IBM® Client Security
解决方案

# 将 Client Security Software 版本 4.0 与 Policy Director 一起使用

IBM® Client Security
解决方案

# 将 Client Security Software 版本 4.0 与 Policy Director 一起使用

**第一版（2002 年 3 月）**

在使用本资料及其支持的产品之前，请务必阅读第 27 页的附录 A，『针对 Client Security Software 的美国出口法规』和第 33 页的附录 D，『**声明和商标**』。

# 目录


**前言 . . . . . v**
应阅读本指南的人员 . . . . . v
如何使用本指南 . . . . . v
*对《Client Security Software 安装指南》*的引用 . . . . . vi
对*《Client Security Software 管理员指南》*的引用. . . . . vi
附加信息 . . . . . vi

**第 1 章 介绍 IBM Client Security Software . . . . . 1**
Client Security Software 应用程序和组件 . . . . . 1
公共密钥基础结构（PKI）功能. . . . . 1

**第 2 章 在 Policy Director 服务器上安装 Client Security 组件 . . . . . 3**
先决条件. . . . . 3
下载并安装 Client Security 组件 . . . . . 3
在 Policy Director 服务器上添加 Client Security 组件 . . . . . 4
在 IBM 客户机和 Policy Director 服务器之间建立安全连接 . . . . . 4

**第 3 章 配置 IBM 客户机 . . . . . 7**
先决条件. . . . . 7
配置 Policy Director 设置信息. . . . . 7
设置并使用本地本地高速缓存功能 . . . . . 7
启用 Policy Director 以控制 IBM 客户机对象 . . . . . 8
编辑本地 UVM 策略 . . . . . 8
编辑和使用远程客户机的 UVM 策略 . . . . . 9

**第 4 章 故障诊断. . . . . 11**
管理员功能 . . . . . 11
设置管理员密码（NetVista） . . . . . 11
设置超级用户密码（ThinkPad） . . . . . 12
保护硬件密码. . . . . 12
清除 IBM 嵌入式安全芯片（NetVista） . . . . . 13
清除 IBM 嵌入式安全芯片（ThinkPad） . . . . . 13
Administrator Utility . . . . . 14
删除用户 . . . . . 14
使用 Policy Director 控件来拒绝访问所选择的对象 . . . . . 14
已知限制 . . . . . 14
将 Client Security Software 与 Windows 操作系统一起使用. . . . . 14
将 Client Security Software 与 Netscape 应用程序一起使用 . . . . . 14
IBM 嵌入式安全芯片证书和加密算法 . . . . . 15
使用 Lotus Notes 用户标识的 UVM 保护 . . . . . 15
Client Utility 限制 . . . . . 15
错误消息 . . . . . 16
故障诊断图表. . . . . 16
安装故障诊断信息 . . . . . 16
Administrator Utility 故障诊断信息 . . . . . 17
Client Utility 故障诊断信息 . . . . . 18
特定于 ThinkPad 的故障诊断信息 . . . . . 19
Microsoft 故障诊断信息 . . . . . 19
Netscape 应用程序故障诊断信息 . . . . . 21

数字证书故障诊断信息 . . . . . 23
Policy Director 故障诊断信息 . . . . . 23
Lotus Notes 故障诊断信息 . . . . . 24
加密故障诊断信息 . . . . . 24
UVM 感知设备故障诊断信息 . . . . . 24

**附录 A. 针对 Client Security Software 的美国出口法规 . . . . . 27**

**附录 B. 密码和密码短语规则 . . . . . 29**
硬件密码规则 . . . . . 29
UVM 密码短语规则 . . . . . 29

**附录 C. 使用系统登录的 UVM 保护的规则 . . . . . 31**

**附录 D. 声明和商标 . . . . . 33**
声明 . . . . . 33
商标 . . . . . 33

# 前言

本指南包含有关设置 Client Security Software 以便与 IBM SecureWay Policy Director（Policy Director）一起使用的有帮助的信息。

本指南组织如下:

“第 1 章, 『**介绍 IBM Client Security Software**』, ” 包含与 Client Security Software 一起提供的组件的概述。

“第 2 章, 『在 Policy Director 服务器上安装 Client Security 组件』, ” 包含有关在 Policy Director 服务器上安装 Client Security 支持的先决条件和指示信息。

“第 3 章, 『配置 IBM 客户机』, ” 包含配置 IBM 客户机以使用 Policy Director 提供的认证服务的先决条件信息和指示信息。

“第 4 章, 『故障诊断』, ” 包含有关解决在使用本指南中提供的指示信息时可能遇到的问题的有帮助的信息。

“附录 A, 『针对 Client Security Software 的美国出口法规』, ” 包含有关软件的美国出口法规信息。

“附录 B, 『密码和密码短语规则』, ” 包含 UVM 密码短语和安全芯片密码的规则。

“附录 C, 『**使用系统登录的 UVM 保护的规则**』, ” 包含有关使用操作系统登录的 UVM 保护的信息。

“附录 D, 『**声明和商标**』, ” 包含法律声明和商标信息。

## 应阅读本指南的人员

本指南是供企业管理员使用的, 这些管理员使用 Policy Director 版本 3.7 或版本 3.8 来管理由 IBM 客户机上的 User Verification Manager（UVM）安全性策略设置的认证对象。

管理员必须在以下概念和过程方面有渊博的知识:

- SecureWay Directory 轻量级目录访问协议（LDAP）的安装和管理
- Policy Director Runtime Environment 的安装和设置过程
- Policy Director 对象空间的管理

## 如何使用本指南

使用本指南来设置 Client Security 支持, 以便与 Policy Director 一起使用。本指南是 *《Client Security Software 安装指南》*、*《Client Security Software 管理员指南》*和 *《Client Security 用户指南》*的姊妹篇。

本指南和所有 Client Security 的其它文档可从 IBM Web 站点下载: http://www.pc.ibm.com/ww/security/secdownload.html。

## 对《*Client Security Software 安装指南*》的引用

本文档中提供了对《*Client Security Software 安装指南*》的引用。设置和配置 Policy Director 服务器并在客户机上安装了 Runtime Environment 后，请使用《*Client Security Software 安装指南*》中的指示信息在 IBM 客户机上安装 Client Security Software。有关更多信息，请参阅第 7 页的第 3 章，『配置 IBM 客户机』。

## 对《*Client Security Software 管理员指南*》的引用

本文档中提供了对《*Client Security Software 管理员指南*》的引用。《*Client Security Software 管理员指南*》包含如何设置 IBM 客户机的用户认证和 UVM 策略的信息。安装了 Client Security Software 后，请使用《*Client Security Software 管理员指南*》来设置用户认证和安全性策略。有关更多信息，请参阅第 7 页的第 3 章，『配置 IBM 客户机』。

---

## 附加信息

可从 IBM Web 站点获取附加信息和安全性产品更新（当可用时）：http://www.pc.ibm.com/ww/security/securitychip.html。

# 第 1 章 介绍 IBM Client Security Software

Client Security Software 是为使用 IBM 嵌入式安全芯片加密并存储加密密钥的 IBM 计算机设计的。此软件由应用程序和组件组成，这些应用程序和组件使 IBM 客户机能够在本地网络、企业或因特网范围内使用客户机安全性。

## Client Security Software 应用程序和组件

当您安装 Client Security Software 时，将安装以下软件应用程序和组件:

- **Administrator Utility**: Administrator Utility 是管理员用于激活或取消激活嵌入式安全芯片，并用于创建、归档和重新生成加密密钥及密码短语的界面。此外，管理员可以使用此实用程序将用户添加到由 Client Security Software 提供的安全性策略。
- **User Verification Manager（UVM）**: Client Security Software 使用 UVM 来管理密码短语和其它元素以认证系统用户。例如，UVM 可以使用指纹阅读器进行登录认证。UVM 软件启用以下功能:
  - **UVM 客户机策略保护**: UVM 软件使管理员可以设置客户机安全性策略，这就指定了客户机用户如何在系统上得到认证。
  - **UVM 系统登录保护**: UVM 软件使管理员可以通过登录界面控制计算机访问。UVM 保护确保只有经安全性策略识别的用户才可以访问操作系统。
  - **UVM Client Security 屏幕保护程序保护**: UVM 软件使用户可以通过 Client Security 屏幕保护程序界面控制对计算机的访问。
- **Client Utility**: Client Utility 使客户机用户可以更改 UVM 密码短语。在 Windows NT 上，Client Utility 使用户可以更改 Windows NT 登录密码以让 UVM 识别，并可以更新密钥压缩文档。用户也可以用 IBM 嵌入式安全芯片创建数字证书的备份副本。

