IBM® Client Security Solutions

Client Security Software Version 2.0 Installation Guide

July 2001

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 21 and "Appendix C - Notices and Trademarks," on page 26.

First Edition (July 2001)

Table of Contents

About this Guide

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

The guide is organized as follows:

"Chapter 1 - Introducing IBM Client Security Software," contains an overview of the components that are included in the Client Security Software.

"Chapter 2 – Getting started," contains computer hardware and software installation prerequisites as well as instructions for downloading the software.

"Chapter 3 – Before installing the software," contains prerequisite instructions for installing Client Security Software.

"Chapter 4 – Installing the software," contains instructions for installing the software.

"Chapter 5 - Uninstalling Client Security Software," contains instructions for uninstalling the software from the IBM client.

"Chapter 6 – Updating a previous version of the software," contains instructions for installing new software when a previous version of the software is already installed.

"Chapter 7 - Troubleshooting," contains helpful information for solving problems you might experience while using the instructions provided in this guide.

"Appendix A - U.S. export regulations for Client Security Software," contains U.S. export regulation information regarding the software.

"Appendix B - Rules for the hardware password," contains rules for setting hardware passwords.

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

Who should read this guide

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

How to use this guide

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

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

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

References to the *Client Security Software Administrator's G*uide are provided in this document. Use the *Administrator's Guide* to enable the IBM embedded Security Chip and install Client Security Software on IBM clients.

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

References to the *Client Security User's Guide*

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

Additional information

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

Chapter 1 - Introducing IBM Client Security Software

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

Client Security Software applications and components

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

? **Administrator Utility:** The Administrator Utility is the interface an administrator uses to activate or deactivate the embedded Security Chip, and to create, archive, and regenerate encryption keys and passphrases. In addition, an administrator can use this utility to add users to the security policy provided by Client Security Software.

? **User Verification Manager (UVM):** Client Security Software uses UVM to manage passphrases and other elements to authenticate system users. For example, a fingerprint reader can be used by UVM for logon authentication. UVM software enables the following features:

  ? **UVM client policy protection:** UVM software enables an administrator to set the client security policy, which dictates how a client user is authenticated on the system.

  ? **UVM system logon protection:** UVM software enables an administrator to control computer access through a logon interface. UVM protection ensures that only users who are recognized by the security policy are able to access the operating system.

  ? **UVM Client Security screen saver protection:** UVM software enables users to control access to the computer through a Client Security screen saver interface.

? **Client Utility:** The Client Utility enables a client user to change the UVM passphrase. On Windows NT, the Client Utility enables users to change Windows NT logon passwords to be recognized by UVM and to update key archives. A user can also create backup copies of digital certificates created with the IBM embedded Security Chip.

Public Key Infrastructure (PKI) features

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

? **Administrator control over client security policy**. Authenticating end users at the client level is an important security policy concern. Client Security Software provides the interface that is required to manage the security policy of an IBM client. This interface is part of the authenticating software User Verification Manager (UVM), which is the main component of Client Security Software.

? **Encryption key management for public key cryptography**[1]. Administrators create encryption keys for the computer hardware and the client users with Client Security Software. When encryption keys are created, they are bound to the IBM embedded Security Chip through a key hierarchy, where a base level hardware key is used to encrypt the keys above it, including the user keys that are associated with each client user. Encrypting and storing keys on the IBM embedded Security Chip adds an essential extra layer of client security, because the keys are securely bound to the computer hardware.

? **Digital certificate creation and storage that is protected by the IBM embedded Security Chip**. When you apply for a digital certificate that can be used for digitally signing or encrypting an e-mail message, Client Security Software enables you to choose the IBM embedded Security Chip as the cryptographic service provider for applications that use the Microsoft? CryptoAPI. These applications include Internet Explorer and Microsoft Outlook Express. This ensures that the private key of the digital certificate is stored on the IBM embedded Security Chip. Also, Netscape users can choose IBM embedded Security Chips as the private key generators for digital certificates used for security. Applications that use the Public-Key Cryptography Standard (PKCS) #11, such as Netscape Messenger, can take advantage of the protection provided by the IBM embedded Security Chip.

