IBM Client Security Solutions

Client Security Software Version 1.0 Administrator's Guide

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 59 and "Appendix C - Notices and Trademarks," on page 61.

First Edition (December 1999)

Table of Contents

About this Guide

The guide contains information to help you install and use Client Security Software on IBM networked computers that have the IBM embedded Security Chip. Throughout this document, these computers are referred to as *IBM clients*.

Instructions for enabling the embedded Security Chip and setting the hardware password for the security chip are included.

The guide is organized as follows:

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

“Chapter 2 - Setting up client security,” contains instructions for enabling the IBM embedded Security Chip and installing Client Security Software on the IBM clients on your network.

“Chapter 3 - Using UVM to set up security policy,” contains instructions for creating new users who want to use the features provided by Client Security Software. Also, instructions for setting up UVM logon protection for the system is included.

“Chapter 4 - Using other features of the Administrator Utility,” contains instructions for using the many features provided by the Administrator Utility.

“Chapter 5 - Instructions for the client user,” contains instructions for different tasks that the client user performs when using Client Security Software. Instructions for using UVM logon protection, the Client Security screen saver, secure e-mail and the Client Utility are included. This information is also provided in the *Client Security User’s Guide*.

“Chapter 6 - Troubleshooting,” contains administrator tips, known limitations and troubleshooting information associated with Client Security Software.

“Appendix A - U.S. export regulations for Client Security Software,” contains information about U.S. export regulations about the software.

“Appendix B - Rules for the hardware password and the UVM passphrase,” contains a description of the rules for the UVM passphrase and hardware password.

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

How to use this guide

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

Quick start

To quickly install and set up Client Security Software on multiple IBM clients, do the following:

1. Read “Chapter 1 - Introducing IBM Client Security Software,” on page 7.

2. Go to "Chapter 2 - Setting up client security," on page 10, and enable the IBM embedded Security Chip and install the software on the IBM clients on your network.
3. Go to "Chapter 3 - Using UVM to set up security policy," on page 26, to set up the security policy for the users of each IBM client.
4. Inform client users of the *Client Security User's Guide* provided on the World Wide Web. The *Client Security User's Guide* contains instructions on how the client user can use the features provided by Client Security Software (see the following section for more information).

Compare to the Client User's Guide

As an administrator, you use this guide to enable the IBM embedded Security Chip and install, set up, and maintain the Client Security Software on IBM clients. After you set up Client Security Software, the client user can read the *Client Security User's Guide* to learn how to use the features provided by Client Security Software. The *Client Security User's Guide* is a companion to this guide and contains information that a client user will find helpful when performing tasks with Client Security Software, such as using UVM logon protection and the screen saver, creating a digital certificate, and using the Client Utility. The *Client User's Guide* is available for download from the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html

Note: Most of the information provided in the *Client User's Guide* is also provided in this guide.

Conventions used in this guide

This guide uses several typeface conventions that have the following meaning:

- **Bold -** Commands, keywords, authorization roles, and other information that you must use literally appear in **bold**.
- *Italics* - Variables and values that you must provide appear in *italic*s. Words and phrases that are emphasized also appear in *italic*s.
- `Monospace` **-** Code examples, output, and system messages appear in `monospace`.

Chapter 1 - Introducing IBM Client Security Software

Client Security Software consists of software applications and components that enable IBM® clients to use client security across a local network, an enterprise, or the Internet. Client Security Software provides many of the components required to create a public key infrastructure (PKI) in your business, including:

- **Encryption key management for public key cryptography**[1]. Client Security Software is designed for IBM computers that use the IBM embedded Security Chip to encrypt and store encryption keys. You create the 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 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, for Netscape users, you can choose the IBM embedded Security Chip as the generator of the private key for digital certificates used for security. Applications such as Netscape Messenger that use Public-Key Cryptography Standard (PKCS) #11 can take advantage of the protection provided by the IBM embedded Security Chip.

  Note: For information on the specific applications that Client Security Software supports, see "Before you install the software," on page 10.
- **Administrator control over client security policy**. A concern of security policy at the client level is authenticating the end user. Client Security Software provides the interface and underlying software required to manage the security policy of the IBM client. This interface is part of the authenticating software User Verification Manager (UVM), the main component of Client Security Software.
- **A key archive and recovery solution**. An important function in a PKI is creating a key archive from which keys can be restored in the event that the original keys are lost or damaged. Client Security Software provides the interface that enables you to set up an archive for the keys and digital certificates (that you create with the IBM embedded Security Chip) and to restore the keys and certificates if necessary.

[1] Public key cryptography uses encryption keys that are issued in pairs. One is the public key; the other is the private key. Both keys are required to encrypt and decrypt information and are also used to identify and authenticate client users.

What software is installed?

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

- **Administrator Utility:** The Administrator Utility is the administrator interface you use to create encryption keys with the IBM embedded Security Chip in your computer. In addition, the Administrator utility enables you to add users to the security policy provided by Client Security Software.
- **User Verification Manager:** User Verification Manager (UVM) is software that enables you to set the security policy for the computer, which dictates how a client user is authenticated on the system. Client Security Software Version 1.0 uses the UVM passphrase to authenticate users to the system. Future versions of Client Security Software will include support for other authenticating devices, such as a fingerprint reader.
- **UVM logon protection:** UVM logon protection enables you to control access to the computer through a logon interface. UVM logon protection ensures that only those users who are recognized by the security policy of the computer are able to access the operating system.
- **Client Security screen saver:** The Client Security screen saver enables you to control access to the computer through a screen saver interface.
- **Client Utility:** The Client Utility enables a client user to change the UVM passphrase. For Windows NT users, the Client Utility enables a user to change the Windows NT logon password so that it is recognized by UVM.[2] Also, the user can update the key archive with the Client Utility. A user can create backup copies of the digital certificates created with the IBM embedded Security Chip by updating the key archive.
- **Support for the Microsoft CryptoAPI:** Support for Microsoft CryptoAPI is built into Client Security Software. Defined by Microsoft, CryptoAPI is used as the default cryptographic service for Microsoft operating systems and applications. With built-in CryptoAPI support, Client Security Software enables you to use the cryptographic operations of the IBM embedded Security Chip when you create digital certificates for Microsoft applications.
- **Support for PKCS#11:** Defined by RSA Data Security Inc., PKCS#11 is used as the cryptographic standard for Netscape and other products. After you install the IBM embedded Security Chip PKCS#11 module, you can use the IBM embedded Security Chip when you generate a digital certificate for Netscape applications and other applications that use PKCS#11.

[2] If you change the Windows NT logon through User Manager, you must also change the password in the Client Utility so that it is recognized by UVM logon protection. For details, see “Using the Client Utility,” on page 44.

Additional information

You can obtain additional information and security product updates, when available, from the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/index.html

Chapter 2 - Setting up client security

This section contains instructions for enabling the IBM embedded Security Chip and installing and setting up Client Security Software on IBM clients. All software components provided by Client Security Software are included within one installable file that you download from the IBM Web site.

Before you install the software

Before you download and install the software, make sure that your computer hardware, software, and operating system are compatible with Client Security Software. The compatibility information in this section is applicable to Client Security Software Version 1.0.

For the most recent information on hardware and software requirements, go to the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html

Supported hardware

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

Supported operating systems

Client Security Software is supported only on the following operating systems:

- Windows NT® 4.0 Workstation, with Service Pack 5 or later
- Windows® 98
- Windows 95, with OEM Service Release 2.5 or later[3]

Supported software

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

- Internet Explorer 4.01 with Service Pack 1a or Internet Explorer 5.0 or later (40 bit)
- Netscape 4.51 or 4.61 or later (40 bit)

To check the encryption strength of your Web browser, use the help system provided with the browser.

Client Security Software supports the following applications for using secure e-mail:

- E-mail applications that use the Microsoft CryptoAPI for cryptographic operations, such as Outlook Express and Outlook

[3] Windows 95 support for Client Security Software is not available for IBM PC 300PL (6584 and 6594) and IntelliStation M Pro (6868).

- E-mail applications that use Public Key Cryptographic Standard #11 (PKCS#11) for cryptographic operations, such as Netscape Messenger

Download the software

Client Security Software is available as a free download from the following IBM Web site:

http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html

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

All the setup files for Client Security Software are included within one self-extracting file called CSEC10WW.EXE.

Important: Client Security Software Version 1.0 contains encryption code that can be downloaded within North America and internationally. If you live in a country where downloading encryption software from a Web site in the United States is prohibited, you cannot download Client Security Software Version 1.0. For more information on the export regulations governing Client Security Software, see “Appendix A - U.S. export regulations for Client Security Software,” on page 59.

Installation instructions

This section details the instructions for installing Client Security Software on IBM clients. The installation program was designed to help you, the administrator, quickly do the following two things:

- Install Client Security Software
- Enable the security subsystem, which includes enabling the IBM embedded Security Chip, setting a hardware password, and generating the encryption keys and key archive for that client

To enable the security subsystem, you must have an admin public key. You create an admin public key when you create an admin key pair, which includes the admin public key and the admin private key.

When you install and set up the software on the first IBM client, you will use the installation program to install the software, but you will use the Administrator Utility to enable the security subsystem and to create the admin key pair. After you install and enable the first IBM client, you can use the installation program to quickly install the software and enable the security subsystem on other IBM clients.

Software installation and set up on the first IBM client

Use the following steps when you install and setup the software on the first IBM client.

1. Install the software on the first IBM client.
2. Use the Administrator Utility to enable the IBM embedded Security Chip and to set a hardware password.
3. Create an admin key pair.

4. Generate the hardware encryption keys and set up the key archive.

- **Install the software on the first IBM client**

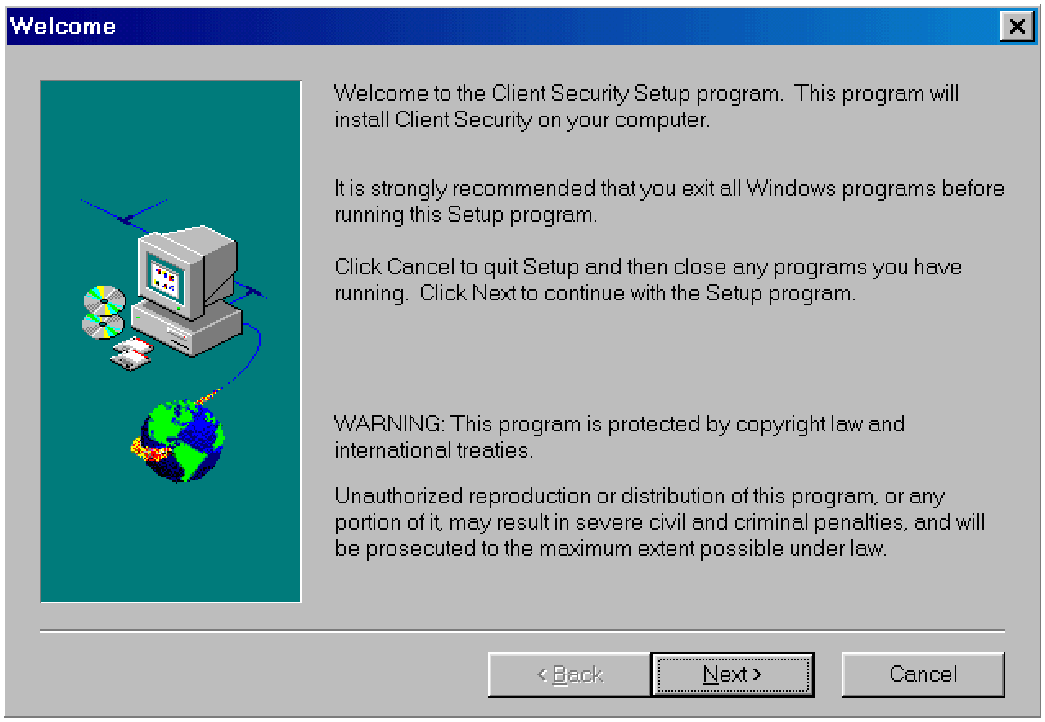
To install Client Security Software on the first IBM client:

1. Run CSEC10WW.EXE to unzip the setup files. When prompted, enter the path to the folder where you want the files to be copied. SETUP.EXE, the file that runs the installation program, is one of the files that will be stored in the folder you specify.
2. From the Windows desktop, click **Start** → **Run**.
3. In the **Run** field, type:

   d:\directory\\`setup.exe`

   where *d:* and *directory* are the drive letter and the directory where the setup file is located.
4. Click **OK**.

   The installation program opens the Welcome window, which warns you to exit from all Windows programs before you begin to install Client Security and notifies you of the copyright laws associated with Client Security Software.



Welcome

Welcome to the Client Security Setup program. This program will install Client Security on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program.

Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5. Click **Next**.