## 公共密钥基础结构（PKI）功能

Client Security Software 提供在商务中创建公用密钥基础结构（PKI）要求的所有组件，例如:

- **对客户机安全性策略的管理员控制。**认证客户机级别的最终用户是安全性策略的一个重要内容。Client Security Software 提供管理 IBM 客户机的安全性策略要求的界面。此界面是认证软件 User Verification Manager（UVM）的一部分，它是 Client Security Software 的主要组件。
- **公用密钥密码术的加密密钥管理。**管理员用 Client Security Software 创建计算机硬件和客户机用户的加密密钥。创建了加密密钥后，它们通过密钥层绑定到 IBM 嵌入式安全芯片，基础级别硬件密钥用于在其上加密密钥，包含与每个客户机用户相关的用户密钥。IBM 嵌入式安全芯片上的加密和存储密钥添加客户机安全性的基本附加层，因为这些密钥已安全地绑定到计算机硬件上。
- **受 IBM 嵌入式安全芯片保护的数字证书创建和存储。**当您应用可以用于数字签名或加密电子邮件消息的数字证书时，Client Security Software 使您可以选择 IBM 嵌入式安全芯片作为使用 Microsoft CryptoAPI 的应用程序的加密服务供应商。这些应用程序包含 Internet Explorer 和 Microsoft Outlook Express。这确保了数字证书的专用密钥存储在 IBM 嵌入式安全芯片上。Netscape 用户也可以选择 IBM 嵌入式安全芯

片作为用于安全性的数字证书的专用密钥生成器。使用公用密钥密码术标准（PKCS）#11 的应用程序（例如 Netscape Messenger）可以利用由 IBM 嵌入式安全芯片提供的保护。

- **密钥压缩文档和恢复解决方案。**一个重要的 PKI 功能是在原密钥丢失或遭破坏时创建一个可以从其恢复密钥的密钥压缩文档。Client Security Software 提供使您可以建立由 IBM 嵌入式安全芯片创建的用于密钥和数字证书的压缩文档的界面，并使您可以在必要时恢复这些密钥和证书。
- **“右键单击加密”。**“右键单击加密”使客户机用户可以通过单击鼠标右键简便地加密其文件。

# 第 2 章 在 Policy Director 服务器上安装 Client Security 组件

认证客户机级别的最终用户的客户机级别是是安全性的一个重要内容。Client Security Software 提供管理 IBM 客户机的安全性策略所要求的界面。此界面是认证软件 User Verification Manager（UVM）的一部分，它是 Client Security Software 的主要组件。

IBM 客户机的 UVM 安全性策略可以通过两种方式来管理:

- 在本地使用驻留在 IBM 客户机上的策略编辑器
- 在企业范围内使用 Policy Director

可以将 Client Security 与 Policy Director 一起使用之前，必须安装了 Policy Director 的 Client Security 组件。此组件可以从 IBM Web 站点下载: http://www.pc.ibm.com/ww/security/secdownload.html。

## 先决条件

可以在 IBM Client 和 Policy Director 服务器之间建立安全连接前，必须在 IBM Client 上安装了以下组件:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Policy Director Runtime Environment

有关安装和使用 Policy Director 的详细信息，请参阅以下 Web 站点上提供的文档: http://www.tivoli.com/products/index/secureway_policy_dir/index.htm。

## 下载并安装 Client Security 组件

Client Security 组件可从 IBM Web 站点免费下载。要在 Policy Director 服务器和 IBM 客户机上下载并安装 Client Security 组件，请完成以下过程:

1. 从以下 Web 站点下载 PDCS.exe: http://www.pc.ibm.com/ww/security/secdownload.html。
2. 单击链接以下载 Client Security Software，然后完成注册表单和问卷。

   PDCS.exe 可从包含 Client Security Software 代码的相同 IBM Web 页面获得。
3. 运行 PDCS.exe 以解压缩以下文件:
   - **PD_Add_ClientSecurity.txt** 此文件用于在 Policy Director 服务器上添加 IBM Solution 对象空间、Client Security Action 和个别 ACL 项。可以编辑或除去个别 ACL，然而，千万不要更改 IBM Solution 对象空间和 Client Security Action。
   - **PD_Remove_ClientSecurity.txt** 此文件可用于除去由 PD_Add_ClientSecurity.txt 文件创建的 OBject Space、Action 和 ACL 项。
   - **PDCS.conf** Policy Director/Client Security 配置文件（PDCS.conf）用作基本配置文件。

## 在 Policy Director 服务器上添加 Client Security 组件

pdadmin 实用程序是管理员可以用于执行大多数 Policy Director 管理任务的命令行工具。多个命令执行使管理员可以使用包含多个 pdadmin 命令的文件来执行完整的任务或系列任务。pdadmin 实用程序和 Management Server（pdmgrd）之间的通信通过 SSL 保护。pdadmin 实用程序作为 Policy Director Runtime Environment（PDRTE）软件包的一部分来安装。

pdadmin 实用程序接受识别这种文件位置的 filename 自变量，例如:

```
MSDOS>pdadmin [-a <admin-user >][-p <password >]<file-pathname >
```

以下命令是如何在 Policy Directory 服务器上创建 IBM Solution 对象空间、Client Security Action 和个别 ACL 项的命令示例:

```
MSDOS>pdadmin -a sec_master -p password C:\PD_Add_ClientSecurity.txt
```

有关 pdadmin 实用程序及其命令语法的更多信息，请参考 *Policy Director Base Administrator Guide*。

## 在 IBM 客户机和 Policy Director 服务器之间建立安全连接

IBM Client 必须在 Policy Director 安全域中建立其自己的认证的标识，以请求来自 Policy Director Authorization Service 的授权决定。

必须在 Policy Director 安全域中为应用程序创建唯一的标识。为了让认证的标识执行认证检查，该应用程序必须是 remote-acl-users 组的一个成员。当应用程序想与安全域服务之一联系时，它必须首先登录到安全域。

svrsslcfg 实用程序使 IBM Client Security 应用程序可以与 Policy Director Management Server / Authorization Server 通信。

svrsslcfg 实用程序执行以下任务:

- 创建应用程序的用户标识。例如，DemoUser/HOSTNAME
- 创建该用户的 SSL 密钥文件。例如，DemoUser.kdb 和 DemoUser.sth
- 将用户添加到 remote-acl-users 组

需要以下参数:

- **-f cfg_file** 使用 PDCS.conf 配置文件路径和文件名
- **-d kdb_dir** 用于包含服务器的密钥环数据库文件的目录。
- **-n server_name** 未来的 IBM Client 用户的实际 Windows Username/UVM 用户名。
- **-P admin_pwd** Policy Director Administrator 密码。
- **-s server_type** 必须指定为远程。
- **-S server_pwd** 新创建的用户的密码。要求此参数。
- **-r port_num** 设置 IBM Client 的监听端口号。这是在 PD Management Server 的 Policy Director Runtime 变量 SSL Server Port 中指定的参数。

要在 IBM 客户机和 Policy Director 服务器之间建立安全连接，请完成以下过程:

1. 创建目录并将 PDCS.conf 文件移动到新目录。

例如，MSDOS> mkdir C:\PDCS MSDOS> move C:\PDCS.conf C:\PDCS\

2. 运行 svrsslcfg 以创建用户。

   MSDOS> svrsslcfg -config -f C:\PDCS\PDCS.conf -d C:\PDCS\ -n <server_name> -s remote -S <server_pwd> -P <admin_pwd> -r 7135

   **注**: 用 IBM 客户机未来的 UVM 用户名和主机名替换 <server_name>。例如: –n DemoUser/MyHostName。通过在 MSDOS 提示符下输入 “hostname” 可以查找 IBM Client Hostname。svrsslcfg 实用程序将在 Policy Director 服务器中创建有效的项并为加密的通信提供唯一的 SSL 密钥文件。

