IBM® Client Security Solutions

Client Security Software Version 2.1 User's Guide

IBM® Client Security Solutions

Client Security Software Version 2.1 User's Guide

First Edition (November 2001)

Before using this information and the product it supports, be sure to read Appendix B, "**Notices and Trademarks**" on page 31.

Contents

Preface

This guide contains information about using Client Security Software on IBM network computers, also referred to as IBM clients which contain IBM embedded Security Chips.

The guide is organized as follows:

″Chapter 1, “**Introducing IBM Client Security Software**”,″ contains an overview of the components provided in the Client Security Software.

″Chapter 2, “Using UVM protection for the system logon”,″ contains instructions on using UVM system logon protection for users of Windows XP, Windows NT Workstation 4.0, and Windows 98.

″Chapter 3, “Instructions for the client user”,″ contains instructions on using the Client Utility and setting up the Client Security screen saver, instructions on changing your UVM passphrase and Windows password, and information on using Client Security Software cryptographic capabilities on Microsoft and Netscape applications.

″Chapter 4, “Troubleshooting”,″ contains helpful information for solving problems you might experience while using the instructions provided in this guide.

″Appendix A, “Password and passphrase rules”,″ contains the rules for UVM passphrases and Security Chip passwords.

″Appendix B, “**Notices and Trademarks**” on page 31,″ contains legal notices and trademark information.

Who should read this guide

This guide is intended for Client Security end users (client users). Client Security Software must be installed and set up on your computer before you can use the information in this guide. Knowledge of using digital certificates and using logon and screen saver programs is required.

How to use this guide

Use this guide to set up the Client Security screen saver, change UVM passphrases and system passwords, and use Client Security cryptographic capabilities on Microsoft and Netscape applications. This guide is a companion to the *Client Security Software Installation Guide*, *Using Client Security with Policy Director*, and *Client Security Software Administrator's Guide*.

Some information provided in this guide is also provided in the *Client Security Software Administrator's Guide*. The *Administrator's Guide* is intended for security administrators who will install and set up Client Security Software on IBM clients.

This guide and all other documentation for Client Security can be downloaded from the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site.

Additional information

You can obtain additional information and security product updates, when available, from the http://www.pc.ibm.com/ww/security/index.html IBM Web site.

Chapter 1. Introducing IBM Client Security Software

Client Security Software is designed for IBM computers that use the IBM embedded Security Chip to encrypt and store encryption keys. This software consists of applications and components that enable IBM clients to use client security throughout a local network, an enterprise, or the Internet.

Client Security Software applications and components

When you install Client Security Software, the following software applications and components are installed:

- **Administrator Utility:** The Administrator Utility is the interface an administrator uses to activate or deactivate the embedded Security Chip, and to create, archive, and regenerate encryption keys and passphrases. In addition, an administrator can use this utility to add users to the security policy provided by Client Security Software.
- **User Verification Manager (UVM):** Client Security Software uses UVM to manage passphrases and other elements to authenticate system users. For example, a fingerprint reader can be used by UVM for logon authentication. UVM software enables the following features:
  - **UVM client policy protection:** UVM software enables an administrator to set the client security policy, which dictates how a client user is authenticated on the system.
  - **UVM system logon protection:** UVM software enables an administrator to control computer access through a logon interface. UVM protection ensures that only users who are recognized by the security policy are able to access the operating system.
  - **UVM Client Security screen saver protection:** UVM software enables users to control access to the computer through a Client Security screen saver interface.
- **Client Utility:** The Client Utility enables a client user to change the UVM passphrase. On Windows NT, the Client Utility enables users to change Windows NT logon passwords to be recognized by UVM and to update key archives. A user can also create backup copies of digital certificates created with the IBM embedded Security Chip.

Public Key Infrastructure (PKI) features

Client Security Software provides all of the components required to create a public key infrastructure (PKI) in your business, such as:

- **Administrator control over client security policy.** Authenticating end users at the client level is an important security policy concern. Client Security Software provides the interface that is required to manage the security policy of an IBM client. This interface is part of the authenticating software User Verification Manager (UVM), which is the main component of Client Security Software.
- **Encryption key management for public key cryptography.** Administrators create encryption keys for the computer hardware and the client users with Client Security Software. When encryption keys are created, they are bound to the IBM embedded Security Chip through a key hierarchy, where a base level hardware key is used to encrypt the keys above it, including the user keys that are associated with each client user. Encrypting and storing keys on the IBM

embedded Security Chip adds an essential extra layer of client security, because the keys are securely bound to the computer hardware.

- **Digital certificate creation and storage that is protected by the IBM embedded Security Chip.** When you apply for a digital certificate that can be used for digitally signing or encrypting an e-mail message, Client Security Software enables you to choose the IBM embedded Security Chip as the cryptographic service provider for applications that use the Microsoft CryptoAPI. These applications include Internet Explorer and Microsoft Outlook Express. This ensures that the private key of the digital certificate is stored on the IBM embedded Security Chip. Also, Netscape users can choose IBM embedded Security Chips as the private key generators for digital certificates used for security. Applications that use the Public-Key Cryptography Standard (PKCS) #11, such as Netscape Messenger, can take advantage of the protection provided by the IBM embedded Security Chip.
- **A key archive and recovery solution.** An important PKI function is creating a key archive from which keys can be restored if the original keys are lost or damaged. Client Security Software provides an interface that enables you to establish an archive for keys and digital certificates created with the IBM embedded Security Chip and to restore these keys and certificates if necessary.
- **Right Click Encryption.** Right Click Encryption enables a client user to encrypt his files simply by clicking the right mouse button.

