IBM® Client Security
Solutions

Client Security Software Version 5.2 Installation Guide

IBM® Client Security
Solutions

Client Security Software Version 5.2 Installation Guide

First Edition (October 2003)

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 45 and Appendix C, “**Notices and Trademarks**,” on page 51.

Contents

Appendix C. Notices and Trademarks 51

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, “Introduction,”″ contains a brief outline of basic security concepts, an overview of the applications and components that are included in the software, and a description of Public Key Infrastructure (PKI) features.

″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 information,”″ contains password criteria that can be applied to a UVM passphrase and rules for Security Chip passwords.

″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 Tivoli Access Manager*, 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 User Configuration 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 User Configuration 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. Introduction

Select ThinkPad™ and ThinkCentre™ computers are equipped with built-in cryptographic hardware that work together with downloadable software technologies to provide a powerful level of security in a client PC platform. Collectively this hardware and software is called the IBM Embedded Security Subsystem (ESS). The hardware component is the IBM Embedded Security Chip and the software component is the IBM Client Security Software (CSS).

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

The IBM Embedded Security Subsystem

The IBM ESS supports key-management solutions, such as a Public Key Infrastructure (PKI), and is comprised of the following local applications:

- File and Folder Encryption (FFE)
- Password Manager
- Secure Windows logon
- Multiple, configurable authentication methods, including:
  - Passphrase
  - Fingerprint
  - Smart Card
  - Proximity Card

In order to effectively use the features of the IBM ESS a security administrator must be familiar with some basic concepts. The following sections describe basic security concepts.

The IBM Embedded Security Chip

The IBM Embedded Security Chip is the built-in cryptographic hardware technology that provides an extra level of security to select IBM PC platforms. With the advent of this chip, encryption and authentication processes are transferred from more vulnerable software and moved to the secure environment of dedicated hardware. The increased security this provides is tangible.

The embedded Security Chip supports:

- RSA3 PKI operations, such as encryption for privacy and digital signatures for authentication
- RSA key generation
- Pseudo random number generation
- RSA-function computation in 200 milliseconds
- EEPROM memory for RSA key pair storage
- All TCPA functions defined in specification Vs. 1.1
- Communication with the main processor through the Low Pin Count (LPC) bus

IBM Client Security Software

IBM Client Security Software comprises the following software applications and components:

- **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.
- **Administrator Console:** The Client Security Software Administrator Console enables a security administrator to remotely perform administrator-specific tasks.
- **User Configuration Utility:** The User Configuration Utility enables a client user to change the UVM passphrase, to enable Windows logon passwords to be recognized by UVM, to update key archives, and to register fingerprints. A user can also create backup copies of digital certificates created with the IBM embedded Security Chip.
- **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 a security administrator to set the client security policy, which dictates how a client user is authenticated on the system.

    If policy indicates that fingerprint is required for logon, and the user has no fingerprints registered, he will be given the option to register fingerprints as part of the logon. Also, if fingerprint verification is required and there is no scanner attached, UVM will report an error. Also, if the Windows password is not registered, or incorrectly registered, with UVM, the user will have the opportunity to provide the correct Windows password as part of the logon.
  - **UVM system logon protection:** UVM software enables a security 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.

The relationship between passwords and keys

Passwords and keys work together, along with other optional authentication devices, to verify the identity of system users. Understanding the relationship between passwords and keys is vital to understand how IBM Client Security Software works.

The administrator password

The administrator password is used to authenticate an administrator to the IBM Embedded Security Chip. This password, which must be eight characters long, is maintained and authenticated in the secure hardware confines of the embedded security chip. Once authenticated, the administrator can perform the following actions:

- Enroll users
- Launch the policy interface
- Change the administrator password

The administrator password can be set in the following ways:

- Through the Client Security Software wizard
- Through the Administrator Utility
- Using scripts
- Through the BIOS interface (ThinkCentre computers only)

It is important to have a strategy for creating and maintaining the administrator password. The administrator password can be changed if it is compromised or forgotten-- but not without impact to the administrator.

For those familiar with Trusted Computing Group (TCG) concepts and terminology, the administrator password is the same as the owner authorization value. Since the administrator password is associated with the IBM Embedded Security Chip it is sometimes also referred to as the *hardware password*.

The hardware public and private keys

The basic premise of the IBM Embedded Security Chip is that it provides a strong *root* of trust on a client system. This root is used to secure other applications and functions. Part of establishing a root of trust is to create a hardware public key and a hardware private key. Public and private keys, also referred to as key pairs, are mathematically related in such a way that:

- Any data encrypted with the public key can only be decrypted with corresponding private key.
- Any data encrypted with the private key can only be decrypted with corresponding public key.

The hardware private key is created, stored and used in the secure confines of the security chip. The hardware public key is also created in the security chip but it is made available for various purposes, hence the name public key. The hardware public and private keys are a critical part of the IBM key-swapping hierarchy described in a following section.

Hardware public and private keys can be created in the following ways:

- Through the Client Security Software wizard
- Through the Administrator Utility
- Using scripts

For those familiar with Trusted Computing Group (TCG) concepts and terminology, the hardware public and private keys are known as the *storage root key* (SRK).

The administrator public and private keys

The IBM ESS administrator public and private keys are an integral part of the IBM ESS key-swapping hierarchy. They also allow for user-specific data to be backed up and restored in the event of system board or hard drive failure.

Administrator public and private keys can either be unique for all systems or they can be common across all systems or groups of systems. It is important to note that these administrator keys must be managed so having a strategy for using unique versus known keys is important.