3. 运行 svrsslcfg 以将 ivacld 的位置添加到 PDCS.conf 文件。

   缺省情况下，PD Authorization 服务器监听端口 7136。这可以通过在 Policy Director 服务器上的 ivacld.conf 文件的 ivacld stanz 中查找 tcp_req_port 参数来验证。获取正确的 ivacld 主机名很重要。请使用 pdadmin 服务器列表命令来获取此信息。服务器名命为: <server_name>-<host_name>。以下是运行 pdadmin 服务器列表的示例:

```
MSDOS> pdadmin server list ivacld-MyHost.ibm.com
```

然后用以下命令为上面显示的 ivacld 服务器添加 replica 项。假定 ivacld 监听缺省端口 7136。

```
svrsslcfg -add_replica  -f <config file path> -h <host_name> MSDOS>svrsslcfg
-add_replica  -f C:\PDCS\PDCS.conf -h MyHost.ibm.com
```

# 第 3 章 配置 IBM 客户机

可以使用 Policy Director 来控制 IBM 客户机的认证对象前，必须通过使用 Administrator Utility 来配置每个客户机，它是 Client Security Software 提供的一个组件。这部分包含配置 IBM 客户机的先决条件和指示信息。

## 先决条件

确保以下软件按下列顺序安装在 IBM 客户机上:

1. **Microsoft Windows 支持的操作系统。**可以使用 Policy Director 来控制仅用于运行 Windows NT Workstation 4.0 或 Windows 2000 的 IBM 客户机的认证要求。
2. **Client Security Software 版本 3.0 或后续版本。**安装该软件，并启用 IBM 嵌入式安全芯片。请使用 Administrator Utility 来设置用户认证并编辑 UVM 安全性策略。有关安装和使用 Client Security Software 的全面的指示信息，请参阅《*Client Security Software 安装指南*》和《*Client Security Software 管理员指南*》。

## 配置 Policy Director 设置信息

通过使用 Administrator Utility 可以配置 Policy Director 设置信息，Administrator Utility 是 Client Security Software 提供的一个软件组件。Policy Director 设置信息由以下设置组成:

- 选择到 Configuration File 的完全路径
- 选择 Local Cache Refresh Interval

要在 IBM 客户机上配置 Policy Director 设置信息，请完成以下过程:

1. 单击**开始 > 程序 > Client Security Software Utilities > Administrator Utility**。
2. 输入硬件密码，并单击 **OK**。

   Administrator Utility 窗口打开。有关使用 Administrator Utility 的完整信息，请参阅《*Client Security Software 管理员指南*》。
3. 在 Administrator Utility 中，单击 **Configure Application Support and Policies** 按钮。
4. 单击 **Policy Configuration** 按钮。
5. 在 Policy Director Setup Information 下，选择到 PDCS.conf 配置文件的完全路径。例如，`C:\PDCS\PDCS.conf`
6. 单击 **Apply** 按钮。

## 设置并使用本地本地高速缓存功能

选择 Policy Director 配置文件后，可以设置本地高速缓存刷新间隔。由 Policy Director 管理的安全性策略信息的本地复本在 IBM 客户机上维护。可以在月（0-12）或日（0-30）的增量中调度本地高速缓存的自动刷新。

要设置或刷新本地高速缓存，请完成以下过程:

1. 单击**开始 > 程序 > Client Security Software Utilities > Administrator Utility**。
2. 输入硬件密码，并单击 **OK**。

Administrator Utility 窗口打开。有关使用 Administrator Utility 的完整信息，请参阅《*Client Security Software 管理员指南*》。

3. 单击 **Configure Application Support and Policies** 按钮。
4. 单击 **Policy Configuration** 按钮。
5. 执行以下操作之一:
   - 要刷新本地高速缓存，请单击 **Refresh Local Cache**。
   - 要设置自动刷新速率，请在提供的字段中输入月（0-12）和天（0-30），然后单击 **Apply**。将更新本地高速缓存文件过期日期以指示下一个自动刷新何时发生。

     **注**: 将刷新间隔至少设置为一天。这将大大提高 Policy Director 保护的 Client Security 操作的性能。

## 启用 Policy Director 以控制 IBM 客户机对象

UVM 策略通过全局策略文件来控制。称作 UVM 策略文件的全局策略文件包含在 IBM 客户机系统上执行的操作的认证要求，例如登录到系统、清除屏幕保护程序或签名电子邮件消息。

允许 Policy Director 控制 IBM 客户机的认证对象前，请使用 UVM 策略编辑器来编辑 UVM 策略文件。UVM 策略文件编辑器是 Administrator Utility 的一部分。

**要点**: 如果允许 Policy Director 控制对象，会将对象控制权交给 Policy Director 对象空间。如果这样做，您必须重新安装 Client Security Software 以重新建立对该对象的本地控制。

## 编辑本地 UVM 策略

试图编辑本地客户机的 UVM 策略前，请确保 UVM 中至少登记了一个用户。否则，当策略编辑器试图打开本地策略文件时，将显示一条错误消息。

编辑本地 UVM 策略并将它仅用于对其进行编辑的客户机上。如果将 Client Security 安装在其缺省位置，则本地 UVM 策略存储为 \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm。只有已添加到 UVM 的用户可以使用 UVM 策略编辑器。

**注**: 如果将 UVM 策略设置为要求认证对象的指纹（例如操作系统登录）时，添加到 UVM 的用户必须已注册其指纹以使用该对象。

要启动 UVM 策略编辑器，请完成以下 Administrator Utility 过程:

1. 单击 **Configure Application Support and Policies** 按钮。
2. 在 UVM Policy 下，单击 **Local Client**，然后单击 **Edit Policy**。Global Policy Access Password 窗口打开。
3. 在 UVM Policy 区域，单击 **Local Client**，然后单击 **Edit Policy**。

   Global Policy Access Password 窗口打开。
4. 输入 `password` 然后按下 Enter 键。

   **注**: UVM 策略文件的缺省访问密码是单词 `password`。在编辑 UVM 策略后，可以更改访问密码。有关 UVM 策略编辑器的更多信息，请参阅《*Client Security Software 管理员指南*》。

5. 在 Policy Selection 页面上，从下拉列表中选择 UVM 策略文件（globalpolicy.gvm）。
6. 单击 **Object Selection** 选项卡，单击 **Action** 或 **Object type**，然后选择您想要为其指定认证要求的对象。

   有效操作的示例包括 System Logon、System Unlock 和 E-mail Decryption；对象类型的一个示例为 Acquire Digital Certificate。
7. 对于选择的每个对象，请选择 **Policy Director controls selected object** 以启用该对象的 Policy Director。

   **要点**：如果允许 Policy Director 控制对象，则您要将控制权交给 Policy Director 对象空间。如果您稍后想重新建立对该对象的本地控制，则必须重新安装 Client Security Software。

   **注**：在编辑 UVM 策略的同时，可以通过单击 **UVM Policy Summary** 查看策略摘要信息。
8. 单击 **Information** 选项卡，然后在适当的字段中输入系统名称、用户详细信息，以及系统和企业管理员详细信息。
9. 单击 **Policy Selection** 选项卡，然后单击 **UVM Policy** 按钮。
   - 要保存策略文件，请单击 **Save** 并按屏幕上的指示信息进行操作。
   - 要使用新密码保存文件，请单击 **Save as** 并按屏幕上的指示信息进行操作。
10. 单击 **OK** 以保存更改并退出。

## 编辑和使用远程客户机的 UVM 策略

要在多个 IBM 客户机上使用 UVM 策略，您必须编辑并保存远程客户机的 UVM 策略，然后将 UVM 策略文件复制到其它 IBM 客户机。如果 Client Security 安装在其缺省位置，则远程 UVM 策略文件存储为 \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm。必须在创建 \remote 子目录及其内容前保存 UVM 策略文件。

**注**：如果将远程客户机的 UVM 策略设置为要求认证对象（例如操作系统登录）的指纹，则添加到 UVM 的用户必须已注册其指纹以使用该对象。所有将使用该策略的远程客户机也必须安装了 UVM 感知指纹传感器。

要启动 UVM 策略编辑器，请完成以下 Administrator Utility 过程：

1. 单击 **Configure Application Support and Policies** 按钮。
2. 在 UVM Policy 区域中，单击 **Remote Clients**，然后单击 **Edit Policy**。

