

IBM<sup>®</sup> Client Security  
Solutions



# Client Security Software Version 5.4 Installation Guide



IBM<sup>®</sup> Client Security  
Solutions



# Client Security Software Version 5.4 Installation Guide

**First Edition (October 2004)**

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 31 and Appendix C, "**Notices and Trademarks**," on page 39.

© **Copyright International Business Machines Corporation 2004. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Preface</b> . . . . .	<b>v</b>
About this guide . . . . .	v
Who should read this guide . . . . .	v
How to use this guide . . . . .	v
References to the <i>Client Security Software Administrator and User Guide</i> . . . . .	vi
Additional information . . . . .	vi
<b>Chapter 1. Introduction</b> . . . . .	<b>1</b>
The IBM Embedded Security Subsystem . . . . .	1
The IBM Embedded Security Chip . . . . .	1
IBM Client Security Software . . . . .	2
The relationship between passwords and keys . . . . .	2
The administrator password . . . . .	2
The hardware public and private keys . . . . .	3
The administrator public and private keys . . . . .	3
ESS archive . . . . .	4
User public and private keys . . . . .	4
The IBM key-swapping hierarchy . . . . .	4
CSS public key infrastructure (PKI) features . . . . .	5
<b>Chapter 2. Getting started</b> . . . . .	<b>7</b>
Hardware requirements . . . . .	7
IBM embedded Security Subsystem . . . . .	7
Supported IBM models . . . . .	7
Software requirements . . . . .	7
Operating systems . . . . .	7
UVM-aware products . . . . .	7
Web browsers . . . . .	8
<b>Chapter 3. Before installing the software</b> . . . . .	<b>11</b>
Before you install the software . . . . .	11
Installing for use with Tivoli Access Manager . . . . .	11
Startup feature considerations . . . . .	11
BIOS update information . . . . .	12
Using the administrator key pair to archive keys . . . . .	12
<b>Chapter 4. Downloading, installing, and configuring the software</b> . . . . .	<b>13</b>
Downloading the software . . . . .	13
Installing the software . . . . .	14
Selecting a configuration option . . . . .	14
Typical configuration . . . . .	14
Advanced configuration . . . . .	16
Using the IBM Client Security Setup Wizard . . . . .	16
Using the Setup Wizard to complete a typical configuration . . . . .	17
Using the Setup Wizard to complete an advanced configuration . . . . .	18
Enabling the IBM Security Subsystem . . . . .	20
Upgrading your version of Client Security Software . . . . .	21
Upgrading using new security data . . . . .	21
Upgrading from CSS 5.0 or later using existing security data . . . . .	21
Uninstalling Client Security Software . . . . .	22
Export regulations . . . . .	23
<b>Chapter 5. Troubleshooting</b> . . . . .	<b>25</b>
Administrator functions . . . . .	25
Authorizing users . . . . .	25
Setting a BIOS administrator password (ThinkCentre) . . . . .	25
Setting a supervisor password (ThinkPad) . . . . .	26
Clearing the IBM embedded Security Subsystem (ThinkCentre) . . . . .	27
Clearing the IBM embedded Security Subsystem (ThinkPad) . . . . .	27
Known issues or limitations with CSS Version 5.4 . . . . .	28
Re-installing Targus fingerprint software . . . . .	28
BIOS supervisor passphrase . . . . .	28
Smart card limitations . . . . .	28
Troubleshooting charts . . . . .	28
Installation troubleshooting information . . . . .	28
<b>Appendix A. U.S. export regulations for Client Security Software</b> . . . . .	<b>31</b>
<b>Appendix B. Password and passphrase information</b> . . . . .	<b>33</b>
Password and passphrase rules . . . . .	33
Administrator password rules . . . . .	33
UVM passphrase rules . . . . .	34
Fail counts on systems using the National TPM . . . . .	35
Fail counts on systems using the Atmel TPM . . . . .	36
Resetting a passphrase . . . . .	36
Resetting a passphrase remotely . . . . .	36
Resetting a passphrase manually . . . . .	37
<b>Appendix C. Notices and Trademarks</b> . . . . .	<b>39</b>
Notices . . . . .	39
Trademarks . . . . .	40



---

## Preface

This section provides information about how to use this guide.

---

### About this guide

This guide contains information on how to install IBM Client Security Software on an IBM network computer, also referred to as an IBM client, which contains the IBM embedded Security Subsystem. This guide also contains instructions on how to enable the IBM embedded Security subsystem and how to set the administrator password for the security subsystem.

The guide is organized as follows:

"Chapter 1, "Introduction,"" contains a brief outline of basic security concepts, an overview of the applications and components that are included in the software, and a description of Public Key Infrastructure (PKI) features.

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

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

"Chapter 4, "Downloading, installing, and configuring the software,"" contains instructions for installing, updating, and uninstalling the software.

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

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

"Appendix B, "Password and passphrase information,"" contains passphrase criteria that can be applied to a UVM passphrase and rules for administrator passwords.

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

---

### Who should read this guide

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

---

### How to use this guide

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

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

## **References to the *Client Security Software Administrator and User Guide***

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

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

---

## **Additional information**

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

---

## Chapter 1. Introduction

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

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

---

### The IBM Embedded Security Subsystem

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

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

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

### The IBM Embedded Security Chip

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

The IBM Embedded Security Subsystem supports:

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

## IBM Client Security Software

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

- **Administrator Utility:** The Administrator Utility is the interface an administrator uses to activate or deactivate the embedded Security Subsystem, and to create, archive, and regenerate encryption keys and passphrases. In addition, an administrator can use this utility to add users to the security policy provided by Client Security Software.
- **Administrator Console:** The Client Security Software Administrator Console enables an administrator to configure a credential roaming network, to create and configure files that enable deployment, and to create a non-administrator configuration and recovery profile.
- **User Configuration Utility:** The User Configuration Utility enables a client user to change the UVM passphrase, to enable Windows logon passwords to be recognized by UVM, to update key archives, and to register fingerprints. A user can also create backup copies of digital certificates created with the IBM embedded Security Subsystem.
- **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. Client Security Software enables the following features:
  - **UVM client policy protection:** Client Security Software enables a security administrator to set the client security policy, which dictates how a client user is authenticated on the system.

