

*IBM® Client Security Solutions*

# **Client Security Software Version 1.3.1 Administrator's Guide**

**August 2000**

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 68 and “Appendix D - Notices and Trademarks,” on page 71.

**First Edition (August 2000)**

**Copyright International Business Machines Corporation 2000. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

---

## Table of Contents

<b>About this guide</b> .....	<b>5</b>
Who should read this guide .....	5
How to use this guide.....	6
Compare to the Installation Guide .....	6
Compare to Using Client Security with Policy Director.....	6
Compare to the Client User's Guide .....	6
What is new in this release .....	6
Conventions used in this guide.....	7
Additional information .....	7
<b>Chapter 1 - Understanding IBM Client Security Software</b> .....	<b>8</b>
Client Security Software components .....	8
How to use Client Security Software .....	9
Example 1 - Two IBM clients that uses Windows NT 4.0 and Outlook Express for e-mail.....	9
Example 2 - Two IBM clients that use Windows 98, Lotus Notes, and will use the Client Security screen saver .....	10
Example 3 - Multiple IBM clients that use Windows NT 4.0, Netscape for e-mail, and that will be managed by Policy Director .....	11
<b>Chapter 2 - Adding users to UVM</b> .....	<b>14</b>
UVM and elements of authentication .....	14
Before you add users to UVM.....	15
Setting up authentication for client users .....	16
Add a user to UVM.....	16
Set up UVM protection for the operating system logon.....	18
Register user fingerprints with UVM.....	18
<b>Chapter 3 - Working with UVM policy</b> .....	<b>20</b>
Editing a local UVM policy.....	21
Editing and using UVM policy for remote clients.....	23
Changing the password for a UVM-policy file.....	25
<b>Chapter 4 - Setting up UVM protection for Lotus Notes</b> .....	<b>27</b>
Enable UVM protection for a User ID.....	27
Disable UVM protection for a User ID.....	29
Set up UVM protection for a switched User ID.....	30
<b>Chapter 5 - Using other features of the Administrator Utility</b> .....	<b>31</b>
Update the key archive .....	31
Reset the authentication fail counter .....	32
Changing information for Policy Director settings .....	33
Editing Policy Director setup information .....	33
Refreshing the local cache.....	33
Change the admin public key.....	34
Restore keys .....	35
System board replacement.....	35
Hard disk drive failure.....	37
Recover a UVM passphrase.....	38
Change the hardware password .....	40
View information about Client Security Software.....	41
Disable the IBM embedded Security Chip .....	41
Enabling the IBM embedded Security Chip and setting a hardware password .....	42
<b>Chapter 6 - Instructions for the client user</b> .....	<b>44</b>

## **Client Security Software**

Using UVM protection for the system logon .....	44
Windows NT.....	44
Windows 98 and Windows 95.....	45
Setting up the Client Security screen saver .....	45
Using the Client Utility .....	46
Using secure e-mail and Web browsing .....	48
Tips for using Client Security Software with Microsoft applications .....	48
Tips for using Client Security Software with Netscape applications.....	49
<b>Chapter 7 - Troubleshooting .....</b>	<b>53</b>
Administrator tips.....	53
Set an administrator password in the Configuration/Setup Utility .....	53
Protect the hardware password .....	54
Clearing the IBM embedded Security Chip.....	54
Known limitations .....	55
Client Security Software and Netscape.....	55
IBM embedded Security Chip certificate and encryption algorithms .....	55
Administrator Utility.....	56
UVM protection for a Lotus Notes User ID.....	56
Event log error messages .....	56
Error messages if access to an authentication object is denied .....	56
Troubleshooting charts.....	57
Client Security Software and Microsoft applications.....	57
Client Security Software and Netscape.....	61
Obtaining a digital certificate .....	64
Client Security Software and Lotus Notes.....	64
Administrator Utility.....	65
UVM-aware devices .....	67
<b>Appendix A - U.S. export regulations for Client Security Software .....</b>	<b>68</b>
<b>Appendix B - Rules for the hardware password and the UVM passphrase .....</b>	<b>69</b>
<b>Appendix C - Rules for using UVM protection for system logon .....</b>	<b>70</b>
<b>Appendix D - Notices and Trademarks .....</b>	<b>71</b>
Notices .....	71
Trademarks .....	72

---

## About this guide

The guide contains information to help an administrator set up and use the security features provided with Client Security Software.

The guide contains the following chapters:

“Chapter 1 - Understanding IBM Client Security Software,” contains an overview of the software components that are included. Also, specific examples are provided that can help you decide how to use Client Security Software.