Chapter 2. Using UVM protection for the system logon

This chapter contains information about using UVM protection for the system logon. Before you can use UVM protection, it must be enabled for the computer. For information on enabling UVM protection for the system logon, contact your security administrator.

UVM protection enables you to control access to the operating system through a logon interface. The logon procedure can differ depending on which operating system is used, Windows 2000, Windows Professional, Windows NT Workstation 4.0,or Windows 98.

Windows XP, Windows NT, and Windows 2000 users

For Windows XP, Windows NT and Windows 2000, the UVM logon interface replaces the Windows logon application, so that, if you try to unlock the computer, the UVM logon interface opens instead of the Windows logon window.

Accessing the UVM logon interface

To access the UVM logon interface, press **Ctrl + Alt + Delete**. From the UVM logon interface, you can do the following:

- Click **Shut down** to shut down the computer
- Click **Lock Workstation** to lock the computer (see below for information on unlocking the computer)
- Click **Task Manager** to open Task Manager
- Click **Logoff** to log off the current user

Unlocking the client

To unlock a client running Windows XP, Windows NT, or Windows 2000 that uses UVM protection, do the following:

1. Press **Ctrl + Alt + Delete** to access the UVM logon interface.
2. Type your user name and the domain where you are logged on, and then click **Unlock**. The UVM passphrase window opens.

   Note: Although UVM recognizes multiple domains, your user password must be the same for all domains.
3. Type your UVM passphrase, and then click **OK** to access the operating system.
   - If the UVM passphrase does not match the user name and domain entered, the UVM logon window opens again.
   - If you type the correct UVM passphrase for the user name and domain entered, the logon is successful.

Depending on what authentication requirements have been set in the security policy for the computer, you might have to type your UVM passphrase and scan your fingerprints to unlock your computer. Contact your security administrator for more information.

Windows 98 Users

For Windows 98, UVM protection supports the use of the operating system logon window. UVM protection forces a Client Security screen saver session to be immediately launched upon logon.

To unlock a computer running Windows 98 that uses UVM protection, do the following:

1. When the operating system logon window opens, type your user name and password information, and click **OK**.
2. Depending on what authentication requirements have been set in the security policy for the computer, you might have to type your UVM passphrase (associated with the user name in the operating system logon) and scan your fingerprints to unlock your computer. Contact your security administrator for more information.
   - If you fulfill the authentication requirements set for the computer, the computer unlocks.
   - If you do not fulfill the authentication requirements, the Client Security screen saver displays without unlocking.

Chapter 3. Instructions for the client user

This section provides information to help a client user do the following:

- Use UVM protection for the system logon
- Set up the Client Security screen saver
- Use the Client Utility
- Use secure e-mail and Web browsing

This information is provided in the *Client Security User's Guide* and the *Client Security Software Administrator's Guide*.

Using UVM protection for the system logon

This section contains information about using UVM logon protection for Windows XP, Windows NT, and Windows 2000 Professional systems. Before you can use UVM protection, it must be enabled for the computer.

UVM protection enables you to control access to the operating system through a logon interface. UVM logon protection replaces the Windows logon application, so that, when a user unlocks the computer, the UVM logon window opens instead of the Windows logon window. After UVM protection is enabled for the computer, the UVM logon interface will open each time you start the computer.

When the computer is running, you can access the UVM logon interface by pressing **Ctrl + Alt + Delete** to shut down or lock the computer, or to open the Task Manager or log off the current user.

To unlock a Windows XP, Windows NT, or Windows 2000 Professional client that uses UVM protection, do the following:

1. Press **Ctrl + Alt + Delete** to access the UVM logon interface.
2. Type your user name and the domain you are logged onto, and then click **Unlock**.

   The UVM passphrase window opens.

   Note: Although UVM recognizes multiple domains, your user password must be the same for all domains.
3. Type your UVM passphrase, and click **OK** to access the operating system. If fingerprint authentication is required by the UVM policy, a message is displayed that prompts you for a fingerprint scan.

   Note: Depending on the UVM policy authentication requirements for the client, further authentication processes might also be required.

The Client Security screen saver

The Client Security screen saver is a series of moving images that display after your computer is idle for a specified period of time. Setting up the Client Security screen saver is a way to control access to the computer through a screen saver application. Once the Client Security screen saver displays on your desktop, you must type your UVM passphrase to access the system desktop.

Setting up the Client Security screen saver

This section contains information about setting up the Client Security screen saver. Before you can use the Client Security screen saver, at least one user must be registered on the security policy of your computer.

To set up the Client Security screen saver, do the following:

1. Click **Start > Settings > Control Panel**.
2. Click the **Display** icon.
3. Click the **Screen Saver** tab.
4. In the Screen Saver drop-down menu, select **Client Security**. To change the speed of the screen saver, click **Settings** and select the desired speed.
5. Click **OK**.

Client Security screen saver behavior

The behavior of the Client Security screen saver differs depending on UVM Administrator Utility and Windows screen saver settings. In Windows XP, Windows NT, and Windows 2000, the system checks Windows settings first, and then the UVM Administrator Utility settings. Consequently, the screen saver only locks if the **Password protected** checkbooks has been selected on the Windows screen saver settings tab.

If this box has been selected, the system requires either the Windows password or the UVM passphrase, depending upon whether the **Use UVM Logon Protection** checkbox has been selected in the Administrator Utility. If it has been selected, the system requires the UVM passphrase. If it has not been selected, the system requires the Windows password.

Also, other authentication requirements might have been set in the security policy for the computer; therefore, further authentication might still be required. For example, you might have to scan your fingerprints to unlock the computer.

Note: If you disable the IBM embedded Security Chip or remove all users from the security policy, the Client Security screen saver becomes unavailable.