If policy indicates that fingerprint is required for logon, and the user has no fingerprints registered, he will be given the option to register fingerprints as part of the logon. Also, if the Windows password is not registered, or incorrectly registered, with UVM, the user will have the opportunity to provide the correct Windows password as part of the logon.
  - **UVM system logon protection:** Client Security Software enables a security administrator to control computer access through a logon interface. UVM protection ensures that only users who are recognized by the security policy are able to access the operating system.

---

## The relationship between passwords and keys

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

### The administrator password

The administrator password is used to authenticate an administrator to the IBM Embedded Security Subsystem. This password is maintained and authenticated in the secure hardware confines of the embedded security subsystem. Once authenticated, the administrator can perform the following actions:

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

The administrator password can be set in the following ways:

- Through the IBM Client Security Setup Wizard

- Through the Administrator Utility
- Using scripts
- Through the BIOS interface (ThinkCentre computers only)

It is important to have a strategy for creating and maintaining the administrator password. The administrator password can be changed if it is compromised or forgotten.

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

## The hardware public and private keys

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

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

The hardware private key is created, stored and used in the secure, hardware confines of the security subsystem. The hardware public key is made available for various purposes (hence the name public key), but it is never exposed outside of the secure, hardware confines of the security subsystem. The hardware public and private keys are a critical part of the IBM key-swapping hierarchy described in a following section.

Hardware public and private keys are created in the following ways:

- Through the IBM Client Security Setup Wizard
- Through the Administrator Utility
- Using scripts

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

## The administrator public and private keys

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

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

Administrator public and private keys can be created in one of the following ways:

- Through the IBM Client Security Setup Wizard
- Through the Administrator Utility

- Using scripts

---

## ESS archive

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

### User public and private keys

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

### The IBM key-swapping hierarchy

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

The next “level” of keys up the hierarchy (above the root) is the administrator public and private keys, or the *administrator key pair*. The administrator key pair can be unique on each machine, or it can be the same on all clients or a subset of clients. How you manage this key pair depends upon how you want to manage your network. The administrator private key is unique in that it resides on the client system (protected by the hardware public key) in an administrator-defined location.

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

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

The private keys are encrypted because they must be heavily protected and because there is limited storage space available in the IBM Embedded Security Subsystem. Only a couple of keys can be stored in the security subsystem at any given time. The hardware public and private keys are the only keys that remain stored in the security subsystem from boot to boot. In order to allow for multiple keys and multiple users, CSS utilizes the IBM key-swapping hierarchy. Whenever a key is needed, it is swapped into the IBM Embedded Security Subsystem. The related, encrypted private keys are swapped into the security subsystem, and can then be used in the protected environment of the chip. The private keys are never exposed or used outside of this hardware environment.

The administrator private key is encrypted with the hardware public key. The hardware private key, which is only available in the security subsystem, is used to decrypt the administrator private key. Once the administrator private key is decrypted in the security subsystem, a user's private key (encrypted with the administrator public key) can be passed into the security subsystem and decrypted with the administrator private key. Multiple users' private keys can be encrypted with the administrator public key. This allows for virtually an unlimited number of users on a system with the IBM ESS; however, best practices suggest that limiting enrollment to 25 users per computer ensures optimal performance.

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

---

## CSS public key infrastructure (PKI) features

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

- **Administrator control over client security policy.** Authenticating end users at the client level is an important security policy concern. Client Security Software provides the interface that is required to manage the security policy of an IBM client. This interface is part of the authenticating software User Verification Manager (UVM), which is the main component of Client Security Software.
- **Encryption key management for public key cryptography.** Administrators create encryption keys for the computer hardware and the client users with Client Security Software. When encryption keys are created, they are bound to the IBM embedded Security Chip through a key hierarchy, where a base level hardware key is used to encrypt the keys above it, including the user keys that are associated with each client user. Encrypting and storing keys on the IBM embedded Security Chip adds an essential extra layer of client security, because the keys are securely bound to the computer hardware.
- **Digital certificate creation and storage that is protected by the IBM embedded Security Chip.** When you apply for a digital certificate that can be used for digitally signing or encrypting an e-mail message, Client Security Software enables you to choose the IBM embedded Security Subsystem 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 encrypted with the user's public key on the IBM embedded Security Subsystem. Also, Netscape users can choose the IBM embedded Security Subsystem as the private key generator 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 Subsystem.

- **The ability to transfer digital certificates to the IBM embedded Security Subsystem.** The IBM Client Security Software Certificate Transfer Tool enables you to move certificates that have been created with the default Microsoft CSP to the IBM embedded Security Subsystem CSP. This greatly increases the protection afforded to the private keys associated with the certificates because they will now be securely stored on the IBM embedded Security Subsystem, instead of on vulnerable software.