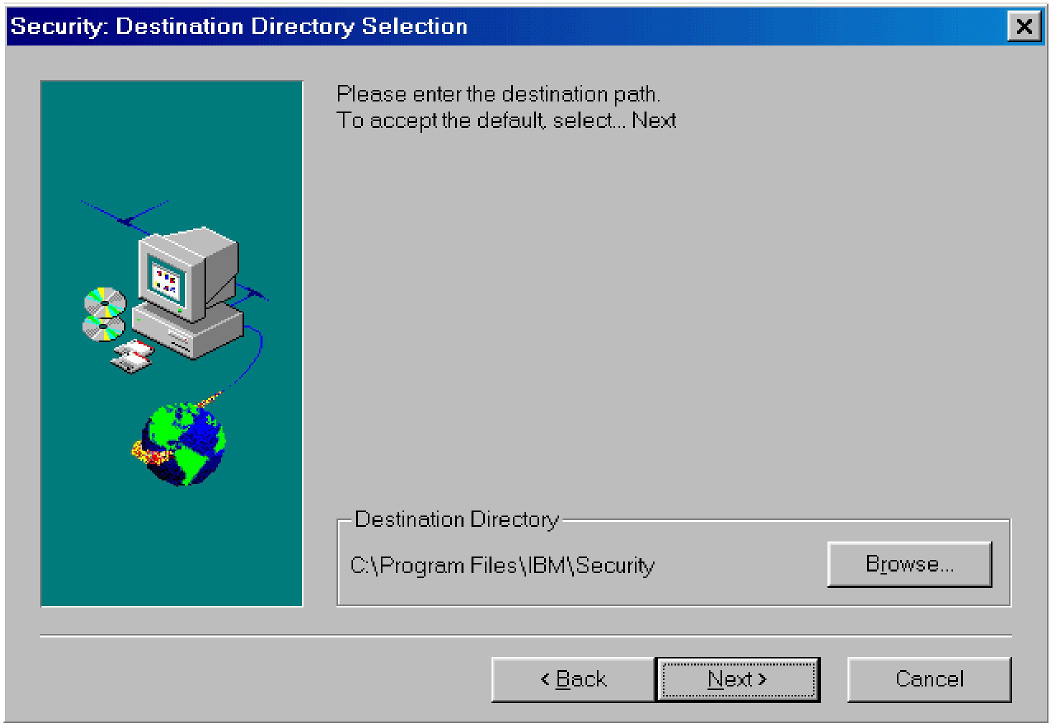
   The installation program opens the Select Language window. Select the language you want to use during installation.
6. Click **Next**.

   The installation program opens the License Agreement window.

7. Click **I Agree** to proceed.

   Note: You must agree to the terms of the License Agreement to install Client Security Software. If you click **I Disagree**, the installation program will close without installing Client Security Software.

   After you click **I Agree**, the Destination Directory Selection window opens.



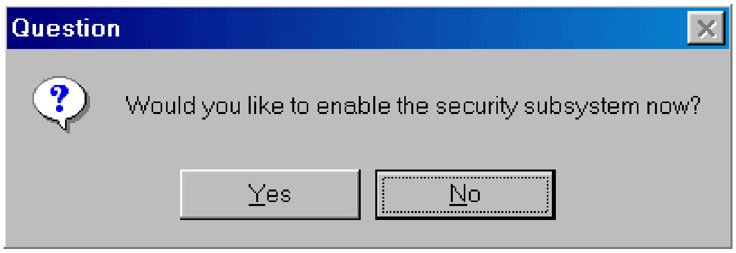
Security: Destination Directory Selection

Please enter the destination path.
To accept the default, select... Next

Destination Directory
C:\Program Files\IBM\Security

8. Click **Next** to accept the default directory, C:\Program Files\IBM\Security, or click **Browse** to choose a different directory, and then click **Next**.

9. A window opens that asks if you want to enable the security subsystem for the IBM client. You can enable the security subsystem with the installation program only if you know the location of the admin public key. Because you have not yet created the admin key pair, click **No**.



Question

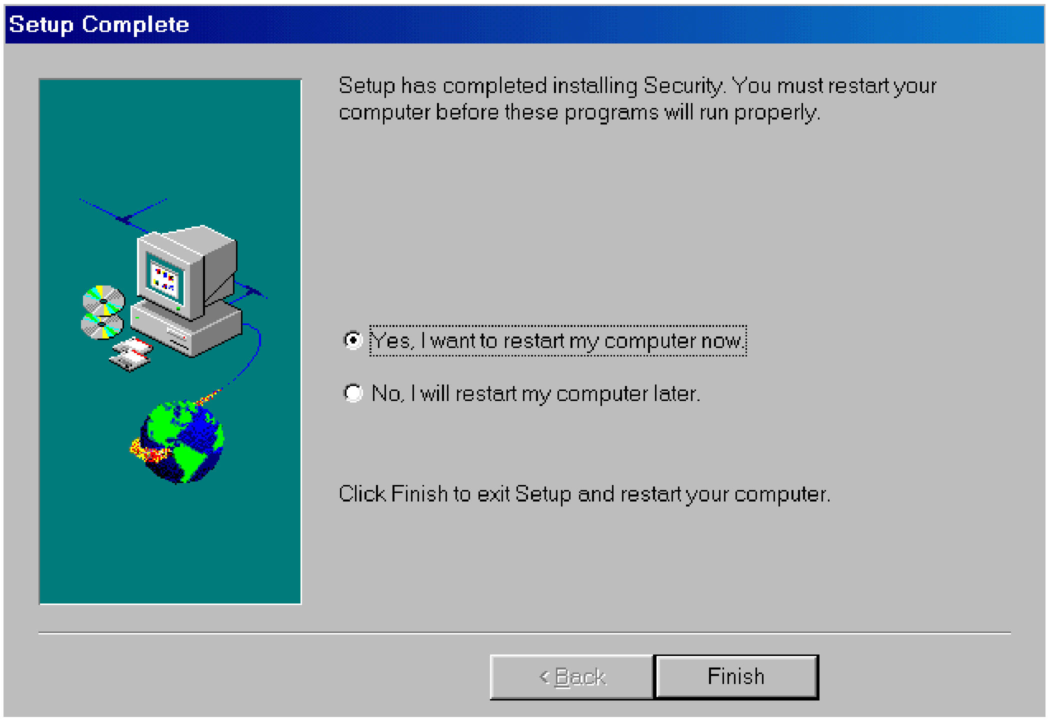
Would you like to enable the security subsystem now?

10. A window opens that notifies you that you must run the Administrator Utility to enable the security subsystem. Click **OK**.

    The installation program installs Client Security Software on the IBM client.

11. The Setup Complete window opens. You must restart the computer before Client Security Software will run properly.

Select **Yes, I want to restart my computer now** to restart the computer, or click **No, I will restart my computer later**; then click **Finish**.



Setup Complete

Setup has completed installing Security. You must restart your computer before these programs will run properly.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Click Finish to exit Setup and restart your computer.

12. After the computer restarts, go the next section to enable the IBM embedded Security Chip and to set a hardware password.

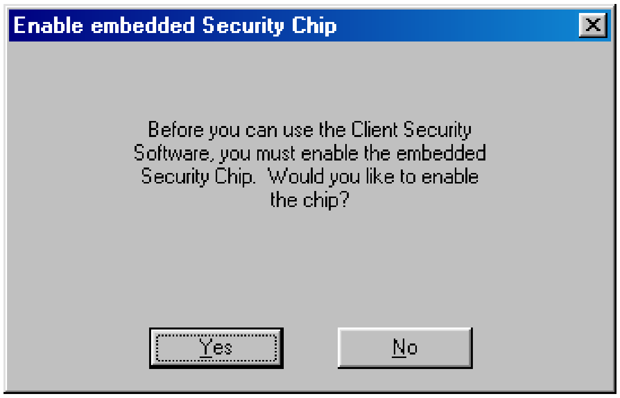
- **Use the Administrator Utility to enable the IBM embedded Security Chip and to set a hardware password**

After the software is installed on the client, use the Administrator Utility to enable the IBM embedded Security Chip and to set the hardware password.

From the Windows desktop, do the following:

1. Click **Start** → **Programs** → **Client Security Software Utilities** → **Administrator Utility**.

   The following window opens and asks you to enable the IBM embedded Security Chip for the IBM client.

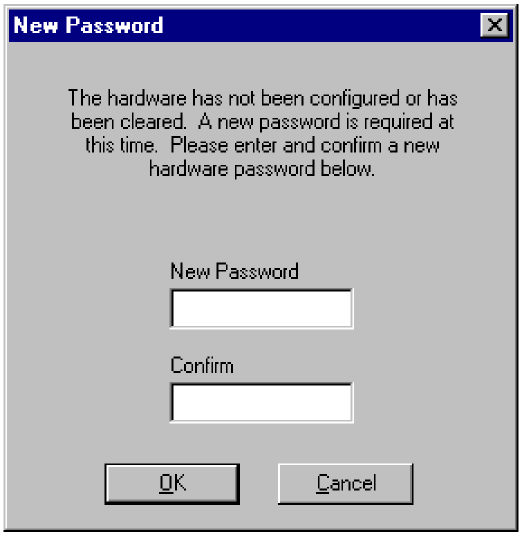


Enable embedded Security Chip

Before you can use the Client Security Software, you must enable the embedded Security Chip. Would you like to enable the chip?

2. Click **Yes**.
3. You must restart the computer before the IBM embedded Security Chip will become enabled. A window opens that asks you to restart the computer. Click **OK**.
4. After the computer restarts, from the Windows desktop, click **Start** → **Programs** → **Client Security Software Utilities** → **Administrator Utility**.

   Because access to the Administrator Utility is protected by the hardware password, the following window opens that asks you to type the hardware password.



New Password

The hardware has not been configured or has been cleared. A new password is required at this time. Please enter and confirm a new hardware password below.

New Password

Confirm

5. Type a new hardware password, and then type it again in the **Confirm** field. Click **OK**. The Administrator Utility window opens.

   For information on the rules for the hardware password, see "Appendix B - Rules for the hardware password and the UVM passphrase," on page 60.
6. Go to the next section to create an admin key pair.

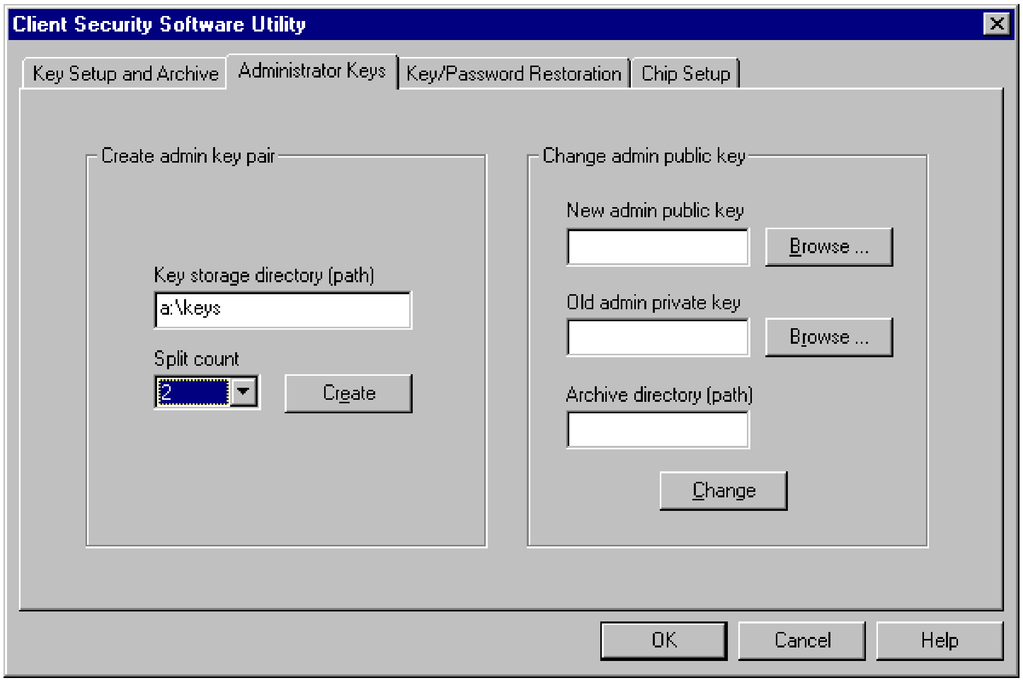
- **Create an admin key pair**

You use the admin key pair to create the hardware encryption keys for each client. In a network environment, you can create one instance of an admin key pair and store the admin public key on a shared directory or diskette so that it is accessible to the other clients on which you want to install Client Security Software.

To create an admin key pair:

1. Click the **Administrator Keys** tab.
2. In the **Key storage directory (path)** field, type the path (not the file names) where the admin key pair files will be stored. If you choose to store the admin key pair files on a diskette, insert a formatted diskette into the diskette drive.

Tip: Use a shared directory or diskette to store the admin public key so that it is accessible to you when you install and set up the software on other IBM clients. The following example shows that the admin keys will be stored on a diskette in the KEYS directory.



Key storage directory (path): a:\keys

Split count: 2

3. Do one of the following:

   - If you do not want to separate the admin private key into multiple files, select the number 1 from the drop-down list in the **Split count** field.

   - If you want to separate the admin private key into multiple files, select a number from 2 to 5 from the drop-down list in the **Split count** field.

   A note about splitting the admin private key: When you create the admin keys, the admin public key file (ADMIN.KEY) and one admin private key file (Private1.key) are always created. To enhance security when the admin private key is required, the admin private key can be split into two, three, four, or five files. The files are named Private2.key, Private3.key, Private4.key, and Private5.key, and they are stored in the same directory when they are created. If the admin private key is split, you can distribute the different files to other administrators (or other trusted parties), which forces all administrators to be present when the admin private key is required, for example to perform a key restoration. It is important that the admin private key files are stored in a safe place.

4. Click **Create**. A window opens that notifies you that the operation was successful. Click **OK**.

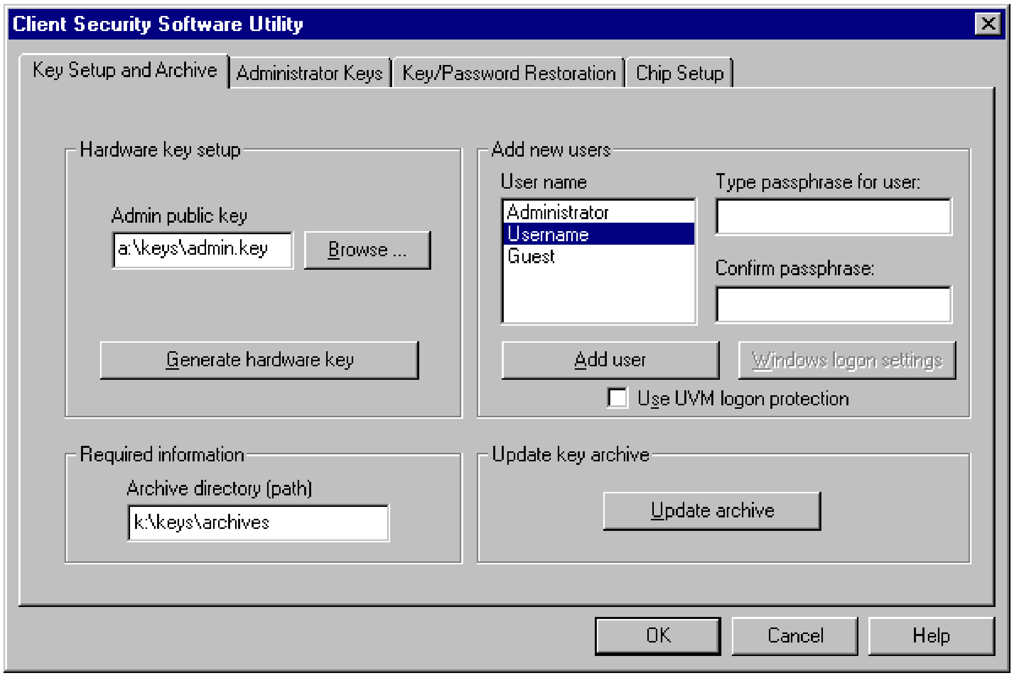
5. Go to the next section to generate the hardware encryption keys and to set up the key archive.