The Client Utility

The Client Utility enables the client user to perform various security maintenance tasks that do not require administrator access.

Client Utility features

The Client Utility enables the client user to do the following:

- **Change the UVM passphrase.** To improve security, you can periodically change the UVM passphrase.
- **Update Windows logon settings.** When you change the Windows XP or Windows NT password for a client user with the User Manager program, you must also change the password by using the Client Utility. If an administrator uses the Administrator Utility to change the Windows logon password for a user, all user encryption keys previously created for that user will be deleted, and the associated digital certificates will become invalid.

  Note: Changing the Windows logon password is applicable for users of Windows XP, Windows NT, and Windows 2000 only.

- **Register user fingerprints.** If you want to use a UVM-aware fingerprint sensor (or scanner) for authentication, you can register your fingerprints with UVM.

  Note: Before you can register fingerprints with UVM, a fingerprint scanner must be attached to the IBM client system. For instructions on how to attach and use the fingerprint scanner, refer to the documentation provided by the hardware vendor.
- **Update the key archive.** If you create digital certificates and want to make copies of the private key stored on the IBM embedded Security Chip, or if you want to move the key archive to another location, update the key archive.

Client Utility Windows XP limitations

Windows XP imposes access restrictions which limit the functions available to a client user under certain circumstances.

Windows XP Professional

In Windows XP Professional, client user restrictions might apply in the following situations:

- Client Security Software is installed on a partition that is later converted to an NTFS format
- The Windows folder is on a partition that is later converted to an NTFS format
- The archive folder is on a partition that is later converted to an NTFS format

In the above situations, Windows XP Professional Limited Users might not be able to perform the following Client Utility tasks:

- Change their UVM passphrases
- Update the Windows password registered with UVM
- Update the key archive

These limitations are cleared after an administrator starts and exits the Administrator Utility.

Windows XP Home

Windows XP Home Limited Users will not be able to use the Client Utility in any of the following situations:

- Client Security Software is installed on an NTFS formatted partition
- The Windows folder is on an NTFS formatted partition
- The archive folder is on an NTFS formatted partition

Using the Client Utility

To use the Client Utility, do the following:

1. Click **Start > Programs > IBM Client Security Software > Client Utility**.

   The UVM passphrase window opens.
2. Type the UVM passphrase for the client user who requires a UVM passphrase or Windows NT password change, and click **OK**.

   The following window opens.
3. In the **Required information** area, type the path to the key archive that was set up for this user.

Note: After you set up a key archive, the Administrator Utility populates the **Archive directory (path)** field with the last path that was entered. If the information in **Archive directory (path)** field is deleted or, if the information is incorrect for the user you want to add, make sure that you re-type the correct information because the archive directory is required information.

4. Do one of the following:
   - To change the UVM passphrase, in the **Change current passphrase** area, type a new passphrase in the **New passphrase** field. Next, type the passphrase again in the **Confirm new passphrase** field, and then click **Change**.
   - To change the Windows XP or Windows NT logon password, in the **Windows password** field, type a new Windows NT password. Next, type the new password again in the **Confirm Windows password** field, and then click **Update**. For rules on the Windows NT logon password, see the operating system documentation.

     Note: Only change Windows logon information in User Manager for the user currently logged on.
   - To update the key archive, click **Update archive**; then click **OK** on the window that notifies you that the operation was successful.
   - To register user fingerprints, click the **Fingerprint Registration** tab; then click the **Click to launch fingerprint registration** button. In the radio boxes, select the hand and finger you will scan for prints, and click **Start registration**. Then, place the selected finger on the fingerprint reader and follow the on-screen instructions to scan four copies of your fingerprint. When you have finished scanning your fingerprints, click **Exit**.
5. Click **OK** to exit.

Using secure e-mail and Web browsing

If you send unsecured transactions over the Internet, they are subject to being intercepted and read. You can prohibit unauthorized access to your Internet transactions by getting a digital certificate and using it to digitally sign and encrypt your e-mail messages or to secure your Web browser.

A digital certificate (also called a digital ID or security certificate) is an electronic credential issued and digitally signed by a certificate authority. When a digital certificate is issued to you, the certificate authority is validating your identity as the owner of the certificate. A certificate authority is a trusted provider of digital certificates and can be a third-party issuer such as VeriSign, or the certificate authority can be set up as a server within your company. The digital certificate contains your identity, such as your name and e-mail address, expiration dates of the certificate, a copy of your public key, and the identity of the certificate authority and its digital signature.

Using Client Security Software with Microsoft Applications

The instructions provided in this section are specific to the use of Client Security Software as it generally relates to obtaining and using digital certificates with applications that support the Microsoft CryptoAPI, such as Outlook Express.

For details on how to create the security settings and use e-mail applications such as Outlook Express and Outlook, see the documentation provided with those applications.

Note: To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. The encryption strength provided by Client Security Software is found in the Administrator Utility.

Obtaining a digital certificate for Microsoft applications

When you use a certificate authority to create a digital certificate to be used with Microsoft applications, you will be prompted to choose a cryptographic service provider (CSP) for the certificate.

To use the cryptographic capabilities of the IBM embedded Security Chip for your Microsoft applications, make sure you select **IBM embedded Security Subsystem CSP** as your cryptographic service provider when you obtain your digital certificate. This ensures that the private key of the digital certificate is stored on the IBM Security Chip.

Also, if available, select strong (or high) encryption for extra security. Because the IBM embedded Security Chip is capable of up to 1024-bit encryption of the private key of the digital certificate, select this option if it is available within the certificate authority interface; 1024-bit encryption is also referred to as strong encryption.