Administrator Public and Private Keys can be created in one of the following ways:

- Through the Client Security Software wizard
- Through the Administrator Utility
- Using scripts

ESS archive

The IBM administrator public and private keys allow user-specific data to be backed up and restored in the event of a system board or hard drive failure.

User public and private keys

The IBM Embedded Security Subsystem creates user public and private keys to protect user-specific data. These key pairs are created when a user is enrolled into IBM Client Security Software. These keys are created and managed transparently by the User Verification Manager (UVM) component of IBM CSS. The keys are managed based upon which Windows user is logged into the operating system.

A key-swapping hierarchy

An essential element of the IBM Embedded Security Subsystem architecture is its key-swapping hierarchy. The base (or root) of the IBM key swapping hierarchy are the hardware public and private keys. The hardware public and private keys, called the hardware *key pair*, are created by IBM Client Security Software and are statistically unique on each client.

The next “level” up the hierarchy (above the root) is the administrator public and private key pair. The administrator key pair can be unique on each machine, or it can be the same on all clients or a subset of clients. This decision depends upon how a network will be managed. The administrator private key is unique in that it resides on the client system (protected by the hardware public key) and in an administrator-define location. Details of why this is done will be discussed below.

IBM Client Security Software enrolls Windows users into the Embedded Security Subsystem environment. When a user is enrolled, a public and private key are created and a new level is created. The user’s private key is encrypted with the administrator public key. The administrator private key is encrypted with the hardware public key. Therefore to use the user’s private key, the administrator private key (which is encrypted with the hardware public key) must be loaded into the chip. Once in the chip, the hardware private key decrypts the administrator private key. The administrator private key is now ready for use inside of the chip so that data that is encrypted with the corresponding administrator public key can be swapped into the chip, decrypted and utilized. The current Windows user’s private key (encrypted with the administrator public key) is passed into the chip. Any data needed by an application that leverages the embedded security chip would also be passed into the chip, decrypted and leveraged within the secure environment of the chip. An example of this is a private key used to authenticate to a wireless network.

Whenever a key is needed, it is swapped into the IBM Embedded Security Chip. The encrypted private keys are swapped into the chip, and can then be used in the protected environment of the chip. The private keys are never exposed or used outside of this hardware environment. This provides for nearly an unlimited quantity of data to be protected through the IBM Embedded Security Chip.

The private keys are encrypted because they must be heavily protected and because there is limited storage space available in the IBM Embedded Security

Chip. Only a couple of keys can be stored in the chip at any given time. The hardware public and private keys are the only keys that remain stored in the chip from boot to boot. In order to allow for multiple keys and multiple users, the IBM ESS implements a key-swapping hierarchy. Whenever a key is needed, it is swapped into the IBM Embedded Security Chip. The related, encrypted private keys are swapped into the chip, and can then be used in the protected environment of the chip. The private keys are never exposed or used outside of this hardware environment.

The administrator private key is encrypted with the hardware public key. The hardware private key, which is only available in the chip, is used to decrypt the administrator private key. Once the administrator private key is decrypted in the chip, a user's private key (encrypted with the administrator public key) can be passed into the chip and decrypted with the administrator private key. Multiple users' private keys can be encrypted with the administrator public key. This allows for virtually an unlimited number of users on a system with the IBM ESS.

The IBM ESS utilizes a key-swapping hierarchy where the hardware public and private keys in the chip are used to secure other data stored outside the chip. The hardware private key is generated in the chip and never leaves this secure environment. The hardware public key is available outside of the chip and is used to encrypt or secure other pieces of data such as a private key. Once this data is encrypted with the hardware public key it can only be decrypted by the hardware private key. Since the hardware private key is only available in the secure environment of the chip, the encrypted data can only be decrypted and used in this same secure environment. It is important to note that each computer will have a unique hardware public and private key. Random number capability on the IBM Embedded Security Chip ensures that each hardware key pair is statistically unique.

CSS 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.

- **The ability to transfer digital certificates to the IBM embedded Security Chip.** The IBM Client Security Software Certificate Transfer Tool enables you to move certificates that have been created with the default Microsoft CSP to the IBM embedded Security System CSP. This greatly increases the protection afforded to the private keys associated with the certificates because they will now be securely stored on the IBM embedded Security Chip, instead of on vulnerable software.
- **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.
- **File and folder encryption.** File and folder encryption enables a client user to encrypt or decrypt files or folders. This provides an increased level of data security on top of the CSS system-security measures.
- **Fingerprint authentication.** IBM Client Security Software supports the Targus PC card fingerprint reader and the Targus USB fingerprint reader for authentication. Client Security Software must be installed before the Targus fingerprint device drivers are installed for correct operation.
- **Smart card authentication.** IBM Client Security Software supports certain smart cards as an authentication device. Client Security Software enables smart cards to be used as a token of authentication for a single user at a time. Each smart card is bound to a system unless credential roaming is being used. Requiring a smart card makes your system more secure because this card must be provided along with a password, which can be compromised.
- **Credential roaming.** Credential roaming enables a UVM-authorized network user to use any computer on the network as though it was his own workstation. After a user is authorized to use UVM on any CSS-registered client, he can then import his personal data to any other registered client in the network. His personal data is then updated automatically and maintained in the CSS archive and on any computer to which it was imported. Updates to this personal data, such as new certificates or passphrase changes, are immediately available on all other computers connected to the roaming network.
- **FIPS 140-1 certification.** Client Security Software supports FIPS 140-1 certified cryptographic libraries. FIPS-certified RSA BSAFE libraries are used on TCPA systems.
- **Passphrase expiration.** Client Security Software establishes a user-specific passphrase and a passphrase expiration policy when each user is added to UVM.