Note: For information about the applications that can be used with Client Security Software, see “Software requirements,” on page 9.

? **A key archive and recovery solution**. An important PKI function is creating a key archive from which keys can be restored if the original keys are lost or damaged. Client Security Software provides an interface that enables you to establish an archive for keys and digital certificates created with the IBM embedded Security Chip and to restore these keys and certificates if necessary.

? **Right Click Encryption:** Right Click Encryption enables a client user to encrypt his files simply by clicking the right mouse button.

[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.

Chapter 2 – Getting started

This chapter contains information about software that is compatible for use with Client Security Software. Also, information about downloading Client Security Software is provided.

Hardware requirements

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

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

IBM embedded Security Chip

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

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

Supported IBM PCD models

Client Security Software is licensed for and supports the following IBM Personal Computing Devices (PCD) models:

? IBM PC 300PL (6565, 6584, 6594)

? IntelliStation E Pro (6867)

? IntelliStation M Pro (6868)

? IntelliStation Z Pro (6869)

? NetVista (6059, 6569, 6579, 6649)*

? NetVista (6646 all Q1x models, 6841)

? New models will be added

*To run Client Security Software 2.0 on these NetVista models (6059, 6569, 6579, 6649), you must use BIOS level xxxx22axx or later. Users who have installed previous versions of Client Security Software should update their BIOS level to xxxx22axx or later. For more information, see the README file included with the software download.

Software requirements

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

Operating systems

Client Security Software requires one of the following operating systems:

? Windows® Millennium

? Windows Professional

? Windows 2000®

? Windows NT® 4.0, with Service Pack 5 or later

? Windows 98

UVM-aware products

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

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

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

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

? **Tivoli SecureWay® Policy Director**

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

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

? **Lotus Notes version 4.5 or later**

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

Web browsers

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

✍ Internet Explorer 4.01 with Service Pack 1a

✍ Internet Explorer 5.0 or later

✍ Netscape 4.51

✍ Netscaper 4.61 or later

Web browser encryption strength information

After the software is installed, a message is displayed that notifies you what Web browser encryption strength your system supports. If support for strong encryption is installed, use the 128-bit version of your Web browser. Otherwise, use the 40-bit version of your Web browser. To check the encryption strength of your Web browser, see the help system provided with the browser.

Cryptographic services

Client Security Software supports the following cryptographic services:

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

E-mail applications

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

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

Downloading the software

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

Registration form

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

The installation files for Client Security Software are included within the self-extracting file named csec20.exe.

Export regulations

Client Security Software Version 2.0 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 2.0. For more information on export regulations that govern Client Security Software, see "Appendix A - U.S. export regulations for Client Security Software," on page 24.

Chapter 3 – Before installing the software

This chapter contains prerequisite instructions for running the installation program and configuring Client Security Software on IBM clients. All files required for the installation are provided within the csec20.exe file that you download from the IBM Web site.

Before you install the software

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

Installing on clients running Windows 2000 and Windows NT

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

Installing for use with Policy Director

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

Startup feature considerations

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

Administrator password

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

Enhanced Security

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

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

Installing on NetVista models 6059, 6569, 6579, 6649 and all NetVist 6646 Q1*x* models

If an administrator password has been set on NetVista models (6059, 6569, 6579, 6649, 6646, and all Q1*x* models), you must open the Administrator Utility to enable the chip and generate the hardware keys.

If Enhanced Security is enabled on these NetVista models, you must use the Administrator Utility to enable the embedded Security Chip and generate the hardware encryption keys after the Client Security Software is installed. If the installation program detects that Enhanced Security is enabled, you will be notified at the end of the installation process.[2] At that time, you must restart the computer and open the Administrator Utility to enable the chip and generate the hardware keys.