After you select **IBM embedded Security Subsystem CSP** as the CSP, you might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements for obtaining a digital certificate. The authentication requirements are defined in the UVM policy for the computer.

Updating the key archive for Microsoft applications

After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive using the Administrator Utility.

Using the digital certificate for Microsoft applications

Use the security settings in your Microsoft applications to view and use digital certificates. See the documentation provided by Microsoft for more information.

After you create the digital certificate and use it to sign an e-mail message, UVM will prompt you for authentication requirements the first time you digitally sign an e-mail message. You might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements for using the digital certificate. The authentication requirements are defined in the UVM policy for the computer.

Using Client Security Software with Netscape applications

The instructions provided in this section are specific to the use of Client Security Software as it generally relates to obtaining and using digital certificates with applications that support PKCS#11, specifically Netscape applications.

For details on how to use the security settings for Netscape applications, see the documentation provided by Netscape.

Note: To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. The encryption strength provided by Client Security Software is found in the Administrator Utility.

Installing the IBM embedded Security Chip PKCS#11 module for Netscape applications

Before you can use a digital certificate, you must install the IBM embedded Security Chip PKCS#11 module onto the computer. Because the installation of the IBM embedded Security Chip PKCS#11 module requires a UVM passphrase, you must add at least one user to the security policy for the computer.

To install the IBM embedded Security Chip PKCS#11 module, complete the following steps:

1. Do one of the following:
   - If Netscape was installed on the computer before Client Security Software was installed, you can run the installation file from the Windows Start menu to add the IBM embedded Security Chip module. Click **Start > Programs > IBM Client Security Software > Add IBM Embedded Security Subsystem Module**.
   - If Netscape was installed on the computer after Client Security Software was installed, open and run the installation file in Netscape. Open Netscape and click **File > Open page**. Locate the install file, IBMPKCSINSTALL.HTML, and open it in Netscape. (If you accepted the default directory when you installed the software, the file is located in C:\Program Files\IBM\Security.) When you open the file in Netscape, the installation file runs.

   The UVM passphrase window opens.
2. Type the UVM passphrase and click **OK**.

   A message is displayed asking if you are sure you want to install this security module.
3. Click **OK**.

   A message is displayed that notifies you that the module was installed.
4. Click **OK**.

Using the PKCS#11 logon protection for Netscape applications

When PKCS#11 logon protection is set up for the computer, you must meet the authentication requirements each time you log on to Netscape. You might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements. The authentication requirements are defined in the UVM policy for the computer.

Selecting the IBM embedded Security Chip to generate a digital certificate for Netscape applications

When you generate a digital certificate in Netscape, select the IBM embedded Security Chip as the generator of the private key associated with the certificate.

During digital certificate creation, you will be asked to select the card or database you wish to generate your key in, select **IBM embedded Security Subsystem**.

For more information on generating a digital certificate and using it with Netscape, see the documentation provided by Netscape.

Updating the key archive for Netscape applications

After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive using the Administrator Utility.

Using the digital certificate for Netscape applications

Use the security settings in your Netscape applications to view, select, and use digital certificates. For example, in the security settings for Netscape Messenger, you must select the certificate before you can use it to digitally sign or encrypt e-mail messages. See the documentation provided by Netscape for more information.

After you have installed the IBM embedded Security Chip PKCS#11 module, UVM will prompt you for authentication requirements each time you use the digital certificate. You might have to type your UVM passphrase, scan your fingerprints, or do both to meet the authentication requirements. The authentication requirements are defined in the UVM policy for the computer.

If you do not meet the authentication requirements set by the UVM policy, an error message is displayed. When you click **OK** on this message, Netscape will open, but you will not be able to use the digital certificate generated by the IBM embedded Security Chip until you restart Netscape and provide the correct UVM passphrase, fingerprints, or both.

Chapter 4. Troubleshooting

The following section presents information that is helpful for preventing, or identifying and correcting problems that might arise as you use Client Security Software.

Administrator functions

This section contains information that an administrator might find helpful when setting up and using Client Security Software.

Setting an administrator password (NetVista)

Security settings available in the Configuration/Setup Utility enable administrators to do the following:

- Change the hardware password for the IBM embedded Security Chip
- Enable or disable the IBM embedded Security Chip
- Clear the IBM embedded Security Chip

Attention:

- In Windows XP, Windows NT, and Windows 2000, do not clear or disable the IBM embedded Security Chip when UVM logon protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.

  To disable UVM protection, open the Administrator Utility and clear the **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** check box. You must restart the computer before UVM protection is disabled.
- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

Because these security settings are accessible through the Configuration/Setup Utility of the computer, set an administrator password to deter unauthorized users from changing these settings.

To set an administrator password:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press **F1**.

   The main menu of the Configuration/Setup Utility opens.
3. Select **System Security**.
4. Select **Administrator Password**.
5. Type your password and press the down arrow on your keyboard.
6. Type your password again and press the down arrow.
7. Select **Change Administrator password** and press Enter; then press Enter again.
8. Press **Esc** to exit and save the settings.

After you set an administrator password, a prompt appears each time you try to access the Configuration/Setup Utility.

Important: Keep a record of your administrator password in a secure place. If you lose or forget the administrator password, you cannot access the Configuration/Setup Utility, and you cannot change or delete the password without removing the computer cover and moving a jumper on the system board. See the hardware documentation that came with your computer for more information.

Setting a supervisor password (ThinkPad)

Security settings available in the IBM BIOS Setup Utility enable administrators to do the following:

- Enable or disable the IBM embedded Security Chip
- Clear the IBM embedded Security Chip

Attention:

- In Windows XP, Windows NT, and Windows 2000, do not clear or disable the IBM embedded Security Chip when UVM logon protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.

