IBM® Client Security
Solutions

# Client Security Software Version 3.0 Installation Guide

IBM® Client Security
Solutions

# Client Security Software Version 3.0 Installation Guide

**First Edition (March 2002)**

Before using this information and the product it supports, be sure to read Appendix A, “U.S. export regulations for Client Security Software” on page 35 and Appendix C, “**Notices and Trademarks**” on page 39.

# Contents

# Preface

This section provides information about how to use this guide.

## About this guide

This guide contains information on installing Client Security Software on IBM network computers, also referred to as IBM clients, which contain IBM embedded Security Chips. This guide also contains instructions on enabling the IBM embedded Security Chip and setting the hardware password for the security chip.

The guide is organized as follows:

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

″Chapter 2, “Getting started”,″ contains computer hardware and software installation prerequisites as well as instructions for downloading the software.

″Chapter 3, “Before installing the software”,″ contains prerequisite instructions for installing Client Security Software.

″Chapter 4, “Installing, updating, and uninstalling the software”,″ contains instructions for installing, updating, and uninstalling the software.

″Chapter 5, “Troubleshooting”,″ contains helpful information for solving problems you might experience while using the instructions provided in this guide.

″Appendix A, “U.S. export regulations for Client Security Software”,″ contains U.S. export regulation information regarding the software.

″Appendix B, “Password and passphrase rules”,″ contains rules for setting passwords and passphrases.

″Appendix C, “**Notices and Trademarks**”,″ contains legal notices and trademark information.

## Who should read this guide

This guide is intended for network or system administrators who set up personal-computing security on IBM clients. Knowledge of security concepts, such as public key infrastructure (PKI) and digital certificate management within a network environment, is required.

## How to use this guide

Use this guide to install and set up personal-computing security on IBM clients. This guide is a companion to the *Client Security Software Administrator's Guide*, *Using Client Security with Policy Director*, and *Client Security User's Guide*.

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.

## References to the *Client Security Software Administrator's Guide*

References to the *Client Security Software Administrator's Guide* are provided in this document. The *Administrator's Guide* contains information about using User Verification Manager (UVM) and working with UVM policy, and information about using the Administrator Utility and the Client Utility.

After you install the software, use the instructions in the *Administrator's Guide* to set up and maintain the security policy for each client.

## References to the *Client Security Software User's Guide*

The *Client Security User's Guide*, a companion to the *Client Security Software Administrator's Guide*, contains helpful information about performing user tasks with Client Security Software, such as using UVM logon protection, creating a digital certificate, and using the Client Utility.

---

# 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. Getting started

This section contains hardware and software compatibility requirements for use with Client Security Software. Also, information about downloading Client Security Software is provided.

## Hardware requirements

Before you download and install the software, make sure that your computer hardware is compatible with Client Security Software.

The most recent information regarding hardware and software requirements is available at the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site.

## IBM embedded Security Chip

The IBM embedded Security Chip is a cryptographic microprocessor that is embedded on the system board of the IBM client. This essential component of IBM Client Security transfers security policy functions from vulnerable software to secure hardware, radically increasing the security of the local client.

Only IBM computers and workstations that contain IBM embedded Security Chips support Client Security Software. If you try to download and install the software onto a computer that does not contain an IBM embedded Security Chip, the software will not install or run properly.

## Supported IBM models

Client Security Software is licensed for and supports numerous IBM desktop and notebook computers. For a complete list of supported models, refer to the http://www.pc.ibm.com/ww/resources/security/secdownload.html Web page.

## Software requirements

Before you download and install the software, make sure that your computer software and operating system are compatible with Client Security Software.

## Operating systems

Client Security Software requires one of the following operating systems:

- Windows XP
- Windows Millennium Edition
- Windows 2000 Professional
- Windows NT 4.0, with Service Pack 5 or later
- Windows 98

## UVM-aware products

User Verification Manager (UVM) software enables you to customize authentication for your desktop machine. This first level of policy-based control increases asset protection and the efficiency of password management. UVM, which is compatible with enterprise-wide security policy programs, enables you to use UVM- aware products, including the following:

- **Biometrics devices, such as fingerprint readers**

UVM provides a plug-and-play interface for biometrics devices. You must install Client Security Software before you install a UVM-aware sensor.

