tootools, 208
- HP Integrity, 370
 - controlling iLO, 375
 - creating user, 372
 - deleting user, 373
 - deploying SSH public key, 375
 - editing user, 372
 - LAN access, 374
 - LDAP settings, 374
 - system locator, 371
 - system power, 371
 - upgrading firmware, 375
- HP Integrity Essentials Capacity Advisor, 490
- HP Integrity Essentials Virtualization Manager, 490
- HP Integrity Global Workload Manager, 490
- HP Integrity Integrated Lights Out, 370
- HP Integrity servers
 - Integrated Lights-Out, 484
- HP Integrity Superdome, 102
- HP NonStop Kernel servers
 - health lifecycle indications, 558
- HP OpenView Network Node Manager , 33
- HP OpenView Operations, 33
- HP OpenView Performance Agent, 488
- HP OpenView Storage Data Protector
 - accessing, 487
 - overview, 487
- HP OpenView Storage Management Appliance
 - accessing, 488
 - overview, 488
- HP Performance Management Pack, 208, 357, 477
 - accessing, 416
- HP ProLiant Essentials, 491
- HP ProLiant Essentials Rapid Deployment Pack , 33
- HP ProLiant Essentials Server Migration Pack, 33, 293, 421
- HP ProLiant Essentials Virtual Machine Management Pack, 33, 208, 421, 477
- HP ProLiant Essentials Vulnerability and Patch Management Pack, 33, 208, 477
 - accessing, 493
 - overview, 493

- HP ProLiant iLO
 - power cycle, 376
 - power off, 376
 - power on, 376
 - turning off UID, 377
 - turning on UID, 377
- HP ProLiant Support Pack
 - installing, 466
- HP Rapid Deployment Pack, 477
- HP Server Migration Pack - Universal Edition, 477
 - accessing, 422
- HP Service Essentials Remote Support Pack, 33, 208, 560
 - case status, case ID, 235
 - collection, 258
 - contract and warranty status, 498, 500–501
 - data collection, 502
 - default tasks, 277
 - overview, 496
 - Remote Support Eligible collection, 258
 - system properties, 586, 592
- HP Serviceguard cluster, 229, 293, 485
- HP Serviceguard Manager, 33, 477, 485
- HP SIM, 611
 - commands, 85
 - overview, 33
 - public key, 413
 - registration, 43
 - setting up, 76
- HP SIM problems, 611
- HP Storage Essentials, 33, 477
 - accessing, 494
 - affect on reports, 269
 - collections, 258
 - data collection report, 452
 - discovery, 97
 - events, 242, 552–553
 - overview, 494
 - storage array Identity tab, 447
 - storage host Identity tab, 443
 - storage switch Identity tab, 445
 - Suspend/Resume Monitoring, 595
 - system properties, 585, 592
 - tape library Identity tab, 450
 - toolboxes, 145
 - using with HP Systems Insight Manager, 270
- HP Storage Essentials Enterprise Edition., 477
- HP StorageWorks Command View EVA
 - accessing, 495
 - overview, 495
- HP StorageWorks Command View SDM
 - accessing, 495
 - overview, 495
- HP StorageWorks Command View TL
 - accessing, 495
 - overview, 495
- HP StorageWorks Command View XP
 - accessing, 496
 - overview, 496
- HP StorageWorks Command View XP Advanced Edition
 - accessing, 496
 - overview, 496
- HP StorageWorks Modular Smart Array 1000
 - accessing, 496
 - overview, 496
- HP System Management Homepage, 33
- HP Version Control Agent
 - reports, 461
- HP Virtual Server Environment
 - accessing, 490
 - overview, 490
- HP Web Jetadmin
 - accessing, 493
 - overview, 493
- HP workstations, 477
- HP-UX, 602
- HP-UX, 175, 337, 570, 583, 611
 - commands, 135
 - configuring language, 82
 - configuring PAM, 162
 - managed systems, 61
 - user authorization, 162
 - viewing MIB list, 407
- HP-UX Bastille
 - overview, 483
- HP-UX commands, 304
- HP-UX systems
 - WBEM indications, 33
- HP-UX webmin-based Admin, 477
- HP-UX Workload Manager, 477
- HTTP, 109, 124, 222, 244, 570
 - event problems, 611
 - setting global defaults, 574
- HTTP events, 611
- HTTPS, 109
- hub, 102

I

- ICMP, 574
- ICMP Settings, 576–577
- icon view, 218
- identification, 33, 222, 611
 - cluster, 569
 - communications, 381
 - DMI, 132
 - initial, 124
 - management processor, 569
 - problems, 611
 - SNMP, 132
 - storage solutions (SNMP), 273
 - system, 124, 535
- Ignite-UX, 337, 477
 - accessing, 484
 - overview, 484
- Ignite-UX Console, 475
- Ignite-UX Restricted Console, 475
- iLO, 102, 109, 124, 208, 226, 484 (see Integrated Lights-Out)
 - associating with a server, 611