“Chapter 2 - Adding users to UVM,” contains instructions for adding new users to User Verification Manager (UVM). Also, instructions about how to set up UVM protection for the operating-system logon are provided.

“Chapter 3 - Working with UVM policy,” contains information about editing and saving UVM policy for IBM clients.

“Chapter 4 - Setting up UVM protection for Lotus Notes” contains instructions for setting up UVM protection for a Lotus Notes® User ID.

“Chapter 5 - Using other features of the Administrator Utility,” contains instructions for using the many features provided by the Administrator Utility.

“Chapter 6 - Instructions for the client user,” contains instructions for different tasks that the client user performs when using Client Security Software. Instructions for using UVM protection for the operating system logon, the Client Security screen saver, secure e-mail and the Client Utility are included. This information is also provided in the *Client Security User's Guide*.

“Chapter 7 - Troubleshooting,” contains administrator tips, known limitations and troubleshooting information associated with Client Security Software.

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

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

“Appendix C - Rules for using UVM protection,” contains important information for using UVM protection for operating system logon.

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

---

## Who should read this guide

This guide is written for security administrators who will do the following:

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

**Policy Director administrators:** An enterprise security administrator who plans to use IBM Tivoli® SecureWay® Policy Director to manage authentication objects

## Client Security Software

provided in UVM policy should read this guide. The Policy Director administrator must be able to do the following:

- manage the Policy Director object space
- manage authentication, authorization, and credentials acquisition and have knowledge of these processes
- manage the IBM Distributed Computing Environment (DCE) and the IBM SecureWay Directory's lightweight directory access protocol (LDAP)

---

### How to use this guide

Use this guide to set up user authentication and UVM security policy for IBM clients. This guide is a companion to the *Client Security Software Installation Guide*, *Using Client Security with Policy Director*, and *Client Security User's Guide*. All guides are available for download from the following IBM Web site:

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

### Compare to the Installation Guide

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

### Compare to Using Client Security with Policy Director

If you are a security administrator who plans to use Policy Director to manage the authentication objects for UVM policy, read *Using Client Security with Policy Director*.

### Compare to the Client User's Guide

As an administrator, you can use this guide to set up and maintain UVM policy on IBM clients that use Client Security Software. After you set up user authentication and UVM security policy, the client user can read the *Client Security User's Guide* to learn how to use the features provided by Client Security Software.

The *Client Security User's Guide* contains information that a client user will find helpful when performing tasks with Client Security Software, such as using UVM protection for the operating system logon and the screen saver, creating a digital certificate, and using the Client Utility.

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

---

### What is new in this release

The new features in Client Security Software version 1.3.1 are:

- Windows 2000 support
- Support for select NetVista computers

---

## **Conventions used in this guide**

Throughout this document, IBM networked computers that have the IBM embedded Security Chip are referred to as *IBM clients* or *clients*.

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

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

---

## **Additional information**

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

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

---

## Chapter 1 - Understanding IBM Client Security Software

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

- Encryption key management for public key cryptography.
- Digital certificate creation and storage that is protected by the IBM embedded Security Chip.
- Administrator control over client security policy.
- A key archive and recovery solution.

---

### Client Security Software components

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

- **User Verification Manager:** User Verification Manager (UVM) is software that enables you to set a security policy (called UVM policy) for clients. UVM policy dictates how a client user is authenticated on the system. You can set up both a UVM passphrase and user fingerprints as elements of authentication. Fingerprint registration with UVM is possible with an optional UVM-aware fingerprint sensor.
- **UVM protection for the system logon:** UVM protection for the system logon enables you to control access to the computer through a logon interface. UVM protection ensures that only those users who are recognized by the security policy of the computer are able to access the operating system.
- **Administrator Utility:** The Administrator Utility is the administrator interface that you use to set up user authentication and UVM policy. Also, any management of the key archive, admin keys, and embedded Security Chip are controlled through the Administrator Utility.
- **Client Security screen saver:** The Client Security screen saver enables you to control access to the computer through a screen saver interface.
- **Client Utility:** The Client Utility enables a client user to change the UVM passphrase. For Microsoft Windows NT® 4.0 users, the Client Utility enables a user to change the Windows NT logon password so that it is recognized by UVM.<sup>1</sup> Also, the user can update the key archive with the Client Utility. A user can create backup copies of the digital certificates created with the IBM embedded Security Chip by updating the key archive.
- **Support for the Microsoft CryptoAPI:** Support for Microsoft CryptoAPI is built into Client Security Software. Defined by Microsoft, CryptoAPI is used as the default cryptographic service for Microsoft operating systems and

---

<sup>1</sup> If you change the Windows NT logon through User Manager, you must also change the password in the Client Utility so that it is recognized by UVM protection. For details, see “Using the Client Utility,” on page 46.



