IBM® Client Security
Solutions

Client Security Software Version 5.2 Administrator's Guide

IBM® Client Security
Solutions

Client Security Software Version 5.2 Administrator's 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 67 and Appendix D, "**Notices and Trademarks**," on page 75.

Contents

Preface

This guide contains information on setting up and using the security features provided with Client Security Software.

This guide is organized as follows:

″Chapter 1, “Introduction,”″ contains an overview of the applications and components that are included in the software, and a description of Public Key Infrastructure (PKI) features.

″Chapter 2, “File and folder encryption”″ contains information about how to use IBM Client Security Software to protect sensitive files and folders.

″Chapter 3, “CSS Credential Roaming,”″ contains information about how to configure a CSS Credential Roaming network, register a roaming client, authorize and import users, synchronize user data, and restore a roaming network.

″Chapter 4, “How to use Client Security Software,”″ contains examples about how to use the components provided by Client Security Software to set up the security features that IBM client users require.

″Chapter 5, “Authorizing users,”″ contains information about the authentication of client users, including how to authorize and remove users in the User Verification Manager (UVM).

″Chapter 6, “After users have been authorized with UVM,”″ contains information instructions about how to set up UVM protection for the operating-system logon, using UVM protection for Lotus Notes, and using Client Security Software with Netscape applications.

″Chapter 7, “Working with UVM policy,”″ contains instructions about how to edit a local UVM policy, use UVM policy for a remote client, and change the password for a UVM-policy file.

″Chapter 8, “Other security administrator functions,”″ contains instructions about how use the Administrator Utility to change the key archive location, restore keys from archive, recover a UVM passphrase, and to enable or disable the IBM embedded Security Chip.

″Chapter 9, “Instructions for the client user,”″ contains instructions about different tasks that the client user performs when using Client Security Software. This chapter includes instructions about how to use UVM logon protection, the Client Security screen saver, secure e-mail and the User Configuration Utility.

″Chapter 10, “Troubleshooting,”″ contains helpful information for overcoming known limitations and 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, "**Rules for using UVM protection for system logon**,"" contains information about using UVM protection for operating-system logon.

"Appendix D, "**Notices and Trademarks**,"" contains legal notices and trademark information.

Who should read this guide

This guide is intended for security administrators who will:

- Set up user authentication for the IBM client
- Set up and edit the UVM security policy for IBM clients
- Use the Administrator Utility to manage the security subsystem (IBM embedded Security Chip) and associated settings for IBM clients

This guide is also intended for Tivoli Access Manager administrators who will use IBM Tivoli Access Manager to manage authentication objects provided in UVM policy. Tivoli Access Manager administrators must be able to manage the following:

- The Tivoli Access Manager object space
- The authentication, authorization, and credential acquisition processes
- The IBM Distributed Computing Environment (DCE)
- The IBM SecureWay Directory lightweight directory access protocol (LDAP)

How to use this guide

Use this guide to set up user authentication and UVM security policy for IBM clients. This guide is a companion to the *Client Security Software Installation 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 Installation Guide*

References to the *Client Security Software Installation Guide* are provided in this document. You must install Client Security Software on an IBM client before you can use this guide. Instructions for installing the software are provided in the *Client Security Software Installation Guide*.

References to *Using Client Security with Tivoli Access Manager*

References to *Using Client Security with Tivoli Access Manager* are provided in this document. Security administrators who will use Tivoli Access Manager to manage authentication objects for UVM policy should read *Using Client Security with Tivoli Access Manager*.

References to the *Client Security User's Guide*

References to the *Client Security User's Guide* are provided in this document. Administrators can use this guide to set up and maintain UVM policy on IBM clients that use Client Security Software. After an administrator has set up user authentication and UVM security policy, a client user can read the *Client Security User's Guide* to learn how to use Client Security Software.

The User's Guide contains information about performing Client Security Software tasks, such as using UVM logon protection, setting up the Client Security screen saver, 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. File and folder encryption

The IBM File and Folder Encryption Utility, which can be downloaded from the IBM Client Security Web site, enables Client Security Software users to protect sensitive files and folders using the right-click button of their mouse. How the utility protects a file and folder differs depending upon how the file or folder is initially encrypted. Read the following information to determine which encryption technique you should use to protect your data. IBM Client Security Software must be installed *before* you install the IBM File and Folder Encryption utility.

The Check Disk utility might run when restarting the operating system after protecting or unprotecting folders. Wait for the system to be checked before using your computer.

Right-click file protection

Files can be encrypted and decrypted manually through the right-click menu. When files are encrypted in this manner, the encryption operation appends a .enc extension to the files. These encrypted files can then be securely stored on remote servers. They will remain encrypted and unavailable to applications for use until the right-click facility is used again to decrypt them.

Right-click folder protection

A UVM-enrolled user can select a folder to protect or unprotect through the right-click interface. This will encrypt all of the files contained in the folder or any of its subfolders. When files are protected in this manner, no extension is appended to the file name. When an application tries to access a file in an encrypted folder, the file will be decrypted into memory and will be re-encrypted before it is saved on the hard disk.

Any Windows operation that tries to access a file in a protected folder will be given access to the data in a decrypted form. This feature adds ease-of-use so that a file doesn't have to be decrypted before it is used, and then re-encrypted after a program is finished with it.

Folder encryption status

IBM Client Security Software enables users to protect sensitive files and folders using the right-click button of their mouse. How the software protects a file and folder differs depending upon how the file or folder is initially encrypted.

A folder can be in any one of the following states; each state is handled differently by the right-click protect folder option:

- **An Unprotected Folder**

  Neither this folder, its subfolders, nor any of its parents has been designated as protected. The user is given the option to protect this folder.
- **A Protected Folder**

  A protected folder can be in one of three states:
  - **Protected by the current user**

The current user has designated this folder as protected. All files are encrypted, including files in all subfolders. The user is given the option to unprotect the folder.

  - **A subfolder of a folder protected by the current user**

    The current user has designated one of this folder's parents as protected. All files are encrypted. The current user has no right-click options.

  - **Protected by a different user**

    A different user has designated this folder as protected. All files are encrypted, including files in all subfolders, and are unavailable to the current user. The current user has no right-click options.

- **A Parent of a Protected Folder**

  A parent of a protected folder can be in one of three states:

  - **It can contain one or more subfolders protected by the current user**

    The current user has designated one or more subfolders as protected. All files in the protected subfolders are encrypted. The user is given the option to protect the parent folder.

  - **It can contain one or more subfolders protected by one or more different users**

    A different user or users have designated one or more subfolders as protected. All files in the protected subfolders are encrypted, and are unavailable to the current user. The current user has no right-click options.

  - **It can contain subfolders protected by the current user and one or more different users**

    Both the current user and one or more different users have designated subfolders as protected. The current user has no right-click options.

- **A Critical Folder**

  A critical folder is a folder in a critical path and, therefore, cannot be protected. There are two critical paths: the Windows path and the Client Security path.

Each state is handled differently by the right-click protect folder option.

File and Folder Encryption (FFE) utility tips

The following information might be useful when performing certain file and folder encryption functions.

Drive-letter protection

The IBM FFE utility can be used to encrypt files and folders on the C drive only. This utility does not support encryption on any other hard-disk partition or physical drive.

Deleting protected files and folders

To ensure that no sensitive files or folders are left unprotected in the Recycle Bin, you must use the Shift+Del key combination to delete protected folders and files. The Shift+Del key sequence performs an unconditional delete operation and does not attempt to put deleted files in the Recycle Bin.

Before upgrading from a previous version of the IBM FFE utility

If you intend to upgrade from a previous version of the IBM FFE utility (version 1.04 or earlier) and you have protected folders on drives other than the C drive,

unprotect those folders before you install version 1.05 of the IBM FFE utility. If you need to re-protect those folders after you install version 1.05, move those folders to the C drive and then protect them.

Before uninstalling the IBM FFE utility

Before you uninstall the IBM FFE utility, use the IBM FFE utility to unprotect any files or folders that are currently protected.

File and Folder Encryption (FFE) utility limitations

The IBM FFE utility has the following limitations:

Limitations when moving protected files and folders

The IBM FFE utility does not support the following actions:

- Moving files and folders within protected folders
- Moving files or folders between protected and unprotected folders

If you attempt to perform either of these unsupported Move operations, an ″Access Denied″ message will be displayed by the operating system. This message is normal. It simply provides notification that this Move operation is not supported. As an alternative to using a Move operation, do the following:

1. Copy the protected files or folders to the new location.
2. Delete the original files or folders by using the Shift+Del key combination.

Limitations when running applications

The IBM FFE utility does not support running applications from a protected folder. For example, if you have an executable named PROGRAM.EXE, you cannot run that application from a protected folder.

Path name length limitations

As you attempt to protect a folder using the IBM FFE utility or attempt to copy or move a file or folder from an unprotected folder to a protected folder, you might receive a ″One or more path names are too long″ message from the operating system. If you receive this message, you have one or more files or folders that have a path that exceeds the maximum allowable character length. To correct the problem, either rearrange the folder structure to shorten its depth or shorten some folder or file names.