- configuring, 368
- importing
 - CSR, 174
 - hosts file, 120
 - server certificates, 167, 171
 - SSH keys, 597, 599
 - submitting CSR, 173
 - trusted certificates, 177–178, 391
- initial data collection, 583
- initial ProLiant Pack install, 33
- Initial ProLiant Support Pack Install, 475
- initial setup, 76
- initial status polling, 124
- Insight Management Agent, 477
- Insight Manager 7, 583
- Install OpenSSH, 475
- Install or Recover System, 475
- Install Software, 475
- Install WLM Configuration, 475
- installation, 33, 611
 - problems, 611
- installing
 - HP ProLiant Support Pack, 466
 - Installing and using the HP ProLiant Essentials HP Performance Management Pack Data Migration Tool, 89
 - Installing HP SIM, 89
 - Installing the System Management Homepage individually, 89
 - Installing version control individually , 89
 - OpenSSH, 412–413
 - OpenSSH tool, 33
 - RPM Package Manager, 419–420
 - SNMP provider, 318
 - SSH provider, 319
 - version control, 319
 - WMI/WBEM provider, 317
- Integrated Lights-Out, 226
 - accessing, 484
 - HP Integrity servers, 484
 - overview, 484
- Integrated Lights-Out Advanced, 477
- Integrated Lights-Out Standard, 477
- integration, 457
 - Integrity Essentials, 480
- Intelligent Networking Pack, 477
- Internet Explorer, 611
 - language, 82
 - problems, 611
- IP, 109, 423
- IP address, 355, 611
 - problems, 611
- IP ranges
 - reference, 124
 - specifying, 109
- IPX address, 355
- IPX SAP, 109

J

- Japanese, 82
- java, 611

K

- kernel parameters, 611
- keystore, 175
- known_hosts file, 597
- KVM switch, 102

L

- LAN access
 - HP 9000 iLO, 374
 - HP Integrity, 374
- language
 - English, 82
 - Internet Explorer, 82
 - Japanese, 82
 - Mozilla, 82
 - setting, 82
- launching
 - application, 322
 - custom tools, 322
 - VM remote console, 434
- LDAP settings
 - HP 9000 iLO, 374
 - HP Integrity, 374
- learning
 - Learning more about the ProLiant or Integrity Support Packs., 89
 - Learning more about the ProLiant Remote Deployment Utility, 89
- legal notices, 29
- legend, 78
- license database
 - viewing licensed systems, 361
- license keys
 - adding from file, 365
 - adding individually, 364
 - assigning and un-assigning, 366
 - iLO, 362
 - managing, 362, 369
- license management, 357, 369
- license manager, 293, 359
- licenses
 - activation key agreement, 358
 - beta, 358
 - demo, 358
 - demo (seats and time), 358
 - evaluation, 358
 - flexible quantity, 358
 - individual, 358
 - intrinsic, 358
 - reporting, 368
 - subscription, 358
- licensing
 - about licenses, 358
 - adding keys from file, 365
 - adding keys individually, 364

- assigning and un-assigning , 366
- assigning licenses, 357
- collecting license information, 357, 359
- iLO, 357
- managing keys, 362
- managing licenses, 357
- PMP, 597
- ProLiant Essentials, 357
- SMP Universal, 421
- viewing licensed systems, 361
- Linux, 175, 570, 583, 602, 611
 - commands, 135
 - configuring language, 82
 - managed systems, 58
 - user authorization, 162
 - VCA, 455
 - viewing MIB list, 407
- Linux commands, 304
- Linux IPF, 473
- Linux systems
 - WBEM indications, 33
- lists
 - task results, 289
- locale
 - English, 82
 - Japanese, 82
- log.properties, 600, 602
- logging in
 - CLI, 44
- login, 611
 - single, 162
- logs, 611
 - all scheduled tasks, 286
- ls, 135, 337

M

- Manage SSH Keys, 597
- manage system types page
 - navigating, 126
- Managed Environment
 - First Time Wizard, 56
- managed environment, 48
 - First Time Wizard, 49
- managed system, 40
 - overview, 40
- managed systems, 175, 466
 - Automating Software Maintenance in an HP Environment, 89
 - communications, 377
 - configuring, 48, 53
 - HP-UX, 61
 - Linux, 58
 - overview, 58
 - quick repair, 383
 - recommendation for repair, 380
 - repairing communication, 380
 - repairing communication problems, 383
 - setting up, 58
 - Windows, 69
 - management, 458
 - management agents, 58, 61, 69, 208
 - management domain
 - overview, 40
 - Management HTTP Server
 - trust relationships, 181
 - Management Processor , 477
 - management processor, 102, 124, 208, 222, 293, 423, 428
 - identification, 569
 - System tab, 428
 - management processors
 - creating user, 370
 - deleting user, 370
 - deploying SSH public key, 370
 - editing user, 370
 - iLO control, 370
 - LAN access, 370
 - LDAP settings, 370
 - system locator, 370
 - system power, 370
 - upgrading firmware, 370
 - management protocols, 58, 61, 69
 - management proxies
 - deleting host systems, 225
 - managing
 - automatic event handling task, 540
 - automatic event handling tasks, 538, 542
 - cluster collections, 229
 - CMS communications, 377
 - custom tools, 322, 329
 - discovery task, 97
 - events, 538
 - license keys, 362, 369
 - licenses, 357
 - Managing HP servers through firewalls with HP SIM, 89
 - Managing WBEM Event Subscriptions for HP-UX Systems with HP SIM, 89
 - reports, 511
 - SSH keys, 33, 598
 - system groups from CLI, 155
 - system groups from GUI, 155
 - system types, 126
 - time filters, 283
 - managing communications
 - HP ProLiant Support Pack, 402
 - protocols, 389
 - SNMP;, 394
 - SSH, 401
 - WBEM;, 394
 - manual discovery, 76
 - adding system, 114
 - hosts files, 93
 - mcompile, 85, 408
 - menu
 - problems, 611
 - menus
 - quick launch, 295