- **Generate the hardware encryption keys and set up the key archive**

The hardware encryption keys are the base keys that are created and stored on the IBM embedded Security Chip. You must generate the hardware keys before you can use the IBM embedded Security Chip for cryptographic operations, such as creating a digital certificate that can be used for digital signatures or encryption.

To create the hardware keys and setup the key archive:

1. Click the **Key Setup and Archive** tab.
2. In the **Admin public key** field, type the path and file name of the admin public key or click **Browse** to search for the file. The following example shows that ADMIN.KEY is stored on a diskette in the KEYS directory. If you stored ADMIN.KEY on a diskette, insert the diskette into the diskette drive.



Admin public key: a:\keys\admin.key

User name: Administrator, Username, Guest

☐ Use UVM logon protection

Archive directory (path): k:\keys\archives

3. In the **Required information** area, type the path (not the file name) where the key archive will be stored. Store the archive on a network directory or diskette. The previous example shows that the archive will be stored on a network directory, K:\KEYS\ARCHIVES.

   Note: Because a hard disk drive failure can damage files, do not store the key archive on a local drive.

4. Click **Generate hardware key**. A window opens that notifies you that the operation was successful. Click **OK**.

   The hardware keys are generated for the client and copies of the keys are stored in the archive.

   Notes:

   - When you create a key archive for a client, a subdirectory is automatically created that is named the same as the computer name. For example, if the computer name is CLIENT1, all archived keys for that computer would be stored in the subdirectory named CLIENT1. If you had typed in the path in the previous example, the archived files would be stored in K:\KEYS\ARCHIVES\CLIENT1.

- If hardware keys exist for an IBM client and you choose to generate hardware keys again for that client, any existing user keys and digital certificates associated with the IBM embedded Security Chip will become invalid.

This completes the installation and setup of Client Security Software on the first IBM client.

Next, you can do one of the following:

- Go to “Chapter 3 - Using UVM to set up security policy,” on page 26 to set up the security policy for the IBM client. You must set up the security policy before you can use the IBM embedded Security Chip for creating digital certificates or before you can use client authentication on the computer.
- Go to the next section and use the installation program to install the software, enable the IBM embedded Security Chip, set a hardware password, and generate the hardware encryption keys on other IBM clients.

Software installation and set up on other IBM clients

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

Note: The following instructions describe an attended installation, an installation where you physically reside at the computer during installation. For information on performing an unattended installation, see “Using the unattended installation option” on page 21.

To install and set up the software on other IBM clients:

1. Go to the next IBM client and run CSEC10WW.EXE to unzip the setup files. When prompted, enter the path to the folder where you want the files to be copied. SETUP.EXE, the file that runs the installation program, is one of the files that will be stored in the folder you specify.

   Tip: Copy the admin public key (ADMIN.KEY) to the same directory where you unzip the setup files. This will save you a step during installation.

2. From the Windows desktop, click **Start** → **Run**.
3. In the **Run** field, type:

   d:\directory\\`setup.exe`

   where *d:* and *directory* are the drive letter and the directory where the Client Security Software setup file is located.

4. Click **OK**.

   The installation program opens the Welcome window, which warns you to exit from all Windows programs before you begin to install Client Security and notifies you of the copyright laws associated with Client Security Software.

5. Click **Next**.

The installation program opens the Select Language window. Select the language you want to use during installation.

6. Click **Next**.

   The installation program opens the License Agreement window.

7. Click **I Agree** to proceed.

   Note: You must agree to the terms of the License Agreement to install Client Security Software. If you click **I Disagree**, the installation program will close without installing Client Security Software.

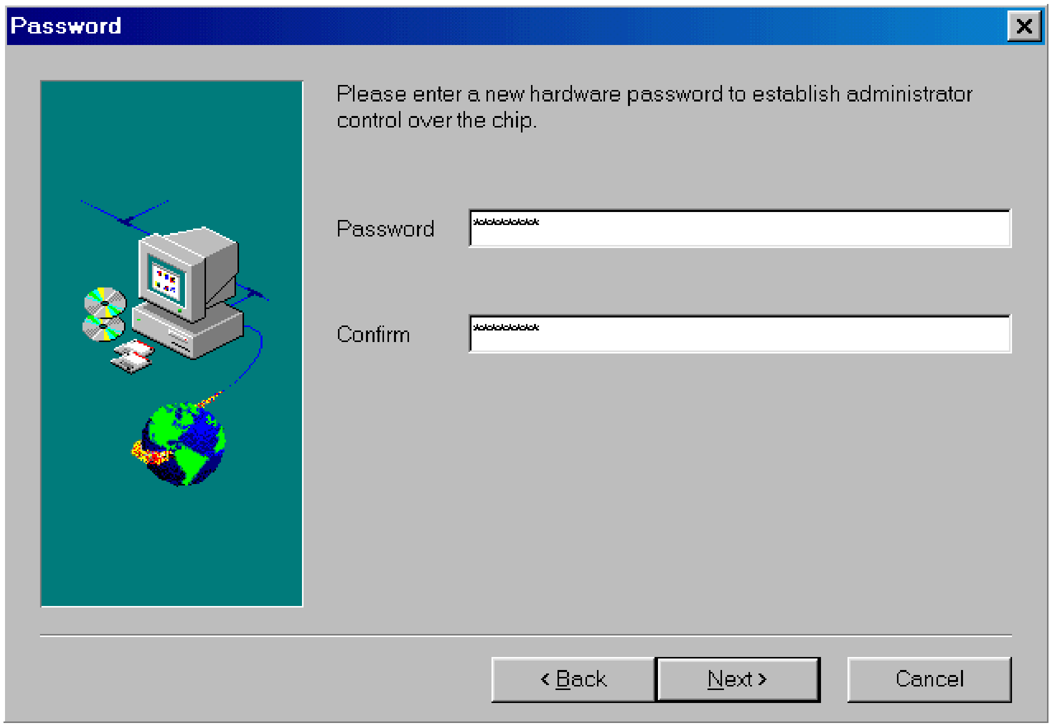
   After you click **I Agree**, the Destination Directory Selection window opens.

8. Click **Next** to accept the default directory, C:\Program Files\IBM\Security, or click **Browse** to choose a different directory, and then click **Next**.

   The installation program installs Client Security Software on the IBM client.

9. A new window opens that asks if you want to enable the security subsystem for the IBM client. Click **Yes**.

   The Password window opens.



Please enter a new hardware password to establish administrator control over the chip.

Password *********

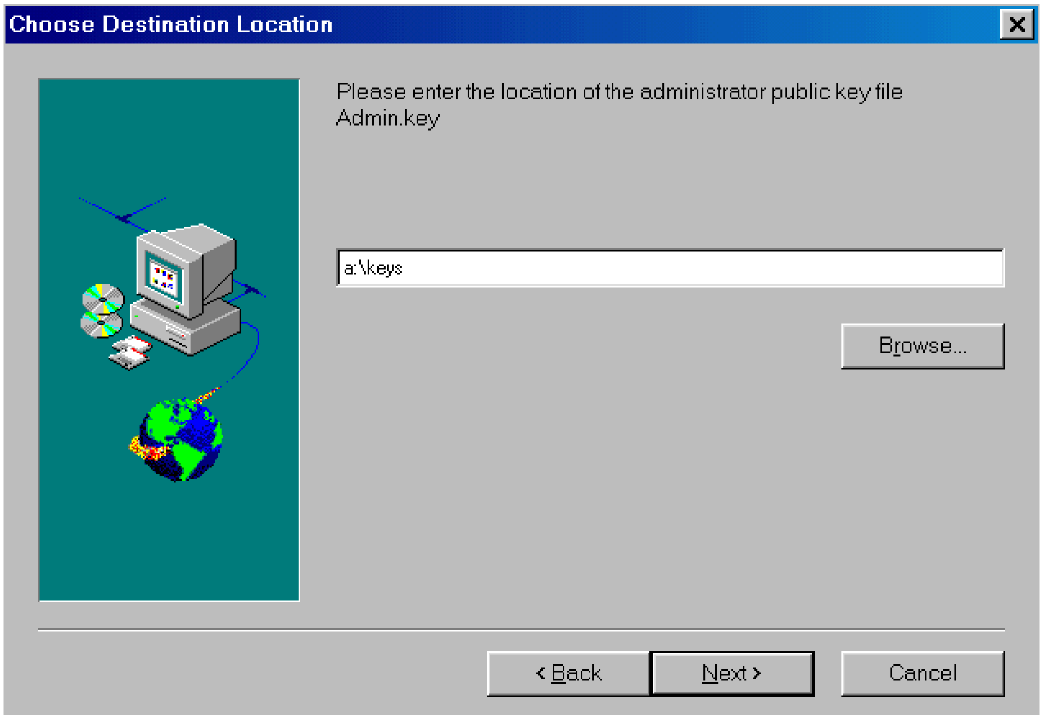
Confirm *********

10. In the **Password** field, type a hardware password. Next, in the **Confirm** field, type the password again to confirm it. Click **Next** to proceed to the next window.

    For information on the rules for the hardware password, see "Appendix B - Rules for the hardware password and the UVM passphrase," on page 60.

11. If you stored the ADMIN.KEY file in the same directory as SETUP.EXE, the installation program automatically detects the admin public key file, and you do not need to provide the file name. Skip to step 12.

If the Choose Destination Location window opens, type the path to ADMIN.KEY or click **Browse** to search for the directory, and then click **Next**.



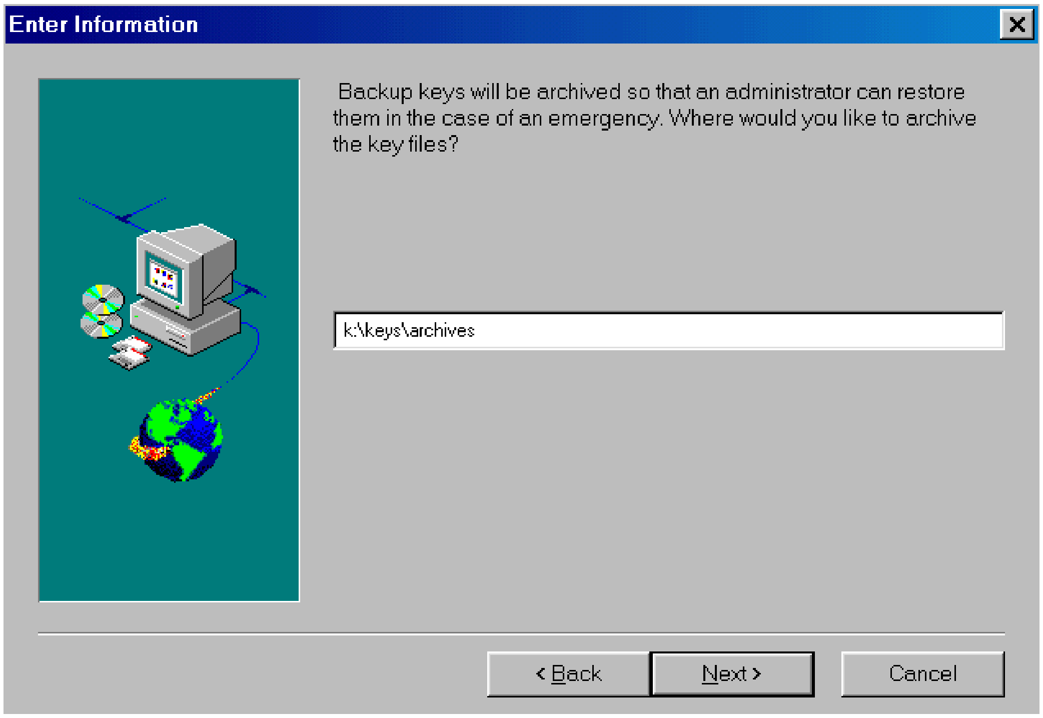
Choose Destination Location

Please enter the location of the administrator public key file Admin.key

a:\keys

12. The Enter Information window opens and asks you where you would like to archive the key files. Type the path and directory to the key archive, and then click **Next** to install Client Security Software on the IBM client.

    Note: The path and directory will be created by the installation program if it does not exist.



Enter Information

Backup keys will be archived so that an administrator can restore them in the case of an emergency. Where would you like to archive the key files?

k:\keys\archives

13. The Setup Complete window opens and asks you to restart the computer. Select **Yes, I want to restart my computer now** to restart the computer, or click **No, I will restart my computer later**.

    Note: You must restart the computer before Client Security Software will run properly.

14. Click **Finish**.

Next, you can do one of the following:

- Go to "Chapter 3 - Using UVM to set up security policy," on page 26 to set up the security policy for the IBM client.
- Repeat the steps in this section to install and set up the software on other IBM clients by exclusively using the installation program.

Using the unattended installation option

The unattended installation option enables you to install Client Security Software without being present at the computer to enter information during installation.