   Global Policy Access Password 窗口打开。
3. 输入 `password` 然后按下 Enter 键。

   **注**：UVM 策略文件的缺省访问密码是单词 `password`。在编辑 UVM 策略后，可以更改访问密码。
4. 在 Policy Selection 页面上，从下拉列表中选择 UVM 策略文件（globalpolicy.gvm）。
5. 单击 **Object Selection** 选项卡，单击 **Action** 或 **Object type**，然后选择您想要为其指定认证要求的对象。

   操作示例包含 System Logon、System Unlock 和 E-mail Decryption；对象类型的一个示例是 Acquire Digital Certificate。

6. 对于选择的每个对象，请单击 **Policy Director controls selected object** 以启用该对象的 Policy Director。

   **要点**: 如果允许 Policy Director 控制对象，则您要将控制权交给 Policy Director 对象空间。如果您稍后想重新建立对该对象的本地控制，则必须重新安装 Client Security Software。

   **注**: 编辑 UVM 策略文件时，通过单击 UVM Policy Summary 可以查看策略摘要信息。

7. 单击 **Information** 选项卡，然后在适当的字段中输入系统名称、用户详细信息，以及系统和企业管理员详细信息。
8. 单击 **Remote Configuration** 选项卡。
9. 选择将使用此 UVM 策略的远程客户机上可用的认证元素，然后选择 **Policy Director enabled client** 复选框。
10. 单击 **Policy Selection** 选项卡，然后单击 **UVM Policy** 按钮。
    - 要保存策略文件，请单击 **Save** 并按屏幕上的指示信息进行操作。
    - 要使用新密码保存文件，请单击 **Save as** 并按屏幕上的指示信息操作。
11. 单击 **OK** 以保存更改并退出。
12. 将以下文件复制到将使用此 UVM 策略的远程 IBM 客户机上:
    - \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
    - \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

**注**:

1. 如果将 Client Security Software 安装在其缺省位置，则前述文件的根目录是 \Program Files。
2. 必须将两个文件都复制到远程客户机上的 \IBM\Security\UVM_Policy\ 目录路径。

# 第 4 章 故障诊断

以下部分提供对防止或识别并纠正使用 Client Security Software 时可能产生的问题有帮助的信息。

## 管理员功能

本部分包含对管理员设置和使用 Client Security Software 可能有帮助的信息。

## 设置管理员密码（NetVista）

在 Configuration/Setup Utility 中可用的安全性设置使管理员可以执行以下操作:

- 更改 IBM 嵌入式安全芯片的硬件密码
- 启用或禁用 IBM 嵌入式安全芯片
- 清除 IBM 嵌入式安全芯片

**注意**:

- 在 Windows XP、Windows NT 和 Windows 2000 中，启用 UVM 登录保护时不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要禁用 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。必须重新启动计算机，禁用 UVM 保护才会生效。
- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。
- 清除了 IBM 嵌入式安全芯片 时，存储在该芯片上的所有加密密钥和证书将丢失。

因为这些安全性设置可以通过计算机的 Configuration/Setup Utility 访问，所以请设置管理员密码以阻止未经授权的用户更改这些设置。

要设置管理员密码:

1. 关闭并重新启动计算机。
2. 当屏幕上出现 Configuration/Setup Utility 提示时，请按下 **F1**。

   Configuration/Setup Utility 的主菜单打开。
3. 选择 **System Security**。
4. 选择 **Administrator Password**。
5. 输入您的密码并按下键盘上的向下箭头。
6. 再次输入密码并按下向下箭头。
7. 选择 **Change Administrator password** 并按下 Enter 键；然后再次按下 Enter 键。
8. 按下 **Esc** 退出并保存设置。

设置了管理员密码后，每次试图访问 Configuration/Setup Utility 时都会出现一个提示。

**要点**: 请将管理员密码记录在安全的地方。如果丢失或忘记了管理员密码，您就不能访问 Configuration/Setup Utility，也不能更改或删除密码，而无需卸下计算机机箱盖并移动系统板上的跳线。有关更多信息，请参阅计算机随附的硬件文档。

## 设置超级用户密码（ThinkPad）

在 IBM BIOS Setup Utility 中可用的安全性设置使管理员可以执行以下操作:

- 启用或禁用 IBM 嵌入式安全芯片
- 清除 IBM 嵌入式安全芯片

**注意**:

- 在 Windows XP、Windows NT 和 Windows 2000 中，启用 UVM 登录保护时不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要禁用 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。必须重新启动计算机，禁用 UVM 保护才会生效。
- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。
- 清除 IBM 嵌入式安全芯片 时，存储在芯片上的所有加密密钥和证书将丢失。

设置 Client Security Software 后，请设置超级用户密码以阻止未经授权的用户更改这些设置。

要设置超级用户密码，请完成以下过程:

1. 关闭并重新启动计算机。
2. 当屏幕上出现 IBM BIOS Setup Utility 提示符时，请按下 **F1**。

   IBM BIOS Setup Utility 的主菜单打开。
3. 选择 **Password**。
4. 选择 **Supervisor Password**。
5. 输入密码并按下 Enter 键。
6. 再次输入密码并按下 Enter 键。
7. 单击 **Continue**。
8. 按下 F10 保存并退出。

设置了超级用户密码后，每次试图访问 IBM BIOS Setup Utility 时都会出现一个提示。

**要点**: 请将超级用户密码记录存在安全的地方。如果丢失或忘记了超级用户密码，您就不能访问 IBM BIOS Setup Utility，也不能更改或删除密码。有关更多信息，请参阅计算机随附的硬件文档。

## 保护硬件密码

设置安全芯片密码以启用客户机的 IBM 嵌入式安全芯片。设置了安全芯片密码后，对 Administrator Utility 的访问由此密码保护。应该保护安全芯片密码以禁止未经授权的用户更改 Administrator Utility 中的设置。

## 清除 IBM 嵌入式安全芯片（NetVista）

如果要从 IBM 嵌入式安全芯片擦除所有用户加密密钥并清除芯片的硬件密码，则必须清除该芯片。清除 IBM 嵌入式安全芯片前请阅读以下“注意”框中的信息。

**注意**:

- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要清除 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。必须重新启动计算机，禁用 UVM 保护才会生效。
- 清除了 IBM 嵌入式安全芯片后，存储在芯片上的所有加密密钥和证书将丢失。

要清除 IBM 嵌入式安全芯片，请执行以下操作:

1. 关闭并重新启动计算机。
2. 当屏幕上出现 Configuration/Setup Utility 提示出现时，请按下 F1。

   Configuration/Setup Utility 的主菜单打开。
3. 选择 **System Security**。
4. 选择 **IBM Embedded Security Chip**。
5. 选择 **Clear IBM Security Chip**。
6. 选择 **Yes**。
7. 按下 Esc 继续。
8. 按下 Esc 退出并保存设置。

## 清除 IBM 嵌入式安全芯片（ThinkPad）

如果要从 IBM 嵌入式安全芯片擦除所有用户加密密钥并清除芯片的硬件密码，则必须清除该芯片。清除 IBM 嵌入式安全芯片前请阅读以下“注意”框中的信息。

**注意**:

- 如果启用了 UVM 保护，请不要清除或禁用 IBM 嵌入式安全芯片。否则，硬盘的内容将变得不可使用，而您必须重新格式化硬盘驱动器并重新安装所有软件。

  要清除 UVM 保护，请打开 Administrator Utility 并清除 **Replace the standard Windows logon with UVM's secure logon** 复选框。必须重新启动计算机，禁用 UVM 保护才会生效。
- 清除了 IBM 嵌入式安全芯片时，存储在芯片上的所有加密密钥和证书将丢失。

要清除 IBM 嵌入式安全芯片，请执行以下操作:

1. 关闭并重新启动计算机。
2. 当 IBM BIOS Setup Utility 提示出现在屏幕上后，请按下 Fn。

   **注**: 在某些 ThinkPad 机型上，您可能需要在电源打开时按下 F1 键以清除安全芯片。有关详细信息，请在 IBM BIOS Setup Utility 参考帮助消息。

   IBM BIOS Setup Utility 的主菜单打开。
3. 选择 **Security**。
4. 选择 **IBM TCPA Feature Setup**。