## Client Security Software

applications. With built-in CryptoAPI support, Client Security Software enables you to use the cryptographic operations of the IBM embedded Security Chip when you create digital certificates for Microsoft applications.

- **Support for PKCS#11:** Defined by RSA Data Security Inc., PKCS#11 is used as the cryptographic standard for Netscape and other products. After you install the IBM embedded Security Chip PKCS#11 module, you can use the IBM embedded Security Chip when you generate a digital certificate for Netscape applications and other applications that use PKCS#11.
- **Support for Lotus Notes:** Use the Lotus Notes Configuration feature to set up UVM protection for your Lotus Notes User ID.

---

## How to use Client Security Software

The information in this section provides different examples for using Client Security Software. As an administrator, you can use the multiple components provided by Client Security Software to set up the security features that IBM client users require. For example, Windows NT users can set up UVM protection for their system logon which prohibits unauthorized users from logging on to the IBM client.

### Example 1 - Two IBM clients that uses Windows NT 4.0 and Outlook Express for e-mail

For example 1, note the following:

- Two IBM clients (client 1 and client 2) have both Windows NT 4.0 and Outlook Express installed.
- Three users will require authentication setup with UVM on client 1; one client user will require authentication setup with UVM on client 2.
- All client users will register their fingerprints so that they can be used for authentication. A UVM-aware fingerprint sensor will be installed during this example.
- Both client 1 and client 2 will require UVM protection for the Windows NT logon.
- A local UVM policy will be edited and used at each client.

To set up client security, do the following:

1. Install the software on client 1 and client 2. Read the *Client Security Software Installation Guide* for details.
2. Install the UVM-aware fingerprint sensors and any associated software on client 1 and client 2. For information about UVM-aware products, go to the following IBM Web site:  
<http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html>
3. Set up user authentication with UVM for client 1 and client 2. Read "Chapter 2 - Adding users to UVM," on page 14 for details. Do the following:
  - Add users to UVM by assigning them a UVM passphrase. Because client 1 has three users, you must repeat the process for adding users to UVM until all users have been added.
  - Set up UVM protection for the Windows NT logon on each client.

## Client Security Software

- Register user fingerprints. Because a policy will be set three users will use client 1, all three users must register their fingerprints.

**Note:** If you set fingerprint as an authentication requirement as part of UVM policy for a client, each user must register his or her fingerprints.

4. Edit and save a local UVM policy at each client that requires authentication for the following:
  - logging on the operating system
  - acquiring a digital certificate
  - using a digital signature for e-mail messages

For details, see “Editing a local UVM policy,” on page 21.

5. Restart each client to enable the UVM protection for the Windows NT logon.
6. Inform the users of the following:
  - The UVM passphrases that you have set for them.
  - The authentication requirements that you set in UVM policy for the IBM client.

Next, the users can do the following:

- Use UVM protection to lock and unlock the operating system.
- Apply for a digital certificate and choose the embedded Security Chip as the cryptographic service provider associated with the certificate.
- Use the digital certificate to encrypt e-mail messages created with Outlook Express. For more information, see “Tips for using Client Security Software with Microsoft applications,” on page 48.
- Read the *Client Security User's Guide* to learn how to use the Client Utility.

### Example 2 - Two IBM clients that use Windows 98, Lotus Notes, and will use the Client Security screen saver

For example 2, note the following:

- Two IBM clients (client 1 and client 2) have Windows® NT 98 and Lotus Notes installed.
- Two users will require authentication setup with UVM on client 1; one user will require authentication setup with UVM on client 2.
- Both client 1 and client 2 will require UVM protection for the system logon.
- Both client 1 and client 2 will use the Client Security screen saver.
- Both client 1 and client 2 will use UVM protection for Lotus Notes.
- A UVM policy for remote clients will be edited on client 1, and then the policy will be copied to client 2.

To set up client security, do the following:

1. Install the software on client 1 and client 2. Because a UVM policy for remote clients will be used, you must use the same admin public key when you install the software on both client 1 and client 2. Read *the Client Security Software Installation Guide* for details about the software installation.