**Note:** Digital certificates protected by the IBM embedded Security Subsystem CSP cannot be exported to another CSP.

- **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. IBM Client Security Software provides an interface that enables you to establish an archive for keys and digital certificates created with the IBM embedded Security Subsystem and to restore these keys and certificates if necessary.
- **File and folder encryption.** File and folder encryption enables a client user to encrypt or decrypt files or folders. This provides an increased level of data security on top of the CSS system-security measures.
- **Fingerprint authentication.** IBM Client Security Software supports the Targus PC card fingerprint reader and the Targus USB fingerprint reader for authentication. Client Security Software must be installed before the Targus fingerprint device drivers are installed for correct operation.
- **Smart card authentication.** IBM Client Security Software supports certain smart cards as an authentication device. Client Security Software enables smart cards to be used as a token of authentication for a single user at a time. Each smart card is bound to a system unless credential roaming is being used. Requiring a smart card makes your system more secure because this card must be provided along with a password, which can be compromised.
- **Credential roaming.** Credential roaming enables an authorized network user to use any computer on the network as though it was his own workstation. After a user is authorized to use UVM on any Client Security Software-registered client, he can then import his personal data to any other registered client in the credential roaming network. His personal data is then updated automatically and maintained in the CSS archive and on any computer to which it was imported. Updates to this personal data, such as new certificates or passphrase changes, are immediately available on all other computers connected to the roaming network.
- **FIPS 140-1 certification.** Client Security Software supports FIPS 140-1 certified cryptographic libraries.
- **Passphrase expiration.** Client Security Software establishes a user-specific passphrase and a passphrase expiration policy when each user is added to UVM.

---

## Chapter 2. Getting started

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

---

### Hardware requirements

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

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

### IBM embedded Security Subsystem

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

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

### Supported IBM models

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

---

### Software requirements

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

### Operating systems

IBM Client Security Software requires one of the following operating systems:

- Windows XP
- Windows 2000 Professional

### UVM-aware products

IBM Client Security comes with User Verification Manager (UVM) software that enables you to customize authentication for your desktop computer. 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 IBM 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 IBM Client Security Software, and then reinstall the UVM-aware sensor.

- **Tivoli Access Manager version 5.1**

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

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

- **Lotus Notes version 4.5 or later**

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

- **Entrust Desktop Solutions 5.1, 6.0, or 6.1**

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

- **RSA SecurID Software Token**

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

- **Gemplus GemPC400 smart card reader**

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

## Web browsers

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

- Internet Explorer 5.0 or later
- Netscape 4.8 and Netscape 7.1

### Browser encryption strength information

If support for strong encryption is installed, use the 128-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

IBM 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, IBM Client Security Software enables you to use the cryptographic operations of the IBM embedded Security Subsystem when you create digital certificates for Microsoft applications.
- **PKCS#11:** PKCS#11 is the cryptographic standard for Netscape, Entrust, RSA and other products. After you install the IBM embedded Security Subsystem PKCS#11 module, you can use the IBM embedded Security Subsystem to generate digital certificates for Netscape, Entrust, RSA and other applications that use PKCS#11.

## **E-mail applications**

IBM 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)
- Lotus Notes support through enhanced logon authentication protection



---

## Chapter 3. Before installing the software

This section contains prerequisite instructions for running the installation program and configuring IBM Client Security Software on IBM clients.

All files required for the installation of Client Security Software are provided on the <http://www.pc.ibm.com/us/security/index.html> IBM Web site. The Web site provides information that helps ensure that your system contains the IBM embedded Security Subsystem, and that enables you to select the appropriate IBM Client Security offering for your system.

---

### Before you install the software

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

Users must log on with administrator rights to install IBM Client Security Software.

### Installing for use with Tivoli Access Manager

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

### Startup feature considerations

Two IBM startup features might affect the way that you enable the IBM embedded Security Subsystem and generate the encryption keys. These features are the BIOS administrator password and Enhanced Security and can be accessed from the Configuration/Setup Utility of an IBM computer. IBM Client Security Software has a separate administrator password. To avoid confusion, the administrator password that is set in the Configuration/Setup Utility is referred to as the *BIOS administrator password* in the Client Security Software manuals.

#### BIOS Administrator password

A BIOS administrator password prevents unauthorized persons from changing the configuration settings of an IBM computer. This password is set using the Configuration/Setup Utility program on a NetVista or ThinkCentre computer or the IBM BIOS Setup Utility program on a ThinkPad computer. The appropriate program can be accessed by pressing Enter or F1 during the computer startup sequence. This password is called the *administrator password* in the ThinkCentre Configuration/Setup Utility and the *supervisor password* in the ThinkPad BIOS Setup Utility.

#### Enhanced Security

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

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

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

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

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

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

## BIOS update information

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

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

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

---

## Using the administrator key pair to archive keys

The archive key pair is simply a copy of the administrator key pair that you store on an external media for restoration. Because the Administrator Utility is used to create the archive key pair, you must install IBM Client Security Software on an initial IBM client before you can create the administrator key pair.

---

## Chapter 4. Downloading, installing, and configuring the software

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

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

---

### Downloading the software

All files required for the installation of Client Security Software are provided on the <http://www.pc.ibm.com/us/security/index.html> IBM Web site. The Web site provides information that helps ensure that your system contains the IBM embedded Security Subsystem, and that enables you to select the appropriate IBM Client Security offering for your system.

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

1. Using a Web browser, go to the <http://www.pc.ibm.com/us/security/index.html> IBM Web site.
2. In the Resources box, click **Support and downloads**.
3. In the Embedded Security Subsystem and IBM Client Security Software section of the Web page, click **Software download**.
4. In the Select a system box, click **Detect my system & continue** or enter your seven-digit machine type-model number in the provided field.
5. Enter your email address in the provided field and select your Country/Region from the drop-down menu.
6. Select the appropriate check box regarding whether you want to be sent information about other offerings.
7. Review the License Agreement by clicking **View Licence**; then click **Accept Licence**.

You will automatically be redirected to the IBM Client Security download page.

8. Find the link for Client Security Software 5.4 and click **Download Now**.

**Note:** See the `css54readme.html` file for specific upgrade and limitation information.

9. Click **Save** to save a copy of the installation executable file on your hard drive.
10. Specify the Save As location and click **Save**. To begin the installation of the software, click **Open** when the download is complete, or double-click the executable file icon.