Installing on all other NetVista models (other than models 6059, 6569, 6579, 6649 and all NetVist 6646 Q1*x* models)

If an administrator password on other NetVista models has been, you are not required to type the administrator password during the installation process.

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

BIOS update information

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

If you plan to install Client Security Software on a NetVista model 6059, 6569, 6579 or 6649, you must have BIOS code level xxxx22A or later.

To find the latest BIOS code updates for your computer, go to the http://www.pc.ibm.com/support IBM Web site, type `bios` in the search field, and select downloads from the drop-down list; then press Enter. A list of BIOS code updates is displayed. Click the appropriate NetVista model number and follow the instruction on the Web page.

[2] The notification about Enhanced Security does not display if you are performing an unattended installation.

Using admin keys

Admin keys, which are actually a key pair that includes the admin public key and the admin private key, enable you to generate the hardware encryption keys for an IBM client.

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

After you create the admin keys, you can use the installation program to quickly install and configure the software on other IBM clients without the Administrator Utility. See “Installing the software on other IBM clients when the admin public key is available” on page 17 for more information.

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

Chapter 4 – Installing the software

This chapter contains instructions for running the installation program and configuring Client Security Software on IBM clients. All files required for the installation are provided within the csec20.exe file that you download from the IBM Web site.

Installing the software on the first IBM client

Before starting the installation procedure, close all open programs, and restart the computer; then complete the following procedures to install Client Security Software on the first IBM client:

Using the IBM Client Security Software – InstallShield Wizard

1. From the Windows desktop, click **Start** > **Run**.
2. In the Run field, type:

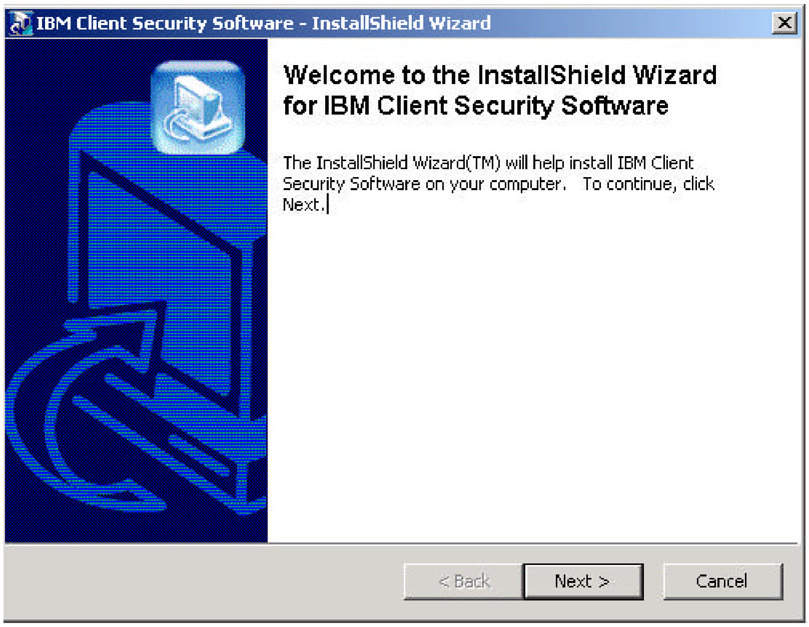
   d:\directory\csec20.exe

   where *d:* and *directory* are the drive letter and the directory where the file is located.

   The version of Client Security Software that you will install is displayed.

   Note: You can use a zip program to extract all files from csec20.exe into a common directory. If you extract the files, you must run setup.exe to install the software.
3. Click **Setup** to continue.

   The IBM Client Security Software – InstallShield Wizard opens.



IBM Client Security Software - InstallShield Wizard

Welcome to the InstallShield Wizard for IBM Client Security Software

The InstallShield Wizard(TM) will help install IBM Client Security Software on your computer. To continue, click Next.