## Client Security Software

2. Set up user authentication with UVM for client 1 and client 2. Read “Chapter 2 - Adding users to UVM,” on page 14 for details. Do the following:
  - Add users to UVM by assigning them a UVM passphrase. Because client 1 has two users, you must repeat the process for adding users to UVM until both users have been added.
  - Set up UVM protection for Windows 98 logon on each client.
3. Enable UVM protection for Lotus Notes on both clients. For more information, see “Chapter 4 - Setting up UVM protection for Lotus Notes,” on page 27.
4. Edit and save a UVM policy for remote clients on client 1, and then copy that policy to client 2. UVM policy would require user authentication for clearing the screen saver, logging on to Lotus Notes, and logging on the operating system. For details, see “Editing and using UVM policy for remote clients,” on page 23.
5. Restart each client to enable the UVM protection for the system logon.
6. Inform the client users of the UVM passphrases and the policy that has been set for each client. Next, the users can read the *Client Security User’s Guide* to learn how to do the following:
  - enable the Client Security screen saver
  - use UVM protection for Windows 98

### **Example 3 - Multiple IBM clients that use Windows NT 4.0, Netscape for e-mail, and that will be managed by Policy Director**

The intended audience for the following example is an enterprise administrator who plans to use Policy Director to manage the authentication objects that are set by UVM policy. For example 3, note the following:

- Multiple IBM clients have both Windows NT 4.0 and Netscape installed.
- All clients have NetSEAT client, a Policy Director component, installed. Although NetSEAT client can be installed on Windows 98 and Windows 95 clients, you can use Policy Director in conjunction with Client Security software only on IBM clients running Windows NT 4.0. For details, see *Using Client Security with Policy Director*.
- If required, all clients have LDAP client installed. Install LDAP client only if Policy Director is used with an LDAP server.
- One user will require authentication setup with UVM on each client.
- All users will register their fingerprints so that they can be used for authentication. A UVM-aware fingerprint sensor will be installed during this example.
- All clients will require UVM protection for the Windows NT logon.
- UVM policy for remote clients will be installed on all clients. UVM policy will enable Policy Director to control selected authentication objects for the clients.

To set up client security, do the following:

## Client Security Software

1. Install the Client Security component on the Policy Director server. For details, see *Using Client Security with Policy Director*.
2. Install Client Security Software on all clients. Because a UVM policy for remote clients will be used, you must use the same admin public key when you install the software on all clients. Read *the Client Security Software Installation Guide* for details about the software installation.
3. Install the UVM-aware fingerprint sensors and any associated software on each client. For information about available UVM-aware products, go to the following IBM Web site:  
<http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html>
4. Set up user authentication with UVM on each client. Read “Chapter 2 - Adding users to UVM,” on page 14 for details. Do the following:
  - Add users to UVM by assigning them a UVM passphrase.
  - Set up UVM protection for the Windows NT logon on each client.
  - Register the fingerprints for each client user.

**Note:** If fingerprint authentication is required on an IBM client, all users of that client must register their fingerprints.
5. Configure the Policy Director setup information at each client. For details, see *Using Client Security with Policy Director*.
6. Edit and save a UVM policy for remote clients on one of the clients, and then copy that UVM policy to the other clients. Set UVM policy so that Policy Director will control the following authentication objects:
  - logging on the operating system
  - acquiring a digital certificate
  - using a digital signature for e-mail message

For details, see “Editing and using UVM policy for remote clients,” on page 23.
7. Restart each client to enable the UVM protection for the Windows NT logon.
8. Install the IBM embedded Security Chip PKCS#11 module onto each client. This module provides cryptographic support on clients that use Netscape for sending and receiving e-mail messages, and the IBM embedded Security Chip for acquiring digital certificates. For more information, see “Install the IBM embedded Security Chip PKCS#11 module,” on page 50.
9. Use Policy Director to control the IBM Client Security Solutions objects that appear in the Policy Director Management Console.
10. Inform the client users of the following:
  - the UVM passphrases that have been set
  - the policy that has been set for each client

## **Client Security Software**

Next, the client users can read the *Client Security User's Guide* to learn how to do the following:

- use UVM protection to lock and unlock the operating system
- use the Client Utility
- apply for digital certificate that uses the embedded Security Chip as the cryptographic service provider associated with the certificate
- use the digital certificate to encrypt e-mail messages created with Netscape

---

## Chapter 2 - Adding users to UVM

End user authentication is one of the most important aspects of client security. The software component of Client Security Software that enables user authentication and security policy on the IBM client is User Verification Manager (UVM). Before you can use a security policy (called UVM policy) at the client level, you must add users to UVM. The Administrator Utility provides the interface for adding users and creating user authentication settings that are required by UVM.