Note: To perform an unattended installation, you must have an admin public key (ADMIN.KEY). You create the admin key pair during the installation of Client Security Software on the first IBM client. If the ADMIN.KEY file you use is stored on a diskette, copy it to the hard disk of the IBM client or to a shared network directory so that it is available for the unattended installation.

To use the unattended installation option:

1. Run CSEC10WW.EXE on the IBM client to unzip the setup files. When prompted, enter the path to the folder where you want the files to be copied. Note that SETUP.EXE and SETUP.ISS are stored in the folder you specify.

2. Open the SETUP.ISS file in a text editor such as Notepad. The SETUP.ISS file is shown below.

```
[InstallShield Silent]
Version=v3.00.000
File=Response File

[Application]
Name=Client Security Software
Version=1.0 Beta
Company=IBM

[DlgOrder]
Dlg0=Welcome-0
Count=7
Dlg1=AskDestPath-0
Dlg2=AskYesNo-0
Dlg3=SdShowUserAndPassword-0
Dlg4=AskText-0
Dlg5=AskPath-0
Dlg6=SdFinishReboot-0

[Welcome-0]
Result=1

[AskDestPath-0]
szPath=C:\Program Files\IBM\Security
Result=1

[AskYesNo-0]
Result=1

[SdShowUserAndPassword-0]
svPassword=password
Result=1

[AskText-0]
szText=C:\Program Files\IBM\Security
Result=1

[AskPath-0]
szPath=C:\Program Files\IBM\Security
Result=1

[SdFinishReboot-0]
Result=1
BootOption=1
```

3. If desired, edit the SETUP.ISS file as shown below in bold and save the file. All bold entries are examples only. You can run the unattended installation without changing any values in SETUP.ISS, but make sure that the path to the ADMIN.KEY file is correct.

```
[InstallShield Silent]
Version=v3.00.000
File=Response File

[Application]
Name=Client Security Software
Version=1.0 Beta
Company=IBM

[DlgOrder]
Dlg0=Welcome-0
Count=7
Dlg1=AskDestPath-0
Dlg2=AskYesNo-0
Dlg3=SdShowUserAndPassword-0
Dlg4=AskText-0
Dlg5=AskPath-0
Dlg6=SdFinishReboot-0

[Welcome-0]
Result=1

[AskDestPath-0]
szPath=C:\MySecurity
Result=1

[AskYesNo-0]
Result=1

[SdShowUserAndPassword-0]
svPassword=12345678
Result=1

[AskText-0]
szText=C:\keydir
Result=1

[AskPath-0]
szPath=K:\keys\archives
Result=1

[SdFinishReboot-0]
Result=1
BootOption=1
```

Notes:

- szPath=C:\MySecurity designates where Client Security Software will be installed.
- svPassword=12345678 assigns the hardware password for the IBM embedded Security Chip as "12345678." You can assign any hardware password you want, as long as it adheres to the rules for the hardware password. For information on the rules for the hardware password, see "Appendix B - Rules for the hardware password and the UVM passphrase," on page 60.

- szText=C:\keydir designates the path to the ADMIN.KEY file. For the unattended installation to run properly, ADMIN.KEY must be in the specified path on the client hard disk or on a shared network directory. If the ADMIN.KEY file you use is stored on a diskette, copy it to the client hard disk or to a shared network directory so that it is available for the unattended installation.
- szPath= K:\keys\archives designates the path where the keys are archived. For the unattended installation to run properly, do not store the key archive on a diskette. If you want to store the key archive on a diskette, store the key archive on the client hard disk or a shared network directory during the unattended installation, and then copy it to a diskette after the installation is complete.[4]

4. From the Windows desktop, click **Start** → **Run**.
5. Type the path to SETUP.EXE, and add [space]-s to the path (for example, `C:\Security\setup.exe -s`). All files will be installed in the path specified for szPath, and the computer will restart.

Uninstalling Client Security Software

You can use the operating system feature Add/Remove Programs to uninstall Client Security Software.

To uninstall Client Security Software:

1. Click **Start** → **Settings** → **Control Panel**.
2. Click the **Add/Remove Programs** icon.
3. In the list of software that can be automatically removed, select **IBM Client Security**.
4. Click **Add/Remove....**
5. Click **Yes** to uninstall the software.
6. Click **OK** after the software is removed. You must restart the computer after uninstalling Client Security Software.

When you uninstall Client Security Software, you are removing only the software components that were installed. Any encryption keys that you created remain stored on the IBM embedded Security Chip. Also, the key archive is not affected when Client Security Software is removed from an IBM client.

[4] Hard disk failures can damage files; store key archive files on hard disks on a temporary basis only.

Chapter 3 - Using UVM to set up security policy

When you set up security policy on an IBM client, you create a means by which users that are recognized by the operating system can be authenticated through Client Security Software. The software component of Client Security Software that enables authentication in the IBM client is User Verification Manager (UVM).

In Version 1.0 of Client Security Software, the element of authentication that UVM uses when authenticating users is the UVM passphrase. When you add a user to the security policy of an IBM client, encryption keys for that user are created and a UVM passphrase is assigned to that user. Users must then type their UVM passphrase to perform cryptographic operations with the security hardware, such as creating an e-mail digital certificate.

Future versions of Client Security Software will include support for other devices of authentication such as a fingerprint reader. These authentication devices will interact with the UVM passphrase to provide another level of security when user authentication is required.

Use the operating-system software to create new users

Client Security Software uses features of the operating system that identify which users can access the computer. For example, when you want to create user keys for a user (also called adding a user), Client Security Software provides you with a list of user names to choose from. The names in this list are the user accounts that have been added by using the operating system.

Before you set up security policy with Client Security Software, use the operating-system software to create user accounts and profiles. The following list describes the programs or procedures you can use to add new users for the respective operating system.

- **Windows NT Workstation 4.0**. Use the User Manager program to create new user accounts and manage user accounts or groups. See the operating system documentation for more information.
- **Windows 95 and Windows 98**. New users can be added by typing in a new user name and password in the logon application. See the operating system documentation for more information.

  Notes:

  - In Windows 98, if you delete a user from the computer, the user name is not deleted from the list of users in the Administrator Utility.
  - When you use the operating system software to add new users, the domain password for each new user must be the same.
  - Client Security Software works in parallel with the security features provided by the operating system.

Add a user to the security policy

When you add a user to the security policy set up by Client Security Software, you create the following:

- **user encryption keys** for that client user. All user encryption keys are stored in a single file that is managed by the IBM embedded Security Chip.
- a **UVM passphrase** for that client user. Client Security Software uses the UVM passphrase to authenticate the users before they can perform cryptographic operations with the IBM embedded Security Chip, such as create a digital certificate. In future versions of Client Security Software, you can set up other authenticating devices, such as a fingerprint reader, in combination with the UVM passphrase to authenticate client users to the system.

After you a add a user, you can set up the following features that are provided by Client Security Software:

- **UVM logon protection** for the IBM client. UVM logon protection ensures that only those users who are recognized by the security policy set for the computer are able to access the computer.

  Important: UVM logon protection differs by operating system. For Windows NT, 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. For Windows 98 and Windows 95, UVM logon protection uses the Client Security screen saver to secure the logon. For more information about using UVM logon protection, see “Using UVM logon protection,” on page 42.

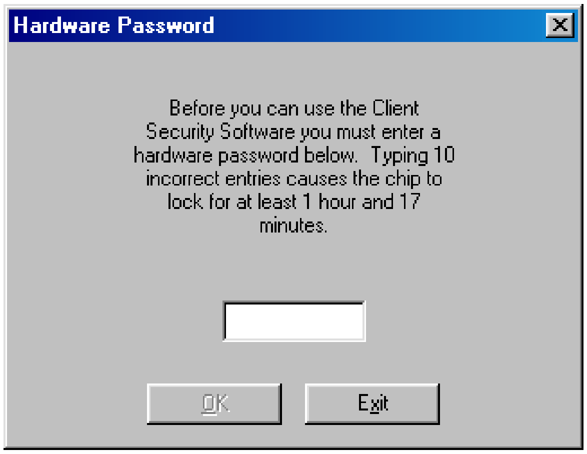
- **Client Security screen saver**. After you create a new user, the user can set up and use the Client Security screen saver provided by Client Security Software. The Client Security screen saver is set up through the Display feature provided by the operating system. For more information, see “Setting up the Client Security screen saver,” on page 44.

  Note: You do not need to set up UVM logon protection to use the Client Security screen saver.

To add a new user to the security policy for the computer:

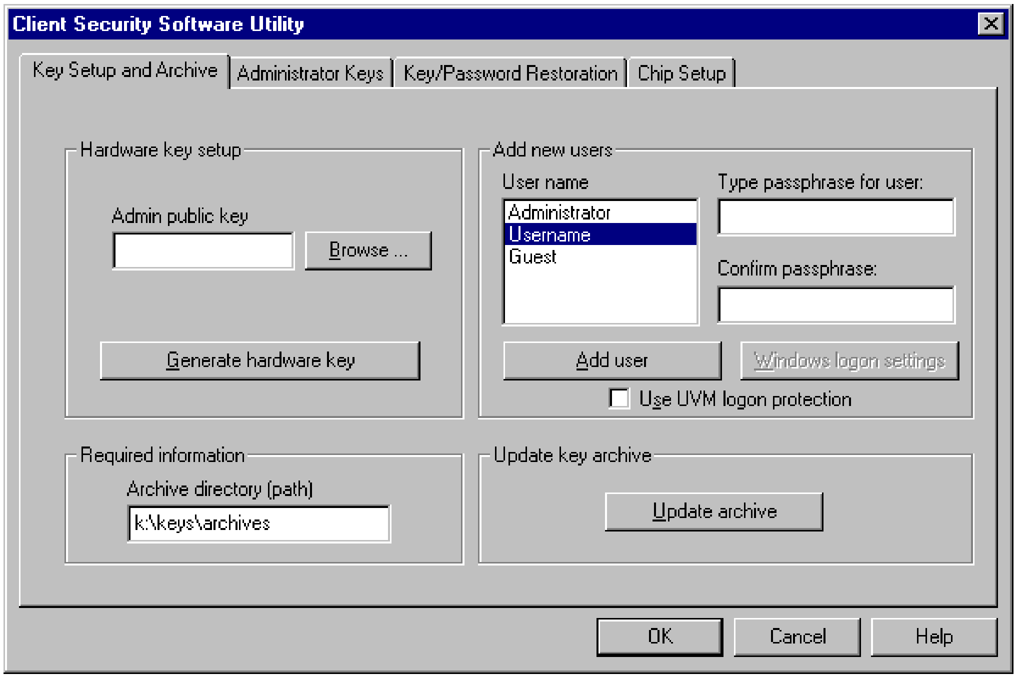
1. From the Windows desktop of the IBM client, click **Start** → **Programs** → **Client Security Software Utilities** → **Administrator Utility**.

   Because access to the Administrator Utility is protected by the hardware password, the following window opens and asks you to type the hardware password.



Before you can use the Client Security Software you must enter a hardware password below. Typing 10 incorrect entries causes the chip to lock for at least 1 hour and 17 minutes.

2. Type the hardware password; then click **OK**. The Administrator Utility window opens.
3. Click the **Key Setup and Archive** tab.
4. In the **Add new users** area, select a user name from the list. The user names in the list are defined by the user accounts created in the operating system.



☐ Use UVM logon protection

Archive directory (path): k:\keys\archives

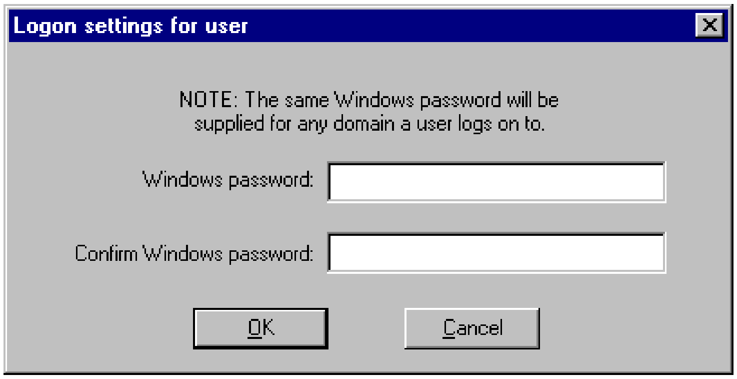
Note: After you set up a key archive, the Administrator Utility populates the **Archive directory (path)** field with the last path that was typed. If the information in this field is correct, you do not need to change it. If the information in field is deleted or, if the information is incorrect for the user you want to add, make sure that you re-type the correct information because the archive directory is required information when adding a user.

5. In the **Type passphrase for user** field, type a passphrase. This is the UVM passphrase that is associated with the user you want to add.

For information on the rules for the UVM passphrase, see “Appendix B - Rules for the hardware password and the UVM passphrase,” on page 60.

6. In the **Confirm passphrase** field, type the passphrase again.
7. Click **Add user**. A window opens that notifies you that the operation was successful. Click **OK**. The **Windows logon settings** button becomes active.
8. Click **Windows logon settings**.

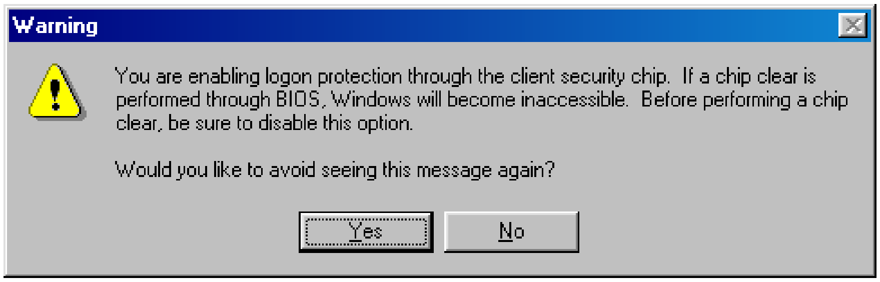
   The logon settings window opens.



NOTE: The same Windows password will be supplied for any domain a user logs on to.