- MIB, 132, 293, 560
 - compiling, 408
 - editing, 408
 - internet management, 579
 - preloaded, 409
 - registering, 407, 409
 - rules, 132
 - unregistering, 411
 - vendor, 579
 - viewing list, 407, 409
- MIF
 - example, 132
- migrating
 - Manually Migrating to HP SIM, 89
 - Moving HP SIM to a new system, 89
 - P2V, 421
 - SMP Universal, 421
 - V2P, 421
 - V2V, 421
- modem settings, 538, 540
 - automatic event handling tasks, 538
 - configuring, 552
- monitoring (see enabling) (see suspending)
 - clusters, 187
 - events, 187
 - MSCS status, 302
 - systems, 187
- moving
 - cluster collections, 197
 - event collections, 205
 - system collections, 197, 205
- Mozilla, 611
 - language, 82
- MSA (see multiple-system aware) (see multiple-system aware tools)
- MSA tools, 293, 475
- MSCS
 - clusters, 298
- MSCS polling rate, 299
- MSCS resource, 302
- MSCS status
 - monitoring, 302
- multiple-system aware tools, 82, 289, 337
- multiple-system aware, 286, 322
- mx.log, 602
- mxagentconfig, 33, 85, 322, 373, 412
- mxauth, 85, 150, 154
- mxcert, 85
- mxcollection, 85, 192, 194, 197–200, 202–203, 205, 207
- mxdomainmgr, 85
- mxdtf, 85, 600
- mxexec, 82, 85, 138–139, 141–143, 145–148, 150, 154, 280, 284, 304, 556
- mxgethostname, 85
- mxglobalprotocolsettings, 85
- mxglobalsettings, 85
- mxinitconfig, 85
- mxmib, 85, 407, 411
- mxngroup, 85, 150, 153–155
- mxnode, 85, 114, 154
- mxnodesecurity, 85, 574, 578
- mypassword, 85
- mxquery, 85
- mxreport, 85, 506–507, 510–512
- mxstart, 85
- mxstm, 85, 128–129, 131–132
- mxstop, 85, 602
- mxtart, 602
- mxtask, 82, 85, 98, 280, 284, 288, 544, 556, 585
- mxtool, 85, 322, 373
 - document type definition, 337
 - other requirements, 337
 - parameterized strings, 337
 - strings substitution table, 337
 - tool filtering, 337
 - tool types, 337
 - version numbers, 337
- mxttoolbox, 85, 145–148
- mxuser, 85, 138–139, 141–143
- mxwbemsub, 85, 556, 558
- mxwsman, 85

N

- naming conventions
 - custom tools, 324, 326
- NAS Management, 477
- navigating
 - All Scheduled Tasks page, 290
 - cluster table view page, 229
 - event table view page, 235
 - Home page, 78
 - manage system types page, 126
 - picture view page, 219
 - System and Event Collections panel, 189
 - system table view page, 208
- network client
 - overview, 40
- network clients, 40
- node status, 300
- nodes
 - status, 300
- notebook, 102

O

- Open Service Event Manager, 560
- OpenSSH, 293, 319, 389, 394, 413–414, 466, 556, 611
 - command line, 414
 - install, 33
 - installing, 412–413
 - problems, 611
- OpenSSH tool
 - installing, 33
- OpenSSL, 175, 611
- OpenView GlancePlus , 477
- OpenView Performance Agent, 477
- operating system, 208, 611

- name, 124, 208
- type, 124
- version, 124
- operator-template, 144
- Oracle Viewer, 477
- orphan systems, 423
- OS name, 208
- OSEM (see Open Service Event Manager)
- other requirements
 - mxtool, 337
- overview, 177, 357
 - authorizations, 135
 - Event Monitoring Service, 483
 - GlancePlus Pak, 484
 - HP Array Configuration Utility, 492
 - HP BladeSystem Integrated Manager in HP Systems Insight Manager, 492
 - HP Client Manager, 493
 - HP Insight Power Manager, 488
 - HP OpenView Performance Agent, 488
 - HP OpenView Storage Data Protector, 487
 - HP OpenView Storage Management Appliance, 488
 - HP SIM, 33
 - HP Storage Essentials, 494
 - HP StorageWorks Command View EVA, 495
 - HP StorageWorks Command View SDM, 495
 - HP StorageWorks Command View TL, 495
 - HP StorageWorks Command View XP, 496
 - HP StorageWorks Command View XP Advanced Edition, 496
 - HP StorageWorks Modular Smart Array 1000, 496
 - HP Web Jetadmin, 493
 - HP-UX Bastille, 483
 - Ignite-UX, 484
 - Integrated Lights-Out, 484
 - managed systems, 58
 - Partition Manager, 485
 - reporting, 505
 - security, 161
 - Security Patch Check, 485
 - service notifications, 560
 - Software Distributor, 486
 - storage solutions (SNMP), 272
 - storage systems, 265
 - System Fault Management, 474
 - version control, 454
 - VPM, 493
 - VSE, 490
 - WBEM Providers for Linux, 474
 - WMI Mapper Proxy, 571
 - Workload Manager, 487
- overwrite existing data set
 - append new data set, 585