Problems protecting a folder

If you attempt to protect a folder and receive a message stating, `"The folder cannot be protected. One or more files may be in use,"` check the following:

- Verify that none of the files contained in the folder are currently in use.
- If Windows Explorer is displaying one or more subfolders of a folder that you are attempting to protect, make sure that the folder you are attempting to protect is highlighted and active, not any of the subfolders.

Chapter 3. CSS Credential Roaming

The credential roaming feature of IBM Client Security Software enables a UVM user's credentials to be used on all TCPA-enabled computers within a network. This network, called a roaming network, enhances users' flexibility and increases application availability by enabling users to easily work from any computer in the network.

CSS Credential Roaming network requirements

CSS Credential Roaming networks have the following requirements:

- Roaming server
- Authorized CSS-registered clients
- Shared, mapped network drive to store UVM user archives

Note: The roaming server and authorized CSS-registered clients are simply TCPA-enabled computers with established administrator passwords that have IBM Client Security Software 5.1 or higher installed.

Configuring a CSS Credential Roaming network

To configure a CSS Credential Roaming network, you must designate one TCPA computer as the roaming *server* (referred to as system A). The other computers, once registered by the roaming server, are authorized CSS-registered clients. (The first registered client is referred to as system B.)

There is nothing special about the computer that you designate the roaming server. You can use any computer that will be a part of the roaming network. The roaming server is simply the computer designated to establish which computers are ″trusted″ by the roaming network. After a computer is registered with the roaming server, it is trusted by all computers in the network.

One thing to consider when deciding which computer to designate as the roaming server, however, is the computer's reliability. Because all computers on the roaming network are bound to the roaming server by its administrator key pair, it is important that this computer be stable. If this computer were to become disabled, it would be difficult to add new computers to the roaming network. If this were to occur, the entire network would have to be re-registered using a new roaming server.

Configuring a CSS Credential Roaming Network is a two step process:

1. Configure system A (server) by establishing the keys, archive location, and roaming users.
2. Register system B and all other computers in the CSS Credential Roaming network.

The roaming server defines the CSS Credential Roaming network and initiates registration of the client computers, but the focal point of a CSS Credential Roaming network is the mapped, network drive where UVM-user archives are stored. This archive location is where all updates to user credentials are stored.

Updates are *not* stored on the roaming server. After initializing the CSS clients, the roaming server acts like any other CSS-registered client.

Configuring the roaming server

To configure a roaming server, complete the following procedure:

1. On the designated computer, start the Administrator Console, and then click **Configure Credential Roaming**. Or, if the computer is already configured for roaming, select Reconfigure this system as a CSS Roaming Server, click **Next**, and then click **OK**.
2. Click **Configure**.
3. Choose to use an existing key pair or to create a new key pair, and then click **Next**.
4. Enter the archive location, and then click **Next**.

   Note: The archive location must be accessible to the other computers that are registered for roaming.

   If the archive currently has files in it, the next wizard page prompts you on how to handle the files.
5. Click **Finish**.

Registering a client

To register a client, complete the following procedure:

1. Immediately after completing roaming server configuration, the Credential Roaming Network Configuration wizard page is displayed. Select Enable System Registration, and then click **Next**.
2. Enter the name of the user on system B with administrator rights who will complete the client registration.
3. Enter and confirm an 8-character password to be used by that user. (Do not confuse this process with authorizing a user to use UVM, which happens later.)
4. If you want to register the client using the User Configuration Utility, you need to create an administrator configuration file for that user. This process generates a file that is unique to this user. Store this file in a location accessible to the user and to system B.

   Note: This file does not need to be generated when registering a client using the Administrator Utility.
5. Click **Next**.
6. If you created an administrator configuration file, save the file in a location accessible to the user and to system B.

After completing the previous procedures, the CSS Credential Roaming network is configured for roaming. Roaming clients must still be registered before the CSS Credential Roaming network is ready for use.

Registering a roaming client

The roaming server must be running and connected to the archive before you can register any clients.

Registering a roaming client using the Administrator Utility

To register a roaming client using the Administrator Utility, complete the following procedure:

1. Click **Key Configuration**.
2. Click **No** if you are asked if you want to restore keys from the archive.
3. Select Register this system with a CSS Roaming Server, and then click **Next**.
4. Enter the archive location created by system A, type the system-registration password designated for this user on system A, and then click **Next**.

   It takes about a minute to complete the registration.

Registering a roaming client using the User Configuration Utility

To register a roaming client using the User Configuration Utility, complete the following procedure:

1. From the User Configuration tab, click **Register with a CSS Roaming Server**.
2. Select the administrator configuration file you generated on system A, type the system-registration password designated for this user on system A, and then click **Next**.
3. Enter the archive location created by system A, and then click **Next**.

   It takes about a minute to complete the registration.

Registering a roaming client using mass deployment (silently)

To register a roaming client silently using mass deployment, complete the following Administrator Console procedure:

1. Decrypt a previously generated CSEC.INI file. This file contains the administrator password and the users to enroll.
2. In the csssetup section of the file, add `"enableroaming=1"`. This indicates that the computer should be registered as a roaming client.
3. In the same section, add the entry `"username=OPTION"`. There are three possible options for this value:
   a. **The string `"[promptcurrent]"` - brackets included.** This designation should be used if a .dat file for the currently logged on user has been generated on the roaming server and the current user knows the system-registration password. This option causes a pop-up window to prompt the user to enter the system-registration password (`sysregpwd`). Obviously, if this is a truly silent install, the administrator will want to avoid this setting as it requires a user to be at the keyboard.
   b. **The string `"[current]"` - brackets included.** This designation should be used if a .dat file for the currently logged on user has been generated on the server. The `sysregpwd` is handled as described in the next step.
   c. **An actual user name such as `"joseph"`.** If such a designated user name is used, `"joseph.dat"` must have been previously generated by the roaming server. The `sysregpwd` for this case is also handled as described in the next step.
4. If options two or three above are used, another entry `"sysregpwd=SYSREGPW"` must be supplied. This is the eight-digit password associated either with the current user (if option two is implemented) or the designated user (if option three is implemented).

5. To complete the client registration, connect the computer to the archive location setup by the roaming server. This archive location is designated in the CSEC.INI file.

Examples of the CSEC.INI file

The examples below show a sample CSEC.INI file, and how it changes depending upon which credential roaming option is selected. These options are as follows:

- **No roaming values.** This base file is not enabled for credential roaming.
- **Roaming option 1.** This file is enabled for roaming using option 1 for client registration. The current user must present the system-registration password.
- **Roaming option 2.** This file is enabled for roaming using option 2 for client registration. The current user must present his userID and the system-registration password.
- **Roaming option 3.** This file is enabled for roaming using option 3 for client registration. The user is designated. The designated user must present the system-registration password.

Examples of four separate CSEC.INI file are as follows:

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
pub=
c:\jk\admin.key
pri=
c:\jk\private1.key
wiz=0
clean=0

[UVMEnrollment]
enrollall=0
enrollusers=1
user1=joseph
user1uvmpw=
q1234r
user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=
184

[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
pub=
c:\jk\admin.key
pri=
c:\jk\private1.key
wiz=0
enableroaming=1
username=
[promptcurrent]

clean=0

[UVMEnrollment]
enrollall=0
enrollusers=1
user1=joseph
user1uvmpw=q1234r

user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184

[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
pub=
c:\jk\admin.key
pri=
c:\jk\private1.key
wiz=0
enableroaming=1
username=
[current]
sysregpwd=12345678
clean=0

[UVMEnrollment]
enrollall=0
enrollusers=1
user1=joseph
user1uvmpw=q1234r

user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184

[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
```

```
[CSSSetup]
suppw=bootup
hwpw=11111111
newkp=1
keysplit=1
kpl=c:\jgk
kal=c:\jgk\archive
pub=
c:\jk\admin.key
pri=
c:\jk\private1.key
wiz=0
enableroaming=1
username=
joseph
sysregpwd=12345678
clean=0