9. In the **Windows password** field, type the operating system password (the Windows password, not the UVM passphrase) associated with the user.

   Note: The same Windows password will be supplied for any domain the user logs on to.
10. In the **Confirm Windows password** field, type the password again.
11. Click **OK**. A window opens that notifies you that the operation was successful. Click **OK**.
12. Do one of the following:
    - To set up UVM logon protection for the computer, go to step 13.
    - Repeat steps 4 through 11 to add another user to the security policy for this IBM client.
    - To exit the Administrator Utility, go to step 15.
13. Select the **Use UVM logon protection** check box and the following window opens.



You are enabling logon protection through the client security chip. If a chip clear is performed through BIOS, Windows will become inaccessible. Before performing a chip clear, be sure to disable this option.

Would you like to avoid seeing this message again?

Attention: Do not clear the IBM embedded Security Chip while 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. For more information, see "Administrator tips," on page 52.

Note: If you activate UVM logon protection and then clear the **Use UVM logon protection** check box, the system returns to the Windows logon process without UVM logon protection.

14. Click **Yes** or **No** to exit the warning window**.**
15. Click **OK** to exit the Administrator Utility.

Next, you can do the following:

- Activate UVM logon protection by shutting down and restarting the computer. When the computer restarts, you will be prompted to log on to the computer. For details on using UVM logon protection, see "Using UVM logon protection," on page 42.
- Notify the client users of the UVM passphrases that have been set. Users can change the UVM passphrase by using the Client Utility. For details, see "Using the Client Utility," on page 44.
- Set up and use the Client Security screen saver. For details, see "Setting up the Client Security screen saver," on page 44.
- Install the Client Security Software on more IBM clients. For instructions, see "Software installation and set up on other IBM clients," on page 18.

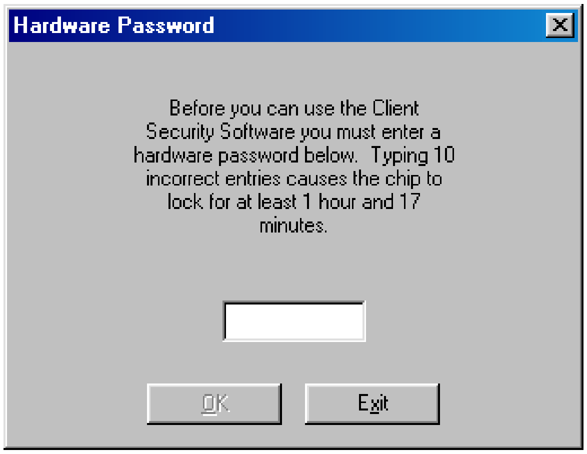
Chapter 4 - Using other features of the Administrator Utility

If you set up Client Security Software on IBM clients, you used the Administrator Utility to enable the IBM embedded Security Chip, set a hardware password, generate the hardware keys, and set up the security policy. This chapter provides instructions for using other features that the Administrator Utility provides.

To perform the instructions in the sections of this chapter, you must open the Administrator Utility by doing the following:

1. From the Windows desktop of the IBM client, click **Start** → **Programs** → **Client Security Software Utilities** → **Administrator Utility**.

   Because access to the Administrator Utility is protected by the hardware password, the following window opens and asks you to type the hardware password.

   Before you can use the Client Security Software you must enter a hardware password below. Typing 10 incorrect entries causes the chip to lock for at least 1 hour and 17 minutes.

2. Type the hardware password, and then click **OK**. The Administrator Utility window opens.

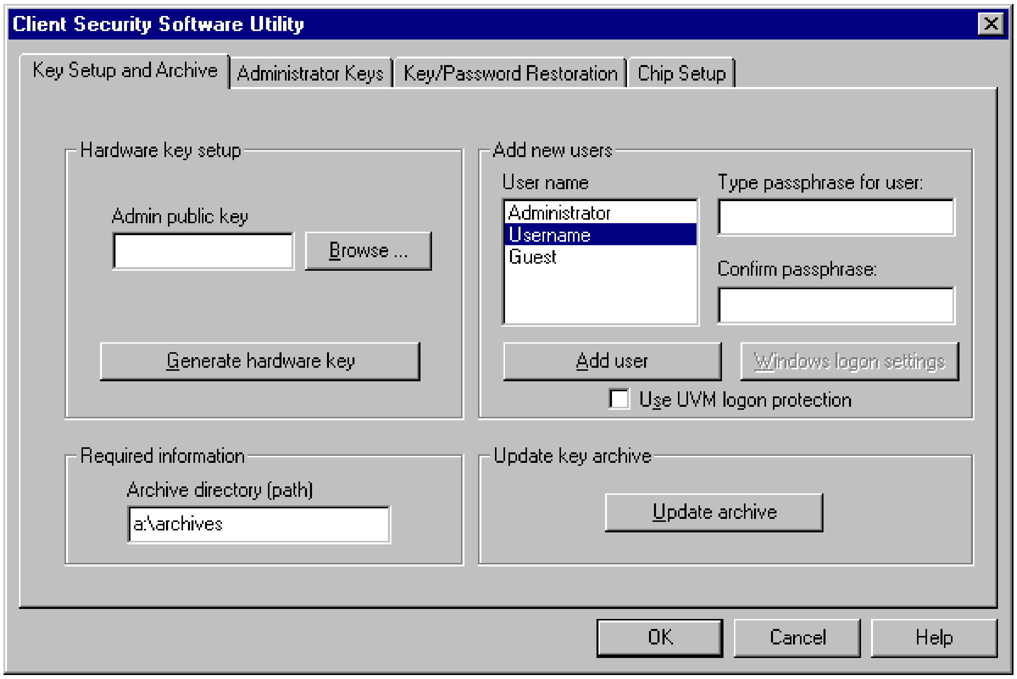
Update the key archive

When the key archive is first created, copies of all encryption keys are created. Reasons why updating the key archive might be necessary are 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.

Note: The client user can also update the key archive by using the Client Utility. For more information, see "Using the Client Utility," on page 44.

To update the key archive:

1. Open the Administrator Utility.
2. Click the **Key Setup and Archive** tab.



Archive directory (path): a:\archives

3. In the **Required information** area, type the path (not the file name) where the key archive will be stored. Store the archive on a network directory or diskette.

4. Click **Update archive**. A window opens that notifies you that the operation was successful. Click **OK**.

Change the admin public key

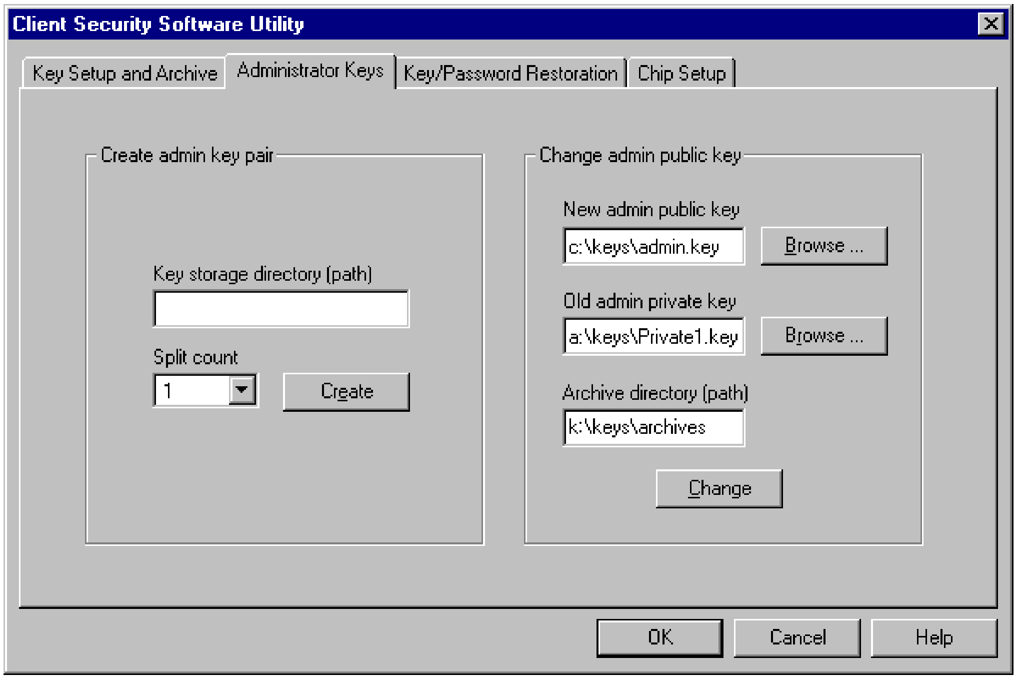
When the admin public key is first created, it is usually stored on a shared directory or diskette that is accessible to all users. If the admin public key becomes damaged, you can change to a different admin public key.

To change the admin public key:

1. Open the Administrator Utility; for details, see the instructions on page 31.

2. Click the **Administrator Keys** tab.

3. In the **New admin public key** field, type the file name for the new admin public key, or click **Browse** to search for the file.



Key storage directory (path):

Split count: 1

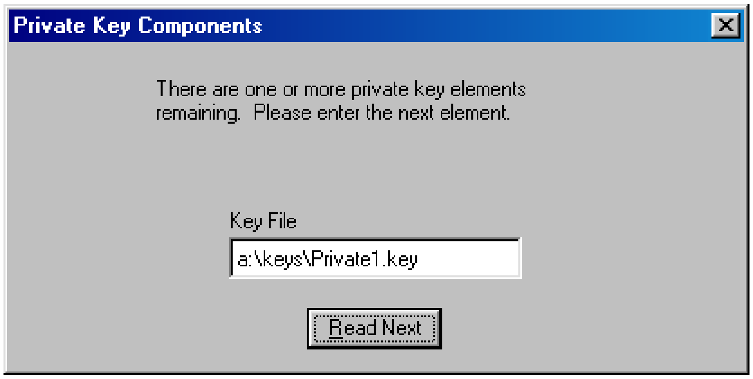
New admin public key: c:\keys\admin.key

Old admin private key: a:\keys\Private1.key

Archive directory (path): k:\keys\archives

4. In the **Old admin private key** field, type the file name for the old admin private key, or click **Browse** to search for the file.
5. In the Archiv**e directory (path)** field, type the path where the key archive is stored.
6. Click **Change**.

   Note: If the admin private key was split into multiple files, a window opens 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.



There are one or more private key elements remaining. Please enter the next element.

Key File: a:\keys\Private1.key

7. A window opens that notifies you that the operation was successful. Click **OK**.

Restore keys

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 of the computer. 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.

Reasons why key restoration might be necessary are if you replace a system board or a failed hard disk drive.

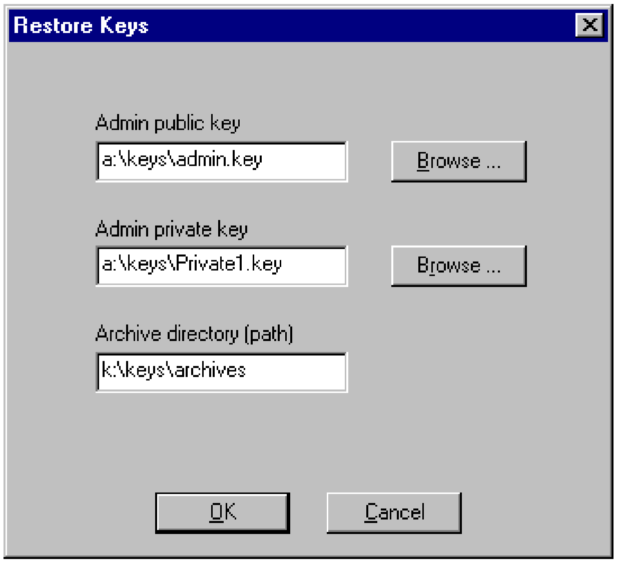
System board replacement

If you replace the system board in the computer with another system board that has 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 can perform the key restoration after you have enabled the new chip and set a hardware password. For details, see “Enabling the IBM embedded Security Chip and setting a hardware password,” on page 40.

To restore keys after a system board replacement, do the following:

1. Open the Administrator Utility. The following window opens.



Admin public key

a:\keys\admin.key

Admin private key

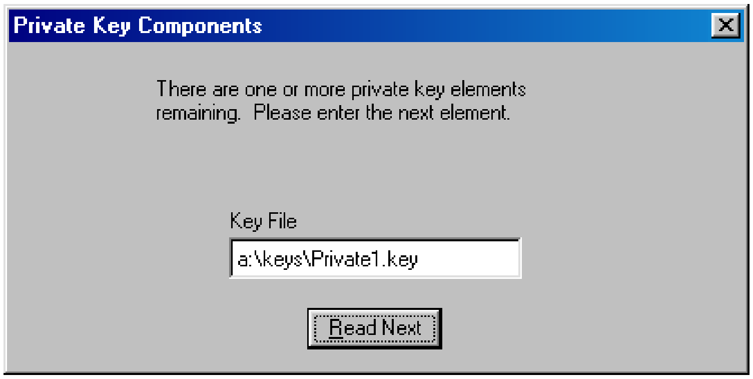
a:\keys\Private1.key

Archive directory (path)

k:\keys\archives

2. In the **Admin public key** field, type the path and file name of the admin public key or click **Browse** to search for the file. The previous example shows that the admin public key file (ADMIN.KEY) is stored on a diskette in the KEYS directory.
3. In the **Admin private key** field, type the path and file name of the admin private key or click **Browse** to search for the file. The previous example shows that the admin private key file (Private1.key) is stored on a diskette in the KEYS directory.
4. In the **Archive directory (path)** field, type the path to the archive directory.
5. Click **OK**.

   Note: If the admin private key was split into multiple files, a window opens 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.



Private Key Components

There are one or more private key elements remaining. Please enter the next element.