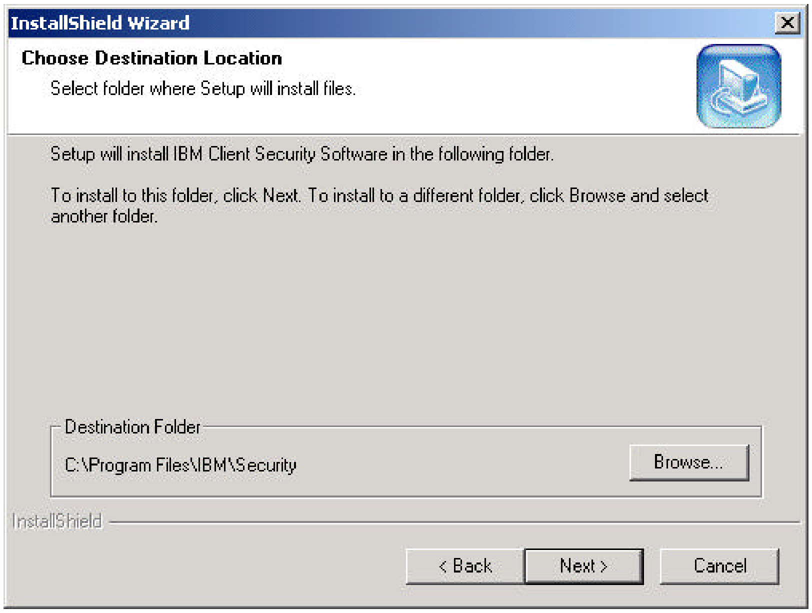
4. Click **Next**.

   The License Agreement window opens.

5. Click **Yes** to accept the License Agreement.

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

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



InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install IBM Client Security Software in the following folder.

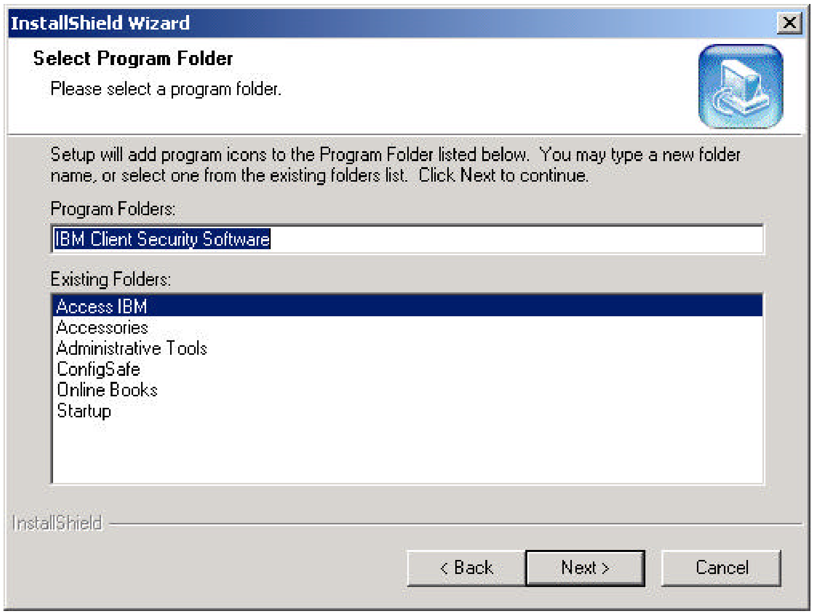
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\IBM\Security

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

7. The Select Program Folder window opens.



InstallShield Wizard

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

Program Folders:

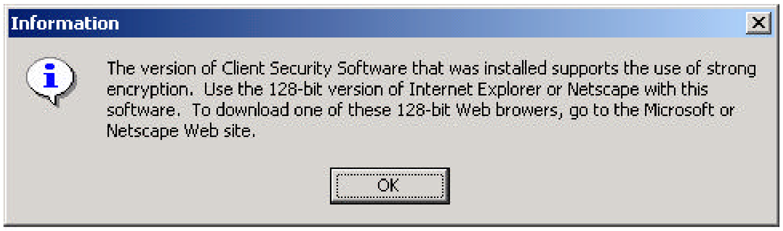
IBM Client Security Software

Existing Folders:

Access IBM
Accessories
Administrative Tools
ConfigSafe
Online Books
Startup

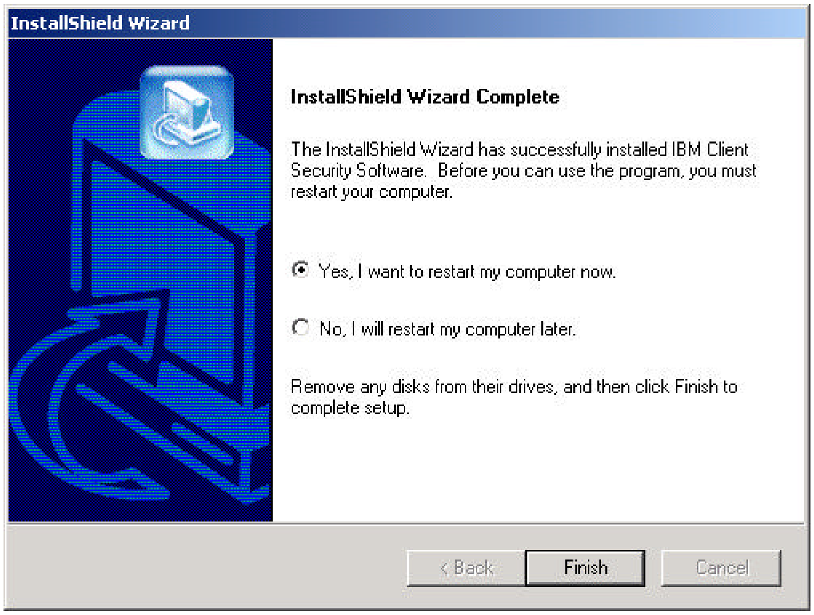
8. Click **Next** to accept the default program folder, IBM Client Security Software, then click **Next**.

A message is displayed that notifies you of the Web browser encryption strength that must be used with Client Security Software.



The version of Client Security Software that was installed supports the use of strong encryption. Use the 128-bit version of Internet Explorer or Netscape with this software. To download one of these 128-bit Web browers, go to the Microsoft or Netscape Web site.

9. Click **OK** to continue.



InstallShield Wizard Complete

The InstallShield Wizard has successfully installed IBM Client Security Software. Before you can use the program, you must restart your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

The InstallShield Wizard Complete window is displayed. You must restart the computer before using Client Security Software.

10. Click **Yes, I want to restart my computer now**, then click **Finish**.

The Client Security Software has been successfully installed and the IBM embedded Security Chip has been enabled. You must restart your system before using Client Security Software.

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

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

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

Performing an unattended installation

Before you begin an unattended installation, read "Chapter 3 – Before installing the software," on page 11.

You perform an unattended installation of Client Security Software without having to be present at the computer.

- ✍ Windows NT or Windows 2000 users must log on with administrator user rights to install Client Security Software.
- ✍ If you are installing Client Security Software on a NetVista 6059, 6569, 6579, 6649, or 6646 Q1*x* model and an administrator password has been set for the computer, you must edit the szPAP field.

To perform an unattended installation, complete the following procedure:

1. Use a zip program to extract all files from csec20.exe into a common folder. Note that the setup.exe and setup.iss files are stored in a folder that you specify.
2. Copy the admin.key file to the hard disk of the IBM client or to a shared network directory so that it is available for the unattended installation.