P

- pager settings
 - configuring, 76, 138
- pager support, 33
- paging notification, 611
- problems, 611
- PAM (see Pluggable Authentication Modules)
- parameterized strings
 - mxtool, 337
 - strings substitution table, 337
- parameters
 - examples, 336
- partition, 102
 - System tab, 442
- Partition Manager, 477
 - accessing, 485
 - overview, 485
- passwords
 - database account, 611
 - service account, 611
- path.properties, 602
- pausing
 - virtual machine guest, 435
- permissions, 150
- Personal Digital Assistant, 102
- physical-to-virtual
 - migrating, 421
- picture view page, 223
 - navigating, 219
- ping, 355, 402
 - alternate, 33
 - problems, 611
 - settings, 574
- plug-in tools, 419, 477, 484
 - Event Monitoring Service, 483
 - HP Array Configuration Utility, 492
 - HP BladeSystem Integrated Manager in HP Systems Insight Manager, 492
 - HP Insight Power Manager, 488
 - HP Integrity Integrated Lights Out, 370
 - HP OpenView Performance Agent, 488
 - HP OpenView Storage Data Protector, 487
 - HP OpenView Storage Management Appliance, 488
 - HP Storage Essentials, 270, 494
 - HP StorageWorks Command View EVA, 495
 - HP StorageWorks Command View SDM, 495
 - HP StorageWorks Command View TL, 495
 - HP StorageWorks Command View XP Advanced Edition, 496
 - HP StorageWorks Modular Smart Array 1000, 496
 - HP Web Jetadmin, 493
 - HP-UX Bastille, 483
 - JHP StorageWorks Command View XP, 496
 - Partition Manager, 485
 - Software Distributor, 486
 - System Fault Management, 474
 - VPM, 493
 - VSE, 490
 - WBEM Providers for Linux, 474
- Pluggable Authentication Modules, 162
 - configuring, 162
- PMP, 33, 208, 293, 535, 597 (see HP Performance Management Pack)
 - CSV file generator, 532

- offline analysis, 416
- online analysis, 416
- polling rate
 - cluster resource, 299
- polling tasks
 - customizing, 569
 - default, 277
- port 162, 579
- port 25, 611
- power cycle
 - HP ProLiant iLO, 376
- power distribution unit, 102
- power off
 - HP ProLiant iLO, 376
- power on
 - HP ProLiant iLO, 376
- power supply, 102
- printer, 102
- printing, 611
 - cluster collections, 229
 - cluster table view, 229
 - communications table, 386
 - event table view, 235
 - problems, 611
 - reports, 506–507, 510
 - system table view, 208
 - task results, 287
- printing results
 - canceling, 225, 234, 243
 - cluster search, 253
 - cluster table view page, 234
 - event search, 251
 - event table view page, 243
 - system search, 249
 - system table view page, 225
- printing search results
 - canceling, 249, 251, 253
- private collections, 189
- Process Resource Manager, 293, 489
 - accessing, 489
- product architecture, 40
- product name, 124, 208
- program
 - launching, 322
- program launch tool, 293
- program launch tools, 337
- ProLiant Support Pack, 58, 61, 69
- property pages, 33
 - accessing, 473
 - WBEM, 33, 473
- protocol
 - problems, 611
- protocol settings
 - configuring, 76
- protocols, 58, 61, 69, 581
 - configuring, 576–577
 - DMI, 93, 124, 389, 570, 574, 579, 583
 - global, 573
 - group, 576
 - HTTP, 124, 222, 244, 570, 579
 - ICMP, 574
 - IP, 93
 - OpenSSH, 317, 389
 - setting, 573
 - setting global, 50–51, 109, 268, 574
 - single system, 573, 576–577
 - SNMP, 51, 93, 114, 124, 222, 244, 319, 389, 569–570, 574, 579, 583
 - SNMP;, 394
 - SSH, 124, 389, 401
 - TCP, 574
 - WBEM, 50, 93, 114, 124, 389, 574, 578–579, 583
 - WBEM;, 394
 - WMI, 389
 - WMI Mapper Proxy, 571–573
- Provisioning Manager, 477
- public key, 597
 - security level, 597

Q

- querying
 - RPM Package Manager, 419–420
- quick launch menu
 - customizing, 295
 - system page, 295

R

- R_ArrayControllers, 513
- R_Batteries, 513
- R_CellularSysParComplex, 513
- R_CellularSysParIOChassis, 513
- R_CellularSysPartition, 513
- R_ChangerDevices, 513
- R_CPU, 513
- R_deviceLicenseInfo, 513
- R_DIMMSlots, 513
- R_EventSummary, 513
- R_Fans, 513
- R_HPUNIXFileSystem, 513
- R_HPUNIXKernelParam, 513
- R_HPUNIXLogicalVolume, 513
- R_HPUNIXNetworkDetails, 513
- R_HPUNIXPhysicalVolume, 513
- R_HPUNIXSoftwareBundle, 513
- R_HPUNIXSoftwareProduct, 513
- R_HPUNIXVolumeGroup, 513
- R_HPVMGuests, 513
- R_InstalledBoards, 513
- R_Inventory, 513
- R_lockdownStatus, 513
- R_LogicalDisks, 513
- R_MediaAccessDevices, 513
- R_NetworkInterface, 513
- R_OperatingSystem, 513
- R_PhysicalDisks, 513
- R_PowerSupply, 513
- R_Process, 513
- R_Racks, 513