To use a UVM-aware sensor that is already installed on an IBM client, you must uninstall the UVM-aware sensor, install Client Security Software, and then reinstall the UVM-aware sensor.

- **Tivoli SecureWay Policy Director versions 3.7 or 3.8**

  UVM software simplifies and improves policy management by smoothly integrating with a centralized, policy-based access control solution, such as Policy Director.

  UVM software enforces policy locally whether the system is on the network (desktop) or stands alone, thus creating a single, unified policy model.

- **Lotus Notes version 4.5 or later**

  UVM works with Client Security Software to improve the security of your Lotus Notes logon (Lotus Notes version 4.5 or later).

- **Entrust Entelligence**

  Entrust Entelligence support enhances Internet security capabilities so that critical enterprise processes can be moved to the Internet. Entrust Entelligence provides a single security layer that can encompass an enterprise's entire set of enhanced security needs including identification, privacy, verification, and security management.

- **RSA SecurID Software Token**

  The RSA SecurID Software Token enables the same seed record that is used in traditional RSA hardware tokens to be embedded on existing user platforms. Consequently, users can authenticate to protected resources by accessing the embedded software instead of having to carry dedicated authentication devices.

## Web browsers

Client Security Software supports the following Web browsers for requesting digital certificates:

- Internet Explorer 5.0 or later
- Netscape 4.51 or later

### Web browser encryption strength information

If support for strong encryption is installed, use the 128-bit version of your Web browser. Otherwise, use the 40-bit version of your Web browser. To check the encryption strength of your Web browser, see the help system provided with the browser.

### Cryptographic services

Client Security Software supports the following cryptographic services:

- **Microsoft CryptoAPI:** CryptoAPI is the default cryptographic service for Microsoft operating systems and applications. With built-in CryptoAPI support, Client Security Software enables you to use the cryptographic operations of the IBM embedded Security Chip when you create digital certificates for Microsoft applications.
- **PKCS#11:** PKCS#11 is the cryptographic standard for Netscape, Entrust, RSA and other products. After you install the IBM embedded Security Chip PKCS#11 module, you can use the IBM embedded Security Chip to generate digital certificates for Netscape, Entrust, RSA and other applications that use PKCS#11.

### E-mail applications

Client Security Software supports the following application types using secure e-mail:

- E-mail applications that use the Microsoft CryptoAPI for cryptographic operations, such as Outlook Express and Outlook (when used with a supported version of Internet Explorer)
- E-mail applications that use Public Key Cryptographic Standard #11 (PKCS#11) for cryptographic operations, such as Netscape Messenger (when used with a supported version of Netscape)

## Downloading the software

Client Security Software can be downloaded from the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site.

### Registration form

When you download the software, you must complete a registration form and questionnaire, and agree to the license terms. Follow the instructions that are provided at the Web site to download the software.

The installation files for Client Security Software are included within the self-extracting file named csec30.exe.

### Export regulations

Client Security Software contains encryption code that can be downloaded within North America and internationally. If you live in a country where downloading encryption software from a Web site in the United States is prohibited, you cannot download Client Security Software. For more information on export regulations that govern Client Security Software, see Appendix A, “U.S. export regulations for Client Security Software” on page 35.

# Chapter 3. Before installing the software

This section contains prerequisite instructions for running the installation program and configuring Client Security Software on IBM clients. All files required for the installation are provided within the csec3_0.exe file that you download from the IBM Web site.

## Before you install the software

The installation program installs Client Security Software on the IBM client and enables the IBM embedded Security Chip; however, installation specifics vary depending on a number of factors.

## Installing on clients running Windows XP, Windows NT, and Windows 2000

Windows XP, Windows NT, and Windows 2000 users must log on with administrator rights to install Client Security Software.

## Installing for use with Policy Director

If you intend to use Policy Director to control the authentication requirements for your computer, you must install some Policy Director components before you install Client Security Software. For details, see *Using Client Security with Policy Director*.