The Welcome to the InstallShield Wizard for IBM Client Security Software window opens.

---

## Installing the software

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

1. Double-click the executable file.  
The Welcome to the InstallShield Wizard for IBM Client Security Software window opens.
2. Click **Next**.  
The IBM Client Security Software Licence Agreement is displayed.
3. Read the terms of the license agreement, select the **I accept the terms in the license agreement** radio button, and then click **Next**.  
The Product Selection screen is displayed.
4. Select one of the following radio buttons and click **Next**.
  - **IBM Client Security Software and IBM Password Manager**. This selection will install or upgrade IBM Client Security Software, IBM Password Manager, and all of the necessary device drivers.
  - **IBM Client Security Software only**. This selection will install or upgrade IBM Client Security Software and all of the necessary device drivers.The Destination Folder screen is displayed.
5. Click **Next** to accept the default installation location, or click **Change** to browse to the desired destination folder.  
The Ready to Install the Program screen is displayed.
6. Click **Install** to begin the installation, or click **Back** to review or change any of your installation settings.  
A status bar displays the progress of the installation, and then the InstallShield Wizard Completed screen is displayed.
7. Click **Finish** to exit the wizard.

You must restart your computer for the installation changes made to your computer to take effect.

---

## Selecting a configuration option

The first screen of the IBM Client Security Setup Wizard enables you to select a configuration option. Selecting the appropriate configuration option is very important. Review the following information carefully before selecting a configuration option. Novice security users should select the *typical configuration* option.

### Typical configuration

When you select the typical configuration of IBM Client Security Software using the Client Security Setup Wizard, you configure the following Client Security features:

- IBM Password Manager (if selected at installation)
- Right-click file encryption
- Passphrase and fingerprint authentication
- Digital signature support

Using the recommended *typical configuration* option in the Client Security Setup Wizard makes the configuration process simple. However, some advanced features of Client Security Software are disabled when this configuration is selected, causing some CSS features to be unavailable.

### Typical configuration default settings

The typical configuration hard-coded defaults settings are as follows:

- **Archive location:** C:\documents and settings\all users\application data\ibm\security\archive
  - **Administrator key pair location:** C:\documents and settings\all users\application data\ibm\security\keys
- The administrator private key is not split, and is encrypted with the CSS administrator passphrase.

Other settings include the following:

- IBM Password Manager support is enabled
- Security policy is medium: each available authentication method will only be required the first time a CSS feature is used.
- Passphrase authentication is always required.
- Fingerprint authentication is required when an integrated fingerprint reader is detected at setup.
- The UVM passphrase of the user who set up CSS is also the CSS *administrator password*. Changing the UVM passphrase will also change the CSS administrator password. The CSS administrator passphrase never expires.

### Typical configuration component limitations

Some features of Client Security Software that are enabled after an advanced configuration are disabled when a typical configuration is selected. These features cannot be used under a typical configuration of CSS. To enable these functions, you must convert your configuration to an advanced configuration. The functional differences after a typical configuration are as follows:

- **Administrator Utility**

The following actions are not allowed under a typical configuration:

- Reset User
- Remove User
- Changing the administrator password using the Chip Settings button
- Key Configuration functions

If a user attempts one of the above operations, he will be prompted to convert to the CSS advanced configuration. The conversion process decrypts the administrator private key and moves the administrator key pair to a location specified by the user.

- **Administrator Console**

The following usage differences apply under a typical configuration:

- The archive directory, private key location, and public key location are hard coded and cannot be changed. The archive can only be edited on the local computer.
- The option to configure credential roaming is not available under the typical configuration. If you select a typical configuration, and then want to set up a credential roaming network, you must first convert your typical configuration to an advanced configuration.

- A UVM-passphrase bypass operation cannot be performed for the CSS administrator.
- **User Configuration Utility**  
The following usage differences apply under a typical configuration:
  - The UVM passphrase of the user who set up CSS is also the administrator password. Changing the UVM passphrase will also change the administrator password.
  - The CSS administrator user cannot be reset.
  - The option to configure credential roaming is not available under the typical configuration.

### **Converting a typical configuration to an advanced configuration**

To convert a Client Security Software typical configuration to an advanced configuration, complete the following procedure:

1. Start the Administrator Utility.
2. Enter the CSS administrator password.
3. Click the **Key Configuration** button.
4. Click **OK** to continue.
5. Enter the location where you want to store the decrypted administrator key pair. The decrypted key pair should not be stored on the local hard disk drive. The conversion process is now complete.
6. Change the archive location. The archive should not be stored on the local hard disk drive.

After Client Security Software is converted to an advanced configuration, it cannot be converted back to a typical configuration.

## **Advanced configuration**

The *advanced configuration* of IBM Client Security Software configures the following *additional* Client Security features:

- **UVM-logon protection**
- **Key storage location selection**
- **Application support:** Entrust, File and Folder Encryption, Lotus Notes

---

## **Using the IBM Client Security Setup Wizard**

The IBM Client Security Setup Wizard provides an interface that helps you install Client Security Software and enable the IBM embedded Security Chip. Complete the following procedure to allow the IBM Client Security Setup Wizard to guide you through the necessary tasks involved in setting up a security policy on an IBM client.

The general steps that the IBM Client Security Setup Wizard guides you through are as follows. The specific steps differ depending upon the configuration option you select.

- **Set a Security Administrator Password**  
The security administrator password, referred to in these manuals as the administrator password, is used to control access to the IBM Client Security Administrator Utility, which is used to change the security settings for this computer.
- **Create Administrator Security Keys**

Administrator security keys are a set of digital keys that are stored in a computer file. These key files are also referred to as the administrator keys, administrator key pair, or the archive key pair. It is recommended that you save these vital security keys on a removable disk or drive. When a change to the security policy is made in the Administrator Utility, you will be prompted for an administrator key to prove that the policy change is authorized.