[UVMEnrollment]
enrollall=0
enrollusers=1
user1=joseph
user1uvmpw=q1234r

user1winpw=
user1domain=0
user1ppchange=0
user1ppexppolicy=0
user1ppexpdays=184

[UVMAppConfig]
uvmlogon=0
entrust=0
notes=0
netscape=0
passman=0
```

folderprotect=0 autoprotect=0	folderprotect=0 autoprotect=0	folderprotect=0 autoprotect=0	folderprotect=0 autoprotect=0

Authorizing users

After completing the previous procedures, the CSS Credential Roaming network is configured and registered for roaming. Users can now be authorized using the Administrator Utility.

Importing users

If you have user profiles already defined, CSS enables you to import users rather than having to create new user profiles.

Importing a user profile

A user profile can be imported to a new computer on the roaming network using the Administrator Utility, the User Configuration Utility, or the UVM GINA.

Importing a user profile using the User Configuration Utility

To import a user profile to a new computer on the roaming network using the User Configuration Utility, click **Import existing configuration from archive** on the User Configuration tab.

Importing a user profile using the Administrator Utility

To import a user profile to a new computer on the roaming network using the Administrator Utility, select the user and then click **Authorize**. Click **Yes** when asked if you want to import the user from the archive.

Note: In order to import a user to a roaming network, the user must be authorized on another computer in the roaming network.

Importing a user profile using the UVM GINA

A user profile can be imported to a new computer on the roaming network using the UVM GINA. This process is begun from the UVM logon screen. If a user is not yet authorized to use UVM on a given system in the network, a message box is displayed asking if the user wants to be imported from the archive.

To import a user profile to a new computer on the roaming network using the UVM GINA, complete the following procedure:

1. Attempt to log on to UVM on a new computer on the network.

   A message box is displayed asking if the user wants to be imported from the archive.
2. Click **Yes**.

   A dialog box is displayed prompting the user to provide his Windows password.
3. Enter your Windows password.

   A dialog box is displayed prompting the user to provide the name of the shared archive directory.
4. Provide the name of the shared archive directory for the network.

   The archive directory must be mapped to a drive letter on the computer. This name of the shared archive directory provided must match the one that is mapped.

A dialog box is displayed prompting the user to provide a network user name and password.

5. Provide your network user name and password.

   Note: This is not necessarily the user name and password used to log on to Windows.

   The user profile is now successfully imported.

After importing the user profile, authentication with UVM is based on that computer's security policy. The security requirements for that computer must be successfully provided before the user can log on.

Synchronizing user data

Each user's data is stored in the archive location. A copy of that data is also stored locally on every computer to which he has roamed. When changes are made, such as obtaining a certificate or changing a passphrase, the local data is updated. If the computer is connected to the archive, the user's data is also updated. When the user logs onto another computer, updates are automatically downloaded to that computer, provided that it is also connected to the archive.

Connection to the archive is not always guaranteed, however, so sometimes a user's data can be inconsistent between computers and the archive. If a user's data is changed on a computer that is not connected to the archive, the changes are not reflected in the archive and, consequently, not on other computers either. Once the computer is connected to the archive, the changes are updated in the archive and any data inconsistencies are subsequently resolved on other connected computers as well. However, if changes are made on another computer that is connected to the archive before the first computer that contained changes gets connected to the archive, a non-correctable data inconsistency issue arises. The data in the archive contains changes that are not present on the first computer, while that computer contains changes that are not in the archive. If this occurs, the user is notified of the two different configurations and is prompted to choose which configuration to preserve, the local one or the archived one. The configuration changes that are not chosen are lost. It is important, therefore, to make sure that any changes made to a user's configuration are updated to the archive before making changes on any other computer.

Restoring a roaming network

In the event of a software or hardware failure, the roaming network might need to be restored. The following sections describe the restoration procedure.

Restoring a roaming server due to hard drive or chip failure

If the roaming server is corrupted, restore the data using the Administrator Utility in the same manner as a non-roaming environment. After restoration, however, no additional clients can be registered in the roaming network. If more clients need to be registered after a restoration is performed, the server must be re-configured and all existing clients must be re-registered along with the additional clients to be added.

Restoring a roaming client due to hard drive failure

If the data used by CSS is corrupted on a registered client, restore the data using the Administrator Utility just like you would when restoring a computer in a non-roaming environment.

Restoring a roaming client due to a chip failure

If the security chip on a registered client fails or is cleared, the client must be re-registered with the roaming server. No other action is necessary.

Changing the administrator key pair

It is not recommended that you change the administrator key pair in a roaming network.

To change the administrator key pair in a roaming network, the following steps must be completed for the change to be reflected on all computers in the network.

1. On the roaming server, change the administrative key pair using the Administrator Utility.
2. Re-register all the clients in the network.
3. Preserve existing files whenever prompted.

Changing the archive location

Changing the archive location in a roaming environment differs slightly from a non-roaming environment because each computer in the network accesses the same archive location.

To change the archive location on a roaming network, complete the following procedure:

1. Copy the files from the old archive location to the new using the following procedure:
   a. Start the Administrator Utility and enter the administrator password.
   b. Click **Key Configuration**.
   c. Select Change the archive location, and then click **Next**.
   d. Enter the new location of the archive, and then click **Next**.
   e. Click **Yes** when prompted to copy all the files from the old location to the new one.
2. Update all other computers on the network to use the new archive location using the following procedure:
   a. Start the Administrator Utility and enter the administrator password.
   b. Click **Key Configuration**.
   c. Select Change the archive location, and then click **Next**.
   d. Enter the new location of the archive, and then click **Next**.
   e. Click **No** when prompted to copy all the files from the old location to the new one.

File and Folder Encryption (FFE)

File and Folder Encryption functionality is unaffected by a roaming environment. However, protected folders are managed on a computer-by-computer basis. Thus, if a folder is protected by user A on system A, a folder of the same name on system B, if it exists, is not protected unless the user actively protects it on system B.

IBM Password Manager

All passwords protected using the IBM Password Manager are available on all computers in the roaming network.

Roaming terms and definitions

The following terms are useful to understand when discussing the concepts and procedures involved in setting up a roaming network:

Client registration
The process of registering a computer with the roaming server.

Registered clients
All trusted TCPA computers in the roaming network.

Roaming server
The TCPA computer used to initiate the roaming network.

System-registration password
The password used to register the computer with the roaming server.

Chapter 4. How to use Client Security Software

Administrators can use the multiple components provided by Client Security Software to set up the security features that IBM client users require. Use the following examples to guide your thinking as you plan your Client Security policy and configuration. For example, Windows NT users can set up UVM protection for system logon which prohibits unauthorized users from logging onto the IBM client.

Example 1 - One Windows 2000 client and one Windows XP client that both use Outlook Express

In this example, one IBM client (client 1) has Windows 2000 and Outlook Express installed, the other client (client 2) has Windows XP and Outlook Express installed. There are three users who will require authentication setup with UVM on client 1; one client user will require authentication setup with UVM on client 2. All client users will register their fingerprints so that they can be used for authentication. A UVM-aware fingerprint sensor will be installed during this example. It has also been established that both clients will require UVM protection for Windows logon. The administrator decided that the local UVM policy will be edited and used at each client.

To set up client security, complete the following procedure:

1. Install the software on client 1 and client 2. Refer to the *Client Security Software Installation Guide* for details.
2. Install the UVM-aware fingerprint sensors and any associated software on each client.

   For information about UVM-aware products, go to http://www.pc.ibm.com/ww/security/secdownload.html on the World Wide Web.
3. Set up user authentication with UVM for each client. Do the following:
   a. Add users to UVM by assigning them a UVM passphrase. Because client 1 has three users, you must repeat the process for adding users to UVM until all users have been added.
   b. Set up UVM protection for the Windows logon for each client.
   c. Register user fingerprints. Because a policy will be set stating three users will use client 1, all three users must register their fingerprints.

      Note: If you set fingerprint as an authentication requirement as part of UVM policy for a client, each user must register his or her fingerprints.
4. Edit and save a local UVM policy at each client that requires authentication for the following:
   - Logging on the operating system
   - Acquiring a digital certificate
   - Using a digital signature for e-mail messages
5. Restart each client to enable the UVM protection for the Windows logon.
6. Inform the users of the UVM passphrases that you have set for them and of the authentication requirements that you set in the UVM policy for the IBM client.

Client users can now perform the following tasks:

- Use UVM protection to lock and unlock the operating system.
- Apply for a digital certificate and choose the embedded Security Chip as the cryptographic service provider associated with the certificate.
- Use the digital certificate to encrypt e-mail messages created with Outlook Express.

Example 2 - Two Windows 2000 IBM clients that use Lotus Notes and the Client Security screen saver

In this example, the two IBM clients (client 1 and client 2) both have Windows 2000 and Lotus Notes installed. Two users will require authentication setup with UVM on client 1; one user will require authentication setup with UVM on client 2. Both clients will require UVM protection for the system logon, and will use the Client Security screen saver and UVM protection for Lotus Notes. The administrator decided a UVM policy for remote clients will be edited on client 1, and then be copied to client 2.

To set up client security, complete the following procedure:

1. Install the software on client 1 and client 2. Because a UVM policy for remote clients will be used, you must use the same administrator public key when you install the software on both client 1 and client 2. Read the *Client Security Software Installation Guide* for details about the software installation.