## Startup feature considerations

Two IBM startup features might affect the way that you enable the security subsystem (embedded Security Chip) and generate hardware encryption keys. These features are the administrator password and Enhanced Security.

### Administrator password (NetVista)

Administrator passwords prevent unauthorized persons from changing the configuration settings of an IBM computer. These passwords are set using the Configuration/Setup Utility program, which is accessed by pressing F1 during the system startup sequence.

### Supervisor password (ThinkPad)

Supervisor passwords prevent unauthorized persons from changing the configuration settings of an IBM ThinkPad computer. These passwords are set using the IBM BIOS Setup Utility program, which is accessed by pressing F1 during the system startup sequence.

Due to the nature of Client Security Software, the supervisor password must be disabled temporarily to perform the following functions:

- Installing or upgrading Client Security Software
- Enabling, disabling, or clearing the IBM embedded Security Chip
- Generating or restoring encryption or user keys
- Adding users to UVM

Client Security Software might generate the following message when the supervisor password needs to be disabled:

**ThinkPad computers:** `If you have a supervisor password enabled, you must disable it in the BIOS Setup before continuing. If you have a supervisor`

password enabled, click Cancel. Otherwise, click OK to continue. After this operation has been completed, re-enable the supervisor password to maintain your system security.

See “Supervisor password (ThinkPad)” on page 7 for more information about setting a supervisor password.

### Enhanced Security

Enhanced Security provides extra protection for your administrator password, as well as your startup sequence settings. You can find out if Enhanced Security is enabled or disabled by using the Configuration/Setup Utility program, which is accessed by pressing F1 during the system startup sequence.

For more information about the administrator password and Enhanced Security, see the documentation provided with your computer.

***Enhanced Security on NetVista models 6059, 6569, 6579, 6649, and all NetVista Q1x models:*** If an administrator password has been set on NetVista models (6059, 6569, 6579, 6649, 6646, and all Q1x models), you must open the Administrator Utility to enable the chip and generate the hardware keys.

When Enhanced Security is enabled on these NetVista models, you must use the Administrator Utility to enable the embedded Security Chip and generate the hardware encryption keys after the Client Security Software is installed. If the installation program detects that Enhanced Security is enabled, you will be notified at the end of the installation process. Restart the computer and open the Administrator Utility to enable the chip and generate the hardware keys.

***Enhanced Security on all other NetVista models (other than models 6059, 6569, 6579, 6649, and all NetVista Q1x models):*** If an administrator password on other NetVista models has been set, you are not required to type the administrator password during the installation process.

When Enhanced Security is enabled on these NetVista models, you can use the installation program to install the software, but you must use the Configuration/Setup Utility to enable the embedded Security Chip. After you have enabled the chip, you can use the Administrator Utility to generate the hardware keys.

## BIOS update information

Before you install the software, you might need to download the latest basic input/output system (BIOS) code for your computer. To determine the BIOS level that your computer uses, restart your computer and press F1 to start the Configuration/Setup Utility. When the main menu for the Configuration/Setup Utility opens, select Product Data to view information about the BIOS code. The BIOS code level is also called the EEPROM revision level.

To run Client Security Software 2.1 or later on NetVista models (6059, 6569, 6579, 6649), you must use BIOS level xxxx22axx or later; to run Client Security Software 2.1 on NetVista models (6790, 6792, 6274, 2283), you must use BIOS level xxxx20axx or later. For more information, see the README file included with the software download.

To find the latest BIOS code updates for your computer, go to the http://www.pc.ibm.com/support IBM Web site, type bios in the search field, and

select downloads from the drop-down list; then press Enter. A list of BIOS code updates is displayed. Click the appropriate NetVista model number and follow the instruction on the Web page.

## Using archive keypair

The archive keypair, which includes the admin public key and the admin private key, enables you to generate hardware encryption keys for an IBM client, and to keep copies of the key data elsewhere for restoration.

Because you use the Administrator Utility to create the archive keypair, you must install Client Security Software on an initial IBM client, and then use the Administrator Utility to create the archive keypair. Instructions for installing and configuring the software on the first IBM client are provided below.