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 2000 Professional

UVM-aware products

IBM Client Security comes with User Verification Manager (UVM) software that 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 Access Manager versions 3.8 or 3.9**

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

  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 Desktop Solutions 5.1, 6.0, or 6.1**

  Entrust Desktop Solutions 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.
- **Targus fingerprint reader**

  The Targus fingerprint reader provides a simple easy interface that enables the security policy to include fingerprint authentication.
- **Gemplus GemPC400 smart card reader**

  The Gemplus GemPC400 smart card reader enables the security policy to include smart card authentication, adding an additional layer of security to the standard passphrase protection.

Web browsers

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

- Internet Explorer 5.0 or later
- Netscape 4.51 to Netscape 7

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 csec51.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 45.

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 csec51.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 and Windows 2000

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

Installing for use with Tivoli Access Manager

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

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.

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

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 downloading, installing and configuring Client Security Software on IBM clients. This section also contains instructions for uninstalling the software. Be sure that you install IBM Client Security Software prior to installing any of the various utilities that enhance Client Security functionality.

Important: If you are upgrading from a version prior to Client Security Software 5.0, you must decrypt all encrypted files before installing Client Security Software 5.1. Client Security Software 5.1 cannot decrypt files that were encrypted using versions prior to Client Security Software 5.0 because of changes in its file encryption implementation.

Downloading and installing the software

All files required for the installation of Client Security Software are provided within the csec51.exe file that you download from the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site. The Web site provides information that helps you ensure that your system has the IBM embedded Security Chip, and that enables you to select the appropriate Client Security offering for your system.

To download the appropriate files for your system, complete the following procedure:

1. Using a Web browser, go to the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site
2. Using the information on the Web site, ensure that the IBM integrated security chip is on your system by matching your model number to one provided in the system requirements table; then click **Continue**.
3. Select the radio button that matches your Machine Type and click **Continue**.
4. Create a user ID, register with IBM by filling out the online form, and review the License Agreement; then click **Accept Licence**.

   You will automatically be redirected to the Client Security download page.
5. Follow the steps on the download page to download the necessary device drivers, the readme files, software, reference documents, and additional utilities that constitute IBM Client Security Software. Follow the download sequence specified on the Web site.
6. From the Windows desktop, click **Start > Run**.
7. In the Run field, type `d:\directory\csec51.exe`, where d:\directory\ is the drive letter and directory where the file is located.
8. Click **OK**.

   The Welcome to the InstallShield Wizard for IBM Client Security Software window opens.
9. Click **Next**.

   The wizard will extract the files and install the software. When the installation is complete, you will be given the option to restart your computer now or to wait until later.
10. Select to restart your computer now and click **OK**.

The IBM Client Security Software Setup Wizard will open when your computer restarts.

Using the IBM Client Security Software Setup Wizard

The IBM Client Security Software Setup Wizard provides an interface that helps you install Client Security Software and enable the IBM embedded Security Chip. The IBM Client Security Software Setup Wizard also guides users through the necessary tasks involved in setting up a security policy on an IBM client.

These steps are as follows:

- **Setting a Security Administrator Password**

  The Security Administrator Password is used to control access to the IBM Client Security Administrator Utility, which is used to change the security settings for this computer.
- **Creating Administrator Security Keys**

  Administrator Security Keys are a set of digital keys that are stored in a computer file. It is recommended that you save these security keys on a removable disk or drive. When a change to the security policy is made in the Security Administrator Utility, you will be prompted for this file to prove that the policy change is authorized.

  Backup Security Information is also saved in case you ever need to replace the system board or hard drive of your computer. This backup information should be stored somewhere off the system.
- **Protecting Applications with IBM Client Security**

  Select the applications that you want to protect with IBM Client Security. Some options might not be available if you do not have other necessary applications installed.
- **Authorizing Users**

  Users need to be authorized before they can access the computer. When you authorize a user, you must specify that user’s passphrase. Unauthorized users are not permitted to use the computer.
- **Selecting a System Security Level**

  Selecting a system security level enables you to establish a basic security policy quickly and easily. You can define a custom security policy in the IBM Client Security Administrator Utility later.

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

1. If the Wizard is not already open, click **Start > Programs > Access IBM > IBM Client Security Software > IBM Client Security Setup Wizard**.

   The Welcome to the IBM client Security Setup Wizard screen displays an overview of the wizard steps.

   Note: If you intend to use fingerprint authentication, you must install the fingerprint reader and software before continuing.
2. Click **Next** to begin using the wizard.

   The Set Security Administrator Password screen is displayed.
3. Type your Security Administrator Password in the Enter Administrator Password field and click **Next**.

Note: Upon initial installation or after the IBM embedded Security Chip has been cleared, you will be required to confirm your Security Administrator Password in the Confirm Administrator Password field. You might also be required to provide your supervisor password, if applicable.

The Create Administrator Security Keys screen is displayed.

4. Do one of the following:
   - **Create new security keys**

     To create new security keys, use the following procedure:

     a. Click the **Create new security keys** radio button.

     b. Specify where you want to save the administrator security keys by either typing the path name in the provided field or by clicking **Browse** and selecting the appropriate folder.

     c. If you want to split the security key for increased protection, click the **Split the backup security key for increased security** check box so that a check mark appears in the box, and then use the arrows to select the desired number in the **Number of splits** scroll box.
   - **Use an existing security key**

     To use an existing security key, use the following procedure:

     a. Click the **Use an existing security key** radio button.

     b. Specify the location of the Public Key by either typing the path name in the provided field or by clicking **Browse** and selecting the appropriate folder.

     c. Specify the location of the Private Key by either typing the path name in the provided field or by clicking **Browse** and selecting the appropriate folder.
5. Specify where you want to save the backup copies of your security information by either typing the path name in the provided field or by clicking **Browse** and selecting the appropriate folder.
6. Click **Next**.