2. Set up user authentication with UVM for each client. Then, do the following:
   a. Add users to UVM by assigning them a UVM passphrase. Because client 1 has two users, you must repeat the process for adding users to UVM until both users have been added.
   b. Set up UVM protection for Windows logon on each client.
3. Enable UVM protection for Lotus Notes on both clients. For more information, see "Using UVM protection for Lotus Notes" on page 28.
4. Edit and save a UVM policy for remote clients on client 1, and then copy it to client 2. UVM policy would require user authentication for clearing the screen saver, logging on to Lotus Notes, and logging on the operating system. For details, see "Editing and using UVM policy for remote clients" on page 36.
5. Restart each client to enable the UVM protection for the system logon.
6. Inform the client users of the UVM passphrases and the policy that has been set for each client.

The users can now read the *Client Security Software User's Guide* to learn how to perform the following tasks:

- Enable the Client Security screen saver
- Use UVM protection for Windows 2000

Example 3 - Multiple Windows 2000 IBM clients that are managed by Tivoli Access Manager and that use Netscape for e-mail

The intended audience for the following example is an enterprise administrator who plans to use Tivoli Access Manager to manage the authentication objects that are set by UVM policy. In this example, multiple IBM clients have both Windows 2000 and Netscape installed. All clients have NetSEAT client, a Tivoli Access Manager component, installed. All clients using an LDAP server have LDAP client

installed. UVM policy for remote clients will be installed on all clients. UVM policy will enable Tivoli Access Manager to control selected authentication objects for the clients.

In this example, one user will require authentication setup with UVM on each client. All users will register their fingerprints so that they can be used for authentication. A UVM-aware fingerprint sensor will be installed during this example and all clients will require UVM protection for Windows logon.

To set up client security, complete the following procedure:

1. Install the Client Security component on the Tivoli Access Manager server. For details, see *Using Client Security with Tivoli Access Manager*.
2. Install Client Security Software on all clients. Because a UVM policy for remote clients will be used, you must use the same administrator public key when you install the software on all clients. Read the *Client Security Software Installation Guide* for details about the software installation.
3. Install the UVM-aware fingerprint sensors and any associated software on each client. For information about available UVM-aware products, go to http://www.pc.ibm.com/ww/security/secdownload.html on the World Wide Web.
4. Set up user authentication with UVM on each client. See "Removing users" on page 25 for details. Then, do the following:
   a. Add users to UVM by assigning them a UVM passphrase.
   b. Set up UVM protection for the Windows logon on each client.
   c. Register the fingerprints for each client user. If fingerprint authentication is required on an IBM client, all users of that client must register their fingerprints.
5. Configure the Tivoli Access Manager setup information at each client. For details, see *Using Client Security with Tivoli Access Manager*.
6. Edit and save a UVM policy for remote clients on one of the clients, and then copy it to the other clients. Set UVM policy so that Tivoli Access Manager will control the following authentication objects:
   - Logging on the operating system
   - Acquiring a digital certificate
   - Using a digital signature for e-mail message

   For details, see "Editing and using UVM policy for remote clients" on page 36.
7. Restart each client to enable the UVM protection for the Windows logon.
8. Install the IBM Embedded Security Chip PKCS#11 module onto each client. This module provides cryptographic support on clients that use Netscape for sending and receiving e-mail messages, and the IBM Embedded Security Chip for acquiring digital certificates. For more information, see the *Client Security Software Installation Guide*.
9. Enable Tivoli Access Manager to control the IBM Client Security Solutions objects that appear in the Tivoli Access Manager Management Console.
10. Inform client users of the UVM passphrases that have been set and the policy that has been set for each client.
11. Advise client users to read the *Client Security Software User's Guide* to learn how to perform the following tasks:
    - Use UVM protection to lock and unlock the operating system
    - Use the User Configuration Utility

- Apply for a digital certificate that uses the embedded Security Chip as the cryptographic service provider associated with the certificate
- Use the digital certificate to encrypt e-mail messages created with Netscape

Chapter 5. Authorizing users

The following information is useful when authorizing Windows users to use User Verification Manager (UVM).

Authentication for client users

Authenticating end users at the client level is an important computer security 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.

The UVM security policy for an IBM client can be managed in two ways:

- Locally, using a policy editor that resides on the IBM client
- Throughout an enterprise, using Tivoli Access Manager

Hardware encryption keys are generated when you add the first user.

Elements of authentication

Elements of authentication (such as UVM passphrases or user fingerprints) are used to authorize users with the IBM client. When you authorize a Windows user to use UVM, you assign a UVM passphrase for the client user. The UVM passphrase, which can be up to 256 characters long, is the main authentication element used by UVM. When you assign a UVM passphrase, user encryption keys are created for that client user that are stored in a file that is managed by the IBM embedded Security Chip. If the IBM client uses a UVM-aware device for authentication, the authentication element, for example user fingerprints, must also be registered with UVM.

During user authentication setup, you can select the following security features that are provided by Client Security Software:

- **UVM protection for the operating-system logon.** UVM protection ensures that only those users who are recognized by UVM are able to access the computer. Before you enable UVM protection for the system logon, see Setting up UVM operating-system logon protection for important information.
- **Client Security screen saver.** After you add a client user, the user can set up and use the Client Security screen saver. The Client Security screen saver is set up through the Display option within the operating-system software.

Before you authorize users

Important: Only authorize user accounts that can be used to logon to the operating system. If a user account that *cannot* be used to logon to the operating system is authorized, **all** users will be locked out of the system when UVM logon protection is enabled.

When you authorize a client user, the Administrator Utility provides you with a list of user names from which you can select. The names in that list are the user accounts that have been added by using the operating system. Before you add client users to UVM, use the operating-system software to create user accounts and

profiles for those users. Client Security Software works in conjunction with the security features provided by the operating system.

Windows XP and Windows 2000.

Use the Users and Passwords program to create new user accounts and manage user accounts or groups. See the operating-system documentation for more information.

In Windows XP, the Select Windows Users to Aurhorize field does not refresh when you click the **Create New Windows User** button. You must exit and restart the Administrator Utility to refresh this field.

Notes:

1. When you use the operating-system software to create new users, the domain password for each new user must be the same.
2. Do not authorize a user that previously had a Windows user name changed. UVM will point to the former user name while Windows will only recognize the new user name.
3. When a user account that has been authorized is deleted from Windows, the UVM logon protection interface incorrectly continues to list the account as one that can be used to log on to Windows. This account *cannot* be used to log on to Windows.
4. After a user has been authorized, do not change his Windows user name. If you do, you will have to re-authorize the new user name in UVM and request all new credentials.

Authorizing users

Users must log on with administrator rights to use the Administrator Utility.

To authorize users with UVM, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   The Enter Administrator Password message is displayed.
2. Type the Administrator password, and then click **OK**.

   The IBM Security Subsystem Administrator Utility main window opens.
3. In the Select Windows Users To Authorize area, select a user name from the list.

   Note: The user names in the list are defined by the user accounts created in the operating system or network.
4. Click **Authorize**.

   The User Authentication Setup screen is displayed.
5. Enter and confirm an initial User Verification Manager passphrase for the newly authorized user, and then click **Next**.

   If the passphrase does not meet the security policy requirements, a screen displays that the passphrase entered is invalid. If this happens, click **OK**, and then click **View Passphrase Requirements** to view the parameters that a valid passphrase must meet.

   When the passphrase is accepted, a message is displayed indicating that the operation completed successfully.
6. Click **OK** to continue.

The Windows Logon Password screen is displayed. If secure UVM logon is enabled, the user's current Windows password must be stored so that the user can log on to the system. This screen enables the Administrator to either:

- **Store the user's current Windows password now.** To store the user's current Windows password now, enter and confirm the user's password in the provided fields, and then click **Next**.

  Note: The password entered here must match the user's current Windows password. This setting does not affect the password that is stored with the operating system.
- **Have the user store his Windows password later using the User Configuration Utility.** To have the user store his Windows password later using the User Configuration Utility, select the appropriate radio button, and then click **Next**.

A message is displayed indicating that the operation completed successfully.

7. Click **Finish**.

Removing users

Users must log on with administrator rights to use the Administrator Utility.

To unauthorize users with UVM, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   The Enter Administrator Password message is displayed.
2. Type the Administrator password, and then click **OK**.

   The IBM Security Subsystem Administrator Utility main window opens.
3. In the Windows Users Authorized to use UVM area, select a user name from the list.
4. Click **Remove User**.

   A message is displayed warning that the selected user's security information, including all of the user's existing keys, certificates, registered fingerprints and stored passwords, will be lose.
5. Click **Yes** to continue.

   A message is displayed asking if you would like to remove the user's archived information. If you remove this information, the user will not be able to restore any previously saved settings onto any system.
6. Click **Yes** to complete the operation.

Creating new users

Users must log on with administrator rights to use the Administrator Utility.

To create new users, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   The Enter Administrator Password message is displayed.
2. Type the Administrator password, and then click **OK**.

   The IBM Security Subsystem Administrator Utility main window opens.

3. In the Select Windows Users To Authorize area, click **Create New Windows User**.

   The Windows User Accounts screen is displayed.
4. Click **Create a new account**.