  To disable UVM protection, open the Administrator Utility and clear the **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** check box. You must restart the computer before UVM protection is disabled.
- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

After setting up Client Security Software, set a supervisor password to deter unauthorized users from changing these settings.

To set a supervisor password, complete the following procedure:

1. Shut down and restart the computer.
2. When the IBM BIOS Setup Utility prompt appears on the screen, press **F1**.

   The main menu of the IBM BIOS Setup Utility opens.
3. Select **Password**.
4. Select **Supervisor Password**.
5. Type your password and press Enter.
6. Type your password again and press Enter.
7. Click **Continue**.
8. Press F10 to save and exit.

After you set a supervisor password, a prompt appears each time you attempt to access the IBM BIOS Setup Utility.

Important: Keep a record of your supervisor password in a secure place. If you lose or forget the supervisor password, you cannot access the IBM BIOS Setup Utility, and you cannot change or delete the password without moving a jumper on the system board. See the hardware documentation that came with your computer for more information.

Protecting the hardware password

You set a Security Chip password to enable the IBM embedded Security Chip for a client. After you set a Security Chip password, access to the Administrator Utility is protected by this password. You should protect the Security Chip password to prohibit unauthorized users from changing settings in the Administrator Utility.

the IBM embedded Security Chip (NetVista)

If you want to erase all user encryption keys from the IBM embedded Security Chip and clear the hardware password for the chip, you must clear the chip. Read the information in the Attention box below before clearing the IBM embedded Security Chip.

Attention:

- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.

  To clear UVM protection, open the Administrator Utility and clear the **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** check box. You must restart the computer before UVM protection is disabled.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

To clear the IBM embedded Security Chip, do the following:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press F1.

   The main menu of the Configuration/Setup Utility opens.
3. Select **System Security**.
4. Select **IBM Embedded Security Chip**.
5. Select **Clear IBM Security Chip**.
6. Select **Yes**.
7. Press Esc to continue.
8. Press Esc to exit and save the settings.

Clearing the IBM embedded Security Chip (ThinkPad)

If you want to erase all user encryption keys from the IBM embedded Security Chip and clear the hardware password for the chip, you must clear the chip. Read the information in the Attention box below before clearing the IBM embedded Security Chip.

Attention:

- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.

  To clear UVM protection, open the Administrator Utility, click the **Key Configuration** button, and clear the **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** check box. You must restart the computer before UVM protection is disabled.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

To clear the IBM embedded Security Chip, do the following:

1. Shut down and restart the computer.
2. When the IBM BIOS Setup Utility prompt appears on the screen, press F1.
   The main menu of the IBM BIOS Setup Utility opens.
3. Select **Config**.
4. Select **IBM Security Chip**.
5. Select **Clear IBM Security Chip**.
6. Select **Yes**.
7. Press Enter to continue.
8. Press F10 to save and exit.

The Administrator Utility

The following section contains general information to keep in mind when using the Administrator Utility, as well as troubleshooting information that might be helpful if you experience problems using the Administrator Utility.

Administrator Utility information

The following section contains information to keep in mind when using the Administrator Utility.

Deleting users

When you delete a user from Windows XP, Windows NT, and Windows 2000, the user name is deleted from the list of users in the Administrator Utility.

When you delete a user from Windows 98, the user name is **not** deleted from the list of users in the Administrator Utility.

Denying access to selected objects with Policy Director control

The **Deny all access to selected object** check box is not disabled when Policy Director control is selected. In the UVM-policy editor, if you select **Policy Director controls selected object** to enable Policy Director to control an authentication object, the **Deny all access to selected object** check box is not disabled. Although the **Deny all access to selected object** check box remains active, it cannot be selected to override Policy Director control.

Known limitations

This section contains information about known limitations related to Client Security Software.

Using Client Security Software with Windows operating systems

All Windows operating systems have the following known limitation: If a client user that is enrolled in UVM changes his Windows user name, all Client Security functionality is lost. The user will have to re-enroll the new user name in UVM and request all new credentials.

Windows XP operating systems have the following known limitation: Users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. UVM will point to the former user name while Windows will only recognize the new user name. This limitation occurs even if the Windows user name was changed prior to installing Client Security Software.

Windows 98 and Windows Millennium operating systems have known security limitations: Operating systems derived for the Windows NT kernel adhere to more stringent security standards than operating systems derived from the Windows 9X kernel. Consequently, operating systems derived from the 9X kernel are not as secure, and some Client Security Software features might behave differently. For example, Windows 9X-based operating systems do not report suspend or resume events to the screen saver. Therefore, the Client Security screen saver might not provide the same level of security as it does under NT-based operating systems.

Using Client Security Software with Netscape applications

Netscape opens after an authorization failure: If the UVM passphrase window opens, you must type the UVM passphrase and click **OK** before you can continue. If you type an incorrect UVM passphrase (or provide an incorrect fingerprint for a fingerprint scan), an error message is displayed. If you click **OK**, Netscape will open, but you will not be able to use the digital certificate generated by the IBM embedded Security Chip. You must exit and re-enter Netscape, and type the correct UVM passphrase before you can use the IBM embedded Security Chip certificate.

Algorithms do not display: All hashing algorithms supported by the IBM embedded Security Chip PKCS#11 module are not selected if the module is viewed in Netscape. The following algorithms are supported by the IBM embedded Security Chip PKCS#11 module, but are not identified as being supported when viewed in Netscape:

- SHA-1
- MD5

IBM embedded Security Chip certificate and encryption algorithms

The following information is provided to help identify issues about the encryption algorithms that can be used with the IBM embedded Security Chip certificate. See Microsoft or Netscape for current information about the encryption algorithms used with their e-mail applications.