Key File
a:\keys\Private1.key

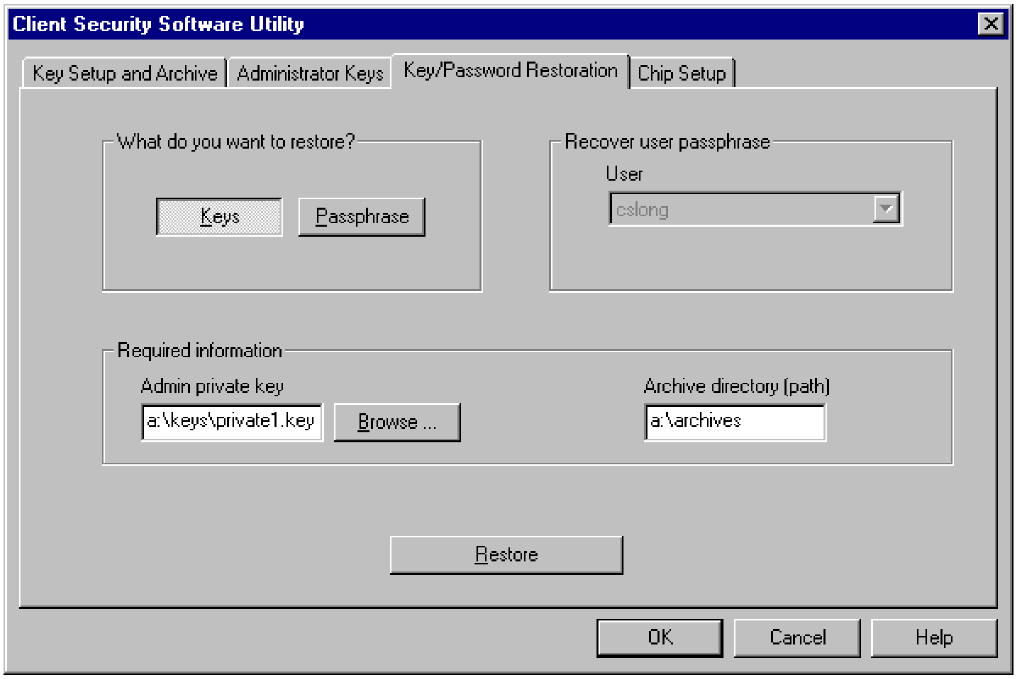
Hard disk drive failure

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 could still be stored but damaged.

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

To restore user keys from a key archive:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Key/Password Restoration** tab.
3. In the **What do you want to restore?** area, click the **Keys** button.



Client Security Software Utility

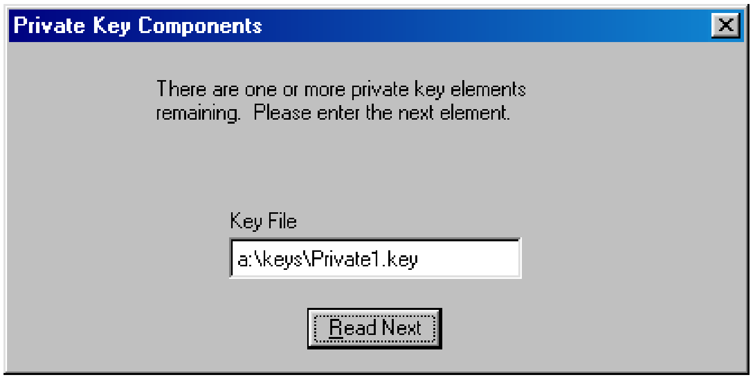
What do you want to restore?

Recover user passphrase
User
cslong

Required information
Admin private key
a:\keys\private1.key
Archive directory (path)
a:\archives

4. In the **Admin private key** field, type the path and file name for the admin private key (Private1.key), or click **Browse** to locate the file.
5. In the **Archive directory (path)** field, type the path (not the file name) where the key archive is stored.
6. Click **Restore**.

   Note: If the admin private key was split into multiple files, a window opens 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.



There are one or more private key elements remaining. Please enter the next element.

Key File: a:\keys\Private1.key

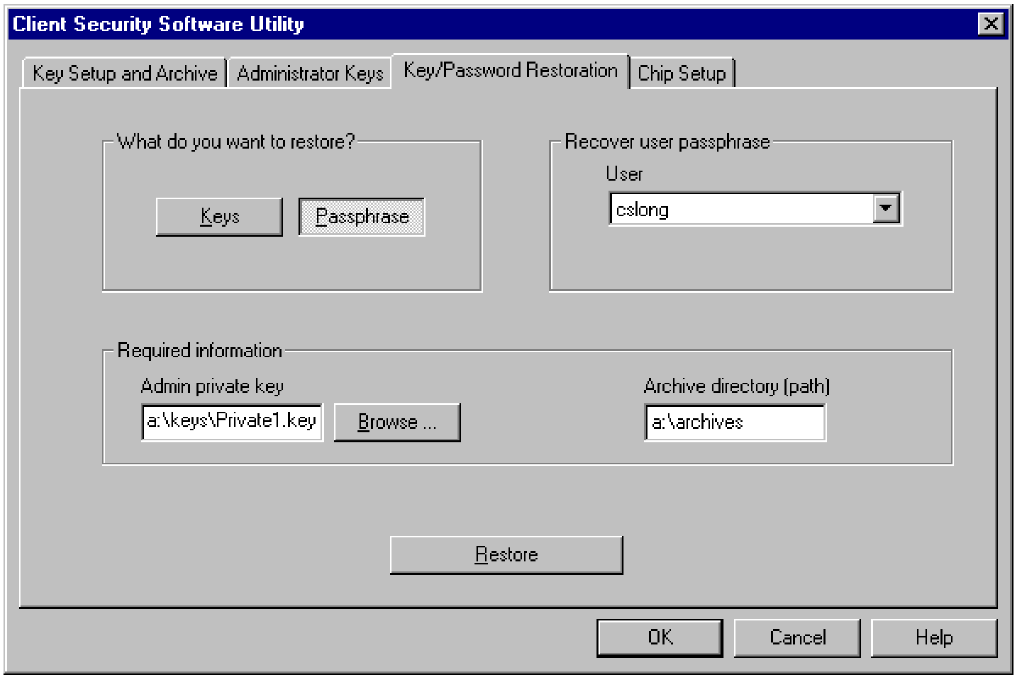
7. A window opens that notifies you that the operation was successful. Click **OK**.

Recover a UVM passphrase

A UVM passphrase is created for each user that you add to the security policy for the IBM client. Because passphrases can be lost or forgotten, or they can be changed by the client user, the Administrator Utility provides a way to recover the passphrase.

To recover the passphrase:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Key/Password Restoration** tab.
3. In the **What do you want to restore?** area, click the **Passphrase** button.



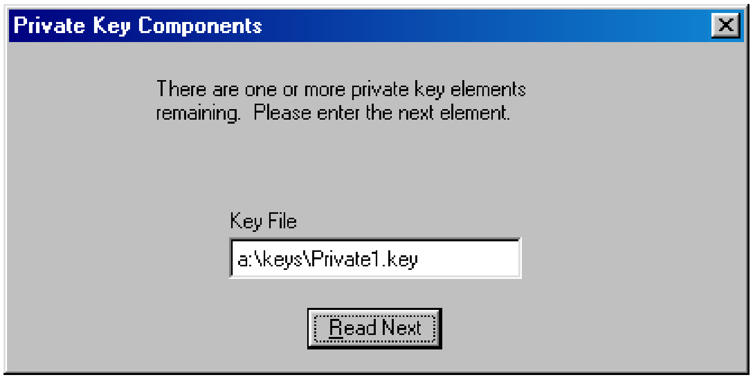
User: cslong

Admin private key: a:\keys\Private1.key

Archive directory (path): a:\archives

3. In the **Admin private key** field, type the path and file name for the admin private key (Private1.key), or click **Browse** to locate the file.
4. In the **Archive directory (path)** field, type the path (not the file name) where the key archive is stored.
5. Click **Restore**.

   Note: If the admin private key was split into multiple files, a window opens 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.



There are one or more private key elements remaining. Please enter the next element.

Key File: a:\keys\Private1.key

6. A window opens that shows you the UVM passphrase for the user.

Change the hardware password

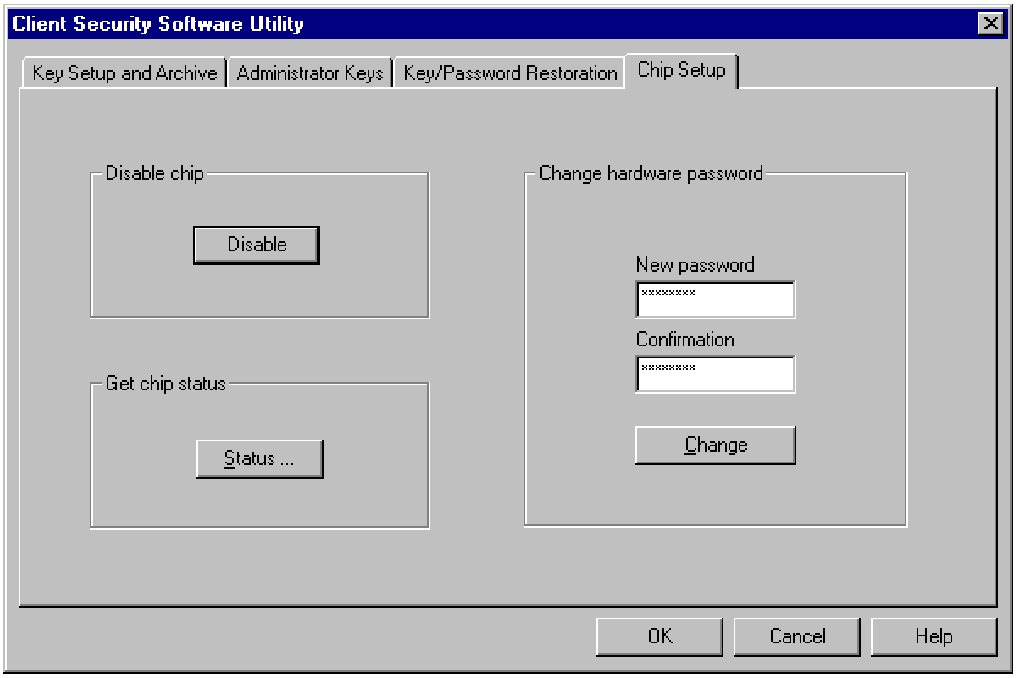
You must set a hardware password to enable the IBM embedded Security Chip. Access to the Administrator Utility is also protected by the hardware password.

Notes:

- For improved security, change the hardware password periodically. A password that remains unchanged for a long period of time can be more vulnerable to outside parties.
- For information on the rules of the hardware password, see "Appendix B - Rules for the hardware password and the UVM passphrase," on page 60.

To change the hardware password:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Chip Setup** tab.
3. In the **Change hardware password** area, type a new password in the **New password** field.



4. In the **Confirmation** field, type the password again.
5. Click **Change**.
6. A window opens that notifies you that the operation was successful. Click **OK**.

View information about Client Security Software

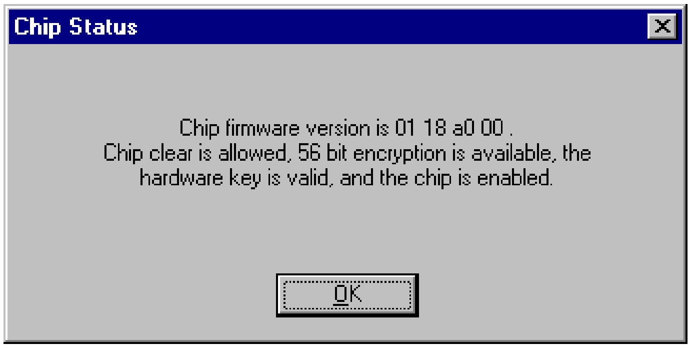
The following information about the IBM embedded Security Chip and Client Security Software is available through the Chip Setup screen:

- Encryption status of the embedded Security Chip
- Status on enablement of the IBM embedded Security Chip
- Version number of the firmware used with Client Security Software

- The validity of the hardware encryption keys

To view client security information:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Chip Setup** tab.
3. In the **Get chip status** area, click **Status**. A window opens containing information about the IBM embedded Security Chip and the software.



Chip Status

Chip firmware version is 01 18 a0 00 .
Chip clear is allowed, 56 bit encryption is available, the hardware key is valid, and the chip is enabled.

4. Click **OK** to exit.

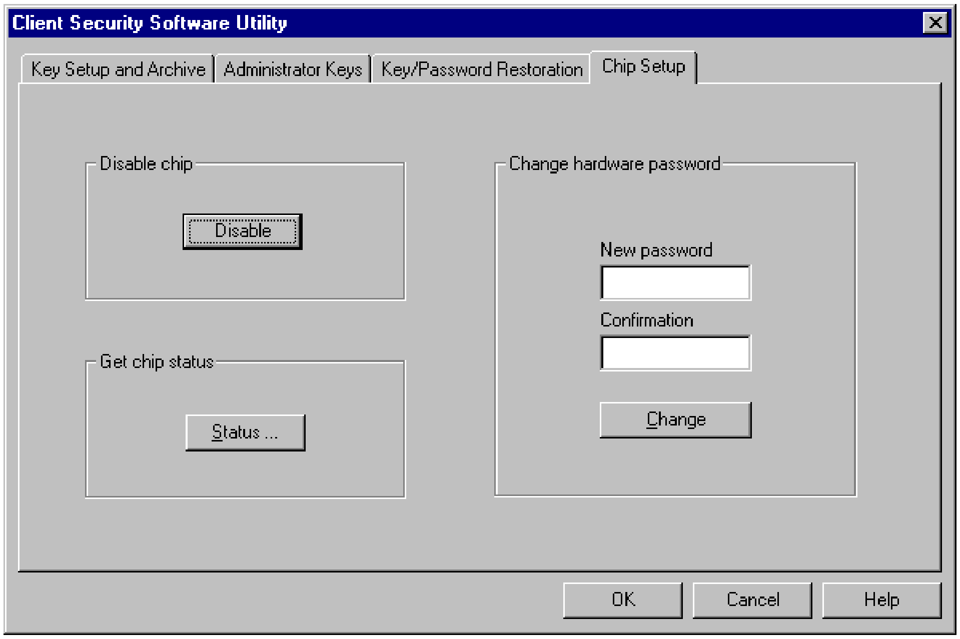
Disable the IBM embedded Security Chip

Attention: Do not disable the chip if 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 clear UVM logon protection, open the Administrator Utility, click the **Key Setup and Archive** tab, and clear the **UVM logon protection** check box. You must shut down and restart the computer before UVM logon protection is disabled.