3. Edit and save the setup.iss file. Parameters you might need to edit in the file are shown in bold below.

```
[InstallShield Silent]
Version=v6.00.000
File=Response File
szAdminPassword=11111111
szHWPassword=password
szKeyFile=C:\MyKeyFile
szArchivePath=C:\MyArchive
[File Transfer]
OverwrittenReadOnly=NoToAll
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-DlgOrder]
Dlg0={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdWelcome-0
Count=6
Dlg1={355B3C24-68B7-11D4-B3EC-000629B04E58}-SdLicense-0
Dlg2={355B3C24-68B7-11D4-B3EC-000629B04E58}-
SdAskDestPath-0
Dlg3={355B3C24-68B7-11D4-B3EC-000629B04E58}-
SdSelectFolder-0
Dlg4={355B3C24-68B7-11D4-B3EC-000629B04E58}-MessageBox-0
Dlg5={355B3C24-68B7-11D4-B3EC-000629B04E58}-
SdFinishReboot-0
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdWelcome-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdLicense-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdAskDestPath-0]
szDir=C:\Program Files\IBM\Security
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdSelectFolder-0]
szFolder=IBM Client Security Software
Result=1
[Application]
Name=IBM Client Security Software
Version=1.04.001a
Company=IBM
Lang=0009
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-MessageBox-0]
Result=1
[{355B3C24-68B7-11D4-B3EC-000629B04E58}-SdFinishReboot-0]
Result=1
BootOption=3
```

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

? `szDir=C:\Program Files\IBM\Security` designates the directory where Client Security Software will be installed.

? `szFolder=IBM Client Security Software` designates the folder where Client Security Software will be installed.

? `szHWPassword=password` assigns the hardware password for the IBM embedded Security Chip as “password.” You can assign any hardware password you want, as long as it adheres to the rules for the hardware password. For information on the rules for the hardware password, see “Appendix B - Rules for the hardware password,” on page 25.

? `szKeyFile=C:\MyKeyFile` designates the path to the admin.key file. For the unattended installation to run properly, admin.key must be in the specified path on the client hard disk or on a shared network directory. If the admin.key file you use is stored on a diskette, copy it to the client hard disk or to a shared network directory so that it is available for the unattended installation.

? `szArchivePath=C:\MyArchive` designates the path where the keys are archived. For the unattended installation to run properly, do not store the key archive on a diskette. If you want to store the key archive on a diskette, store the key archive on the client hard disk or a shared network directory during the unattended installation, and then copy it to a diskette after the installation is complete.[3]

? (some systems only) `szAdminPassword=11111111` designates the administrator password that has been set for the computer. If you are installing Client Security Software on one of the following computers:

? NetVista 6059, 6569, 6579, 6649

? NetVista 6646 all Q1*x* models

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

Note: If you provide an incorrect administrator password, the software will install, but the embedded Security Chip will not be enabled and hardware keys will not be generated. See "Startup feature considerations," on page 11 for more information.

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

[3] Hard disk failures can damage files; store key archive files on hard disks on a temporary basis only. Also, if you want to save the key archive to a shared directory, you must map a drive letter to the shared network resource where that directory exists before you can use the uninstallation program. For information on mapping a drive letter to a shared network resource, see your Windows operating system documentation.

Chapter 5 - Uninstalling Client Security Software

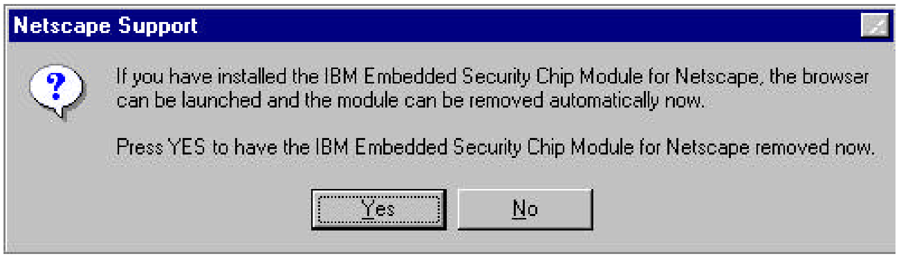
Windows NT or Windows 2000 users must log on with administrator user rights to uninstall Client Security Software.