When sending e-mail from one Outlook Express (128-bit) client to another Outlook Express (128-bit) client: If you use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0 to send encrypted e-mail to other clients using Outlook Express (128-bit), e-mail messages encrypted with the IBM embedded Security Chip certificate can only use the 3DES algorithm.

When sending e-mail between an Outlook Express (128-bit) client and a Netscape client: An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm.

Some algorithms might not be available for selection in the Outlook Express (128-bit) client: Depending on how your version of Outlook Express (128-bit) was configured or updated, some RC2 algorithms and other algorithms might not be available for use with the IBM embedded Security Chip certificate. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.

Using UVM protection for a Lotus Notes User ID

UVM protection does not operate if you switch User IDs within a Notes session: You can set up UVM protection only for the current user ID of a Notes session. To switch from a User ID that has UVM protection enabled to another User ID, do the following:

1. Exit Notes.
2. Disable UVM protection for the current User ID.
3. Enter Notes and switch User IDs. See your Lotus Notes documentation for information about switching User IDs.

   If you want to set up UVM protection for the User ID that you have switched to, proceed to step 4.
4. Enter the Lotus Notes Configuration tool provided by Client Security Software and set up UVM protection.

Client Utility limitations

Windows XP imposes access restrictions which limit the functions available to a client user under certain circumstances.

Windows XP Professional

In Windows XP Professional, client user restrictions might apply in the following situations:

- Client Security Software is installed on a partition that is later converted to an NTFS format
- The Windows folder is on a partition that is later converted to an NTFS format
- The archive folder is on a partition that is later converted to an NTFS format

In the above situations, Windows XP Professional Limited Users might not be able to perform the following Client Utility tasks:

- Change their UVM passphrases
- Update the Windows password registered with UVM
- Update the key archive

These limitations are cleared after an administrator starts and exits the Administrator Utility.

Windows XP Home

Windows XP Home Limited Users will not be able to use the Client Utility in any of the following situations:

- Client Security Software is installed on an NTFS formatted partition
- The Windows folder is on an NTFS formatted partition
- The archive folder is on an NTFS formatted partition

Error messages

Error messages related to Client Security Software are generated in the event log: Client Security Software uses a device driver that might generate error messages in the event log. The errors associated with these messages do not affect the normal operation of your computer.

UVM invokes error messages that are generated by the associated program if access is denied for an authentication object: If UVM policy is set to deny access for an authentication object, for example e-mail decryption, the message stating that access has been denied will vary depending on what software is being used. For example, an error message from Outlook Express that states access is denied to an authentication object will differ from a Netscape error message that states that access was denied.

Troubleshooting charts

The following section contains troubleshooting charts that might be helpful if you experience problems with Client Security Software.

Installation troubleshooting information

The following troubleshooting information might be helpful if you experience problems when installing Client Security Software.

Problem Symptom	Possible Solution
An error message is displayed during software installation	**Action**
A message is displayed when you install the software that asks if you want to remove the selected application and all of its components.	Click **OK** to exit the window. Begin the installation process again to install the new version of Client Security Software.
A message is displayed during installation stating that a previous version of Client Security Software is already installed.	Click **OK** to exit from the window. Do the following: 1. Uninstall the software. 2. Reinstall the software. **Note:** If you plan to use the same hardware password to secure the IBM embedded Security Chip, you do not have to clear the chip and reset the password.
Installation access is denied due to an unknown hardware password	**Action**
When installing the software on an IBM client with an enabled IBM embedded Security Chip, the hardware password for the IBM embedded Security Chip is unknown.	Clear the chip to continue with the installation.
An unattended installation will not start	**Action**
The SMBus device driver must be installed to perform an unattended installation.	Install the SMBus device driver and restart the installation.
An unattended installation ends prematurely	**Action**
No error messages are displayed during unattended installations.	Perform an attended installation to view any error messages that might be displayed.
The setup.exe file does not respond properly	**Action**
If you extract all files from the csec21.exe file into a common directory, the setup.exe file will not work properly.	Run the smbus.exe file to install the SMBus device driver, and then run the csec21.exe file to install the Client Security Software code.
An error message displays when you install a UVM-aware fingerprint sensor	**Action**
During installation of the DigitalPersona U.are.UPro fingerprint sensor, a message is displayed that asks you to do the following: 1. Attach the fingerprint sensor. 2. Wait for the red light to illuminate on the sensor. 3. Click **OK**. 4. Select **Yes, I want to restart my computer now** and click **Finish**. The system will restart.	No further action is required. The fingerprint sensor will install correctly.

Administrator Utility troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using the Administrator Utility.

Problem Symptom	Possible Solution
An error message displays when you change the admin public key	**Action**
When you clear the embedded Security Chip and then restore the key archive, an error message might display if you change the admin public key.	Add the users to UVM and request new certificates, if applicable.
An error message displays when you attempt to recover a UVM passphrase	**Action**
When you change the admin public key and then attempt to recover a UVM passphrase for a user, an error message might display.	Do one of the following: • If the UVM passphrase for the user is not needed, no action is required. • If the UVM passphrase for the user is needed, you must add the user to UVM, and request new certificates, if applicable.
An error message displays when you try to save the UVM-policy file	**Action**
When you attempt to save a UVM-policy file (globalpolicy.gvm) by clicking **Apply** or **Save**, an error message might display.	Exit the error message, edit the UVM-policy file again to make your changes, and then save the file.
An error message displays when you try to open the UVM-policy editor	**Action**
When the current user (logged on to the operating system) has not been added to UVM, the UVM-policy editor will not open.	Add the user to UVM and open the UVM-policy editor.
An error message displays when you are using the Administrator Utility	**Action**
When you are using the Administrator Utility, the following error message might display: A buffer I/O error occurred while trying to access the Client Security chip. This might be corrected by a reboot.	Exit the error message and restart your computer.
A disable chip message is displayed when change the Security Chip password	**Action**
When you attempt to change the Security Chip password, and you press Enter or Tab > Enter after you type the confirmation password, the Disable chip button will be enabled and a disable chip confirmation message is displayed.	Do the following: 1. Exit from the disable chip confirmation window. 2. To change the Security Chip password, type the new password, type the confirmation password, and then click **Change**. Do not press Enter or Tab > Enter after you type the confirmation window.