After you create the archive keypair, you can use the installation program to quickly install and configure the software on other IBM clients without the Administrator Utility. See “Installing the software on other IBM clients when the admin public key is available - unattended installations only” on page 12 for more information.

**Note:** If you intend to use a UVM policy that can be used on remote clients, you must use the same archive keypair when you install the software on those clients.

# Chapter 4. Installing, updating, and uninstalling the software

This section contains instructions for installing and configuring Client Security Software on IBM clients. All files required for the installation are provided within the csec3_0.exe file that you download from the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site. This section also contains instructions for uninstalling the software.

**Important:** You must decrypt all files that were encrypted using prior versions of Client Security Software *before* installing Client Security Software 3.0. Client Security Software 3.0 cannot decrypt files that were encrypted using prior versions of Client Security Software because of changes in its file encryption implementation.

## Installing the software on the first IBM client

Before starting the installation procedure, close all open programs, and restart the computer (if you have not done so already); then complete the following procedures to install Client Security Software on the first IBM client.

## Using the IBM Client Security Software - InstallShield Wizard

The IBM Client Security Software - InstallShield Wizard provides an interface that helps you install Client Security Software and enable the IBM embedded Security Chip.

**Note:** Before performing this task on a ThinkPad computer, you must disable the supervisor password.

To use the IBM Client Security Software - InstallShield Wizard, complete the following procedure:

1. From the Windows desktop, click **Start > Run**.
2. In the Run field, type `d:\directory\csec3_0.exe`, where d:\directory\ is the drive letter and directory where the file is located.
3. Click **Setup** to continue.

   The IBM Client Security Software - InstallShield Wizard opens.
4. Click **Next**.

   The License Agreement window opens.
5. Click **Yes** to accept the License Agreement.

   You must agree to the terms of the License Agreement to install Client Security Software. If you click **No**, the installation program will close without installing Client Security Software.

   After you click **Yes**, the Choose Destination Location window opens.

   If your system does not have the appropriate SMBus device driver, a message is displayed indicating that the SMBus device driver will be installed at this time. On some systems, this will require the system to restart before completing the installation.
6. Click **Next** to accept the default directory, c:\Program Files\IBM\Security, or click **Browse** to choose a different directory; then click **Next**.

   The Select Program Folder window opens.
7. Click **Next** to accept the default program folder, IBM Client Security Software, then click **Next**.
8. Click **Finish**.

Client Security Software has been successfully installed and the IBM embedded Security Chip has been enabled. Your computer will restart.

**Note:** If Enhanced Security is enabled, the Install Wizard prompts you to restart the computer to enable the IBM embedded Security Chip through the F11 setup utility.

## Installing the software on other IBM clients when the admin public key is available - unattended installations only

If you have installed the software on the first IBM client and created an admin key pair, you can install the software and enable the security subsystem on other IBM clients by using the installation program.

During the installation, you must choose a location for the admin public key and the key archive. If you want to use an admin public key that resides on a shared directory or save the key archive to a shared directory, you must first map a drive letter to the destination directory before you can use the installation program. For information on mapping a drive letter to a shared network resource, see your Windows operating system documentation.

**Note:** Before performing this task on a ThinkPad computer, you must disable the supervisor password.

## Performing an unattended installation

Before you begin an unattended installation, read Chapter 3, “Before installing the software” on page 7. No error messages are displayed during unattended installations. If an unattended installation ends prematurely, perform an attended installation to view any error messages that might be displayed.

An unattended installation enables an administrator to install Client Security Software on a remote IBM client without having to physically go to the client computer.

**Notes:**

1. Before performing this task on a ThinkPad computer, you must disable the supervisor password.
2. Windows NT or Windows 2000 users must log on with administrator user rights to install Client Security Software.
3. You must install the SMBus device driver to perform an unattended installation.
4. If you are installing Client Security Software on a NetVista 6059, 6569, 6579, 6649, or 6646 Q1x model and an administrator password has been set for the computer, you must edit the szAdminPassword field.