   The Protect Applications with IBM Client Security screen is displayed.
7. Enable IBM Client Security protection by selecting the appropriate check boxes so that a check mark appears in each selected box, and clicking **Next**. The available Client Security selections are as follows:
   - **Secure access to your by replacing the normal Windows logon with the Client Security secure logon**

     Select this box to replace the normal Windows logon with the Client Security secure logon. This increases the security of your system, and allows logon only after authentication with the IBM Embedded Security Chip and optional devices, like fingerprint readers.
   - **Enable file and folder encryption**

     Select this box if you want to secure files on your hard drive with the IBM Embedded Security Chip. (Requires you to download the IBM Client Security File and Folder Encryption utility).
   - **Enable IBM Client Security Password Manager support**

     Select this box if you want to use the IBM Password Manager to conveniently and securely store passwords for your Web site logons and applications. (Requires you to download the IBM Client Security Password Manager application).

- **Replace Lotus Notes logon with IBM Client Security logon**

  Select this box if you want Client Security to authenticate Lotus Notes users through the IBM embedded Security Chip.
- **Enable Entrust support**

  Select this box if you want to enable integration with Entrust security software products.
- **Protect Microsoft Internet Explorer**

  This protection enables you to secure your e-mail communications and Web browsing with Microsoft Internet Explorer (requires a digital certificate). Support for Microsoft Internet Explorer is enabled by default.

After you have selected the appropriate check boxes, the Authorizing Users screen is displayed.

8. Complete the Authorizing Users screen by completing one of the following procedures:
   - To authorize users to perform IBM Client Security functions, do the following:
     a. Select a user in the Unauthorized Users area.
     b. Click **Authorize User**.
     c. Type and confirm your IBM Client Security passphrase in the provided fields and click **Finish**.
     d. Click **Next**.
   - To unauthorize users from performing IBM Client Security functions, do the following:
     a. Select a user in the Authorized Users area.
     b. Click **Unauthorize User**.
     c. Type and confirm your IBM Client Security passphrase in the provided fields and click **Finish**.
     d. Click **Next**.

   The Select System Security Level screen is displayed.
9. Select a system security level using the following procedure:
   a. Select the authentication requirements that you will use by clicking the appropriate check boxes. You can select more than one authentication requirement.
   b. Select a system security level by dragging the slide selector to the desired security level and click **Next**.

   Note: You can define a custom security policy later using the IBM Client Security Policy Editor.
10. Review your security settings and take one of the following actions:
    - To accept the settings, click **Finish**.
    - To change the settings, click **Back**, make the appropriate changes; then return to this screen and click **Finish**.

    IBM Client Security Software configures your settings through the IBM embedded Security Chip. A message is displayed confirming that your computer is now protected by IBM Client Security.
11. Click **OK**.

You can now install and configure the IBM Client Security Password Manager and the IBM Client Security File and Folder Encryption utilities.

Enabling the IBM Security Chip

The IBM Security Chip must be enabled before you can use Client Security Software. If the chip has not been enabled, you can enable it by using the Administrator Utility. Instructions for using the Setup Wizard are contained in the previous section.

To enable the IBM Security Chip using the Administrator Utility, complete the following procedure:

1. Click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   A screen displays a message that states that the IBM Security Chip has not been enabled, and that asks if you would like to enable the chip.
2. Click **Yes**.

   A message is displayed stating that if you have a supervisor password enabled, you must disable it in the BIOS Setup before continuing.
3. Do one of the following:
   - If you have a supervisor password enabled, click **Cancel**, disable your supervisor password, and then complete this procedure.
   - If you do not have a supervisor password enabled, click **OK** to continue.
4. Close all open applications and click **OK** to restart the computer.
5. After the system restarts, click **Start > Settings > Control Panel > IBM Client Security Subsystem** to open the Administrator Utility.

   A message is displayed stating that the IBM Security Chip has not been configured or has been cleared. A new password is required at this time.
6. Enter and confirm a new IBM Security Chip password in the appropriate fields and click **OK**.

   Note: The password must be eight characters in length.

   The operation is complete and the Administrator Utility main screen is displayed.

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

If you have installed the software on the first IBM client and created an administrator 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 administrator public key, the administrator private key, and the key archive. If you want to use an administrator 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.

Performing an unattended installation

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.

Before you begin an unattended installation, read Chapter 3, “Before installing the software,” on page 11. No error messages are displayed during unattended installations. If an unattended installation ends prematurely, you must perform an attended installation to view any error messages that might be displayed.

Note: Users must log on with administrator user rights to install Client Security Software.

For complete information on how to perform an unattended installation, complete the following procedure, see the css51readme file available on the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site

Mass deployment

Mass deployment enables security administrators to initiate security policy on multiple computers simultaneously. This makes it easier to manage and deploy security measures and helps ensure that the correct security policies are implemented.

The following device drivers must be installed before completing the mass deployment procedure:

- The SM bus device driver
- The LPC bus device driver (for TCPA systems)

There are two major steps to a mass deployment:

- Mass installation
- Mass configuration

Mass installation

You must perform an unattended installation to install IBM Client Security Software on a multitude of clients simultaneously. You must use the unattended installation parameter when initiating a mass deployment.

To initiate a mass installation, complete the following procedure:

1. Create the CSS.ini file.

   This step is only required if you intend to perform a mass configuration.
2. Extract the contents of the CSS installation package with Winzip using folder names.
3. Edit the `szIniPath` and `szDir` entries, which are required for a mass configuration, in the setup.iss file.