Client Utility troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using the Client Utility.

Problem Symptom	Possible Solution
Limited Users are unable to perform certain Client Utility functions in Windows XP Professional	**Action**
Windows XP Professional Limited Users might not be able to perform the following Client Utility tasks: • Change their UVM passphrases • Update the Windows password registered with UVM • Update the key archive	These limitations are cleared after an administrator starts and exits the Administrator Utility.
Limited Users are unable to use the Client Utility in Windows XP Home	**Action**
Windows XP Home Limited Users will not be able to use the Client Utility in any of the following situations: • Client Security Software is installed on an NTFS formatted partition • The Windows folder is on an NTFS formatted partition • The archive folder is on an NTFS formatted partition	This is a known limitation with Windows XP Home. There is no solution to this problem.

ThinkPad-specific troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Client Security Software on ThinkPad computers.

Problem Symptom	Possible Solution
An error message is displayed on Client Security reboot	**Action**
The following error message is displayed after trying to perform a Client Security administrator function: ERROR 0197: Invalid Remote change requested. Press <F1> to Setup	The ThinkPad supervisor password must be disabled to perform certain Client Security administrator functions. To disable the supervisor password, do the following: 1. Press F1 to access the IBM BIOS Setup Utility. 2. Enter the current supervisor password. 3. Enter a blank new supervisor password, and confirm a blank password. 4. Press Enter. 5. Press F10 to save and exit.

Microsoft troubleshooting information

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security Software with Microsoft applications or operating systems.

Problem Symptom	Possible Solution
Client Security does not work properly for a user enrolled in UVM	**Action**
The enrolled client user might have changed his Windows user name. If that occurs, all Client Security functionality is lost.	Re-enroll the new user name in UVM and request all new credentials.
Note: In Windows XP, users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. This limitation occurs even if the Windows user name was changed prior to installing Client Security Software.	
Problems reading encrypted e-mail using Outlook Express	**Action**
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient. **Note:** To use 128-bit Web browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility.	Verify the following: 1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.
Problems using a certificate from an address that has multiple certificates associated with it	**Action**
Outlook Express can list multiple certificates associated with a single e-mail address and some of those certificates can become invalid. A certificate can become invalid if the private key associated with the certificate no longer exists on the IBM embedded Security Chip of the sender's computer where the certificate was generated.	Ask the recipient to resend his digital certificate; then select that certificate in the address book for Outlook Express.
Failure message when trying to digitally sign an e-mail message	**Action**
If the composer of an e-mail message tries to digitally sign an e-mail message when the composer does not yet have a certificate associated with his or her e-mail account, an error message displays.	Use the security settings in Outlook Express to specify a certificate to be associated with the user account. See the documentation provided for Outlook Express for more information.
Outlook Express (128 bit) only encrypts e-mail messages with the 3DES algorithm	**Action**
When sending encrypted e-mail between clients that use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0, only the 3DES algorithm can be used.	To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. See Microsoft for current information on the encryption algorithms used with Outlook Express.

Problem Symptom	Possible Solution
Outlook Express clients return e-mail messages with a different algorithm	**Action**
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
Error message when using a certificate in Outlook Express after a hard disk drive failure	**Action**
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, do one of the following: • obtain new certificates • register the certificate authority again in Outlook Express
Outlook Express does not update the encryption strength associated with a certificate	**Action**
When a sender selects the encryption strength in Netscape and sends a signed e-mail message to a client using Outlook Express with Internet Explorer 4.0 (128-bit), the encryption strength of the returned e-mail might not match.	Delete the associated certificate from the address book in Outlook Express. Open the signed e-mail again and add the certificate to the address book in Outlook Express.
An error decryption message displays in Outlook Express	**Action**
You can open a message in Outlook Express by double-clicking it. In some instances, when you double-click an encrypted message too quickly, a decryption error message appears.	Close the message, and open the encrypted e-mail message again.
Also, a decryption error message might display in the preview pane when you select an encrypted message.	If an error message appears in the preview pane, no action is required.
An error message displays when you click the Send button twice on encrypted e-mails	**Action**
When using Outlook Express, if you click the send button twice to send an encrypted e-mail message, an error message displays stating that the message could not be sent.	Close the error message and click the **Send** button once.
An error message displays when you requesting a certificate	**Action**
When using Internet Explorer, you might receive an error message if you request a certificate that uses the IBM embedded Security Chip CSP.	Request the digital certificate again.

Netscape application troubleshooting information

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security Software with Netscape applications.