To perform an unattended installation, complete the following procedure:

1. Use a zip program to extract all files from csec30.exe into a common folder. Note that the setup.exe and setup.iss files are stored in a folder that you specify.
2. Copy the admin.key file to the hard disk of the IBM client or to a shared network directory so that it is available for the unattended installation.
3. Edit and save the setup.iss file. Parameters you might need to edit in the file are shown in bold below.

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szAdminPassword=11111111
szHWPassword=password
szKeyFile=C:\MyKeyFile
szArchivePath=C:\MyArchive
[File Transfer]
OverwrittenReadOnly=NoToAll
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-DlgOrder]
Dlg0={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdWelcome-0
Count=6
Dlg1={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdLicense-0
Dlg2={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdAskDestPath-0
Dlg3={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdSelectFolder-0
Dlg4={355B3C24-68B7-11D4-B3EC-000629B04E58}-MessageBox-0
Dlg5={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdFinishReboot-0
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdWelcome-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdLicense-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdSelectFolder-0]
szFolder=IBM Client Security Software
Result=1
[Application]
Name=IBM Client Security Software
Version=2.01.001a
Company=IBM
Lang=0009
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-MessageBox-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdFinishReboot-0]
Result=1
BootOption=3
```

These parameters of the setup.iss file designate the following functions:

- **szDir=C:\Program Files\IBM\Security** designates the directory where Client Security Software will be installed.
- **szFolder=IBM Client Security Software** designates the folder where Client Security Software will be installed.
- **szHWPassword=password** assigns the hardware password for the IBM embedded Security Chip as ″password.″ You can assign any hardware password you want, as long as it adheres to the rules for the hardware password. For information on the rules for the hardware password, see Appendix B, “Password and passphrase rules” on page 37.
- **szKeyFile=C:\MyKeyFile** designates the path to the admin.key file. For the unattended installation to run properly, admin.key must be in the specified path on the client hard disk or on a shared network directory. If the admin.key file you use is stored on a diskette, copy it to the client hard disk or to a shared network directory so that it is available for the unattended installation.

- **szArchivePath=C:\MyArchive** designates the path where the keys are archived. For the unattended installation to run properly, do not store the key archive on a diskette. If you want to store the key archive on a diskette, store the key archive on the client hard disk or a shared network directory during the unattended installation, and then copy it to a diskette after the installation is complete.
- **(some systems only) szAdminPassword=11111111** designates the administrator password that has been set for the computer. If you are installing Client Security Software on one of the following computers:
  - NetVista 6059, 6569, 6579, 6649
  - NetVista 6646 all Q1x models

  and an administrator password has been set for the computer, you must type the administrator password beside `szAdminPassword =`. If the computer on which you are installing the software is not listed above, you do not have to edit the szAdminPassword entry.

  **Note:** If you provide an incorrect administrator password, the software will install, but the embedded Security Chip will not be enabled and hardware keys will not be generated. See "Startup feature considerations" on page 7 for more information.

4. From the Windows desktop, click **Start > Run**.
5. Type the path to setup.exe, and add [space]-s to the path (for example, `C:\Security\setup.exe -s`).

   All files will be installed in the directory specified for szDir, and the computer will restart.

## Upgrading your version of Client Security Software

Clients that have previous versions of Client Security Software installed might need to be updated to take advantage of new Client Security Software features.

**Note:** Before performing this task on a ThinkPad computer, you must disable the supervisor password.

To update your system from a previous version of Client Security Software, complete the following procedure:

1. Uninstall the previous software.
2. Install the new software.

   **Note:** To use the same hardware password that was set for the IBM embedded Security Chip, do not clear the IBM embedded Security Chip.
3. Create new user encryption keys.
4. Set up user authentication.
5. Obtain new digital certificates for e-mail use.

For more information, see the *Client Security Software Administrator's Guide*.

## Uninstalling Client Security Software

Windows NT or Windows 2000 users must log on with administrator rights to uninstall Client Security Software.

**Note:** You must uninstall all UVM-aware sensor software before you uninstall IBM Client Security Software.

To uninstall Client Security Software, complete the following procedure:

1. Close all Windows programs.
2. From the Windows desktop, click **Start > Settings > Control Panel**.
3. Click the **Add/Remove Programs** icon.
4. In the list of software that can be automatically removed, select **IBM Client Security**.
5. Click **Add/Remove**.
6. Click **Yes** to uninstall the software.
7. Do one of the following:
   - If you installed the IBM embedded Security Chip PKCS#11 module for Netscape, a message is displayed that asks you to start the process to disable the IBM embedded Security Chip PKCS#11 module. Click **Yes** to proceed.

     A series of messages will be displayed. Click **OK** for each message until the IBM embedded Security Chip PKCS#11 module is removed.

     Removing the PKCS#11 module does not remove or delete the digital certificates in the system. It eliminates communication between Netscape and the IBM embedded Security Chip.
   - If you did not install the IBM embedded Security Chip PKCS#11 module for Netscape, a message is displayed that asks if you want to delete shared DLL files that were installed with Client Security Software.

     Click **Yes** to uninstall these files, or click **No** to leave the files installed. Leaving these files installed has no affect on the normal operation of your computer.
8. Click **OK** after the software is removed.

   You must restart the computer after uninstalling Client Security Software.

When you uninstall Client Security Software, you remove only the installed software components. Any encryption keys that you created remain stored on the IBM embedded Security Chip. The key archive is not affected when Client Security Software is uninstalled; however, all digital certificates obtained through the IBM embedded Security Chip are deleted.

# Chapter 5. 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, disable, or clear the IBM embedded Security Chip
- Generating or restoring encryption or user keys
- Adding users to UVM

**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 **Replace the standard Windows logon with UVM's secure logon** 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)

Supervisor passwords prevent unauthorized persons from changing the configuration settings of an IBM ThinkPad computer. These passwords are set using the IBM BIOS Setup Utility program, which is accessed by pressing F1 during the system startup sequence.

Due to the nature of Client Security Software, the supervisor password must be disabled temporarily to perform the following functions:

- Installing or upgrading Client Security Software
- Enabling, disabling, or clearing the IBM embedded Security Chip
- Generating or restoring encryption or user keys
- Adding users to UVM

Client Security Software might generate the following message when the supervisor password needs to be disabled:

**ThinkPad computers:** `If you have a supervisor password enabled, you must disable it in the BIOS Setup before continuing. If you have a supervisor password enabled, click Cancel. Otherwise, click OK to continue. After this operation has been completed, re-enable the supervisor password to maintain your system security.`

**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 **Replace the standard Windows logon with UVM's secure logon** 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.

## Clearing 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 **Replace the standard Windows logon with UVM's secure logon** 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)

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.

**Note:** Before performing this task on a ThinkPad computer, you must disable the supervisor password.

**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 **Replace the standard Windows logon with UVM's secure logon** 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 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:<br>1. Uninstall the software.<br>2. Reinstall the software.<br>**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 csec3_0.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 csec3_0.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:<br>1. Attach the fingerprint sensor.<br>2. Wait for the red light to illuminate on the sensor.<br>3. Click **OK**.<br>4. Select **Yes, I want to restart my computer now** and click **Finish**.<br>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 |
| --- | --- |
| **The Next button is unavailable after entering and confirming your UVM passphrase in the Administrator Utility** | **Action** |
| On systems running Windows NT, Windows 2000, or Windows XP, when you add users to UVM, the **Next** button might not be available after you enter and confirm your UVM passphrase in the Administrator Utility. | Click the **Information** item on the Windows Task Bar and continue the procedure. |
| **An error message displays when you attempt to edit local UVM policy** | **Action** |
| When you edit the local UVM policy, an error message might display if no users are enrolled in UVM. | Add a user to UVM before attempting to edit the policy file. |
| **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:<br>• If the UVM passphrase for the user is not needed, no action is required.<br>• 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:<br><br>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** |

| Problem Symptom | Possible Solution |
| --- | --- |
| 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:<br>1. Exit from the disable chip confirmation window.<br>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:<br>• Change their UVM passphrases<br>• Update the Windows password registered with UVM<br>• 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:<br>• Client Security Software is installed on an NTFS formatted partition<br>• The Windows folder is on an NTFS formatted partition<br>• 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** |

| Problem Symptom | Possible Solution |
|---|---|