5. 选择 **Clear IBM TCPA Security Feature**。
6. 选择 **Yes**。
7. 按下 Enter 键继续。
8. 按下 F10 保存并退出。

## Administrator Utility

以下部分包含使用 Administrator Utility 时要记住的信息。

### 删除用户

从 Windows XP、Windows NT 和 Windows 2000 删除用户时，将从 Administrator Utility 的用户列表中删除用户名。

### 使用 Policy Director 控件来拒绝访问所选择的对象

当选择了 Policy Director 控件时，未禁用 **Deny all access to selected object** 复选框。在 UVM 策略编辑器中，如果选择 **Policy Director controls selected object** 以启用 Policy Director 来控制认证对象，则不禁用 **Deny all access to selected object** 复选框。虽然 **Deny all access to selected object** 复选框保持活动，但不能选择它来覆盖 Policy Director 控件。

## 已知限制

本部分包含有关与 Client Security Software 相关的已知限制的信息。

### 将 Client Security Software 与 Windows 操作系统一起使用

**所有 Windows 操作系统有以下已知限制**：如果在 UVM 中登记的客户机用户更改了其 Windows 用户名，所有 Client Security 功能性将丢失。该用户必须在 UVM 中重新登记新用户名并请求所有新凭证。

**Windows XP 操作系统有以下已知限制**：在 UVM 中登记的用户如果先前已经更改了其 Windows 用户名，则无法被 UVM 认出。UVM 将指向先前的用户名而 Windows 只能认出新用户名。即使在安装 Client Security Software 前已经更改了 Windows 用户名，此限制仍然会发生。

### 将 Client Security Software 与 Netscape 应用程序一起使用

**权限故障后 Netscape 打开**：如果 UVM 密码短语窗口打开，则可以继续前必须输入 UVM 密码短语并单击 **OK**。如果输入不正确的 UVM 密码短语（或对指纹扫描提供了不正确的指纹），则会显示错误消息。如果单击 **OK**，将打开 Netscape，但是您不能使用由 IBM 嵌入式安全芯片生成的数字证书。必须退出并重新进入 Netscape，然后在可以使用 IBM 嵌入式安全芯片证书前输入正确的 UVM 密码短语。

**不显示算法**：如果在 Netscape 中查看了 IBM 嵌入式安全芯片 PKCS#11 模块，则不选择该模块支持的所有散列算法。以下算法由 IBM 嵌入式安全芯片 PKCS#11 模块支持，但在 Netscape 中查看时不识别为受支持的：

- SHA-1
- MD5

## IBM 嵌入式安全芯片证书和加密算法

提供以下信息以帮助识别有关可与 IBM 嵌入式安全芯片证书一起使用的加密算法的问题。有关可与其电子邮件应用程序一起使用的加密算法的最新信息，请参阅 Microsoft 或 Netscape。

**当将电子邮件从一个 Outlook Express（128 位）客户机发送到另一个 Outlook Express（128 位）客户机时**: 如果将 Outlook Express 与具有 128 位版本的 Internet Explorer 4.0 或 5.0 一起使用以将加密的电子邮件发送到使用 Outlook Express（128 位）的其它客户机，则使用 IBM 嵌入式安全芯片证书加密的电子邮件消息只能使用 3DES 算法。

**在 Outlook Express（128 位）客户机和 Netscape 客户机之间发送电子邮件时**: 从 Netscape 客户机到 Outlook Express（128 位）客户机的 RC2（40）、RC2（64）或 RC2（128）加密请求始终返回到使用 RC2（40）的算法的 Netscape 客户机。

**对于在 Outlook Express（128 位）客户机中的选择，某些算法可能不可用**: 取决于您所使用的 Outlook Express（128位）版本是如何配置或更新的，某些 RC2 算法和其它算法可能不能与 IBM 嵌入式安全芯片证书一起使用。有关与 Outlook Express 的版本一起使用的加密算法的当前信息，请参阅 Microsoft。

## 使用 Lotus Notes 用户标识的 UVM 保护

**如果在 Notes 会话中切换用户标识，则 UVM 保护不运行**: 您可以只为 Notes 会话的当前用户标识设置 UVM 保护。要从一个启用了 UVM 保护的用户标识切换到另一个用户标识，请执行以下操作:

1. 退出 Notes。
2. 禁用当前用户标识的 UVM 保护。
3. 进入 Notes 并切换用户标识。有关切换用户标识的信息，请参阅 Lotus Notes 文档。

   如果要设置切换到的用户标识的 UVM 保护，请继续步骤 4。
4. 进入由 Client Security Software 提供的 Lotus Notes Configuration 工具并设置 UVM 保护。

## Client Utility 限制

Windows XP 强制访问限制，这些访问限制对某些环境下的客户机用户的可用功能进行限制。

### Windows XP Professional

在 Windows XP Professional 中，客户机用户限制可能应用于以下情形:

- Client Security Software 安装在稍后转换为 NTFS 格式的分区中
- Windows 文件夹位于稍后转换为 NTFS 格式的分区中
- 压缩文档文件夹位于稍后转换为 NTFS 格式的分区中

在以上情况中，Windows XP Professional Limited User 可能不能执行以下 Client Utility 任务:

- 更改其 UVM 密码短语
- 更新用 UVM 注册的 Windows 密码
- 更新密钥压缩文档

管理员启动并退出 Administrator Utility 后，这些限制被清除。

### Windows XP Home

Windows XP Home Limited User 不能使用以下任何情形中的 Client Utility:

- Client Security Software 安装在 NTFS 格式的分区中
- Windows 文件夹位于 NTFS 格式的分区中
- 压缩文档文件夹位于 NTFS 格式的分区中

## 错误消息

**与 Client Security Software 相关的错误消息在事件日志中生成**: Client Security Software 使用可能在事件日志中生成错误消息的设备驱动程序。与这些消息相关的错误不影响计算机的正常运行。

**如果对认证对象的访问被拒绝，则 UVM 调用由相关程序生成的错误消息**: 如果 UVM 策略设置为拒绝对认证对象（例如电子邮件解密）的访问，则声明被拒绝访问的消息将根据使用的软件而不同。例如，来自 Outlook Express 的一条错误消息声明对认证对象的访问被拒绝，这与来自 Netscape 的错误消息不同，来自 Netscape 的错误消息声明访问被拒绝。

## 故障诊断图表

如果 Client Security Software 遇到问题，则以下部分包含的故障诊断图表可能有帮助。

## 安装故障诊断信息

如果安装 Client Security Software 时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **软件安装过程中显示一条错误消息** | **操作** |
| 安装软件时显示一条消息，询问您是否想要除去选择的应用程序及其所有组件。 | 单击 **OK** 退出该窗口。再次开始安装过程以安装 Client Security Software 的新版本。 |
| 安装过程中显示一条消息，声明已经安装了 Client Security Software 的先前版本。 | 单击 **OK** 从该窗口退出。请执行以下操作:<br>1. 卸载该软件。<br>2. 重新安装该软件。<br>**注**: 如果您计划使用相同的硬件密码来保护 IBM 嵌入式安全芯片，则不必清除该芯片并重新设置密码。 |
| **安装访问由于未知硬件密码被拒绝** | **操作** |
| 当在启用 IBM 嵌入式安全芯片的 IBM 客户机上安装软件时，IBM 嵌入式安全芯片的硬件密码未知。 | 清除该芯片以继续安装。 |
| **无人照管安装不开始** | **操作** |
| 必须安装 SMBus 设备驱动程序以执行无人照管安装。 | 安装 SMBus 设备驱动程序并重新开始安装。 |
| **无人照管安装过早结束** | **操作** |
| 在无人照管安装过程中，不显示错误消息。 | 执行照管安装以查看可能显示的任何错误消息。 |
| **setup.exe 文件响应不正确** | **操作** |
| 如果从 csec4_0.exe 文件将所有文件解压缩到公共目录中，则 setup.exe 文件将不正常工作。 | 运行 smbus.exe 文件以安装 SMBus 设备驱动程序，然后运行 csec4_0.exe 文件以安装 Client Security Software 代码。 |
| **安装 UVM 感知指纹传感器时显示一条错误消息** | **操作** |
| 在 DigitalPersona U.are.UPro 指纹传感器安装过程中，显示一条消息要求您执行以下操作:<br>1. 连接指纹传感器。<br>2. 等待传感器上的红灯闪亮。<br>3. 单击 **OK**。<br>4. 选择 **Yes, I want to restart my computer now**，然后单击 **Finish**。<br>系统将重新启动。 | 不要求更多操作。指纹传感器将正确安装。 |