5. Name the new account by typing a name in the provided field; then click **Next**.
6. Pick an account type by selecting the appropriate radio button.
7. Click **Create Account**.
8. Return to the IBM Client Security Subsystem Administrator Utility.

   The new user account is displayed in the Select Windows Users To Authorized area.

Chapter 6. After users have been authorized with UVM

After users have been authorized, additional Client Security functions can be utilized, such as the following:

- **Setting up UVM protection for the operating system logon.** See "Setting UVM operating-system logon protection" for more information.
- **Archiving user encryption keys.** See "Changing the key archive location" on page 38 for more information.
- **Setting up the Client Security screen saver.** See Chapter 9, "Instructions for the client user," on page 45 for more information.
- **Registering user fingerprints with UVM.** See "Registering user fingerprints with UVM" on page 28 for more information.

  If a UVM-aware fingerprint sensor is installed prior to adding users to UVM, fingerprint registration can be done at that time.

UVM operating-system logon protection

UVM system logon protection enhances the password feature provided with your operating system. The UVM logon interface replaces the operating system logon so that the UVM logon window opens each time a user tries to log on to the system.

Setting UVM operating-system logon protection

Read the following information before you set and use UVM protection for the system logon:

- If UVM policy indicates that fingerprint authentication is required for system logon and the user has no fingerprints registered, the user must register fingerprints to log on.

  Also, if the user Windows password is not registered (or registered incorrectly) with UVM, the user must provide the correct Windows password to log on.
- Do not clear the IBM embedded Security Chip while UVM protection is enabled. If you do, you will be completely locked out of the system. For more information, see "Administrator tips" in Chapter 10, "Troubleshooting," on page 51.
- If you clear the **Replace the standard Windows logon with UVM's secure logon** check box in the Administrator Utility, the system returns to the Windows logon process without utilizing UVM logon protection.
- If you replace the standard Windows logon with UVM secure logon and enable the Cisco LEAP function, you must reinstall the Cisco Aironet Client Utility (ACU).

Setting up UVM operating-system logon protection

To set up UVM protection for your operating system, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   The Administrator Utility main window is displayed.
2. Click **Configure Application Support and Policies**.

   The UVM Application and Policy Configuration screen is displayed.

3. Select the **Replace the standard Windows logon with UVM's secure logon** checkbox.
4. Click **OK**.
5. Restart the computer.

When the computer restarts, you will be prompted to log on to the computer. For more information about UVM protection, see "UVM operating-system logon protection" on page 27.

Registering user fingerprints with UVM

When UVM policy has been edited to include fingerprint authentication, each user must register fingerprints with UVM.

Note: Windows XP does not support Digital Persona U.are.U Pro fingerprint sensors.

To register user fingerprints with UVM, complete the following Administrator Utility procedure:

1. In the Windows Users Authorized to use UVM area, select a user name from the list.
2. Click **Edit User**.

   The Modify Client Security Key Configuration- Edit UVM User Attributes window is displayed.
3. Select the **Register with UVM-aware device** check box, and then click **Next**.

   The Modify Client Security Key Configuration- UVM Enabled Devices window is displayed.
4. Click **Register user fingerprints**.
5. In the Select a hand area, click **Left** or **Right**.
6. In the Select a finger area, click to select the finger you will scan for prints, and then click **Start registration**.
7. Place your finger on the UVM-aware fingerprint sensor and follow the on-screen instructions.

   Depending upon your scanner model, you might need to scan each fingerprint four times. Click **Cancel this finger** to cancel the fingerprint scan.
8. Specify another finger to register, or click **Exit** to finish.

Using UVM protection for Lotus Notes

UVM provides enhanced security protection for Lotus Notes users.

Enabling and configuring UVM protection for a Lotus Notes User ID

Before you can enable UVM protection for Lotus Notes, Notes must be installed on the IBM client, a Notes User ID and password must be established for the user, and the Notes user must be authorized to use UVM.

To set up UVM protection for Lotus Notes, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   The Administrator Utility main window is displayed.
2. Click **Configure Application Support and Policies**.

The UVM Application and Policy Configuration screen is displayed.

3. Select the **Enable Lotus Notes support** checkbox.

   UVM protection for the Lotus Notes User ID is now enabled. If necessary continue with the following optional steps to configure policy for Lotus Notes logon.

4. Click **Application Policy**.

   The Modify Client Security Policy Configuration screen is displayed.

5. Click **Edit Policy**.
6. Enter the administrator password, and then click **OK**. The IBM UVM Policy: Lotus Notes Logon screen is displayed.
7. On the Object Selection tab, select Lotus Notes Logon from the Action drop-down menu.
8. On the Authentication Elements tab, select the authentication elements that you want to require for Lotus Notes Logon.
9. Click **Apply** to save the selections.

   The Administrator Private Key Required screen is displayed.

10. 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.
11. Click **OK**.

    The IBM User Verification Manager: Summary of Policy screen displays a summary of objects controlled by the local client policy.

12. Start Lotus Notes.

    UVM Password registration is complete when Lotus Notes is started.

Using UVM protection within Lotus Notes

Before you can use UVM protection for Lotus Notes, you must follow the steps in "Setting up UVM protection within Lotus Notes."

Setting up UVM protection within Lotus Notes

To set up UVM protection within Lotus Notes, do the following:

1. Log in to Lotus Notes.

   The IBM User Verification Manager window is displayed.

2. Enter and verify your Lotus Notes password in the available fields.

   Your Lotus Notes password is now registered with UVM.

Re-setting your Lotus Notes password

To reset your Lotus Notes password, do the following:

1. Log in to Lotus Notes.
2. From the Lotus Notes menu bar, click **File > Tools > User ID**.

   The IBM User Verification Manager window is displayed.

3. Enter your UVM passphrase, and then click **OK**.

   The User ID window is displayed.

4. Click **Set Password**.

   The IBM User Verification Manager window is displayed.

5. Select the **Create your own password** radio button.
6. Enter and verify your new Lotus Notes password in the available fields, and then click **OK**.

Note: When you change your password within Lotus Notes to a value that you have used before, Notes rejects the password change, but does not inform the Client Security Software. Consequently, UVM stores the password that Notes rejected.

If you receive a message indicating that the password has been used before when changing your password within Lotus Notes, you will need to exit Lotus Notes, start the User Configuration Utility, and restore the Lotus Notes password to the value it was before.

If your Lotus Notes password was randomly generated, and you get this error, you have no way of knowing what the password was, and therefore you can not reset it manually. You must request a new ID file from your administrator or restore a previously-saved copy of your ID file.

Disabling UVM protection for a Lotus Notes User ID

If you want to disable UVM protection for a Lotus Notes User ID, do the following:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**. After you enter your password, t he Administrator Utility main window is displayed.
2. Click **Configure Application Support and Policies**.
   The UVM Application and Policy Configuration screen is displayed.
3. Unselect the **Enable Lotus Notes support** checkbox.
4. Click **OK**.
   The Application Support Actions screen is displayed with a message indicating that Lotus Notes support is disabled.

Setting up UVM protection for a switched Lotus Notes User ID

To switch from a User ID that has UVM protection enabled to another User ID, do the following:

1. Exit Lotus Notes.
2. Disable UVM protection for the current User ID. See "Disabling UVM protection for a Lotus Notes User ID" for details.
3. Enter Lotus Notes and switch User IDs. See your Lotus Notes documentation for information on switching User IDs.
4. To set up UVM protection for the User ID that you have switched to, enter the Lotus Notes Configuration tool (provided by Client Security Software), and set up UVM protection. See "Using UVM protection within Lotus Notes" on page 29.

Using Client Security Software with Netscape applications

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

For details on how to use the security settings for Netscape applications, see the documentation provided by Netscape. IBM Client Security Software only supports Netscape Version 4.7x.

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

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

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

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

1. Open Netscape, and then click **File > Open page**.
2. Locate the IBMPKCSINSTALL.HTML install file.

   (If you accepted the default directory when you installed the software, the file is located in C:\Program Files\IBM\Security.)
3. Open the IBMPKCSINSTALL.HTML install file in Netscape.

   When you open the file in Netscape, the installation sequence begins and the UVM passphrase window opens.
4. Type the UVM passphrase, and then click **OK**.

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

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

Using the PKCS#11 logon protection for Netscape applications

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

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

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

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

Updating the key archive for Netscape applications

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

Using the digital certificate for Netscape applications

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

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

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

Chapter 7. Working with UVM policy

Before attempting to edit the UVM Policy for the local client, make sure at least one user is authorized to use UVM. Otherwise, an error message will be displayed when the policy editor attempts to open the local policy file.

After users have been authorized to use UVM, you must edit and save a security policy for each IBM client. The security policy provided by Client Security Software is called UVM policy, which combines the settings that you provided in "Authorizing users" with authentication requirements at the client level. UVM policy can be used to control the security policy of a local client or it can be copied to remote clients across a network.

The Administrator Utility has a built-in UVM policy editor that you can use to edit and save UVM policy for a local client. Tasks performed at the IBM client, such as logging on to the operating system or clearing the screen saver, are called authentication objects, and these objects have authentication requirements assigned to them within UVM policy. For example, you can set UVM policy to require the following:

- Each user must type a UVM passphrase and use proximity badge authentication to log on to the operating system.
- Each user must type a UVM passphrase each time a digital certificate is acquired.

You can also use Tivoli Access Manager to control specific authentication objects as set in UVM policy.