Backup security information is also saved in case you ever need to replace the system board or hard drive of your computer. Store this backup information somewhere off the local system.

- **Protect Applications with IBM Client Security**

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

- **Authorize Users**

Users need to be authorized before they can access the computer. When you authorize a user, you must specify that user's passphrase. Unauthorized users are not permitted to use the computer.

- **Select a System Security Level**

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

## Using the Setup Wizard to complete a typical configuration

To use the IBM Client Security Setup Wizard to complete a typical configuration, complete the following procedure:

1. Click **Start > Programs > Access IBM > IBM Client Security Software > IBM Client Security Setup Wizard**.

The Welcome to the IBM client Security Setup Wizard screen enables you to select a configuration option.

2. Select the Typical configuration (recommended) radio buttons and click **Next**.

This selection enables IBM Password Manager and requires entry of only a few parameters. When you select the typical configuration, CSS stores your backup information and security keys on your hard drive. Novice security users should use the typical configuration option. This is the default setting.

The Passphrase Entry screen is displayed.

3. Complete the following tasks:

- a. Enter a passphrase in the Enter passphrase field. If necessary, click the **View passphrase requirements** button for help establishing a valid passphrase.

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

- b. Type a word or phrase in the passphrase hint field.

- c. Click **Next**.

If a fingerprint reader is detected on your computer, the Fingerprint Storage screen is displayed. The **Yes, I would like to store fingerprints now** check box is checked by default.

4. Do one of the following:

- Clear the **Yes, I would like to store fingerprints now** check box and then click **Next**.

- Click **Next** and follow the onscreen instructions to begin registering your fingerprints now.

The Authorize Additional Users screen is displayed.

5. Do one of the following:

- Check the **Select additional users to authorize now (Optional)** check box and then click **Next**.
- Click **Skip** to skip this task.

The Summary of Your Security Settings and Features screen is displayed.

6. Click **Finish** to implement the security settings you have selected. This process might take a few minutes. A message is displayed indicating that your computer is now protected by IBM Client Security.
7. Click **OK**.

---

## Using the Setup Wizard to complete an advanced configuration

To use the IBM Client Security Setup Wizard to complete a typical configuration, complete the following procedure:

1. Click **Start > Programs > Access IBM > IBM Client Security Software > IBM Client Security Setup Wizard**.

The Welcome to the IBM client Security Setup Wizard screen enables you to select a configuration option.

2. Select the **Advanced configuration** radio button and click **Next**.

This selection requires you to specify configuration information, such as a key storage location and a security level, and it allows you to enable CSS logon protection, Lotus Notes protection and IBM Password Manager.

The Set Security Administrator Password screen is displayed.

3. Type your Security Administrator Password in the Enter Administrator Password field and click **Next**.

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

The Create Administrator Security Keys screen is displayed.

4. Do one of the following:

- **Create new security keys**

To create new security keys, use the following procedure:

- a. Click the **Create new keys** radio button.
- b. Specify where you want to save the administrator security keys by either typing the path name in the provided field or by clicking **Browse** and selecting the appropriate folder.
- c. If you want to split the security key for increased protection, click the **Split the archive key for increased security** check box so that a check mark appears in the box, and then use the arrows to select the desired number in the **Number of splits** scroll box.

- **Use an existing security key**

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

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

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

The Protect Applications with IBM Client Security screen is displayed.

7. Enable IBM Client Security protection by selecting the appropriate check boxes so that a check mark appears in each selected box, and clicking **Next**. The available Client Security selections are as follows:

- **Secure access to your system by replacing the normal Windows logon with the Client Security secure logon**

Select this box to replace the normal Windows logon with the Client Security secure logon. This increases the security of your system, and allows logon only after authentication with the IBM Embedded Security Chip and optional devices, like fingerprint readers or smart cards.

- **Enable file and folder encryption**

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

- **Enable IBM Client Security Password Manager support**

Select this box if you want to use the IBM Password Manager to conveniently and securely store passwords for your Web site logons and applications.

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

Select this box if you want Client Security to authenticate Lotus Notes users through the IBM embedded Security Chip.

- **Enable Entrust support**

Select this box if you want to enable integration with Entrust security software products.

- **Protect Microsoft Internet Explorer**

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

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

8. Complete the Authorizing Users screen by completing one of the following procedures:

- To authorize users to perform IBM Client Security functions, do the following:
  - a. Select a user in the Unauthorized Users area.
  - b. Click **Authorize User**.
  - c. Type and confirm your IBM Client Security passphrase in the provided fields and click **Next**.

The UVM Passphrase Expiration screen is displayed.

- d. Set the passphrase expiration for the user and click **Finish**.

- e. Click **Next**.
- To unauthorize users from performing IBM Client Security functions, do the following:
  - a. Select a user in the Authorized Users area.
  - b. Click **Unauthorize User**.  
The message, "Are you sure you want to unauthorize?" is displayed.
  - c. Click **Yes**.
  - d. Click **Next**.

The Select System Security Level screen is displayed.

9. Select the desired authentication requirements by clicking the appropriate check boxes. You can select more than one authentication requirement.
  - The **Use UVM passphrase** check box is selected as default.
  - The fingerprint reader device driver and smart card reader device driver must be installed before starting the IBM Client Security Setup Wizard for these devices to be available to the Setup Wizard.
  - Select a system security level by dragging the slide selector to the desired security level and click **Next**.

**Note:** You can define a custom security policy later using the Policy Editor in the Administrator Utility.

The Setup Complete - Review Security Settings screen is displayed.