- R_Software, 513
- R_StorageDeviceCapacity, 513
- R_StorageDeviceControllers, 513
- R_StorageDeviceInventory, 513
- R_StorageHostBusAdapters, 513
- R_StorageLogicalUnits, 513
- R_StoragePorts, 513
- R_SWFWBaselineInformation, 513
- R_UnixIODevices, 513
- R_UnixIPRoute, 513
- R_UnixLogicalMemory, 513
- R_UnixOSDetails, 513
- R_WarrantyContract, 513
- rack, 102, 109, 219, 223, 235, 244
 - adding a rack, 220
 - edit a rack, 222
 - editing, 222
- Rack and Power Management, 477
- rack view, 219
- racks
 - creating, 220
- Rapid Deployment Pack, 413
- RDP, 33
- Really Simple Syndication, 81
- receiving
 - Receiving alerts, 89
- recommendation
 - repair managed system communication, 380
- reference
 - commands, 85
- registering
 - MIB, 407, 409
- registration
 - HP SIM, 43
- release history, 29
- remote access device, 102
- Remote Insight Board EISA, 222
- Remote Insight Board PCI, 222
- Remote Insight Lights-Out Edition (RILOE), 222
- Remote Support Pack (see HP Service Essentials Remote Support Pack)
- remote tool, 324, 330
- Remove Depot Software, 475
- Remove Software, 475
- remove tool
 - running, 334
- removing
 - custom tools, 322
 - disk thresholds, 355
- repairing
 - communications, 380, 383
 - Configure or Repair Agents, 305–306, 312
- Replicate Agent Settings, 175, 293
 - problems, 611
- replicate agent settings
 - accessing, 417
 - creating task, 418
 - events, 419
 - trust relationship, 417, 419
- replicating, 175, 418
- Report Designer, 477
- reporting, 531–532, 611, 663
 - creating a report, 507
 - deleting a report, 512
 - editing a report, 510
 - license, 368
 - license information, 368
 - overview, 505
 - problems, 611
 - running reports, 506
 - SQL queries, 512
 - storage array capacity, 270
 - storage systems, 269
 - VCA, 461
 - views, 368, 505, 512–513
- reports, 33, 505, 532
 - authorizations, 154
 - copying, 511
 - creating, 507
 - deleting, 512
 - editing, 510
 - HP Version Control Agent, 461
 - license information, 368
 - managing, 511
 - printing, 506–507, 510
 - running, 506
 - showing SQL, 512
 - snapshot comparison, 33
 - sort order, 506–507, 510
 - storage systems, 269
 - toolbox, 148
 - user, 143
 - user groups, 143
 - version control, 461
 - views, 513
 - with HP Storage Essentials installed, 269
- requiring
 - trusted certificates, 181, 391
- resetting
 - virtual machine guest, 435
- resource library, 89
 - Changing the HP SIM system name, 89
 - HP StorageWorks Management Software, 89
 - Using OpenView, 89
 - Using the HP ProLiant Essentials Server Migration Pack, 89
- resources
 - assistance, 41
 - cluster monitor, 302, 304
 - thresholds, 304
- response, 611
 - problems, 611
- restarting
 - virtual machine guest, 435
- resuming
 - virtual machine guest, 434
- retries
 - setting global defaults, 574

- Retrieve WLM Configuration, 475
- rights, 135
- ROM flash, 465
- router, 102, 124
- RPM (see RPM Package Manager)
- RPM Package Manager, 419
 - accessing, 419
 - installing, 419–420
 - querying, 419–420
 - uninstalling, 419–420
 - verifying, 419, 421
- RSS (see Really Simple Syndication)
- rules
 - creating STM rules, 129
 - deleting STM rules, 126
 - DMI, 132
 - editing STM rules, 131
 - SNMP, 132
 - STM, 132
 - System Type Manager, 402
- run tools tab
 - communications, 382
- running
 - clear events task, 552
 - custom tools, 329
 - data collection task, 585
 - discovery task, 97, 101
 - events task, 565
 - remove tool, 334
 - reports, 506
 - tasks, 284, 290

S

- saving
 - collections, 196, 565
 - system collection, 208
- scheduling
 - clear events task, 552, 565
 - custom tools, 329
 - data collection task, 585
 - discovery task, 98
 - event tasks, 565–566
 - tasks, 277, 283
- script launch tools, 337
- SD Job Browser, 475
- search, 78
 - problems, 611
 - saving, 196
 - system, 196
- search criteria, 223, 235, 570, 583
 - cluster, 253
 - event, 253
 - system, 253
- searching, 611
 - advanced, 245–246, 248, 250, 252
 - basic, 245–247
 - clusters, 252
 - criteria, 253
 - deleting clusters, 253

- deleting events, 251
- deleting systems, 250
- event, 245
- events, 250
- hierarchical displays, 246
- system, 245
- systems, 248
- tools, 245, 296–297
- secure shell, 33, 597
 - install, 33
- Secure Sockets Layer, 161
- secure sockets layer, 33
- secure task execution, 164
- security, 175, 611
 - about trust relationships, 181, 393
 - options, 161
 - overview, 161
 - problems, 611
 - role-based, 33
 - secure task execution, 164
 - sign-in, 162
 - sign-in event settings, 166
 - System Link Configuration, 165
 - timeout, 166
- security alert, 611
- security level
 - SSH keys, 598
- Security Patch Check, 477
 - overview, 485
- server, 102
 - protocols, 581
 - system tab, 423
- server blade, 423
- server certificate, 175
- Server Certificate page, 167
- server certificates, 167, 173–175
 - creating, 167, 169
 - editing, 167, 170
 - exporting, 172
 - importing, 167, 171
 - synchronizing, 175
- service account
 - password, 611
- service and support, 723
- service events (see service notifications)
- service notifications
 - configuring, 560
 - details, 560
 - overview, 560
- Serviceguard Manager, 208, 611
 - problems, 611
- setting
 - disk thresholds, 355
 - global protocols, 109
 - language, 82
 - locale, 82
 - ping, 574
 - trust relationships, 181, 393
- setting global defaults