   The full contents of this file is listed below. The `szIniPath` parameter is only required if you intend to perform a mass configuration.
4. Copy the files to the target system.
5. Create the `\setup -s` command-line statement.

This command-line statement should be run from the desktop of a user who has administrator rights. The StartUp program group or the Run key is a good place to do this.

6. Remove the command-line statement on the next boot.

The full contents of the setup.iss file is listed below with a few descriptions:

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szIniPath=d:\csssetup.ini
```

(The above parameter is the name and location of the .ini file, which is required for mass configuration. If this is a network drive, it must be mapped. When a mass configuration is not being used with a silent installation, remove this entry.)

```
[File Transfer]
OverwrittenReadOnly=NoToAll
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-DlgOrder]
Dlg0={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0
Count=4
Dlg1={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0
Dlg2={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0
Dlg3={7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdLicense-0]
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
```

(The above parameter is the directory used to install Client Security. It must be local to the computer.)

```
Result=1
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdSelectFolder-0]
szFolder=IBM Client Security Software
```

(The above parameter is the program group for Client Security.)

```
Result=1
[Application]
Name=Client Security
Version=5.00.002f
Company=IBM
Lang=0009
[{7BD2CFF6-B037-47D6-A76B-D941EE13AD96}-SdFinishReboot-0]
Result=6
BootOption=3
```

Mass configuration

The following file is also essential when initiating a mass configuration. The file can be named anything, as long as it has a .ini extension. Below is how the file should look. To the side is a brief description not to be included in the file. The following command runs this file from the command line when the mass configuration is not done along with a mass installation:

```
<CSS installation folder>\acamucli /ccf:c:\csec.ini
```

Note: If any files or paths are on a network drive, the drive must be mapped to a letter.

[CSSSetup]	Section header for CSS setup.

suppw=bootup	Administrator/Supervisor password. Leave blank if not required.
hwpw=11111111	CSS hardware password. Must be eight characters. Always required. Must be correct if hardware password has already been set.
newkp=1	1 to generate a new administrator key pair 0 to use an existing administrator key pair.
keysplit=1	When newkp is 1, this determines the number of private key components. **Note:** If the existing keypair uses multiple private key parts, all private key parts must be stored in the same directory.
kpl=c:\jgk	Location of the administrator key pair when newkp is 1, if this is a network drive it must be mapped.
kal=c:\jgk\archive	Location of the user key archive, if this is a network drive it must be mapped.
pub=c:\jk\admin.key	Location of the administrator public key when using an existing administrator key pair, if this is a network drive it must be mapped.
pri=c:\jk\private1.key	Location of the administrator private key when using an existing administrator key pair, if this is a network drive it must be mapped.
wiz=0	Determines if this file was generated by the CSS setup wizard. This entry is not necessary. If you include it in the file the value should be 0.
clean=0	1 to delete the .ini file after initialization, 0 to leave the .ini file after initialization.
enableroaming=1	1 to enable roaming for the client, 0 to disable roaming for the client.
username= [promptcurrent]	[promptcurrent] to prompt the current user for the system registration password. [current] when the system registration password for the current user is provided by the sysregpwd entry and the current user has been authorized to register the system with the roaming server. [<specific user account>] if the designated user has been authorized to register the system with the roaming server and if the system registration password for that user is provided by the sysregpwd entry. Do not use this entry if the enableroaming value is 0, or if the enableroaming entry is not present.
sysregpwd=12345678	System registration password. Set this value to the correct password to enable the system to be registered with the roaming server. Do not include this entry if the username value is set to [promptcurrent], or if the username entry is not present.
[UVMEnrollment]	Section header for user enrollment.
enrollall=0	1 to enroll all local user accounts in UVM, 0 to enroll specific user accounts in UVM.
defaultuvmpw=top	When enrollall is 1, this will be the UVM passphrase for all users.
defaultwinpw=down	When enrollall is 1, this will be the Windows password registered with UVM for all users.
defaultppchange=0	When enrollall is 1, this will establish the UVM passphrase change policy for all users. 1 to require the user to change the UVM passphrase at next logon, 0 to not require the user to change the UVM passphrase at next logon.

defaultppexppolicy=1	When enrollall is 1, this will establish the UVM passphrase expiration policy for all users. 0 to indicate that the UVM passphase expires 1 to indicate that the UVM passphrase does not expire
defaultppexpdays=0	When enrollall is 1, this will establish the number of days until the UVM passphase expires for all users. When ppexppolicy is set to 0, set this value to establish the number of days until the UVM passphrase expires.
enrollusers=2	When enrollall is 0, this is the number of users that will be enrolled in UVM.
user1=jknox	Enumerate number of users to be enrolled starting with 1, user names must be the account names. In order to get the actual account name on XP, do the following 1. Start Computer Management (Device Manager). 2. Expand the Local Users and Groups node. 3. Open the Users folder. The items listed in the Name column are the account names.
user1uvmpw=chrome	Enumerate number of users to be enrolled UVM passphrase starting with 1.
user1winpw=spinning	Enumerate number of users to be enrolled Windows passphrase registered with UVM starting with 1.
user1domain=0	0 to indicate that this account is local, 1 to indicate that this account is on the domain.
user1ppchange=0	1 to require the user to change theUVM passphrase at next logon, 0 to not require the user to change the UVM passphrase at next logon.
user1ppexppolicy=1	0 to indicate that the UVM passphrase expires, 1 to indicate that the UVM passphrase does not expire.
user1ppexpdays=0	When ppexppolicy is set to 0, set this value to indicate the number of days until the UVM passphase expires.
user2=russell	
user2uvmpw=left	
user2winpw=right	
user2domain=0	
user2ppchange=1	
user2ppexppolicy=0	
user2ppexpdays=90	
[UVMAppConfig]	Section header for UVM-aware application setup and UVM-aware module setup.
uvmlogon=0	1 to use UVM logon protection, 0 to use Windows logon.
entrust=0	1 to use UVM for entrust authentication, 0 to use entrust authentication.
notes=1	1 to use UVM protection for lotus notes, 0 to use notes password protection.
netscape=0	1 to sign and encrypt e-mails with the IBM PKCS#11 module, 0 to not sign and encrypt e-mails with the IBM PKCS#11 module.
passman=0	1 to use Password Manager, 0 to not use Password Manager
folderprotect=0	1 to use File and Folder Encryption, 0 to not use File and Folder Encryption.

autoprotect=0	When folderprotect is set to 1, this will establish whether auto protection is used. 1 to use auto protection, 0 to not use auto protection.

Upgrading your version of Client Security Software

Clients that have installed versions of Client Security prior to Version 5.0 should update their software to Client Security Software Version 5.1 to take advantage of new Client Security features.

Important: TCPA systems that had IBM Client Security Software Version 4.0x installed must clear the chip before installing IBM Client Security Software Version 5.1. Failure to do so might result in an installation failure, or non-responsive software.

Upgrading using new security data

If you would like to completely remove Client Security Software and start over, complete the following procedure:

1. Uninstall your previous version of Client Security Software using the Control Panel Add/Remove Programs applet.
2. Reboot the system.
3. Clear the IBM embedded Security Chip in the BIOS utility.
4. Reboot your system.
5. Install Client Security Software Release 5.1 and configure it using the IBM Client Security Software Setup Wizard.

Upgrading to Client Security Version 5.1 using existing security data

If you would like to upgrade from a release of Client Security Software prior to Version 5.0 using your existing security data, complete the following procedure:

1. Update your archive by completing the following steps:
   a. Click **Start > Programs > Access IBM > IBM Client Security Software > Client Utility**.
   b. Click the **Update Archive** button to ensure that your backup information is updated.

      Note the archive directory.
   c. Exit the IBM Client Security Software Client Utility.
2. Remove the existing version of Client Security Software by completing the following steps:
   a. Locate the Administrator public and private keys that were created when you configured your previous version of Client Security Software.
   b. Click **Start > Settings > Control Panel > Add/Remove Programs** and select to remove IBM Client Security Software.
   c. Select **No** when prompted for reboot.
   d. Shut down the system.
3. Clear the Embedded Security Chip by completing the following steps:
   a. Power on the system.
   b. Press F1 to enter the BIOS Setup utility.

   c. Go to Security Chip settings, and clear the security chip.

   d. Exit the BIOS Setup utility.

      The system will continue its reboot.

4. Run the Client Security Software Version 5.0 installation program.
5. Reboot when prompted.

   After reboot, the Client Security Software Setup Wizard will automatically launch. Do NOT run the Setup Wizard.
6. Press **Cancel** to exit the Setup Wizard.
7. Temporarily back up the default security policy by completing the following steps:

   a. Using Windows Explorer, go to the IBM Client Security Software install directory (default is c:\program files\ibm\security).

   b. Right-click the UVM_Policy folder and select **Copy**.

   c. Right-click on the Windows desktop and click **Paste**.

      This will create a temporary backup on the Windows desktop.

      Note: Your existing security policy settings will be replaced with new defaults.
8. Restore settings from IBM Client Security Software Version 4.0x by completing the following steps:

   a. Click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

      The IBM Client Security Software Administrator Utility main screen is displayed.

   b. Click the **Key Configuration** button.

   c. Select **Yes** to restore keys from the key archive.
9. Provide the location of the previous archive directory.
10. Provide the location of the Administrator public and private key files you created in the previous release.

    You will be notified that your archive will be updated for the new release.
11. Click **OK**.
12. Provide the location to create new Administrator keys. Be sure to create the keys in a location different from the location of your existing Administrator keys. If you have Administrator keys you already created for Release 5.0 on another system, you can select **Use an existing CSS Archive keypair** and provide the location of the existing keys.
13. Click **Next**.

    Your archive will be converted and restored.
14. Exit the application when finished.