10. Review your security settings and take one of the following actions:
  - To accept the settings, click **Finish**.
  - To change the settings, click **Back**, make the appropriate changes; then return to this screen and click **Finish**.

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

11. Click **OK**.

---

## Enabling the IBM Security Subsystem

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

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

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

A screen displays a message that states that the IBM Security Subsystem has not been enabled, and that asks if you would like to enable it now.

2. Click **Yes**.

A message is displayed stating that if you have a supervisor password or a BIOS administrator password enabled, you must disable it in the BIOS Setup Utility before continuing.

3. Do one of the following:
  - If you have a supervisor password enabled, click **Cancel**, disable your supervisor password, and then complete this procedure.
  - If you do not have a supervisor password enabled, click **OK** to continue.

4. Close all open applications and click **OK** to restart the computer.
5. After the system restarts, click **Start > Settings > Control Panel > IBM Embedded Security Subsystem** to open the Administrator Utility.  
A message is displayed stating that the IBM Security Subsystem has not been configured or has been cleared. A new password is required at this time.
6. Enter and confirm a new administrator password in the appropriate fields and click **OK**.  
The operation is complete and the Administrator Utility main screen is displayed.

---

## Upgrading your version of Client Security Software

Clients that have installed previous versions of Client Security Software should update their software to this version to take advantage of new Client Security features.

**Important:** Systems that had IBM Client Security Software Version 4.0x installed must uninstall IBM Client Security Software version 4.0x and clear the chip before installing this version of IBM Client Security Software. Failure to do so might result in an installation failure, or non-responsive software.

### Upgrading using new security data

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

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

### Upgrading from CSS 5.0 or later using existing security data

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

1. Update your archive by completing the following steps:
  - a. Click **Start > Programs > Access IBM > IBM Client Security Software > Modify Your Security Settings**.
  - b. Click the **Update key archive** button to ensure that your backup information is updated.  
Note the archive directory.
  - c. Exit the IBM Client Security Software User Configuration Utility.
2. Upgrade the existing version of Client Security Software by completing the following steps:
  - a. From the Windows desktop, click **Start > Run**.
  - b. In the Run Field, type `d:\directory\csec5xxus_00yy.exe`, where `d:\directory\` is the drive letter and directory where the executable file is located. `xx` and `yy` are alpha-numeric.
  - c. Select **Upgrade**.

- d. Reboot the system.

---

## Uninstalling Client Security Software

Be sure that you uninstall the various utilities (IBM Client Security Password Manager, IBM Client Security File and Folder Encryption (FFE) utility) that enhance Client Security functionality, such as the IBM before you uninstall IBM Client Security Software. Users must log on with administrator rights to uninstall Client Security Software.

**Note:** You must uninstall all IBM Client Security Software utilities and all UVM-aware sensor software before you uninstall IBM Client Security Software. The administrator password is required to uninstall Client Security Software.

To uninstall Client Security Software, complete the following procedure:

1. Close all Windows programs.
2. From the Windows desktop, click **Start > Settings > Control Panel**.
3. Click the **Add/Remove Programs** icon.
4. In the list of software that can be automatically removed, select **IBM Client Security**.
5. Click **Add/Remove**.
6. Select the **Remove** radio button.
7. Click **Next** to uninstall the software.
8. Click **OK** to confirm this action.
9. Type the administrator password in the provided interface and click **OK**.
10. Do one of the following:
  - If you installed the IBM embedded Security Chip PKCS#11 module for Netscape, a message is displayed that asks you to start the process to disable the IBM embedded Security Chip PKCS#11 module. Click **Yes** to proceed.  
A series of messages will be displayed. Click **OK** for each message until the IBM embedded Security Chip PKCS#11 module is removed.
  - If you did not install the IBM embedded Security Chip PKCS#11 module for Netscape, a message is displayed that asks if you want to delete shared DLL files that were installed with Client Security Software.  
Click **Yes** to uninstall these files, or click **No** to leave the files installed.  
Leaving these files installed has no affect on the normal operation of your computer.  
The message "Would you like to remove this system's information from the archive?" is displayed. If you select **No**, you can restore the information when you reinstall the newer version of IBM Client Security Software.
11. Click **Finished** after the software is removed.  
You must restart the computer after uninstalling Client Security Software.

When you uninstall Client Security Software, you remove all installed Client Security software components along with all user keys, digital certificates, registered fingerprints and stored passwords.

---

## Export regulations

IBM Client Security Software contains encryption code that can be downloaded within North America and internationally. If you live in a country where downloading encryption software from a Web site in the United States is prohibited, you cannot download IBM Client Security Software. For more information on export regulations that govern IBM Client Security Software, see Appendix A, “U.S. export regulations for Client Security Software,” on page 31.



---

## Chapter 5. Troubleshooting

The following section presents information that is helpful for preventing, or identifying and correcting problems that might arise as you install or configure Client Security Software.

---

### Administrator functions

#### Authorizing users

Before client user information can be protected, IBM Client Security Software **must** be installed on the client and users **must** be authorized to use the software. An easy-to-use Setup Wizard guides you through the entire installation process.

**Important:** At least one client user **must** be authorized to use UVM during setup. If no user is authorized to use UVM when initially setting up Client Security Software, your security settings will **not** be applied and your information will **not** be protected.

If you completed the Setup Wizard without authorizing any users, shut down and restart your computer; then run the Client Security Setup Wizard from the Windows Start menu and authorize a Windows user to use UVM. This will enable IBM Client Security Software to apply your security settings and protect your sensitive information.

#### Setting a BIOS administrator password (ThinkCentre)

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

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

**Attention:**

- When the IBM embedded Security Subsystem is cleared, all encryption keys and certificates stored on the subsystem are lost.