## Administrator Utility 故障诊断信息

如果使用 Administrator Utility 时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **在 Administrator Utility 中输入并确认您的 UVM 密码短语后，Next 按钮不可用。** | **操作** |

| 问题症状 | 可能的解决方案 |
| --- | --- |
| 在运行 Windows NT、Windows 2000 或 Windows XP 的系统上，当您将用户添加到 UVM 时，在 Administrator Utility 中输入并确认 UVM 密码短语后 **Next** 按钮可能不可用。 | 单击 Windows “任务栏” 上的 **Information** 项并继续该过程。 |
| **试图编辑本地 UVM 策略时显示一条错误消息** | **操作** |
| 编辑本地 UVM 策略时，如果 UVM 中没有用户登记，则可能显示一条错误消息。 | 在试图编辑策略文件前将用户添加到 UVM。 |
| **更改管理员公用密钥时显示一条错误消息** | **操作** |
| 清除嵌入式安全芯片然后恢复密钥压缩文档后，如果更改管理员公用密钥，可能显示一条错误消息。 | 可能的话，请将用户添加到 UVM 并请求新的证书。 |
| **试图恢复 UVM 密码短语时显示一条错误消息** | **操作** |
| 更改了管理员公用密钥然后试图恢复用户的 UVM 密码短语时可能显示一条错误消息。 | 请执行以下操作之一:<br>• 如果不需要用户的 UVM 密码短语，则不需要任何操作。<br>• 如果需要用户的 UVM 密码短语，则必须将用户添加到 UVM 并请求新的证书（可能的话）。 |
| **试图保存 UVM 策略文件时显示一条错误消息** | **操作** |
| 当您试图通过单击 **Apply** 或 **Save** 来保存 UVM 策略文件（globalpolicy.gvm）时，可能显示一条错误消息。 | 退出该错误消息，再次编辑 UVM 策略文件以执行更改，然后保存该文件。 |
| **试图打开 UVM 策略编辑器时显示一条错误消息** | **操作** |
| 当前用户（已登录到操作系统上的）没有添加到 UVM 时，UVM 策略编辑器将不打开。 | 将用户添加到 UVM 并打开 UVM 策略编辑器。 |
| **使用 Administrator Utility 时显示一条错误消息** | **操作** |
| 使用 Administrator Utility 时，可能显示以下错误消息:<br><br>试图访问 Client Security 芯片时发生一个缓冲区 I/O 错误。这可以通过重新引导来纠正。 | 退出错误消息并重新启动计算机。 |
| **更改安全芯片密码时显示一条禁用的芯片消息** | **操作** |
| 试图更改安全芯片密码时，如果输入确认密码后按下了 Enter 键或 Tab > Enter，则启用 Disable 芯片按钮并显示禁用的芯片确认消息。 | 请执行以下操作:<br>1. 从禁用的芯片确认窗口退出。<br>2. 要更改安全芯片密码，请输入新密码，输入确认密码，然后单击 **Change**。输入确认密码后不要按下 Enter 键或 Tab > Enter。 |

## Client Utility 故障诊断信息

如果使用 Client Utility 时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **Limited User 无法执行 Windows XP Professional 中某些 Client Utility 功能** | **操作** |
| Windows XP Professional Limited User 可能不能执行以下 Client Utility 任务:<br>• 更改其 UVM 密码短语<br>• 更新用 UVM 注册的 Windows 密码<br>• 更新密钥压缩文档 | 管理员启动并退出 Administrator Utility 后，这些限制被清除。 |
| **Limited User 不能使用 Windows XP Home 中的 Client Utility** | **操作** |
| 在以下任何情形中，Windows XP Home Limited User 不能使用 Client Utility:<br>• Client Security Software 安装在 NTFS 格式的分区中<br>• Windows 文件夹位于 NTFS 格式的分区中<br>• 压缩文档文件夹位于 NTFS 格式的分区中 | 这是 Windows XP Home 的已知限制。此问题没有解决方案。 |

## 特定于 ThinkPad 的故障诊断信息

如果在 ThinkPad 计算机上使用 Client Security Software 时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **尝试 Client Security 管理员功能时显示一条错误消息** | **操作** |
| 尝试执行 Client Security 管理员功能后显示以下错误消息: ERROR 0197: Invalid Remote change requested.Press <F1> to Setup | 必须禁用 ThinkPad 超级用户密码以执行某些 Client Security 管理员功能。<br>要禁用超级用户密码，请执行以下操作:<br>1. 按下 F1 访问 IBM BIOS Setup Utility。<br>2. 输入当前超级用户密码。<br>3. 输入空的新超级用户密码，然后确认空密码。<br>4. 按下 Enter 键。<br>5. 按下 F10 保存并退出。 |
| **不同的 UVM 感知指纹传感器不正常工作** | **操作** |
| IBM ThinkPad 计算机不支持多个 UVM 感知指纹传感器的相互交换。 | 不要切换指纹传感器型号。远程工作时使用与从扩展坞工作时同样的型号。 |

## Microsoft 故障诊断信息

以下故障诊断图表包含在将 Client Security Software 与 Microsoft 应用程序和操作系统一起使用遇到问题时可能会有帮助的信息。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **UVM 中登记的用户的 Client Security 不能正常工作** | **操作** |
| 登记的客户机用户可能已更改了其 Windows 用户名。如果发生了这种情况，所有 Client Security 功能都将丢失。 | 在 UVM 中重新登记新用户名并请求所有新凭证。 |
| **注**: 在 Windows XP 中，在 UVM 中登记的用户如果先前已经更改了其 Windows 用户名，则不会被 UVM 识别。即使在安装 Client Security Software 前已经更改了 Windows 用户名，此限制仍然会发生。 | |
| **使用 Outlook Express 读取加密的电子邮件的问题** | **操作** |
| 由于发送方和接收方使用的 Web 浏览器的加密强度的差异，所以不能对加密过的电子邮件进行解密。<br><br>**注**: 要将 128 位 Web 浏览器与 Client Security Software 一起使用，IBM 嵌入式安全芯片必须支持 256 位加密。如果 IBM 嵌入式安全芯片支持 56 位加密，则必须使用 40 位 Web 浏览器。可以在 Administrator Utility 中找到 Client Security Software 提供的加密强度。 | 请验证以下情况:<br>1. 发送方使用的 Web 浏览器的加密强度与接收方使用的 Web 浏览器的加密强度兼容。<br>2. Web 浏览器的加密强度与 Client Security Software 的固件提供的加密强度兼容。 |
| **从具有多个与之相关的证书的地址使用证书的问题** | **操作** |
| Outlook Express 可以列出多个与单一电子邮件地址相关的证书，这些证书中的一些可能变为无效。如果与证书相关的专用密钥不再存在于生成证书的发送方计算机的 IBM 嵌入式安全芯片上，则证书可能变为无效。 | 请求接收方重新发送其数字证书；然后在 Outlook Express 的通讯簿中选择证书。 |
| **当尝试数字签名电子邮件消息时出现失败消息** | **操作** |
| 如果电子邮件消息的作者不具有与其电子邮件帐户相关的证书时尝试数字签名电子邮件消息，则显示错误消息。 | 使用 Outlook Express 中的安全性设置来指定要与用户帐户相关的证书。有关更多信息，请参阅 Outlook Express 提供的文档。 |
| **Outlook Express（128 位）只使用 3DES 算法加密电子邮件消息** | **操作** |
| 当在将 Outlook Express 与 128 位版本的 Internet Explorer 4.0 或 5.0 一起使用的客户机之间发送加密的电子邮件时，只能使用 3DES 算法。 | 要将 128 位浏览器与 Client Security Software 一起使用，IBM 嵌入式安全芯片必须支持 256 位加密。如果 IBM 嵌入式安全芯片支持 56 位加密，则必须使用 40 位 Web 浏览器。可以在 Administrator Utility 中找到 Client Security Software 提供的加密强度。<br><br>请参阅 Microsoft 以获取有关与 Outlook Express 一起使用的加密算法的当前信息。 |
| **Outlook Express 客户机返回使用不同算法的电子邮件消息** | **操作** |