UVM policy sets the requirements for authentication objects for the IBM client, not for the individual user. Therefore, if you set UVM policy to require fingerprint authentication for an object (such as the operating-system logon), each user that is authorized to use UVM must register a fingerprint to use that object. For details about authorizing a user, see "Removing users" on page 25.

UVM policy is saved in a file named `globalpolicy.gvm`. To use UVM on remote clients, UVM policy must be saved on one IBM client and then copied to the remote clients. Copying the UVM policy file to remote clients can save you time setting up UVM policy on the remote clients.

Editing a local UVM policy

You edit a local UVM policy and use it only on the client for which it was edited. If you installed Client Security in its default location, the local UVM policy is stored as \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm. Use the UVM-policy editor to edit and save a local UVM policy. Only a user who has been added to UVM can use the UVM-policy editor. The interface for the UVM-policy editor is provided in the Administrator Utility.

When you save changes to the UVM policy, a message is displayed that asks for the administrator private key. Type the administrator private key, and then click **OK** to save your changes. If you provide an incorrect administrator private key, your changes will not be saved.

Authentication occurs based on what you select in the policy editor. For example, if you select “No passphrase required after 1st used this way” for Lotus Notes Logon, then whenever you log on to Lotus Notes it will ask for UVM authentication. Each time you access Lotus Notes after that, until you reboot or log off, the passphrase is not required.

When you set UVM policy to require fingerprint for an authentication object (such as the operating-system logon), each user that is added to UVM must have registered their fingerprints to use that object.

While you are editing UVM policy, you can view the policy summary information by clicking UVM Policy Summary. Also, you can click **Apply** to save your changes. When you click **Apply**, a message is displayed that prompts you for the administrator private key. Type the administrator private key, and then click **OK** to save your changes. If you provide an incorrect administrator private key, your changes will not be saved.

Object selection

UVM policy objects enable you to establish different security policies for various user actions. Valid UVM objects are specified on the **Object Selection** tab of the IBM UVM Policy screen in the Administrator Utility.

Valid UVM policy objects include the following:

System Logon
This object controls authentication requirements necessary to log onto the system.

System Unlock
This object controls authentication requirements necessary to clear the Client Security screen saver.

Lotus Notes Logon
This object controls authentication requirements necessary to log onto Lotus Notes.

Lotus Notes Change Password
This object controls authentication requirements necessary to use UVM to generate a random Lotus Notes password.

Digital Signature (e-mail)
This object controls authentication requirements necessary when you click the Sign button in Microsoft Outlook or Outlook Express.

Decryption (e-mail)
This object controls authentication requirements necessary when you click the Decrypt button in Microsoft Outlook or Outlook Express.

File and Folder Protection
This object controls authentication requirements necessary when right-click encryption and decryption has been selected.

Password Manager
This object controls authentication requirements necessary when you use the IBM Password Manager, which is available from the IBM Web site. When activated, most users should leave this setting on ″No passphrase required after 1st used this way.″

Netscape - PKCS#11 Logon
This object controls authentication requirements necessary when a PKCS#11

C_OpenSession call is received by the PKCS#11 module. Most users should leave this setting on "No passphrase required after 1st used this way."

Entrust Logon
This object controls authentication requirements necessary when Entrust issues a PKCS#11 C_OpenSession call to be received by the PKCS#11 module. Most users should leave this setting on "No passphrase required after 1st used this way."

Change Entrust Logon Password
This object controls authentication requirements necessary to change the Entrust logon password. Entrust does this by issuing a PKCS#11 C_OpenSession call to be received by the PKCS#11 module. Most users should leave this setting on "No passphrase required after 1st used this way."

Authentication elements

UVM policy establishes which available authentication elements will be required for each object you enable. This enables you to establish different security policies for various user actions.

Authentication elements that can be selected on the **Authentication Elements** tab of the IBM UVM Policy screen in the Administrator Utility include the following:

Passphrase Selection
This selection enables an administrator to establish the UVM passphrase be used to authenticate a user in any of the following three manners:

- A new passphrase required each time.
- No passphrase required after 1st used this way.
- No passphrase required if given at system logon.

Fingerprint Selection
This selection enables an administrator to establish that a fingerprint scan be used to authenticate a user in any of the following three manners:

- A new fingerprint required each time.
- No fingerprint required after 1st used this way.
- No fingerprint required if given at system logon.

Global Fingerprint Settings
This selection enables an administrator to establish a maximum number of authentication retries before the system will lock out a user. This area also enables the administrator to allow fingerprint authentication protection to be overridden with the UVM passphrase.

Smart Card Selection
This selection enables an administrator to require that a smart card be provided as an additional authentication device.

Global Smart Card Settings
This selection enables an administrator to set the policy to allow overrides when the UVM passphrase is provided.

Using the UVM-policy editor

To use the UVM-policy editor, complete the following Administrator Utility procedure:

1. Click the **Configure Application Support and Policies** button.

The UVM Application and Policy Configuration screen is displayed.

2. Click the **Application Policy** button.

   The Modify Client Security Policy Configuration screen is displayed.

3. Click the **Edit Policy** button.

   The Enter Administrator Password screen is displayed.

4. Enter your Administrator password, and then click **OK**.

   The IBM UVM Policy screen is displayed.

5. On the Object Selection tab, Click **Action** or **Object Type** and select the object for which you want to assign authentication requirements.

   Actions include System Logon, System Unlock, and E-mail Decryption; an example of an object type is Acquire Digital Certificate.

6. For each object you select, do one the following:
   - Click the **Authentication Elements** tab, and edit the settings for the available authentication elements that you want to assign to the object.
   - Select **Access Manager controls selected object** to enable Tivoli Access Manager to control the object you chose. Select this option only if you want Tivoli Access Manager to control the authentication elements for the IBM client. For more information, see *Using Client Security with Tivoli Access Manager*.

     Important: If you enable Tivoli Access Manager to control the object, you are giving control to the Tivoli Access Manager object space. If you do this, you must reinstall Client Security Software to re-establish local control over that object.
   - Select **Deny all access to selected object** to deny access for the object you chose.

7. Click **OK** to save your changes and exit.

Editing and using UVM policy for remote clients

To use UVM policy across multiple IBM clients, edit and save UVM policy for a remote client, and then copy the UVM-policy file to other IBM clients. If you install Client Security in its default location, the UVM-policy file will be stored as \Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm.

Copy the following files to other remote IBM clients that will use this UVM-policy:

- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
- \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

If you installed Client Security Software in its default location, the root directory for the preceding paths is \Program Files. Copy both files to the \IBM\Security\UVM_Policy\ directory path on the remote clients.

Chapter 8. Other security administrator functions

When you set up Client Security Software on IBM clients, you use the Administrator Utility to enable the IBM embedded Security Chip, set a Security Chip password, generate the hardware keys, and set up the security policy. This section provides instructions for using other Administrator Utility functions.

To open the Administrator Utility, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   Because access to the Administrator Utility is protected by the Security Chip password, a message is displayed that asks you to type the Security Chip password.
2. Type the Security Chip password, and then click **OK**.

Using the Administrator Console

The Client Security Software Administrator Console enables a Security Administrator to perform administrator-specific tasks remotely from his system.

The Administrator Console application (console.exe) must be installed and run from the `\program files\ibm\security` directory.

The Administrator Console enables a Security Administrator to perform the following functions:

- **Bypass or override authentication elements.** The bypass or override functions that the administrator can perform include the following:
  - **UVM passphrase bypass.** This function enables the administrator to provide bypass the UVM passphrase. When this function is used, a random temporary passphrase is created, along with a password file. The administrator send the password file to the user, and communicates the password by some other means. This ensures the security of the new passphrase.
  - **Display/Change Fingerprint/Smart Card Override Password.** This function enables the administrator to override the security policy even if it is set to NOT allow passphrase override for fingerprint or smart card. This might be necessary if a user's fingerprint reader is broken or his smart card is not available. The administrator can read or e-mail the override password to the user.
- **Access archive key information.** The information that the administrator can access includes following:
  - **Archive directory.** This field enables the administrator to locate the archive key information from a remote location.
  - **Administrator private key location.** This field enables the administrator to locate the administrator private key.
- **Other remote administrator functions.** The Administrator console enables security administrators to remotely perform the following functions:
  - **Create the Administrator Configuration file.** This function enables the administrator to generate the administrator configuration file, which is

required when a user wants to enroll or reset himself using the Client Utility. The administrator typically emails this file to a user.

- **Encrypt/Decrypt Setup Configuration File.** This function enables the encryption of the setup configuration file for additional security. It will also decrypt the file so that it can be edited.
- **Configure Credential Roaming.** This function registers this system as a CSS Roaming Server. Once registered, all UVM-authorized users in the network will be able to access their personal data (passphrases, certificate, etc.) on this system.

Changing the key archive location

When the key archive is first created, copies of all encryption keys are created and saved to the location specified at installation.

Note: The client user can also change the key archive location using the User Configuration Utility. For more information, see Chapter 9, "Instructions for the client user," on page 45.

To change the key archive location, complete the following Administrator Utility procedure:

1. Click the **Key Configuration** button.

   The Modify Client Key Configuration- Configure Keys screen is displayed.