- DMI, 574
- HTTP, 574
- retries, 574
- SNMP, 574
- timeouts, 574
- WBEM, 574
- setting properties
 - cluster collections, 199
 - event collections, 207
 - system collections, 199
- setting up
 - HP SIM, 76
 - managed systems, 58
 - managed systems - HP-UX, 61
 - managed systems - Linux, 58
 - managed systems - Windows, 69
- settings
 - disk thresholds, 356
 - sign-in event, 166
 - task wizard, 279
- setup
 - initial, 76
- severity
 - event, 243
- SFM (see System Fault Management)
- shared collections, 189, 258
- sign-in, 161
 - configuring events, 166
 - failure, 162
 - problems, 611
- sign-in address restrictions, 138
- sign-in events
 - settings, 166
- signing in
 - automatically, 162
 - GUI, 44
 - manually, 162
 - remotely, 44
 - using SSL, 44
- signing out
 - CLI, 48
 - GUI, 48
- Simple Network Management Protocol*, 394
- single login, 162, 181
- single system protocol settings, 573
 - setting, 583
- single-system aware tools, 82, 286, 322, 337
- SMI CIMOM, 50, 574
- SMI-S providers
 - storage systems, 268
- SMI-S systems
 - WBEM indications, 33
- SMP Universal (see HP ProLiant Essentials Server Migration Pack)
 - adding license, 421
 - licensing, 421
- SMTP settings, 54, 550
- snapshot comparison, 33, 531
- snapshot comparisons, 585
- SNMP, 48, 51, 54, 58, 61, 69, 109, 124, 222, 244, 318, 389, 394, 423, 428, 485, 569–570, 574, 579, 583, 597–599
 - adding rules, 132
 - agent problems, 611
 - configuring access, 354
 - deleting rules, 126
 - installing provider, 319
 - port 162, 579
 - rules, 128
 - setting global defaults, 574
 - SnmpTrapPortAddress, 579
 - trap, 244, 538, 540
 - trap problems, 611
 - traps, 569
- SNMP access
 - configuring, 293
- SNMP agent, 611
- SNMP provider
 - installing, 318
- SNMP Settings, 576–577
- SNMP status polling, 222
- SNMP trap, 235
- SNMP trap settings
 - events, 538
- SNMP traps, 540, 558, 560
 - configuring, 554
 - fields, 554
- SOAP, 337
- Socks, 611
- software
 - administering, 535
 - status, 228
- software deployment, 477
- Software Distributor, 33, 477
 - accessing, 486
 - overview, 486
 - Virtual Machine Management Pack, 486
- Software Distributor Job Browser, 475
- Software Package Builder, 477
- software status, 208, 423, 611
 - problems, 611
- software status polling, 570
- specifying
 - ip ranges, 109
- SQL queries, 512
- SSA (see single-system aware tools)
- SSH, 33, 58, 61, 69, 82, 124, 319, 322, 389, 401, 597, 599 (see secure shell)
 - Using SSH, 89
- SSH bypass properties
 - configuring, 600
- SSH Keys
 - deleting, 599
- SSH keys, 597
 - deleting, 597
 - exporting, 597, 599
 - importing, 597, 599
 - managing, 33, 598

- security level, 597
- SSH provider
 - installing, 319
- SSH security level, 598
- SSH Settings, 576–577
- SSL (see Secure Sockets Layer) (see secure sockets layer)
- SSL port
 - changing, 167
- start using, 43
- starting
 - virtual machine guest, 434
- status
 - event, 80
 - node, 300
 - software, 228
 - system, 226
 - WBEM status, 227
- status polling
 - DMI, 569
 - hardware, 574
 - hardware status polling, 569
 - initial, 124
 - SNMP, 222
 - software status polling, 569
- STE (see secure task execution)
- STM (see System Type Manager)
 - adding rules, 126
- STM rule reference, 132
- stopping
 - discovery task, 97, 101
 - tasks, 277, 288–289
 - virtual machine guest, 436
- storage array
 - System tab, 447
- storage device, 102
- storage device managers
 - overview, 494
- storage host
 - System tab, 443
- storage integration
 - overview, 265
- storage solutions (SNMP)
 - about, 272
 - configuring event collection, 275
 - discovery, 273–274
 - overview, 265, 272, 275
 - searching for, 275
- storage switch
 - System tab, 445
- storage system problems, 611
- storage systems (SMI-S)
 - discovery, 268
 - overview, 265
 - SMI-S providers, 268
 - storage systems, 269
 - viewing, 268
 - viewing array capacity, 270
 - WBEM event indications, 268
 - with HP Storage Essentials, 270
- submitting
 - CSR, 173
- Subscribe to WBEM Events, 475
- subscribing
 - health lifecycle indications, 558
 - WBEM events, 538, 557
 - WBEM indication events, 268
 - WBEM indications, 556
- Superdome, 33
- support, 41
- suspending
 - system monitoring, 33
- switch, 102, 124, 208, 611
 - problems, 611
- Sybase Viewer, 477
- synchronizing
 - server certificates, 175
- Syntax Check Configuration, 475
- Syntax Check on the Systems Insight Manager Server Configuration, 475
- system, 611
 - identification, 535
 - port types, 452
 - problems, 611
 - search, 196
 - searching, 245
 - status, 226
 - WBEM status, 227
- system address, 208
- System and Event Collections panel
 - navigating, 189
 - tree controls, 189
- system automatic discovery, 52
- system collections
 - copying, 197
 - creating, 192
 - customizing, 191–192, 208
 - deleting, 198
 - editing, 194
 - managing, 208
 - moving, 197
 - overview, 189
 - printing, 208, 225
 - report, 225
 - setting properties, 199
 - shared, 258
- System Fault Management
 - accessing, 474
 - overview, 474
- system filters
 - adding to tasks, 280
- system groups
 - managing, 155
- system key, 78
- system locator
 - HP 9000 iLO, 371
 - HP Integrity, 371
- System Management Homepage, 422
 - accessing, 422