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

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

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

## Setting a supervisor password (ThinkPad)

Security settings available in the IBM BIOS Setup Utility enable administrators to perform the following tasks:

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

### Attention:

- It is necessary to temporarily disable the supervisor password on some ThinkPad models before installing or upgrading Client Security Software.

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

To set a supervisor password, complete one of the following procedures:

### Example 1

1. Shut down and restart the computer.
2. When the Setup Utility prompt appears on the screen, press F1.  
The main menu of the Setup Utility opens.
3. Select **Password**.
4. Select **Supervisor Password**.
5. Type your password and press Enter.
6. Type your password again and press Enter.
7. Click **Continue**.
8. Press F10 to save and exit.

### Example 2

1. Shut down and restart the computer.
2. When the "To interrupt normal startup, press the blue Access IBM button" message is displayed, press the blue Access IBM button.  
The Access IBM predesktop area opens.
3. Double-click **Start setup utility**.
4. Select **Security** using the directional keys to navigate down the menu.
5. Select **Password**.
6. Select **Supervisor Password**.
7. Type your password and press Enter.
8. Type your password again and press Enter.
9. Click **Continue**.

10. Press F10 to save and exit.

After you set a supervisor password, a prompt appears each time you attempt to access the BIOS Setup Utility.

**Important:** Keep a record of your supervisor password in a secure place. If you lose or forget the supervisor password, you cannot access the IBM BIOS Setup Utility, and you cannot change or delete the password. See the hardware documentation that came with your computer for more information.

## Clearing the IBM embedded Security Subsystem (ThinkCentre)

If you want to erase all user encryption keys from the IBM embedded Security Subsystem and clear the administrator password for the subsystem, you must clear the chip. Read the information below before clearing the IBM embedded Security Subsystem.

### Attention:

- When the IBM embedded Security Subsystem is cleared, all encryption keys and certificates stored on the subsystem are lost.

To clear the IBM embedded Security Subsystem, complete the following procedure:

1. Shut down and restart the computer.
2. When the Setup Utility prompt appears on the screen, press F1.  
The main menu of the Setup Utility opens.
3. Select **Security**.
4. Select **IBM TCPA Security Feature** and press Enter.
5. Select **Yes**.
6. Press Enter to confirm your choice.
7. Press F10 to save your changes and exit the Setup Utility.
8. Select **Yes** and press Enter. The computer will restart.

## Clearing the IBM embedded Security Subsystem (ThinkPad)

If you want to erase all user encryption keys from the IBM embedded Security Subsystem and clear the administrator password, you must clear the subsystem. Read the information below before clearing the IBM embedded Security Subsystem.

### Attention:

- When the IBM embedded Security Subsystem is cleared, all encryption keys and certificates stored on the subsystem are lost.

To clear the IBM embedded Security Subsystem, complete the following procedure:

1. Shut down and restart the computer.
2. When the Setup Utility prompt appears on the screen, press F1.  
The main menu of the Setup Utility opens.
3. Select **Security**.
4. Select **IBM Security Chip** and press Enter.
5. Press Enter and select **Disabled**.
6. Press Enter to confirm your choice.
7. Press Enter to continue.

8. Press F10 to save your changes and exit the Setup Utility.
9. Select **Yes** and press Enter. The computer will restart.

---

## Known issues or limitations with CSS Version 5.4

The following information might be helpful when installing or configuring Client Security Software Version 5.4.

### Re-installing Targus fingerprint software

If the Targus fingerprint software is removed and re-installed, the needed registry entries for enabling fingerprint support in Client Security Software must be added manually for fingerprint support to be enabled. Download the registry file that contains the needed entries (atplugin.reg) and double-click it to have the registry entries merged into the registry. Click **Yes**, when prompted, to confirm this operation. The system must be rebooted for Client Security Software to recognize the changes and enable fingerprint support.

**Note:** You must have administrator privileges on the system in order to add these registry entries.

### BIOS supervisor passphrase

IBM Client Security Software 5.4 and earlier does not support the BIOS supervisor passphrase feature available on some ThinkPad systems. If you enable use of the BIOS Supervisor Passphrase, any enabling and disabling of the security subsystem must be done from BIOS Setup.

### Smart card limitations

#### Registering smart cards

Smart cards must be registered with UVM before a user can successfully authenticate using the card. If one card is assigned to multiple users, only the last user to register the card will be able to use the card. Consequently, smart cards should be registered for one user account only.

---

## Troubleshooting charts

The following section contains troubleshooting charts that might be helpful if you experience problems with Client Security Software.

### Installation troubleshooting information

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

Problem Symptom	Possible Solution
<b>An error message is displayed during software installation</b>	<b>Action</b>
A message is displayed when you install the software that asks if you want to remove the selected application and all of its components.	Click <b>OK</b> to exit the window. Begin the installation process again to install the new version of Client Security Software.

Problem Symptom	Possible Solution
A message is displayed during installation stating that you must upgrade or remove the program.	Do one of the following: <ul style="list-style-type: none"> <li>• If a version prior to Client Security Software 5.0 is installed, select <b>Remove</b> to remove it. Then, restart the computer and clear the security subsystem using the IBM BIOS Setup Utility.</li> <li>• Otherwise, select <b>Upgrade</b> and continue the installation.</li> </ul>
<b>Installation access is denied due to an unknown administrator password</b>	<b>Action</b>
When installing the software on an IBM client with an enabled IBM embedded Security Subsystem, the administrator password for the IBM embedded Security Subsystem is unknown.	Clear the security subsystem to continue with the installation.
<b>An error message is displayed when attempting certain Client Security administrator functions</b>	<b>Action</b>
An error message is displayed after trying to perform a Client Security administrator function.	The ThinkPad supervisor password or ThinkCentre BIOS administrator password must be disabled to generate the hardware key pair on a Crypto 1 (non-TCG) system. The CSS installation process cannot enable the IBM embedded Security Subsystem until the appropriate password is disabled.