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

To uninstall Client Security Software:

1. Close all Windows programs.
2. From the Windows desktop, click **Start > Settings > Control Panel**.
3. Click the **Add/Remove Programs** icon.
4. In the list of software that can be automatically removed, select **IBM Client Security**.
5. Click **Add/Remove.**
6. Click **Yes** to uninstall the software.
7. Do one of the following:

   ? If you installed the IBM embedded Security Chip PKCS#11 module for Netscape, the following message is displayed that asks you to start the process to disable the IBM embedded Security Chip PKCS#11 module. Click **Yes** to proceed.

   If you have installed the IBM Embedded Security Chip Module for Netscape, the browser can be launched and the module can be removed automatically now.

   Press YES to have the IBM Embedded Security Chip Module for Netscape removed now.

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

   ? If you did not install the IBM embedded Security Chip PKCS#11 module for Netscape, a message is displayed that asks if you want to delete shared DLL files that were installed with Client Security Software.

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

8. Click **OK** after the software is removed. You must restart the computer after uninstalling Client Security Software.

When you uninstall Client Security Software, you remove only the installed software components. Any encryption keys that you created remain stored on the IBM embedded Security Chip. The key archive is not affected when Client Security Software is uninstalled.

Chapter 6 – Updating a previous version of the software

If you want update your system from a previous version of Client Security Software, you must do the following:

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

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

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

Clearing the IBM embedded Security Chip

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

Attention:

? If you clear 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 protection** check box. You must shut down and restart the computer before UVM logon protection is disabled.

To clear the IBM embedded Security Chip:

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 is displayed.
3. Select **System Security**.
4. Select **IBM Embedded Security Chip**.
5. Select **Clear IBM Security Chip**.

6. Select **Yes**.
7. Press Esc to continue.
8. Press Esc to exit and save the settings.

Chapter 7 - Troubleshooting

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

Installing Client Security Software

Problem	Action
You attempt to install the software and a message is displayed that notifies you that a previous version of Client Security Software is already installed.	Click **OK** to exit from the window and the installation process. Do the following: 1. Uninstall the software. See "Chapter 5 - Uninstalling Client Security Software" for instructions. 2. Reinstall the software. See "Chapter 3 – Before installing the software" for instructions. **Note:** If you plan to use the same hardware password to secure the IBM embedded Security Chip, you do not have to clear the chip and reset the password.

Problem	Action
You attempt to install the software on an IBM client that already has an enabled IBM embedded Security Chip. The hardware password for the IBM embedded Security Chip is unknown.	You must clear the chip to continue with the installation. For more information, see "Clearing the IBM embedded Security Chip" on page 21.

Installing UVM-aware fingerprint sensors

Problem	Action
During installation of the DigitalPersona U.are.UPro fingerprint sensor, a message is displayed and asks that you do the following: 1. Attach the fingerprint sensor 2. Wait for the red light to illuminate on the sensor 3. Click **OK** The system will restart without providing an opportunity for you to click OK.	No action is required. This tip is for informational purposes only. The fingerprint sensor will install correctly.

Appendix A - U.S. export regulations for Client Security Software

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

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

Appendix B - Rules for the hardware password

This appendix contains rules for the hardware password.

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. No exceptional characters, like space, !, ?, %, are allowed.
Properties	Set the hardware password to enable the IBM embedded Security Chip in the computer. This password must be typed each time you access the Administrator Utility.
Incorrect attempts	If you incorrectly type the password ten times, the computer locks up for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly ten more times, the computer locks up for 2 hours and 34 minutes. The time the computer is disabled doubles each time you incorrectly type the password ten times.

Appendix C - Notices and Trademarks

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

Notices

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

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

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

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

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

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

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

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

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

Trademarks

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

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

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

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