- trust relationships, 181
- system monitoring
 - resume, 33, 585
 - resume multiple systems, 596
 - resume single system, 595
 - suspend, 33, 585
 - suspend multiple systems, 596
 - suspend single system, 595
 - when HP Storage Essentials is installed, 270
- system name, 208, 235
- system overview, 187
- system page, 219, 222, 235, 275, 423, 428, 430, 432, 434–438, 440–443, 445, 447, 450, 473, 573, 583, 611
 - Essentials tab, 454
 - event, 423
 - identity, 423
 - links, 423
 - protocols, 581
 - quick launch menu, 295
 - tools & links, 452
- system power
 - HP 9000 iLO, 371
 - HP Integrity, 371
- system properties, 611
 - edit, 33
 - edit for single system, 586
 - editing, 33
 - set for multiple systems, 592
 - when HP Storage Essentials is installed, 270
- system resource, 302
- system search results
 - printing, 249
- system status, 189
- system status panel, 78
 - customizing, 80
 - pop-up window, 81
- system subtypes, 443, 445, 447, 450
 - when HP Storage Essentials is installed, 270
- System tab
 - cluster, 440
 - complex, 441
 - management processor, 428
 - partition, 442
 - storage array, 447
 - storage host, 443
 - storage switch, 445
 - tape library, 450
 - virtual machine guest, 432
 - virtual machine host, 430
- system tab
 - protocols, 581
 - server, 423
- system table view
 - printing results, 208
- system table view page, 109, 120, 189, 219, 222–223, 225, 229, 246, 275, 295, 355, 423, 485, 583, 611
 - adding columns, 224
 - customizing, 208, 224
 - deleting columns, 224
 - deleting systems, 208
 - navigating, 208
 - overview, 208
 - printing, 225
 - saving collection, 208
 - sorting, 224
- system type, 109, 208
- System Type Manager, 102, 126, 128
 - creating new rule, 129
 - deleting rule, 132
 - DMI rules, 132
 - editing SNMP rule, 131
 - SNMP rules, 132
- system types, 102
- systems, 362
 - configuring links, 165
 - deleting, 208, 225, 250
 - identification, 124
 - monitoring, 187
 - orphan, 423
 - searching, 248

T

- tape library
 - System tab, 450
- target system
 - task schedule, 280
- task instance, 277
 - deleting, 288
 - viewing, 286
- task results
 - automatic event handling tasks, 542
 - deleting, 289
 - printing, 287
 - viewing, 283, 286, 289–290, 552, 565–566
- task results list, 289
 - task instance , 289
- task wizard
 - settings, 279
- tasks, 33, 280, 611
 - copying, 548
 - creating, 277, 280
 - data collection, 583
 - default, 277
 - deleting, 277, 286, 290
 - details, 244
 - editing, 277, 285, 290, 547
 - instance, 277
 - paging, 564
 - polling, 277
 - problems, 611
 - Replicate Agent Settings, 418
 - running, 284, 290
 - scheduling, 277, 283
 - status, 289
 - stopping, 277, 288–289
 - time filtering, 283
 - track status, 277

- user privileges, 277, 290
- viewing, 286
- viewing configuration, 548
- viewing results, 549
- TCP, 574
- TDEF (see tool definition files)
- template
 - users, 144
- thin client, 102
- thresholds
 - cluster monitor, 304
- time filters, 283
 - applying, 283, 544, 564, 567
 - copying, 283
 - creating, 283
 - deleting, 283
 - editing, 283
 - managing, 283
- timeout
 - configuring options, 166
 - setting, 570
- timeouts
 - setting global defaults, 574
- tool definition files, 33, 600
- tool definition
 - viewing, 334
- tool filtering
 - mxtool, 337
- tool types
 - mxtool, 337
- toolbox
 - report, 148
- toolboxes, 135, 145, 148
 - create, 145
 - creating, 145
 - delete, 145
 - deleting, 147
 - edit, 145
 - editing, 146
 - HP Storage Essentials, 145, 270
 - reports, 145
- tools, 33, 458–459, 611
 - assistance, 477
 - cluster monitor, 293
 - command line, 293, 304
 - command line tools, 293
 - custom, 293
 - default, 293
 - device ping, 293
 - disk thresholds, 293
 - HP ProLiant Support Pack, 293
 - license manager, 293
 - licensing , 293
 - managing tools, 293
 - OpenSSH, 293
 - ping, 355
 - PMP, 293
 - problems, 611
 - program launch, 293