---

## **Appendix A. U.S. export regulations for Client Security Software**

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

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



---

## Appendix B. Password and passphrase information

This appendix contains password and passphrase information.

---

### Password and passphrase rules

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

#### Administrator password rules

An interface in the Administrator Utility enables security administrators to control administrator password criteria through a simple interface. This interface enables an administrator to establish the following administrator password rules:

**Note:** The default setting for each passphrase criterion is provided in parenthesis below. The administrator password never expires.

- establish whether to set a minimum number of alphanumeric characters allowed (yes, 6)  
For example, when set to "6" characters allowed, 1234567xxx is an invalid password.
- establish whether to set a minimum number of digit characters allowed (yes, 1)  
For example, when set to "1", thisismypassword is an invalid password.
- establish whether to set the minimum number of spaces allowed (no minimum)  
For example, when set to "2", i am not here is an invalid password.
- establish whether to enable the passphrase to begin with a digit (no)  
For example, by default, 1password is an invalid password.
- establish whether to enable the passphrase to end with a digit (no)  
For example, by default, password8 is an invalid password.

The following general rules pertain to the administrator password:

#### Length

The password can be up to 256 characters long.

#### Characters

The password can contain any combination of characters that the keyboard produces, including spaces and non-alphanumeric characters.

#### Properties

The administrator password is different from a password that you might use to log on to an operating system. The administrator password can be used in conjunction with other authenticating devices, such as a UVM-aware fingerprint sensor.

#### Incorrect attempts

If you incorrectly type the administrator password multiple times during a session, the computer will exercise a series of anti-hammering delays.

## UVM passphrase rules

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

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

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

- establish whether to set a minimum number of alphanumeric characters allowed (yes, 6)  
For example, when set to "6" characters allowed, 1234567xxx is an invalid password.
- establish whether to set a minimum number of digit characters allowed (yes, 1)  
For example, when set to "1", thisismypassword is an invalid password.
- establish whether to set the minimum number of spaces allowed (no minimum)  
For example, when set to "2", i am not here is an invalid password.
- establish whether to enable the passphrase to begin with a digit (no)  
For example, by default, 1password is an invalid password.
- establish whether to enable the passphrase to end with a digit (no)  
For example, by default, password8 is an invalid password.
- establish whether to allow the passphrase from containing a user ID (no)  
For example, by default, UserName is an invalid password, where UserName is a User ID.
- establish whether to ensure that the new passphrase is different from the last x passphrases, where x is an editable field (yes, 3)  
For example, by default, mypassword is an invalid password if any of your last three passwords was mypassword.
- establish whether the passphrase can contain more than three identical consecutive characters in any position from the previous password (no)  
For example, by default, paswor is an invalid password if your previous password was pass or word.

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

- establish whether to have the passphrase expire after a set number of days (yes, 184)  
For example, by default the passphrase will expire in 184 days. The new passphrase must adhere to the established passphrase policy.
- establish whether the passphrase will expire (yes)  
When this option is selected, the passphrase will never expire.

The passphrase policy is checked in the Administrator Utility when the user is enrolled, and is also checked when the user changes the passphrase from the

Client Utility. The two user settings related to the previous password will be reset and any passphrase history will be removed.

The following general rules pertain to the UVM passphrase:

**Length**

The passphrase can be up to 256 characters long.

**Characters**

The passphrase can contain any combination of characters that the keyboard produces, including spaces and non-alphanumeric characters.

**Properties**

The UVM passphrase is different from a password that you might use to log on to an operating system. The UVM passphrase can be used in conjunction with other authenticating devices, such as a UVM-aware fingerprint sensor.

**Incorrect attempts**

If you incorrectly type the UVM passphrase multiple times during a session, the computer will exercise a series of anti-hammering delays. These delays are specified in the following section.

---

## Fail counts on systems using the National TPM

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

Attempts	Delay on next failure
7-13	4 seconds each
14-20	8 seconds each
21-27	16 seconds each
28-34	32 seconds each
35-41	64 seconds each (1.07 minutes each)
42-48	128 seconds each (2.13 minutes each)
49-55	256 seconds each (4.27 minutes each)
56-62	512 seconds each (8.53 minutes each)
63-69	1,024 seconds each (17.07 minutes each)
70-76	2,048 seconds each (34.13 minutes each)
77-83	68.26 minutes each (1.14 hours each)
84-90	136.52 minutes each (2.28 hours each)
91-97	273.04 minutes each (4.55 hours each)
98-104	546.08 minutes each (9.1 hours each)
105-111	1,092.16 minutes each (18.2 hours each)
112-118	2,184.32 minutes each (36.4 hours each)

National TPM systems do not distinguish between user passphrases and the administrator password. Any authentication using the IBM Embedded Security Chip adheres to the same policy. There is no maximum timeout. Each failed attempt triggers the delay indicated above. The anti-hammering delays do not end at the 118th attempt; rather, they continue in the manner illustrated above indefinitely.

---

## Fail counts on systems using the Atmel TPM

The following table shows the anti-hammering delay settings for an Atmel TPM system:

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

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

---

## Resetting a passphrase

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

### Resetting a passphrase remotely

To reset a password remotely, complete the following procedure:

- **Administrators**

A remote administrator must do the following:

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

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

- **Users**

The user must do the following:

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

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

This is the recommended manner to reset a lost passphrase.

## **Resetting a passphrase manually**

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



---

## Appendix C. Notices and Trademarks

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

---

### Notices

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

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

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

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

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

---

## Trademarks

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

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

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

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





Printed in USA