The Administrator Utility provides a way to disable the IBM embedded Security Chip. Because the hardware password is required to start the Administrator Utility and disable the chip, as an administrator, you can prohibit unauthorized users from disabling the chip by protecting the hardware password.

To disable the embedded Security Chip:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Chip Setup** tab.



3. In the **Disable Chip** area, click **Disable**.

Note: To use the IBM embedded Security Chip and hardware encryption keys after the chip is disabled, the chip must be re-enabled. For more information, see “Enabling the IBM embedded Security Chip and setting a hardware password.”

Enabling the IBM embedded Security Chip and setting a hardware password

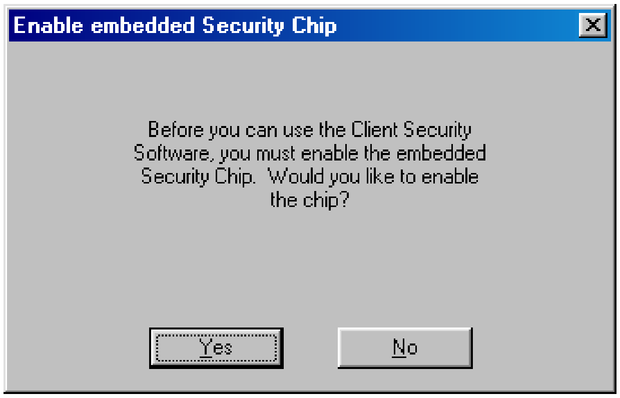
If you need to enable the IBM embedded Security Chip after the software has been installed, you can use the Administrator Utility to reset the hardware password and to set up new encryption keys.

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

To enable the chip and set a hardware password:

1. Click **Start** → **Programs** → **Client Security Software Utilities** → **Administrator Utility**.

   The following window opens and asks you to enable the IBM embedded Security Chip for the IBM client. Click **Yes**.



Enable embedded Security Chip

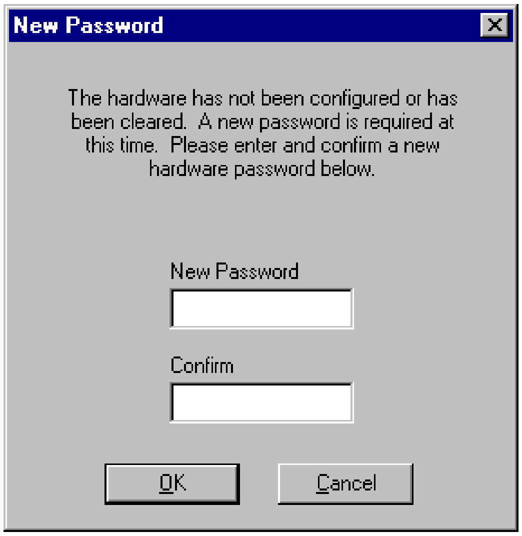
Before you can use the Client Security Software, you must enable the embedded Security Chip. Would you like to enable the chip?

You must restart the computer before the IBM embedded Security Chip will become enabled. A window opens that asks you to restart the computer.

2. Click **OK** to restart the computer

3. From the Windows desktop of the IBM client, click **Start** → **Programs** → **Client Security Software Utilities** → **Administrator Utility**.

   Because access to the Administrator Utility is protected by the hardware password, the following window opens that asks you to type the hardware password.



New Password

The hardware has not been configured or has been cleared. A new password is required at this time. Please enter and confirm a new hardware password below.

New Password

Confirm

4. Type a new hardware password, and then type it again in the **Confirm** field. Click **OK**.

Chapter 5 - Instructions for the client user

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

- use UVM logon protection
- set up the Client Security screen saver
- use the Client Utility
- use secure e-mail and Web browsing

The information in this section is also provided in the *Client Security User's Guide*.

Using UVM logon protection

This section contains information about using UVM logon protection. Before you can use UVM logon protection, it must be enabled for the computer. For information on enabling UVM logon protection, see "Add a user to the security policy," on page 27.

UVM logon protection enables you to control access to the operating system through a logon interface. The logon procedure can differ depending on which operating system is used, Windows NT or Windows 98 and Windows 95.

Windows NT

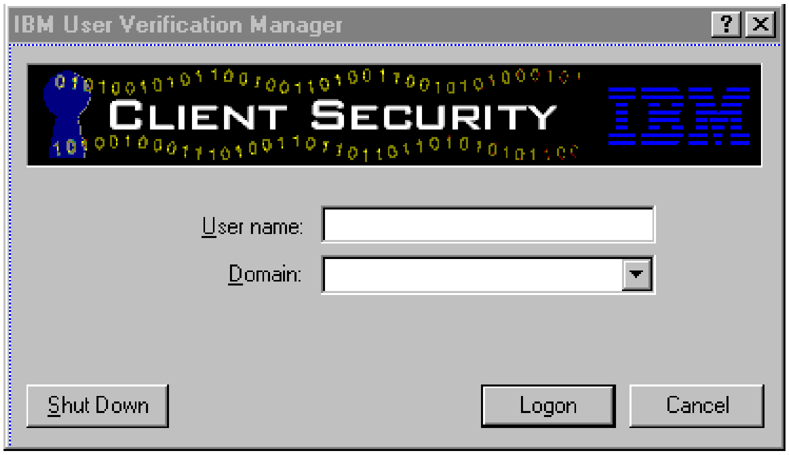
For Windows NT, UVM logon protection *replaces* the Windows NT logon application, so that, if a user tries to unlock the computer, the UVM logon window opens instead of the Windows NT logon window.

Note: You can use also the UVM logon window to perform a Windows shut down of the computer. To shut down the computer, click **Shut Down** on the UVM logon window.

To unlock a computer that uses Windows NT and UVM logon protection:

1. Press **Ctrl + Alt + Delete** to unlock the computer.

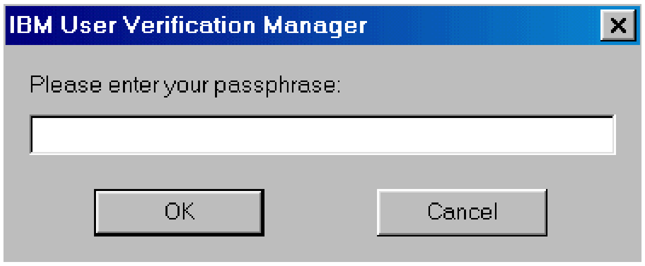
   The following UVM logon window opens.



2. Type the user name and the domain where the user is logged on, and then click **Logon**.

   Note: Although UVM recognizes multiple domains, the user password must be the same for all domains.

   The UVM passphrase window opens.



IBM User Verification Manager

Please enter your passphrase:

3. Type the associated UVM passphrase, and then click **OK** to access the operating system.

   If the UVM passphrase does not match the user name and domain entered, the UVM logon window opens again. If the user types the correct UVM passphrase for the user name and domain entered, the logon is successful.

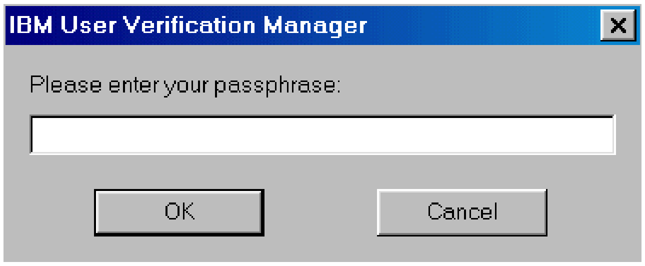
Windows 98 and Windows 95

For Windows 98 and Windows 95, UVM logon protection supports the use of the operating system logon window. UVM logon protection forces a Client Security screen saver session to be immediately launched upon logon.

To unlock a computer that uses Windows 98 or Windows 95 and UVM logon protection:

1. The operating system logon window opens.
2. Type user name and password information, and click **OK**.

   The UVM passphrase window opens.



IBM User Verification Manager

Please enter your passphrase:

3. Type the UVM passphrase associated with the user name typed in the operating system logon, and then click **OK** to access the operating system.

   If the user types the correct UVM passphrase, the computer unlocks.

If the user types an incorrect UVM passphrase, the Client Security screen saver displays; then the UVM passphrase window opens again.[5]

Setting up the Client Security screen saver

This section contains information about setting up the Client Security screen saver. The Client Security screen saver is one of the software components that is automatically installed by Client Security Software. Before you can use the Client Security screen saver, you must add at least one user to the security policy of the computer with the Administrator Utility. For details, follow the steps in "Add a user to the security policy," on page 27.

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.

To set up the Client Security screen saver:

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

If the Client Security is activated, press any key or move the mouse to access the UVM passphrase window. Type your UVM passphrase and click **OK** to access the desktop.

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

Using the Client Utility

The Client Utility enables you or the client user to change the following:

- **UVM passphrase**. To improve security, you can periodically change the UVM passphrase for a client user.
- **Windows logon settings**.[6] If you change the Windows NT password for a client user with the User Manager program, you must also change the password by using the Client Utility. Note that if you use 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.

[5] The Client Security screen saver may or may not be the selected screen saver for your computer. For Windows 98 and Windows 95, UVM logon protection uses the Client Security screen saver to secure the logon.

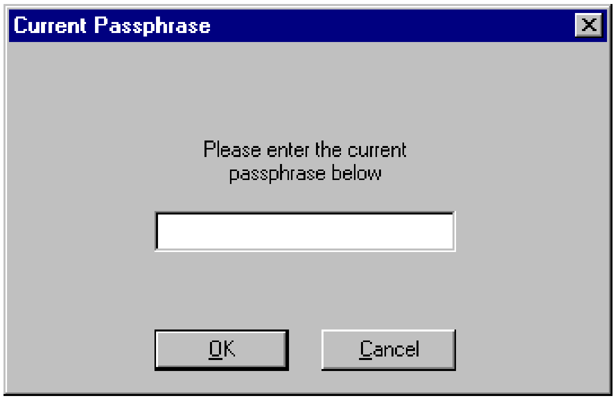
[6] Changing the Windows logon password is applicable for users of Windows NT only.

- **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.

To use the Client Utility:

1. Click **Start** → **Programs** → **Client Security Software Utilities** → **Client Utility**.

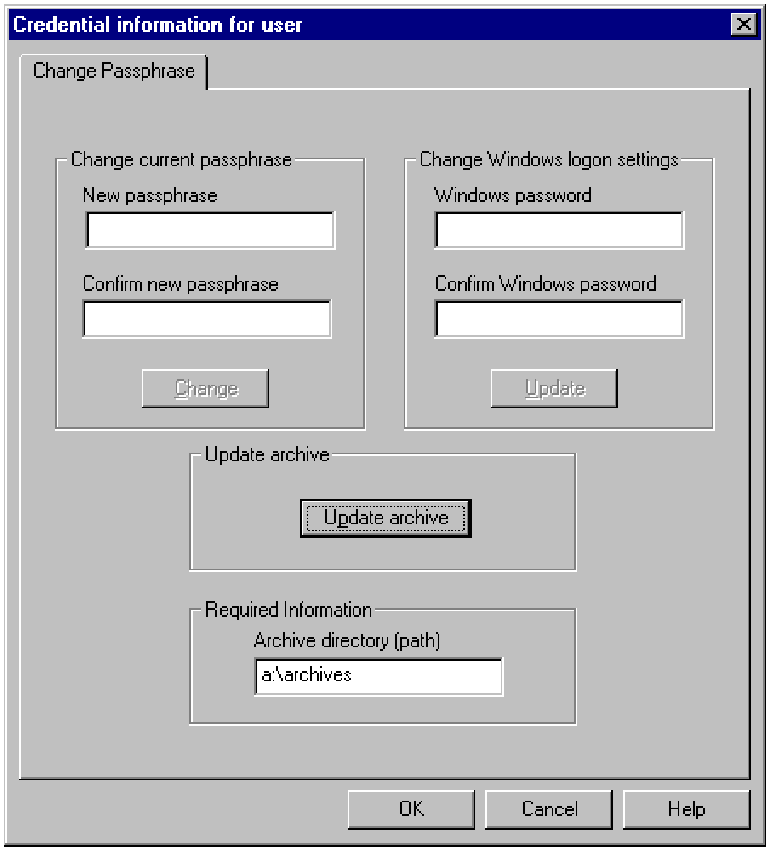
   The following window opens.



Please enter the current passphrase below

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

   The following window opens.



Archive directory (path): a:\archives

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

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

4. Do one of the following:

   - To change the UVM passphrase, in the **Change current passphrase** area, type a new passphrase in the **New passphrase** field. Next, type the passphrase again in the **Confirm new passphrase** field, and then click **Change**. For information on the rules for the UVM passphrase, see "Appendix B - Rules for the hardware password and the UVM passphrase," on page 60.
   - To change the Windows NT logon password, in the **Windows password** field, type a new Windows NT password. Next, type the new password again in the **Confirm Windows password** field, and then click **Update**. For rules on the Windows NT logon password, see the operating system documentation.

     Note: Only change Windows logon information in User Manager for the user currently logged on.
   - To update the key archive, click **Update archive**; then click **OK** on the window that opens and notifies you that the operation was successful.

5. Click **OK** to exit.

Using secure e-mail and Web browsing

If you send unsecured transactions sent 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 (or 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.

Tips for 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.