| 问题症状 | 可能的解决方案 |
| --- | --- |
| 使用 RC2（40）、RC2（64）或 RC2（128）算法加密的电子邮件消息从使用 Netscape Messenger 的客户机被发送到使用 Outlook Express（128 位）的客户机。从 Outlook Express 客户机返回的电子邮件消息使用 RC2（40）算法进行加密。 | 不要求操作。从 Netscape 客户机到 Outlook Express（128 位）客户机的 RC2（40）、RC2（64）或 RC2（128）加密请求总是使用 RC2（40）算法返回到 Netscape 客户机。请参阅 Microsoft 以获取有关与您的 Outlook Express 版本一起使用的加密算法的当前信息。 |
| **硬盘驱动器发生故障后使用 Outlook Express 中的证书时出现错误消息** | **操作** |
| 通过在 Administrator Utility 中使用密钥恢复功能可以恢复证书。某些证书，例如 VeriSign 提供的免费证书，密钥恢复后可能不会恢复。 | 恢复密钥后，请执行以下操作之一:<br>• 获取新证书<br>• 在 Outlook Express 中的认证中心再次注册 |
| **Outlook Express 没有更新与证书相关的加密强度** | **操作** |
| 当发送方在 Netscape 中选择加密强度并将签名的电子邮件消息发送到将 Outlook Express 与 Internet Explorer 4.0（128 位）一起使用的客户机时，返回的电子邮件的加密强度可能不匹配。 | 从 Outlook Express 的通讯簿中删除相关的证书。再次打开签名的电子邮件，并将证书添加到 Outlook Express 的通讯簿中。 |
| **在 Outlook Express 中显示错误解密消息** | **操作** |
| 可以通过在 Outlook Express 中双击消息来打开该消息。在某些情况下，当过快地双击加密的消息时，会出现解密错误消息。 | 关闭该消息，然后再次打开加密的电子邮件消息。 |
| 当选择加密的消息时也会在预览窗格中显示解密错误消息。 | 如果在预览窗格中出现错误消息，则不要求操作。 |
| **当在加密的电子邮件中单击“发送”按钮两次时，显示错误消息。** | **操作** |
| 当使用 Outlook Express 时，如果单击发送按钮两次来发送加密的电子邮件消息，则会显示一条错误消息，声明消息不能发送。 | 关闭错误消息，然后单击**发送**按钮一次。 |
| **当请求证书时显示错误消息** | **操作** |
| 使用 Internet Explorer 时，如果请求使用 IBM 嵌入式安全芯片 CSP 的证书，则会接收到错误消息。 | 再次请求数字证书。 |

## Netscape 应用程序故障诊断信息

以下故障诊断图表包含将 Client Security Software 与 Netscape 应用程序一起使用遇到问题时可能会有帮助的信息。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **读取加密的电子邮件时的问题** | **操作** |

| 问题症状 | 可能的解决方案 |
| --- | --- |
| 由于发送方和接收方使用的 Web 浏览器的加密强度的差异，所以不能对加密过的电子邮件解密。<br><br>**注**: 要将 128 位浏览器与 Client Security Software 一起使用，IBM 嵌入式安全芯片必须支持 256 位加密。如果 IBM 嵌入式安全芯片支持 256 位加密，则必须使用 40 位 Web 浏览器。可以在 Administrator Utility 中找到 Client Security Software 提供的加密强度。 | 请验证以下功能:<br>1. 发送方使用的 Web 浏览器的加密强度与接收方使用的 Web 浏览器的加密强度兼容。<br>2. Web 浏览器的加密强度与 Client Security Software 的固件提供的加密强度兼容。 |
| **当尝试数字签名电子邮件消息时出现失败消息** | **操作** |
| 当没有在 Netscape Messenger 中选择 IBM 嵌入式安全芯片证书，并且电子邮件消息的作者尝试使用证书签名时，会显示错误消息。 | 使用 Netscape Messenger 中的安全性设置来选择证书。当 Netscape Messenger 打开时，单击工具栏上的安全性图标。Security Info 窗口打开。在左面板中单击 **Messenger**，然后选择 **IBM embedded Security Chip certificate**。有关更多信息，请参阅由 Netscape 提供的文档。 |
| **电子邮件消息将以不同的算法返回客户机** | **操作** |
| 使用 RC2（40）、RC2（64）或 RC2（128）算法加密的电子邮件消息从使用 Netscape Messenger 的客户机被发送到使用 Outlook Express（128 位）的客户机。从 Outlook Express 客户机返回的电子邮件消息使用 RC2（40）算法进行加密。 | 不要求操作。从 Netscape 客户机到 Outlook Express（128 位）客户机的 RC2（40）、RC2（64）或 RC2（128）加密请求总是使用 RC2（40）算法返回到 Netscape 客户机。请参阅 Microsoft 以获取有关与您的 Outlook Express 版本一起使用的加密算法的当前信息。 |
| **不能使用由 IBM 嵌入式安全芯片生成的数字证书** | **操作** |
| 由 IBM 嵌入式安全芯片生成的数字证书不可使用。 | 验证当打开了 Netscape 时，已输入了正确的 UVM 密码短语。如果输入不正确的 UVM 密码短语，会显示一条错误消息，声明认证故障。如果单击 **OK**，将打开 Netscape，但您将不能使用由 IBM 嵌入式安全芯片生成的证书。必须退出并重新打开 Netscape，然后输入正确的 UVM 密码短语。 |
| **来自同一个发送方的新数字证书不能在 Netscape 中被替换** | **操作** |
| 当数字签名的电子邮件不止一次被同一个发送方接收到时，则与电子邮件相关的第一个数字证书不会被覆盖。 | 如果接收到多个电子邮件证书，则只有一个证书是缺省证书。请使用 Netscape 中的安全性功能删除第一个证书，然后重新打开第二个证书或要求发送方发送另一个签名的电子邮件。 |
| **不能导出 IBM 嵌入式安全芯片证书** | **操作** |
| 不能在 Netscape 中导出 IBM 嵌入式安全芯片证书。Netscape 中的导出功能可以用于备份证书。 | 请转至 Administrator Utility 或 Client Utility 以更新密钥压缩文档。当更新密钥压缩文档时，将创建与 IBM 嵌入式安全芯片相关的所有证书的副本。 |
| **在硬盘驱动器发生故障后尝试使用恢复的证书时出现的错误消息** | **操作** |

| 问题症状 | 可能的解决方案 |
| --- | --- |
| 通过在 Administrator Utility 中使用密钥恢复功能可以恢复证书。某些证书，例如 VeriSign 提供的免费证书，在密钥恢复后可能不会恢复。 | 恢复密钥后，将获取新证书。 |
| **Netscape 代理程序打开并导致 Netscape 失败** | **操作** |
| Netscape 代理程序打开并关闭 Netscape。 | 关闭 Netscape 代理程序。 |
| **尝试打开 Netscape 时，Netscape 出现延迟** | **操作** |
| 如果添加 IBM 嵌入式安全芯片 PKCS#11 模块后打开 Netscape，则在 Netscape 打开之前会发生短时间的延迟。 | 不要求操作。这仅适用于信息的用途。 |

## 数字证书故障诊断信息

如果在获取数字证书时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **在数字证书请求过程中，多次显示 UVM 密码短语窗口或指纹认证窗口** | **操作** |
| UVM 安全性策略指定用户可以获得数字证书之前提供 UVM 密码短语或指纹认证。如果用户尝试获得证书，则请求 UVM 密码短语或指纹扫描的认证窗口将不止一次显示。 | 每次认证窗口打开时，请输入 UVM 密码短语或扫描您的指纹。 |
| **显示 VBScript 或 JavaScript 错误消息** | **操作** |
| 当请求数字证书时，会显示与 VBScript 或 JavaScript 相关的错误消息。 | 重新启动计算机，再次获得证书。 |