- property pages, 293
- Replicate Agent Settings, 293
- Resource Process Manager, 293
- searching for, 245, 296–297
- Serviceguard clusters, 293
- system information, 293
- system page, 293
- System Type Manager, 126, 128
- update system software, 293
- using, 293
- version control, 293
- WBEM, 473
 - web page tools, 293
- trademarks, 29
- transitioning
 - Transitioning to HP SIM , 89
- trap, 244
 - details, 244
- tree controls, 189
- tree view, 215
- troubleshooting, 89, 611
- trust relationship, 161
 - CMS, 44
- trusted certificate, 177, 181
 - deleting, 180
 - exporting, 179
 - importing, 178
- trusted certificates
 - always accept, 391
 - deleting, 177
 - exporting, 177
 - importing, 177
 - requiring, 391

U

- un-assigning licenses, 366
- understanding
 - Understanding security, 89
- uninstalling
 - RPM Package Manager, 419–420
- UNIX
 - commands, 337
- unknown, 102
- unmanaged, 102
- unregistering
 - MIB, 411
- Unsubscribe to WBEM Events, 475
- unsubscribing
 - health lifecycle indications, 558
 - WBEM events, 538, 557
 - WBEM indications, 556
- updating
 - authorizations, 148, 153
 - communications, 385
 - Configure or Repair Agents, 306, 312
- upgrading, 33
 - HP 9000 iLO firmware, 375
 - HP Integrity firmware, 375
- UPS, 102

- user groups, 139, 148
 - adding, 139
 - administering, 137
 - deleting, 142
 - editing, 141
 - report, 143
- user rights, 135
- user settings, 54
- user templates, 138
 - default, 144
- user-template, 144
- users, 138, 148
 - administering, 137
 - authorizing, 150
 - CMS security configuration rights, 138
 - creating, 76, 138
 - deleting, 142
 - editing, 141
 - overview, 137
 - pager settings, 138
 - report, 143
 - sign-in address restrictions, 138

V

- varbind mappings, 411
- VCRM
 - catalog problems, 611
- verifying
 - RPM Package Manager, 419, 421
- version control, 33, 319, 455–460, 463
 - installing, 319
 - overview, 454
 - reports, 461
 - ROM firmware updates, 465
- version control agent, 208
- version control repository
 - selecting, 596
- version control tab
 - communications, 382
- version numbers
 - mxtool, 337
- viewing
 - audit log, 601
 - cluster CPU utilization, 303
 - data collection task results, 585
 - licensed systems, 361
 - MIB list, 407, 409
 - scheduled tasks, 286
 - task configuration, 548
 - task instance, 286
 - task results, 283, 286, 289–290, 549, 552, 565–566
 - tasks, 286
 - tool definition, 334
- viewing definition
 - automatic event handling tasks, 542
- views, 532
- virtual connect domain, 102
- virtual machine
 - launching remote console, 434

- problems, 611
- virtual machine guest
 - pausing, 435
 - resetting, 435
 - restarting, 435
 - resuming, 434
 - starting, 434
 - stopping, 436
 - System tab, 432
 - virtual machine performance tab, 438
- virtual machine host
 - system tab, 430
 - virtual machine performance tab, 437
- Virtual Machine Management Pack, 33
- virtual machine performance tab
 - virtual machine guest, 438
 - virtual machine host, 437
- virtual-to-physical
 - migrating, 421
- virtual-to-virtual
 - migrating, 421
- virtualization and automation management, 477
- Virtualization Manager, 477
- VM server, 33
- VMS Loader, 477
- VPM, 208

W

- Wake on LAN, 419
- warranty, 29
- WBEM, 48, 50, 54, 58, 61, 124, 161, 317, 389, 394, 423, 428, 485, 574, 583
 - certificates, 394
 - installing provider, 317
 - setting global defaults, 574
 - status, 227
 - tools, 473
- WBEM certificates, 161
- WBEM indications, 33, 558
 - HP-UX systems, 33
 - Linux systems, 33
 - port, 556
 - SMI-S systems, 33
 - subscribing, 556–557
 - subscribing to, 538
 - unsubscribing, 556–557
 - unsubscribing to, 538
- WBEM property pages, 33
- WBEM providers, 394
- WBEM Providers for Linux
 - accessing, 474
 - overview, 474
- WBEM Settings, 576–577
- WBEM status
 - bypassing, 570
- Web JetAdmin, 477
- web launch tools
 - parameters, 336
- web page tool, 293

- creating, 328
- editing, 332
- web page tools, 322
- Web-Based Enterprise Services, 560
- Web-launch aware tools, 337
- WEBES (see Web-Based Enterprise Services)
- Webmin, 486
 - accessing, 486
- what's new, 37
- Windows, 602
 - configuring locale, 82
 - managed systems, 69
 - viewing MIB list, 407
- Windows NT Event Log
 - problems, 611
- Windows NT event log, 611
- Windows XP Service Pack 2, 611
- WLA (see Web-launch aware tools)
- WMI, 389, 394
 - installing provider, 317
- WMI Mapper, 401
- WMI Mapper Proxy, 583
 - adding, 571–572
 - deleting, 225, 571, 573
 - editing, 571–572
 - overview, 571
- WMI/WBEM provider
 - installing, 317
- WMIMapper
 - problems, 611
- Workload Management Pack, 477
- Workload Manager
 - overview, 487
- workstation, 102
- WS-Management, 124

X

- X clients , 82
- X Resource file properties , 82
- xlsfonts, 82