15. Restore policy settings by completing the following steps:

    a. Using Windows Explorer, go to the IBM Client Security Software install directory (default is c:\program files\ibm\security).

    b. Using the left-mouse button, drag the UVM_Policy folder from the desktop to the IBM Client Security Software install directory.

    c. Click **Yes** to all warning messages.

    Your security data has now been migrated to Client Security Software Release 5.0.

Note: If you previously changed your security policy in Client Security Software Version 4.0x, you might want to resubmit your security policy settings by completing the following steps:

1. Click **Start > Settings > Control Panel > IBM Client Security Subsystem**.
2. Click the **Configure Application Support and Policies** button.
3. Click the **Application Policy** button.
4. Click the **Edit Policy** button.

Upgrading from Release 5.1 to later versions using existing security data

If you would like to upgrade from Client Security Software Version 5.0 to later versions of the software using your existing security data, complete the following procedure:

1. Update your archive by completing the following steps:
   a. Click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings**.
   b. Click the **Update Archive** button to ensure that your backup information is updated.

      Note the archive directory.
   c. Exit the IBM Client Security Software User Configuration Utility.
2. Remove the existing version of Client Security Software by completing the following steps:
   a. Locate the Administrator public and private keys that were created when you configured your previous version of Client Security Software.
   b. Run csec51.exe.
   c. Select **Upgrade**.
   d. Reboot the system.

Uninstalling Client Security Software

Be sure that you uninstall the various utilities that enhance Client Security functionality before you uninstall IBM Client Security Software. Users must log on with administrator rights to uninstall Client Security Software.

Note: You must uninstall all IBM Client Security Software utilities and 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. Select the **Remove** radio button.
7. Click **Yes** to uninstall the software.
8. 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.
- 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.

9. 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 all installed Client Security software components along with all user keys, digital certificates, registered fingerprints and stored passwords. However, the key archive is not affected when Client Security Software is uninstalled.

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 (ThinkCentre)

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

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

Attention:

- 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, click **Configure Application Support and Policies**, 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, you will be completely locked out of the system.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

Because your 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 perform the following tasks:

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

Attention:

- Do not clear or disable the IBM embedded Security Chip when UVM logon protection is enabled. If you do, you will be completely locked out of the system.

  To disable UVM protection, open the Administrator Utility, click **Configure Application Support and Policies**, 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.
- It is necessary to temporarily disable the supervisor password on some ThinkPad models before installing or upgrading Client Security Software.

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

To set a supervisor password, complete one of the following IBM BIOS Setup Utility procedures:

Example 1

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.

Example 2

1. Shut down and restart the computer.
2. When the ″To inturrupt normal startup, press the blue Access IBM button″ message is displayed, press the blue Access IBM button.

   The Access IBM predesktop area opens.

3. Double-click **Start setup utility**.
4. Select **Security** using the directional keys to navigate down the menu.
5. Select **Password**.
6. Select **Supervisor Password**.
7. Type your password and press Enter.
8. Type your password again and press Enter.
9. Click **Continue**.
10. 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. See the hardware documentation that came with your computer for more information.

Protecting the administrator password

The administrator password protects access to the Administrator Utility. Guard the administrator password to prohibit unauthorized users from changing settings in the Administrator Utility.

Clearing the IBM embedded Security Chip (ThinkCentre)

If you want to erase all user encryption keys from the IBM embedded Security Chip and clear the administrator password for the chip, you must clear the chip. Read the information 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, you will be locked out of the system.

  To disable UVM protection, open the Administrator Utility, click **Configure Application Support and Policies**, 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, complete the following procedure:

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 **Security**.
4. Select **IBM TCPA Feature Setup**.
5. Select **Clear IBM TCPA Security Feature**.
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 administrator password for the chip, you must clear the chip. Read the information 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 disable UVM protection, open the Administrator Utility, click **Configure Application Support and Policies**, 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, complete the following procedure:

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

   Note: On some ThinkPad models, you might need to press the F1 key at power on to access the IBM BIOS Setup Utility. Refer to the help message at IBM BIOS Setup Utility for details.

   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, the user name is deleted from the list of users in the Administrator Utility.

Denying access to selected objects with Tivoli Access Manager control

The **Deny all access to selected object** check box is not disabled when Tivoli Access Manager control is selected. In the UVM-policy editor, if you select **Access Manager controls selected object** to enable Tivoli Access Manager 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 Tivoli Access Manager 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.

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 then 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, complete the following procedure:

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.

User Configuration 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 User Configuration 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 User Configuration 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 administrator 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 administrator password	**Action**
When installing the software on an IBM client with an enabled IBM embedded Security Chip, the administrator password for the IBM embedded Security Chip is unknown.	Clear the chip to continue with the installation.
The setup.exe file does not respond properly (CSS version 4.0x)	**Action**
If you extract all files from the csec4_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 csec4_0.exe file to install the Client Security Software code.

Administrator Utility troubleshooting information

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

Problem Symptom	Possible Solution
UVM passphrase policy not enforced	**Action**
The **not contain more than 2 repeated characters** check box does not work in IBM Client Security Software Version 5.0	This is a known limitation with IBM Client Security Software Version 5.0.
The Next button is unavailable after entering and confirming your UVM passphrase in the Administrator Utility	**Action**
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 administrator 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 administrator 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 administrator 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 is displayed.	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**

Problem Symptom	Possible Solution
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 password.

User Configuration Utility troubleshooting information

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

Problem Symptom	Possible Solution
Limited Users are unable to perform certain User Configuration Utility functions in Windows XP Professional	**Action**
Windows XP Professional Limited Users might not be able to perform the following User Configuration 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 User Configuration Utility in Windows XP Home	**Action**
Windows XP Home Limited Users will not be able to use the User Configuration 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 when attempting a Client Security administrator function	**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, complete the following procedure: 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.
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
Screen saver only displays on the local screen	**Action**