## Policy Director 故障诊断信息

如果将 Policy Director 与 Client Security Software 一起使用时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **本地策略设置与服务器上的设置不一致** | **操作** |
| Policy Director 允许不受 UVM 支持的某些位配置。因此，配置 PD 服务器时，本地策略要求可以覆盖管理员进行的设置。 | 这是一个已知限制。 |
| **Policy Director 安装设置不可访问** | **操作** |
| Policy Director 设置和本地高速缓存安装设置在 Administrator Utility 的 Policy Setup 页面中不可访问。 | 安装 Policy Director Runtime Environment。如果 Runtime Environment 没有安装在 IBM 客户机上，则 Policy Setup 页面上的 Policy Director 不可用。 |
| **对于用户和组来说，用户控制都是有效的。** | **操作** |
| 配置 Policy Director 服务器时，如果将用户定义到组，且 **Traverse bit** 打开时，则用户控制对于用户和组都是有效的。 | 不要求操作。 |

## Lotus Notes 故障诊断信息

如果在将 Lotus Notes 与 Client Security Software 一起使用时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **启用 Lotus Notes 的 UVM 保护后，Notes 不能完成其安装** | **操作** |
| 使用 Administrator Utility 启用 UVM 保护后，Lotus Notes 不能完成安装。 | 这是一个已知限制。<br><br>在 Administrator Utility 中启用 Lotus Notes 支持前，Lotus Notes 必须已配置并处于运行状态。 |
| **当试图更改 Notes 密码时显示错误消息** | **操作** |
| 使用 Client Security Software 时更改 Notes 密码，会显示一条错误消息。 | 重试密码更改。如果这不起作用，请重新启动客户机。 |
| **随机生成密码后显示错误消息** | **操作** |
| 执行以下操作时可能会显示错误消息:<br>• 使用 Lotus Notes Configuration 工具来设置 Notes 标识的 UVM 保护<br>• 打开 Notes 并使用由 Notes 提供的功能来更改 Notes 标识文件的密码<br>• 更改密码后立即关闭 Notes | 单击 **OK** 以关闭该错误消息。不要求其它操作。<br><br>与错误消息相反，已更改密码。新密码是由 Client Security Software 创建的随机生成的密码。现在 Notes 标识由随机生成的密码来加密，并且用户不需要新的用户标识文件。如果最终用户再次更改密码，UVM 将为 Notes 标识生成新的随机密码。 |

## 加密故障诊断信息

如果在使用 Client Security Software 3.0 或后续版本加密文件时遇到问题，则以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **先前加密的文件将不进行解密** | **操作** |
| 使用先前版本的 Client Security Software 加密的文件在升级到 Client Security Software 3.0 或后续版本后不进行解密。 | 这是一个已知的限制。<br><br>在安装 Client Security Software 3.0 或后续版本*之前*，必须使用先前版本的 Client Security Software 解密所有已加密的文件。由于其文件加密执行中的更改，Client Security Software 3.0 不能解密使用先前版本的 Client Security Software 加密过的文件。 |

## UVM 感知设备故障诊断信息

如果使用 UVM 感知设备时遇到问题，以下故障诊断信息可能有帮助。

| 问题症状 | 可能的解决方案 |
| --- | --- |
| **UVM 感知设备停止正常工作** | **操作** |

| 问题症状 | 可能的解决方案 |
| --- | --- |
| 当从通用串行总线（USB）端口断开连接 UVM 感知设备，然后将该设备重新连接到 USB 端口，该设备可能不正常工作。 | 在设备重新连接到 USB 端口后，请重新启动计算机。 |

# 附录 A. 针对 Client Security Software 的美国出口法规

IBM Client Security Software 软件包已经过 IBM 出口法规办公室（ERO）审核，并按照美国政府出口法规的要求，IBM 已经提交适合的文档，并从美国商务部获得针对国际分发（除了美国政府禁运的那些国家或地区）的不超过 256 位加密支持的零售分类许可。美国和其它国家或地区的法规随各个国家或地区政府的不同而更改。

如果您不能下载 Client Security Software 软件包，请联系本地 IBM 营业部，以与 IBM 国家或地区出口法规合作伙伴（ERC）协商。

# 附录 B. 密码和密码短语规则

本附录包含有关适合于不同系统密码的规则的信息。

## 硬件密码规则

以下规则适合于硬件密码:

**长度** 该密码长度必须恰好为八个字符。

**字符** 该密码必须仅包含字母数字字符。允许字母和数字的组合。不允许特殊字符，如空格、!、?、%。

**属性** 设置安全芯片密码以启用计算机中的 IBM 嵌入式安全芯片。每次访问 Administrator Utility 时必须输入此密码。

**不正确尝试**

如果十次输入不正确密码，则计算机将锁定 1 小时 17 分钟。这段时间过后，如果您又十次输入不正确密码，则计算机将锁定 2 小时 34 分钟。每回您十次输入不正确密码后，计算机禁用的时间将加倍。

## UVM 密码短语规则

为了提高安全性，UVM 密码短语更长些并且可以比传统密码更特别。

以下规则适合于 UVM 密码短语:

**长度** 密码短语可以最多为 256 个字符长度。

**字符** 密码短语可以包含键盘产生的任何字符组合，包含空格和非字母数字字符。

**属性** UVM 密码短语与您可能用于登录操作系统的密码不同。UVM 密码短语可以用于与其它鉴别设备（例如 UVM 感知指纹传感器）联合。

**不正确尝试**

如果您在会话期间多次输入了不正确的 UVM 密码短语，则计算机不锁定。对不正确尝试的次数没有限制。

# 附录 C. 使用系统登录的 UVM 保护的规则

UVM 保护确保只有已经添加到特定 IBM 客户机 UVM 的那些用户才能访问操作系统。Windows 操作系统包含提供登录保护的应用程序。虽然 UVM 保护设计为与 Windows 登录应用程序并行工作，但是 UVM 保护与操作系统不同。

对于 Windows XP、Windows NT 和 Windows 2000，UVM 登录界面替换操作系统登录界面，因此每次用户尝试登录到系统时 UVM 登录窗口打开。

设置和使用系统登录的 UVM 保护前请阅读以下技巧:

- 当启用了 UVM 保护时，不要清除 IBM 嵌入式安全芯片。否则，硬盘上的内容将变为不可用，并且必须重新格式化硬盘驱动器并重新安装所有软件。
- 如果清除 Administrator Utility 中的 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 复选框，则系统返回 Windows 登录过程，而无需 UVM 登录保护。
- 在 Windows XP、Windows NT 和 Windows 2000 中，有选项让您指定 Windows NT 登录应用程序的输入正确密码所允许的最大尝试次数。此选项不应用于 UVM 登录保护。您可以设置输入 UVM 密码短语所允许的尝试次数没有限制。

# 附录 D. 声明和商标

本附录提供 IBM 产品的法律声明和商标信息。

## 声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其它国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的可用产品和服务的信息，请向您当地的 IBM 代理咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能用于 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可证。您可以用书面方式将许可证查询寄往:

IBM Director of Licensing IBM Corporation North Castle Drive Armonk, NY 10504-1785 U.S.A.

**本条款不适用联合王国或任何这样的条款与当地法律不一致的国家或地区**: 国际商业机器公司以“仅此状态”的基础提供本出版物，不附有任何形式的（无论明示的，还是默示的）保证，包括（但不限于）非侵权性、适销性或适用于某特定用途的默示保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本出版物中描述产品和／或程序进行改进和／或更改，而不另行通知。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: (i) 允许在独立创建的程序和其它程序（包含本程序）之间进行信息交换，以及 (ii) 允许对已交换的信息进行相互使用，请与下列地址联系: IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A.。只要遵守适当的条款和条件，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可材料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可证协议或任何同等协议中的条款提供。

## 商标

IBM 和 SecureWay 是 IBM 公司在美国和／或其它国家或地区的商标。

Tivoli 是 Tivoli Systems Inc. 在美国和／或其它国家或地区的商标。

Microsoft、Windows 和 Windows NT 是 Microsoft Corporation 在美国和／或其它国家或地区的商标。

其它公司、产品和服务服务名称可能是其它公司的商标或服务标记。

部件号:  01R2760

中国印刷

(1P) P/N: 01R2760