Notes:

- Client Security Software Version 1.0 supports the use of the 40-bit version of Internet Explorer. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see "View information about Client Security Software," on page 38.
- For information about known limitations when using Client Security Software with Microsoft applications and troubleshooting information, see "Known limitations," on page 53 and "Troubleshooting charts," on 54.

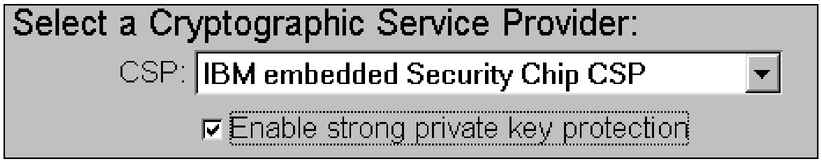
▪ Obtain a digital certificate

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 Chip CSP** as your CSP when you obtain your digital certificate. This ensures that the private key of the digital certificate is stored on the IBM embedded 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.

The following graphic shows what the certificate authority interface might look like when you are prompted to select a CSP.

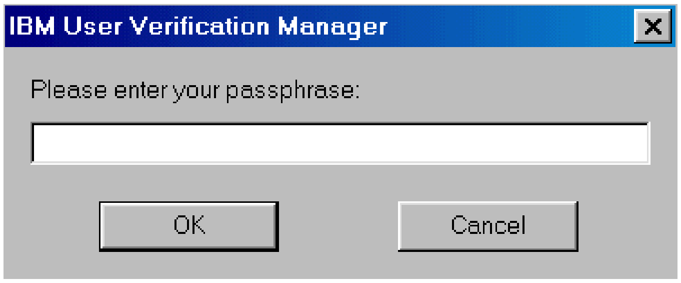


Select a Cryptographic Service Provider:

CSP: IBM embedded Security Chip CSP

☑ Enable strong private key protection

After you select **IBM embedded Security Chip CSP** as the CSP, the UVM component in Client Security Software prompts you for the UVM passphrase. The following window opens, and you must type the UVM passphrase and click **OK** before you can continue.



IBM User Verification Manager

Please enter your passphrase:

- **Update the key archive**

  After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive by using the Administrator Utility. For more information, see “Update the key archive,” on page 31.

- **Use the digital certificate**

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

  In Microsoft e-mail applications, after you create the digital certificate and use it to sign an e-mail message, the UVM passphrase window opens the first time you digitally sign an e-mail message. You must type the UVM passphrase and click **OK** before you can continue.

Tips for 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.

Notes:

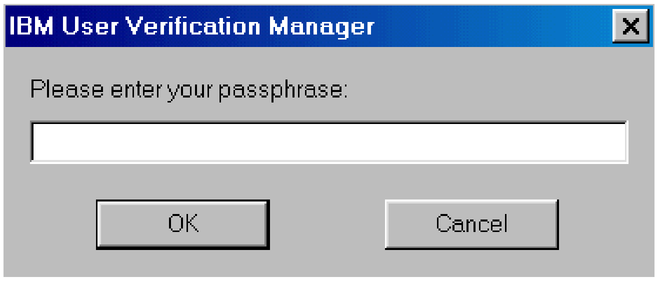
- Client Security Software Version 1.0 supports the use of the 40-bit version of Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see “View information about Client Security Software,” on page 38.
- For information about known limitations when using Client Security Software with Netscape applications and troubleshooting information, see “Known limitations,” on page 53 and “Troubleshooting charts,” on 54.

- **Install the IBM embedded Security Chip PKCS#11 module**

  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. You add a user by using the Administrator Utility. For details, see “Add a user to the security policy,” on page 27.

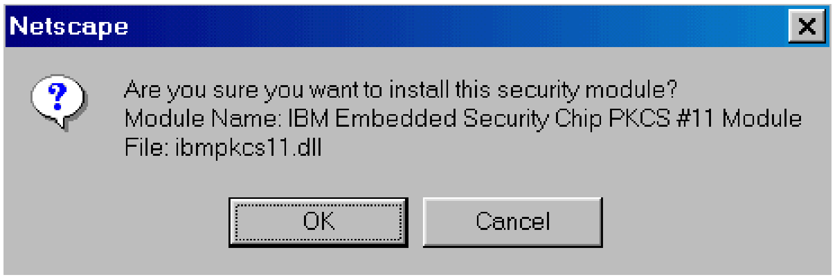
To install the IBM embedded Security Chip PKCS#11 module, do one of the following:

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



Please enter your passphrase:

3. The following window appears when you run the installation file. Click **OK.**



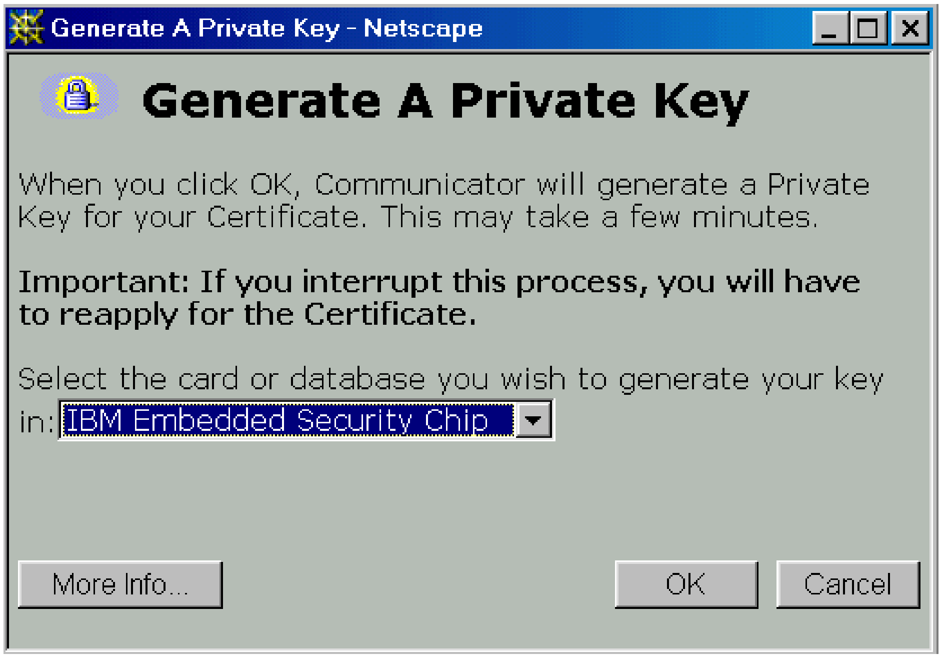
Are you sure you want to install this security module?
Module Name: IBM Embedded Security Chip PKCS #11 Module
File: ibmpkcs11.dll

4. A window opens that notifies you that the module was installed. Click **OK**.

- **Select IBM embedded Security Chip when generating a digital certificate**

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

During digital certificate creation, you will see the following window. Make sure you select **IBM embedded Security Chip**.



Generate A Private Key

When you click OK, Communicator will generate a Private Key for your Certificate. This may take a few minutes.

Important: If you interrupt this process, you will have to reapply for the Certificate.

Select the card or database you wish to generate your key in: IBM Embedded Security Chip

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

- **Update the key archive**

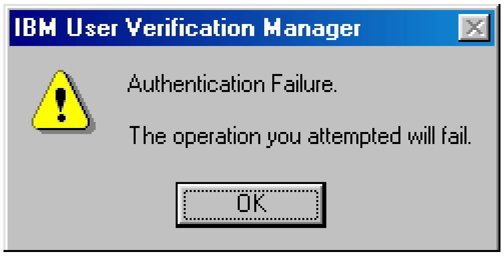
  After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive by using the Administrator Utility. For more information, see “Update the key archive,” on page 31.

- **Use the digital certificate**

  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, the UVM passphrase window opens each time you run Netscape. This is the only time the UVM passphrase window opens when you are using Netscape for sending and receiving secure e-mail or Web browsing. If the UVM passphrase window opens, you must type the UVM passphrase and click **OK** before you can continue.

  Note: You must type the correct UVM passphrase before you can use the digital certificate generated by the IBM embedded Security Chip. If you type the incorrect UVM passphrase, the following window opens.



Authentication Failure.

The operation you attempted will fail.

Click **OK**, and Netscape opens. You will not be able to use the digital certificate generated by the IBM embedded Security Chip until you close and restart Netscape, and type the correct UVM passphrase.

Chapter 6 - Troubleshooting

This chapter presents specific tips, known limitations, and troubleshooting information that is helpful to an administrator. Use this chapter to prevent or identify and correct problems that might come up as you use Client Security Software.

Administrator tips

The information in this section contains helpful tips for an administrator when installing, setting up and using Client Security Software.

Set an administrator password in the Configuration/Setup Utility

Security settings are available in the Configuration/Setup Utility of IBM clients. These settings enable you to do the following:

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

Attention:

- If a user clears the IBM embedded Security Chip, all encryption keys and certificates stored on the chip will be lost and the contents of the hard disk could become unusable.
- Do not clear or disable the IBM embedded Security Chip if 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 clear UVM logon protection, open the Administrator Utility, click the **Key Setup and Archive** tab, and clear the **UVM logon protection** check box. You must shut down and restart the computer before UVM logon protection is disabled.

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

To set an administrator password:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press **F1**. The main menu of the Configuration/Setup Utility opens.
3. Select **System Security**.
4. Select **Administrator Password**.
5. Type your password and press the down arrow on your keyboard.
6. Type your password again and press the down arrow.
7. Select **Change Administrator password** and press Enter; then press Enter again.
8. Press Esc to exit and save the settings.

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

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

Protect the hardware password

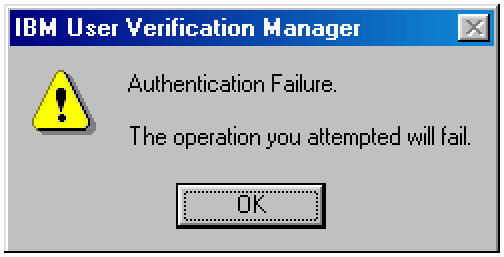
You set a hardware password to enable the IBM embedded Security Chip for a client. After you set a hardware password, access to the Administrator Utility is protected by this password. You should protect the hardware password to prohibit unauthorized users from changing settings in the Administrator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

Known limitations

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

Client Security Software and Netscape

Netscape opens after an incorrect UVM passphrase is entered: The UVM passphrase window opens each time you run Netscape. If the UVM passphrase window opens, you must type the UVM passphrase and click **OK** before you can continue. If you type the incorrect UVM passphrase, the following window opens.



Authentication Failure.

The operation you attempted will fail.

Click **OK** to continue. Although Netscape opens, 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

Client Security Software and Microsoft applications

Outlook Express (128 bit) encrypts at 3DES only: If Outlook Express is used with the 128-bit version of Internet Explorer 4.0 or 5.0, e-mail messages encrypted with the IBM embedded Security Chip certificate can only use the 3DES encryption algorithm. All other encryption algorithms are not supported.

Administrator Utility

Users are not deleted from the Administrator Utility in Windows 98: If you delete a user from Windows 98, the user name is not deleted from the list of users in the Administrator Utility.

Troubleshooting charts

Use the troubleshooting charts in this section to find solutions to problems that have definite symptoms.

Client Security Software and Microsoft applications

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.	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. **Note:** Client Security Software Version 1.0 supports the use of 40-bit Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see “View information about Client Security Software,” on page 38.

Problems using a certificate from an e-mail 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) encrypts e-mail messages with the 3DES encryption algorithm only	**Action**
If Outlook Express is used with the 128-bit version of Internet Explorer 4.0 or 5.0, e-mail messages encrypted with the IBM embedded Security Chip certificate can only use the 3DES encryption algorithm. All other algorithms are not supported.	Verify that you are using the 128-bit version of Internet Explorer 4.0 or 5.0. If you are using one of these browsers and you want to use an algorithm other than 3DES, you must use the 40-bit version of Internet Explorer. **Note:** Client Security Software Version 1.0 supports the use of 40-bit Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see "View information about Client Security Software," on page 38.

Error message when trying to use a certificate that has been restored 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.

Client Security Software and Netscape

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.	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. **Note:** Client Security Software Version 1.0 supports the use of 40-bit Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see "View information about Client Security Software," on page 38.

Failure message when trying to digitally sign an e-mail message when using Netscape Messenger	**Action**
If the IBM embedded Security Chip certificate has not been selected in Netscape Messenger, and a composer 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 and 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.

Unable to use the 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**
If 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; then re-open the second certificate.

Cannot export the IBM embedded Security Chip certificate	**Action**
The IBM embedded Security Chip certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up certificates.	Go to the Administrator Utility or Client Utility to update the key archive. If you update the key archive, copies of all the certificates associated with the IBM embedded Security Chip are created.

Error message when trying to	**Action**

use a certificate that has been restored after a hard disk drive failure	
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 the Netscape application you are working in.	Turn off the Netscape agent.

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 classification approval for 56-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 - Rules for the hardware password and the UVM passphrase

This appendix contains two tables that outline the rules for the hardware password and the UVM passphrase.

The following table describes the rules for the hardware password.

Length	The password must be exactly eight characters long.
Characters	The password must contain alphanumeric characters only. A combination of letters and numbers is allowed.
Properties	You set the hardware password to enable the IBM embedded Security Chip in the computer. The hardware password must also be typed each time you access the Administrator Utility.
Incorrect attempts	If you incorrectly type the password 10 times, the computer locks up for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly 10 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 10 times.

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

The following table describes the rules for 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 nonalphanumeric characters.
Properties	The UVM passphrase is different from a password that you might use to log on to an operating system. The user passphrase can be used in conjunction with other authenticating devices, such as a fingerprint reader or a smart card.
Incorrect attempts	If you incorrectly type the UVM passphrase multiple times during a session, the computer will not lock up.

Appendix C - Notices and Trademarks

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

Notices

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

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

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

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

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

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

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

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer

Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

IBM is a trademark of IBM Corporation in the U.S., other countries, or both.

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

Intel is a trademark of Intel Corp. in the U.S., other countries, both.

Other company, product, and service names mentioned in this document may be trademarks or servicemarks of others.