Problem Symptom	Possible Solution
Problems reading encrypted e-mail	**Action**
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient. **Note:** To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility.	Verify the following: 1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.
Failure message when trying to digitally sign an e-mail message	**Action**
When the IBM embedded Security Chip certificate has not been selected in Netscape Messenger, and the writer of an e-mail message tries to sign the message with the certificate, an error message displays.	Use the security settings in Netscape Messenger to select the certificate. When Netscape Messenger is open, click the security icon on the toolbar. The Security Info window opens. Click **Messenger** in the left panel and then select the **IBM embedded Security Chip certificate**. See the documentation provided by Netscape for more information.
An e-mail message is returned to the client with a different algorithm	**Action**
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
Unable to use a digital certificate generated by the IBM embedded Security Chip	**Action**
The digital certificate generated by the IBM embedded Security Chip is not available for use.	Verify that the correct UVM passphrase was typed when Netscape was opened. If you type the incorrect UVM passphrase, an error message displays stating an authentication failure. If you click **OK**, Netscape opens, but you will not be able to use the certificate generated by the IBM embedded Security Chip. You must exit and re-open Netscape, and then type the correct UVM passphrase.
New digital certificates from the same sender are not replaced within Netscape	**Action**

Problem Symptom	Possible Solution
When a digitally signed e-mail is received more than once by the same sender, the first digital certificate associated with the e-mail is not overwritten.	If you receive multiple e-mail certificates, only one certificate is the default certificate. Use the security features in Netscape to delete the first certificate, and then re-open the second certificate or ask the sender to send another signed e-mail.
Cannot export the IBM embedded Security Chip certificate	**Action**
The IBM embedded Security Chip certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up certificates.	Go to the Administrator Utility or Client Utility to update the key archive. When you update the key archive, copies of all the certificates associated with the IBM embedded Security Chip are created.
Error message when trying to use a restored certificate after a hard disk drive failure	**Action**
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, obtain a new certificate.
Netscape agent opens and causes Netscape to fail	**Action**
Netscape agent opens and closes Netscape.	Turn off the Netscape agent.
Netscape delays if you try to open it	**Action**
If you add the IBM embedded Security Chip PKCS#11 module and then open Netscape, a short delay will occur before Netscape opens.	No action is required. This is for informational purposes only.

Digital certificate troubleshooting information

The following troubleshooting information might be helpful if you experience problems obtaining a digital certificate.

Problem Symptom	Possible Solution
UVM passphrase window or fingerprint authentication window displays multiple times during a digital certificate request	**Action**
The UVM security policy dictates that a user provide the UVM passphrase or fingerprint authentication before a digital certificate can be acquired. If the user tries to acquire a certificate, the authentication window that asks for the UVM passphrase or fingerprint scan displays more than once.	Type your UVM passphrase or scan your fingerprint each time the authentication window opens.
A VBScript or JavaScript error message displays	**Action**
When you request a digital certificate, an error message related to VBScript or JavaScript might display.	Restart the computer, and obtain the certificate again.

Lotus Notes troubleshooting information

The following troubleshooting information might be helpful if you experience problems with using Lotus Notes with Client Security Software.

Problem Symptom	Possible Solution
An error message displays when you try to change the Notes password	**Action**
Changing the Notes password when using Client Security Software might display in an error message.	Retry the password change. If this does not work, restart the client.
An error message displays after you randomly-generate a password	**Action**
An error message might display when you do the following: • Use the Lotus Notes Configuration tool to set UVM protection for a Notes ID • Open Notes and use the function provided by Notes to change the password for Notes ID file • Close Notes immediately after you change the password	Click **OK** to close the error message. No other action is required. Contrary to the error message, the password has changed. The new password is a randomly-generated password created by Client Security Software. The Notes ID file is now encrypted with the randomly-generated password, and the user does not need a new User ID file. If the end user changes the password again, UVM will generate a new random password for the Notes ID.

UVM-aware device troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using UVM-aware devices.

Problem Symptom	Possible Solution
A UVM-aware device stops working properly	**Action**
When you disconnect a UVM-aware device from a Universal Serial Bus (USB) port, and then reconnect the device to the USB port, the device might not work properly.	Restart the computer after the device has been reconnected to the USB port.

Appendix A. Password and passphrase rules

This appendix contains information regarding rules pertaining to various system passwords.

Hardware password rules

The following rules pertain to the hardware password:

Length
The password must be exactly eight characters long.

Characters
The password must contain alphanumeric characters only. A combination of letters and numbers is allowed. No exceptional characters, like space, !, ?, %, are allowed.

Properties
Set the Security Chip password to enable the IBM embedded Security Chip in the computer. This password must be typed each time you access the Administrator Utility.

Incorrect attempts
If you incorrectly type the password ten times, the computer locks up for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly ten more times, the computer locks up for 2 hours and 34 minutes. The time the computer is disabled doubles each time you incorrectly type the password ten times.

UVM passphrase rules

To improve security, the UVM passphrase is longer and can be more unique than a traditional password.

The following rules pertain to the UVM passphrase:

Length
The passphrase can be up to 256 characters long.

Characters
The passphrase can contain any combination of characters that the keyboard produces, including spaces and non alphanumeric characters.

Properties
The UVM passphrase is different from a password that you might use to log on to an operating system. The UVM passphrase can be used in conjunction with other authenticating devices, such as a UVM-aware fingerprint sensor.

Incorrect attempts
If you incorrectly type the UVM passphrase multiple times during a session, the computer will not lock up. There is no limit on the number of incorrect attempts.

Appendix B. Notices and Trademarks

This appendix gives legal notice for IBM products as well as trademark information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who wish to have information about it for the purpose of enabling: (1) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Department 80D, P.O. Box 12195, 3039 Cornwallis, Research Triangle Park, NC 27709, U.S.A. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

IBM and SecureWay are trademarks of the IBM Corporation in the United States, other countries, or both.

Tivoli is a trademark of Tivoli Systems Inc. in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.