2. Click the **Change the archive location** radio button, and then click **Next**.

   The Modify Client Key Configuration- New Key Archive Location screen is displayed.
3. Type the new path or click **Browse** to select the path.
4. Click **OK**.

   A message displays that the operation is complete.
5. Click **Finish**.

Changing the archive key pair

When the archive key pair is first created, it is usually stored on a diskette or network directory. If the archive key pair becomes damaged, you can change to a different archive key pair.

Note: Be sure to update the archive before changing the archive key pair.

To change the archive key pair, complete the following Administrator Utility procedure:

1. Click the **Key Configuration** button.

   The Modify Client Key Configuration- Configure Keys screen is displayed.
2. Click the **Change IBM Security Subsystem Archive key pair** radio button, and then click **Next**.

   The Modify Client Security Key Configuration - New UVM Administrator Public Key File screen is displayed.
3. In the New CSS Archive Key area, type the file name for the new archive public key in the Public Key File field. You can also click **Browse** to search for the new file, or click **Create** to generate a new archive public key.

Note: Make sure you create the new public key in a location other than that which contains the old archive key files.

4. In the New CSS Archive Key area, type the file name for the new archive private key in the Private Key File field. You can also click **Browse** to search for the new file, or click **Create** to generate a new archive key pair.

   Note: Make sure you create the new key pair in a location other than that which contains the old archive key files.

5. In the Old CSS Archive Key area, type the file name for the old archive public key in the Public Key File field, or click **Browse** to search for the file.
6. In the Old CSS Archive Key area, type the file name for the old archive private key in the Private Key File field, or click **Browse** to search for the file.
7. In the Archive Location area, type the file path where the key archive is stored, or click **Browse** to select the path.
8. Click **Next**.

   Note: If the archive key pair was split into multiple files, a message is displayed that asks you to type in the location and name of each file. Click **Read Next** after you type each file name in the Key File field.

   A message displays that the operation completed successfully.
9. Click **OK**.

   A message displays that the operation is complete.
10. Click **Finish**.

Restoring keys from archive

You might need to restore keys if you have replaced a system board or a failed hard disk drive. When you restore keys, you are copying the most recent user key files from the key archive and storing them on the IBM embedded Security Chip. These copied user key files appear in the directory where they were previously stored on the computer, such as on a network directory or diskette.

If a hard disk drive failure in the computer compromises the integrity of the user keys, you can restore the keys from the key archive. Restoring the keys will overwrite any keys that have been stored.

If you replace the system board in your computer with a system board that contains the IBM embedded Security Chip, and the encryption keys are still valid on your hard disk drive, you can restore the encryption keys that were previously associated with the computer by "re-encrypting" them with the IBM embedded Security Chip on the new system board.

You perform a key restoration after you have enabled the new chip and set a Security Chip password. For details, see "Enabling the IBM embedded Security Chip and setting a Security Chip password" on page 43.

Note: UVM logon gets enabled automatically after a key restoration. Consequently, if you had fingerprint authentication required for UVM logon, you MUST install the fingerprint software before rebooting after a restore to avoid being locked out of the system.

The following instructions assume that the Administrator Utility has not been damaged by a hard disk drive failure. If a hard disk drive failure has damaged the client security files, you might need to reinstall Client Security Software.

To restore encryption keys from a key archive, complete the following Administrator Utility procedure:

Note: If you change the administrator key pair after you restore the archive, an error message displays. If this occurs, you must add the users to UVM, and then request new certificates.

1. Click the **Key Configuration** button.

   The Modify Client Key Configuration- Configure Keys screen is displayed.
2. Click the **Restore IBM Security Subsystem keys from archive** radio button, and then click **Next**.

   The Modify Client Key Configuration- Restore All IBM Security Subsystem Keys screen is displayed.
3. In the Archive Directory (Path) field, type the file path of the archive directory, or click **Browse** to search for the directory.
4. In the CSS Archive Public Key File field, type the path and file name of the administrator public key, or click **Browse** to search for the file.
5. In the CSS Archive Private Key File field, type the path and file name of the administrator private key, or click **Browse** to search for the file.
6. Click **Next**.

   A message is displayed indicating that the operation completed successfully.

   Note: If the administrator private key was split into multiple files, a message is displayed that asks you to type in the location and name of each file. Click **Read Next** after you type each file in the Key File field.
7. Click **OK**.
8. Click **Finish**.

Resetting the authentication fail counter

To reset the authentication fail counter for a user, complete the following Administrator Utility procedure:

1. In the Windows users authorized to use UVM area, select a user.
2. Click **Reset Fail Count**.

   The Reset fail count for User screen is displayed.
3. Type the UVM passphrase for the user selected, and then click **OK**.

   A message is displayed that notifies you that the operation was successful.
4. Click **OK**.

Changing Tivoli Access Manager setting information

The following information is intended for security administrators who plan to use Tivoli Access Manager to manage authentication objects for the UVM security policy. For more information, see *Using Client Security with Tivoli Access Manager*.

Accessing the Tivoli Access Manager configuration file

To configure Tivoli Access Manager setup information on the IBM client, Client Security Software uses a configuration file. This configuration file is used to link

Tivoli Access Manager with the objects that UVM policy cedes to its control. To access the Tivoli Access Manager configuration, complete the following Administrator Utility procedure:

1. Click the **Configure Application Support and Policy** button.

   The UVM Application and Policy Configuration screen is displayed.
2. In the Tivoli Access Manager Setup Information area, type the path and file name of the configuration file, or click **Browse** to search for the file.
3. Click the **Edit Policy** button.
4. Continue with the edit policy procedure.

Refreshing the local cache

A local replica of security policy information as managed by Tivoli Access Manager is maintained at the IBM client. You can set the refresh rate of the local cache in increments of months and day, or you can click a button to immediately update the local cache.

To set or refresh the local cache, complete the following Administrator Utility procedure:

1. Click the **Configure Application Support and Policy** button.

   The UVM Application and Policy Configuration screen is displayed.
2. In the Local Cache Refresh Interval area, do one of the following:
   - To refresh the local cache now, click **Refresh Local Cache**.
   - To set the refresh rate, type the number of months and days in the fields provided. The months and days value represent the amount of time between scheduled refreshes.

Recovering a UVM passphrase

A UVM passphrase is created for each user that is authorized by the security policy for the IBM client. Because passphrases can be lost or forgotten, or can be changed by the client user, the Administrator Utility enables an administrator to recover a lost or forgotten passphrase.

To recover a passphrase, complete the following Administrator Utility procedure:

1. Select a user from the Windows Users Authorized to use UVM field.
2. Click the **Change Passphrase** button.

   The Change Passphrase screen is displayed.
3. In the IBM Security Subsystem Archive Location field, type the path and directory name of the key archive, or click **Browse** to locate the directory.
4. In the IBM Security Subsystem Archive Key area, type the path and file name for the private key in the Private Key file field, or click **Browse** to locate the file.
5. In the IBM Security Subsystem Archive Key area, type the path and file name for the administrator public key in the Public Key file field, or click **Browse** to locate the file.
6. Click **OK**.

   A message is displayed that shows you the UVM passphrase for the user.
7. Click **OK**.

If the administrator private key was split into multiple files, a message is displayed that asks you to type in the location and name of each file. Click **Read Next** after you type each file in the Private Key File field.

This procedure will produce a random temporary password and a password file. Both of these elements are necessary to regain access to the locked system.

8. Send the file to the user, and communicate the temporary password by some other means.

Changing the IBM Security Chip password

You must set a Security Chip password to enable the IBM embedded Security Chip for a client. After you set a Security Chip password, access to the Administrator Utility is protected by this password. For improved security, you should change the Security Chip password periodically. A password that remains unchanged for a long period of time can be more vulnerable to outside parties. Protect the Security Chip password to prohibit unauthorized users from changing settings in the Administrator Utility. For information on the rules of the Security Chip password, see Appendix B, "Password and passphrase information," on page 69.

To change the Security Chip password, complete the following Administrator Utility procedure:

1. Click the **Chip Settings** button.

   The Modify IBM Security Chip Settings screen is displayed.
2. Click **Change chip password**.

   The Change IBM Security Chip password screen is displayed.
3. In the New password field, type the new password.
4. In the Confirmation field, type the password again.
5. Click **OK**.

   A message is displayed that notifies you that the operation was successful.

   Attention: Do not press Enter or Tab > Enter to save the changes. If you do, the Disable chip screen will display. If the Disable chip window opens, do not disable the chip; instead, exit the screen.
6. Click **OK**.

Viewing information about Client Security Software

The following information about the IBM embedded Security Chip and Client Security Software is available by clicking the **Chip Settings** button of the Administrator Utility:

- The version number of the firmware used with Client Security Software
- The encryption status of the embedded Security Chip
- The validity of the hardware encryption keys
- The status of the IBM embedded Security Chip

Disabling the IBM embedded Security Chip

The Administrator Utility provides a way to disable the IBM embedded Security Chip. Because the Security Chip password is required to start the Administrator Utility and disable the chip, protect the Security Chip password to prohibit unauthorized users from disabling the chip.

Important: Do not clear the IBM embedded Security Chip while UVM protection is enabled. If you do, you will be completely locked out of the system. To clear UVM protection, open the Administrator Utility and clear the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before UVM protection for the system logon is disabled.

To disable the embedded Security Chip, complete the following Administrator Utility procedure:

1. Click the **Chip Settings** button.
2. Click the **Disable Chip** button and follow the on-screen instructions.
3. If your computer has Enhanced Security enabled, you might have to type the administrator password that was set in the Configuration/Setup Utility to disable the chip.