| 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.<br><br>To disable the supervisor password, do the following:<br>1. Press F1 to access the IBM BIOS Setup Utility.<br>2. Enter the current supervisor password.<br>3. Enter a blank new supervisor password, and confirm a blank password.<br>4. Press Enter.<br>5. Press F10 to save and exit. |
| **Different UVM-aware fingerprint sensor does not work properly** | **Action** |
| The IBM ThinkPad computer does not support the interchanging of multiple UVM-aware fingerprint sensors. | Do not switch fingerprint sensor models. Use the same model when working remotely as when working from a docking station. |

## 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.<br><br>**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:<br>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.<br>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** |

| Problem Symptom | Possible Solution |
| --- | --- |
| 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.<br><br>See Microsoft for current information on the encryption algorithms used with Outlook Express. |
| **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:<br>• obtain new certificates<br>• register the certificate authority again in Outlook Express |
| **Outlook Express does not update the encryption strength associated with a certificate** | **Action** |

| Problem Symptom | Possible Solution |
| --- | --- |
| 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.<br><br>**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 256-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:<br>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.<br>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** |
| 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 | Go to the Administrator Utility or Client Utility to update the key archive. When you update the key archive, copies of all the certificates |

## 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. |

## Policy Director troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Policy Director with Client Security Software.

| Problem Symptom | Possible Solution |
|---|---|
| **Local policy settings do not correspond to those on the server** | **Action** |
| Policy Director allows certain bit configurations that are not supported by UVM. Consequently, local policy requirements can override settings made by an administrator when configuring the PD server. | This is a known limitation. |
| **Policy Director setup settings are not accessible** | **Action** |
| Policy Director setup and local cache setup settings are not accessible on the Policy Setup page in the Administrator Utility. | Install the Policy Director runtime Environment. If the Runtime Environment is not installed on the IBM client, the Policy Director settings on the Policy Setup page will not be available. |
| **A user's control is valid for both the user and the group** | **Action** |
| When configuring the Policy Director server, if you define a user to a group, the user's control is valid for both the user and the group if **Traverse bit** is on. | No action is required. |

## 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 |
|---|---|
| **After enabling UVM protection for Lotus Notes, Notes in not able to finish its setup** | **Action** |
| Lotus Notes is not able to finish setup after UVM protection is enabled using the Administrator Utility. | This is a known limitation.<br><br>Lotus Notes must be configured and running before Lotus Notes support is enabled in the Administrator Utility. |
| **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:<br>• Use the Lotus Notes Configuration tool to set UVM protection for a Notes ID<br>• Open Notes and use the function provided by Notes to change the password for Notes ID file<br>• Close Notes immediately after you change the password | Click **OK** to close the error message. No other action is required.<br><br>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. |

## Encryption troubleshooting information

The following troubleshooting information might be helpful if you experience problems when encrypting files using Client Security Software 3.0 or later.

| Problem Symptom | Possible Solution |
|---|---|
| **Previously encrypted files will not decrypt** | **Action** |
| Files encrypted with previous versions of Client Security Software do not decrypt after upgrading to Client Security Software 3.0. | This is a known limitation.<br><br>You must decrypt all files that were encrypted using prior versions of Client Security Software *before* installing Client Security Software 3.0. Client Security Software 3.0 cannot decrypt files that were encrypted using prior versions of Client Security Software because of changes in its file encryption implementation. |

## 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. U.S. export regulations for Client Security Software

The IBM Client Security Software package has been reviewed by the IBM Export Regulation Office (ERO), and as required by U.S. government export regulations, IBM has submitted appropriate documentation and obtained retail classification approval for up to 256 bit encryption support from the U.S. Department of Commerce for international distribution except in those countries embargoed by the U.S. Government. Regulations in the U.S.A. and other countries are subject to change by the respective country government.

If you are not able to download the Client Security Software package, please contact your local IBM sales office to check with your IBM Country Export Regulation Coordinator (ERC).

# Appendix B. 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 C. 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 U.S.A.