When using the Windows Extended Desktop function, the Client Security Software screen saver will only be displayed on the local screen even though access to your system and its keyboard will be protected.	If any sensitive information is being displayed, minimize the windows on your extended desktop before you invoke the Client Security screen saver.
Windows Media Player files are encrypted rather than being played in Windows XP	**Action**
In Windows XP, when you open a folder and click **Play all**, the contents of the file will be encrypted rather than played by the Windows Media Player.	To enable the Windows Media Player to play the files, complete the following procedure: 1. Start Windows Media Player. 2. Select all the files in the appropriate folder. 3. Drag the files to the Windows Media Player playlist area.
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.

Problem Symptom	Possible Solution
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.
Outlook Express clients return e-mail messages with a different algorithm	**Action**

Problem Symptom	Possible Solution
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 then 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 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: 1. That 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. That 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.

Problem Symptom	Possible Solution
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 User Configuration 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.

Tivoli Access Manager troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Tivoli Access Manager with Client Security Software.

Problem Symptom	Possible Solution
Local policy settings do not correspond to those on the server	**Action**
Tivoli Access Manager 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.
Tivoli Access Manager setup settings are not accessible	**Action**
Tivoli Access Manager setup and local cache setup settings are not accessible on the Policy Setup page in the Administrator Utility.	Install the Tivoli Access Manager runtime Environment. If the Runtime Environment is not installed on the IBM client, the Tivoli Access Manager 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 Tivoli Access Manager 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 is 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. 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**

Problem Symptom	Possible Solution
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.

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 or later.	This is a known limitation. You must decrypt all files that were encrypted using prior versions of Client Security Software *before* installing Client Security Software 3.0 or later. 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**
A UVM-aware security device, such as smart card, smart card reader, or finger print reader, is not working properly.	Confirm whether the device is configured correctly by the system. After a device is configured, you might need to reboot the system to start the service correctly. For device trouble-shooting information, see the device documentation or contact the device vendor.
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 information

This appendix contains password and passphrase information.

Password and passphrase rules

When dealing with a secure system, there are many different passwords and passphrases. Different passwords have different rules. This section contains information about the administrator password and the UVM passphrase.

Administrator password rules

The rules that govern the administrator password can not be changed by a security administrator.

The following rules pertain to the administrator 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 administrator password to enable the IBM Embedded Security Chip in the computer. This password must be typed each time you access the Administrator Utility and Administrator Console.

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

IBM Client Security Software enables security administrators to set rules that govern a user's UVM passphrase. To improve security, the UVM passphrase is longer and can be more unique than a traditional password. UVM passphrase policy is controlled by the Administrator Utility.

The UVM Passphrase Policy interface in the Administrator Utility enables security administrators to control passphrase criteria through a simple interface. The UVM Passphrase Policy interface enables the administrator to establish the following passphrase rules:

Note: The default setting for each passphrase criterion is provided in parenthesis below.

- establish whether to set a minimum number of alphanumeric characters allowed (yes, 6)

  For example, when set to ″6″ characters allowed,`1234567xxx` is an invalid password.

- establish whether to set a minimum number of digit characters allowed (yes, 1)

  For example, when set to ″1″, `thisismypassword` is an invalid password.
- establish whether to set the minimum number of spaces allowed (no minimum)

  For example, when set to ″2″, `i am not here` is an invalid password.
- establish whether to allow more than two repeated characters (no)

  For example, when established,`aaabcdefghijk` is an invalid password.
- establish whether to enable the passphrase to begin with a digit (no)

  For example, by default, `1password` is an invalid password.
- establish whether to enable the passphrase to end with a digit (no)

  For example, by default, `password8` is an invalid password.
- establish whether to allow the passphrase from containing a user ID (no)

  For example, by default, `UserName` is an invalid password, where `UserName` is a User ID.
- establish whether to ensure that the new passphrase is different from the last x passphrases, where x is an editable field (yes, 3)

  For example, by default, `mypassword` is an invalid password if any of your last three passwords was `mypassword`.
- establish whether the passphrase can contain more than three identical consecutive characters in any position from the previous password (no)

  For example, by default, `paswor` is an invalid password if your previous password was `pass` or `word`.

The UVM Passphrase Policy interface in the Administrator Utility also enables security administrators to control passphrase expiration. The UVM Passphrase Policy interface enables the administrator to choose between the following passphrase expiration rules:

- establish whether to have the passphrase expire after a set number of days (yes, 184)

  For example, by default the passphrase will expire n 184 days. The new passphrase must adhere to the established passphrase policy.
- establish whether the passphrase will never expire

  When this option is selected, the passphrase will never expire.

The passphrase policy is checked in the Administrator Utility when the user is enrolled, and is also checked when the user changes the passphrase from the Client Utility. The two user settings related to the previous password will be reset and any passphrase history will be removed.

The following general 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 exercise a series of anti-hammering delays. These delays are specified in the following section.

Fail counts on TCPA and non-TCPA systems

The following table shows the anti-hammering delay settings for a TCPA system:

Attempts	Delay on next failure
15	1.1 minutes
31	2.2 minutes
47	4.4 minutes
63	8.8 minutes
79	17.6 minutes
95	35.2 minutes
111	1.2 hours
127	2.3 hours
143	4.7 hours

TCPA systems do not distinguish between user passphrases and the administrator password. Any authentication using the IBM Embedded Security Chip adheres to the same policy. The maximum timeout is 4.7 hours. TCPA systems will not delay for longer than 4.7 hours.

Non-TCPA systems distinguish between the administrator password and user passphrases. On non-TCPA systems, the administrator password has a 77-minute delay after 10 failed attempts; user passwords have only a one-minute delay after 32 failed attempts, and then the lockout time doubles after every 32 failed attempts.

Recovering a lost password

If a user forgets his passphrase, the administrator can enable the user to reset his passphrase.

Recoverying a password remotely

To recover a password remotely, complete the following procedure:

- **Administrators**

  A remote administrator must do the following:

  1. Create and communicate a new one-time password to the user.
  2. Send a data file to the user.

     The data file can be sent to the user by e-mail, it can be copied to a removable media such as a diskette, or it can be written directly to the user's archive file (assuming the user can get access to this system). This encrypted file is used to match against the new one-time password.

- **Users**

  The user must do the following:

1. Log on to the computer.
2. When prompted for a passphrase, check the ″I forgot my passphrase″ check box.
3. Enter the one-time password communicated by the remote administrator, and provide the location of the file sent by the administrator.

   After UVM verifies that the information in the file matches the provided password, the user is granted access. The user is then immediately prompted to change the passphrase.

This is the recommended manner to reset a lost passphrase.

Recoverying a password manually

If the administrator can go to the system of the user that forgot his passphrase, the administrator can log on to the user's system as the administrator, provide the adminstrator private key to the Administrator Utility, and manually change the user's passphrase. An administrator does not have to know a user's old passphrase to change the passphrase.

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 USA