To use the IBM embedded Security Chip and hardware encryption keys after the chip is disabled, the chip must be re-enabled.

Enabling the IBM embedded Security Chip and setting a Security Chip password

If you need to enable the IBM embedded Security Chip after the software has been installed, you can use the Administrator Utility to reset the Security Chip password and to set up new encryption keys.

You might need to enable the IBM embedded Security Chip to restore the key archive after a system board replacement or if you have disabled the chip.

To enable the chip and set a Security Chip password, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   A message is displayed that asks you to enable the IBM embedded Security Chip for the IBM client.
2. Click **Yes**.

   A message is displayed that asks you to restart the computer. You must restart the computer before the IBM embedded Security Chip will be enabled. If your computer has Enhanced Security enabled, you might need to type the administrator password that was set in the Configuration/Setup Utility to enable the chip.
3. Click **OK** to restart the computer.
4. From the Windows desktop, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   Because access to the Administrator Utility is protected by the Security Chip password, a message is displayed that asks you to type the Security Chip password.
5. Type a new Security Chip password in the New password field, and then type it again in the Confirmation field.
6. Click **OK**.

Enabling Entrust support

The IBM Embedded Security Chip works with Client Security Software to enhance Entrust security features. Enabling Entrust support on a computer with Client Security Software transfers Entrust software security functions to the IBM Security Chip.

Client Security Software will automatically find the entrust.ini file to enable Entrust support; however, if the entrust.ini file is not in the usual path, a dialog opens for the user to browse for the entrust.ini file. After the user locates and selects the file, Client Security can enable Entrust support. After clicking the **Enable Entrust support** check box, a reboot is necessary before Entrust will make use of the IBM Embedded Security Chip.

To enable Entrust support, complete the following procedure:

1. From the Windows desktop of the IBM client, click **Start > Settings > Control Panel > IBM Client Security Subsystem**.

   The Administrator Utility main window is displayed.
2. Click **Configure Application Support and Policies**.

   The UVM Application and Policy Configuration screen is displayed.
3. Select the **Enable Entrust support** check box.
4. Click **Apply**.

   The IBM Client Security Entrust Support screen is displayed with a message indicating that Entrust support is enabled.

Note: You must restart the computer for the changes to take effect.

Chapter 9. Instructions for the client user

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

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

Using UVM protection for the system logon

This section contains information about using UVM logon protection for the system logon. Before you can use UVM protection, it must be enabled for the computer.

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

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

Unlocking the client

To unlock a Windows client that uses UVM protection, complete the following procedure:

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

   The UVM passphrase window opens.

   Note: Although UVM recognizes multiple domains, your user password must be the same for all domains.
3. Type your UVM passphrase, and then click **OK** to access the operating system.

Notes:

1. If the UVM passphrase does not match the user name and domain entered, the UVM logon window opens again.
2. Depending on the UVM policy authentication requirements for the client, further authentication processes might also be required.

The Client Security screen saver

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

Setting up the Client Security screen saver

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

To set up the Client Security screen saver, complete the following procedure:

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

Client Security screen saver behavior

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

If this box has been selected, the system requires either the Windows password or the UVM passphrase, depending upon whether the **Replace the standard Windows logon with UVM's secure logon** check box has been selected in the Administrator Utility. If it has been selected, the system requires the UVM passphrase. If it has not been selected, the system requires the Windows password.

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

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

The User Configuration Utility

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

User Configuration Utility features

The User Configuration Utility enables the client user to do the following:

- **Update passwords and archive.** This tab enables you to perform the following functions:
  - **Change the UVM passphrase.** To improve security, you can periodically change the UVM passphrase.
  - **Update Windows password.** When you change the Windows password for a UVM-authorized client user with the Windows User Manager program, you must also change the password by using the IBM Client Security Software User Configuration Utility. If an administrator uses the Administrator Utility to change the Windows logon password for a user, all user encryption keys previously created for that user will be deleted, and the associated digital certificates will become invalid.

  - **Reset the Lotus Notes password.** To improve security, Lotus Notes users can change their Lotus Notes password.
  - **Update the key archive.** If you create digital certificates and want to make copies of the private key stored on the IBM embedded Security Chip, or if you want to move the key archive to another location, update the key archive.
- **Configure UVM sound preferences.** The User Configuration Utility enables you to select a sound file to be played at authentication success and failure.
- **User configuration.** This tab enables you to perform the following functions:
-
  - **Reset user.** This function enables you to reset your security configuration. When you reset your security configuration, all previous keys, certificates, fingerprints, etc. are erased.
  - **Restore user security configuration from archive.** This function enables you to restore settings from the archive. This is useful if your files have become corrupted or if you want to return to a previous configuration.
  - **Register with a CSS Roaming Server.** This function enables you to register this system with a CSS Roaming Server. Once the system is registered, you will be able to import your current configuration to this system.

User Configuration Utility Windows XP limitations

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

Windows XP Professional

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

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

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

Using the User Configuration Utility

To use the User Configuration Utility, complete the following procedure:

1. Click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings**.

   The IBM Client Security Software User Configuration Utility main screen is displayed.
2. Type the UVM passphrase for the client user who requires a UVM passphrase or Windows password change, and then click **OK**.
3. Select one of the following tabs:
   - **Update Passwords and Archive.** This tab enables you to change your UVM passphrase, update your Windows password in UVM, reset your Lotus Notes password in UVM, and update your encryption archive.
   - **Configure UVM Sounds.** This tab enables you to select a sound file to be played at authentication success and failure.
   - **User Configuration.** This tab enables a user to restore his user configuration from archive or reset his security configuration.
4. Click **OK** to exit.

Using secure e-mail and Web browsing

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

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

Using Client Security Software with Microsoft Applications

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

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

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

Obtaining a digital certificate for Microsoft applications

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

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

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

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

Transferring certificates from the Microsoft CSP

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.

To run the Certificate Transfer Tool, complete the following procedure:

1. Run the `xfercert.exe` program from the root directory of the security software (usually C:\Program Files\IBM\Security). The main dialog displays certificates associated with the default Microsoft software CSP.

   Note: Only certificates whose private keys were marked as *exportable* when created will be displayed in this list.
2. Select the certificates that you want transferred to the IBM embedded Security System CSP.
3. Press the **Transfer Certificates** button.

The certificates are now associated with the IBM embedded Security System CSP, and the private keys are protected by the IBM embedded Security Chip. Any operations using these private keys, such as creating digital signatures or decrypting e-mail, will be done within the protected environment of the chip.

Updating the key archive for Microsoft applications

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

Using the digital certificate for Microsoft applications

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

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

Configuring UVM sound preferences

The User Configuration Utility enables you to configure sound preferences using the provided interface. To change the default sound preferences, complete the following procedure:

1. Click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings**.

   The IBM Client Security Software user Configuration Utility screen is displayed.
2. Select the **Configure UVM Sounds** tab.
3. In the UVM Authentication Sounds area, type the file path to the sound file that you would like to associate with a successful authentication in the Authentication success field, or click **Browse** to select the file.
4. In the UVM Authentication Sounds area, type the file path to the sound file that you would like to associate with an unsuccessful authentication in the Authentication failure field, or click **Browse** to select the file.
5. Click **OK** to complete the process.

Chapter 10. 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. Rules for using UVM protection for system logon

UVM protection ensures that only those users who have been added to UVM for a specific IBM client are able to access the operating system. Windows operating systems include applications that provide logon protection. Although UVM protection is designed to work in parallel with those Windows logon applications, UVM protection does differ by operating system.

The UVM logon interface replaces the operating system logon, so that the UVM logon window opens each time a user tries to log on to the system.

Read the following tips before you set and use UVM protection for the system logon:

- Do not clear the IBM embedded Security Chip while 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.
- If you clear the **Replace the standard Windows logon with UVM's secure logon** check box in the Administrator Utility, the system returns to the Windows logon process without UVM logon protection.
- You have the option of specifying the maximum number of attempts allowed for typing the correct password for the Windows logon application. This option does *not* apply to UVM logon protection. There is no limit that you can set for the number of attempts allowed for typing the UVM passphrase.

Appendix D. 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