---

### UVM and elements of authentication

Elements of authentication (such as the UVM passphrase and fingerprints) are used to verify users to the IBM client. If you add a user to UVM, you do the following:

- Assign a UVM passphrase for the client user. The UVM passphrase, which can be up to 256 characters, is the main authentication element used by UVM. When you assign a UVM passphrase, user encryption keys are created for that client user, and those encryption keys are stored in a single file that is managed by the IBM embedded Security Chip.
- Register user fingerprints with UVM (optional). If the IBM client uses a UVM-aware fingerprint sensor for authentication, you can register the user fingerprints with UVM.

**Note:** Look for future versions of Client Security Software that will include support for other elements of authentication, such as a proximity badge or other biometrics devices. These authentication devices will interact with the UVM passphrase to provide another level of security when user authentication is required.

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

- **UVM protection** for the operating-system logon.<sup>2</sup> UVM protection ensures that only those users who are recognized by UVM are able to access the computer.

Before you enable UVM protection for the system logon, read “Appendix C - Rules for using UVM protection,” on page 70 for important information.

For information about using UVM protection, see “Using UVM protection for the system logon,” on page 44.

- **Client Security screen saver.** After you add a client user, the user can set up and use the Client Security screen saver. The Client Security screen saver is set up through the Display option within the operating-system software. For more information, see “Setting up the Client Security screen saver,” on page 45.

**Note:** You do not need to enable UVM protection for the system logon to use the Client Security screen saver.

---

<sup>2</sup> UVM protection for the system logon is not supported for clients running Windows 2000.

---

## **Before you add users to UVM**

If you add a client user to UVM, the Administrator Utility provides you with a list of user names from which you can select. The names in that list are the user accounts that have been added by using the operating system.

Before you add client users to UVM, use the operating-system software to create user accounts and profiles for those users. The following list describes the programs or procedures you can use to add new users for the respective operating system.

- **Windows 2000.** Use the Users and Passwords program to create new user accounts and manage user accounts or groups. See the operating system documentation for more information.
- **Windows NT Workstation 4.0.** Use the User Manager program to create new user accounts and manage user accounts or groups. See the operating system documentation for more information.
- **Windows 95 and Windows 98.** New users can be added by typing in a new user name and password in the logon application. See the operating system documentation for more information.

### **Notes:**

- If you plan to use the Microsoft Family Logon client with Windows 95 or Windows 98, read the Attention box for important information.
- In Windows 98, if you delete a user from the computer, the user name is not deleted from the list of users in the Administrator Utility.
- When you use the operating system software to add new users, the domain password for each new user must be the same.
- Client Security Software works in parallel with the security features provided by the operating system.

**Attention:** If you use the Microsoft Family Logon client for Windows 95 or Windows 98, do the following:

1. configure Microsoft Family Logon
2. use the operating-system software to create new users
3. assign UVM passphrases for users and set and use UVM protection for the system logon.

If Microsoft Family Logon is configured after UVM protection is enabled, you must immediately assign a UVM passphrase to at least one user ID in the list of users associated with the Microsoft Family Logon client. If you do not assign a UVM passphrase and the system is locked by UVM protection, you will not be able to access the operating system through a user logon.

In Windows 98, if you add a user through the Users program in Control Panel, Microsoft Family Logon might be added automatically, depending on the network settings. See Microsoft for more information on installing and using the Microsoft Family Logon client.

---

## Setting up authentication for client users

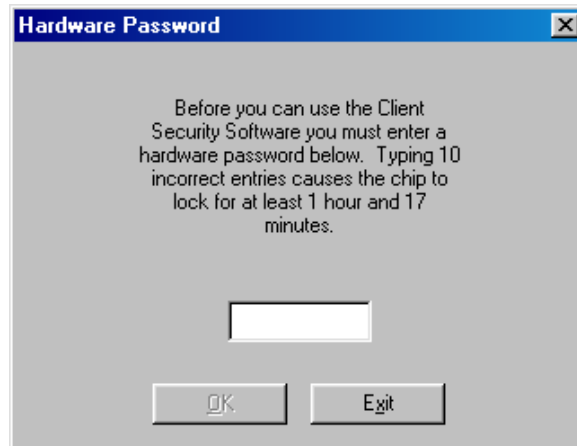
Read the following information before you add a user to UVM.

- You must generate the hardware encryption keys before you can add a new user. Normally, the hardware encryption keys are generated during the installation process. If you did not create the hardware keys, do not attempt to add a user; instead see the *Client Security Software Installation Guide* for instructions on creating the hardware encryption keys.
- For Windows 2000 and Windows NT users, you must log on with a user ID that has administrator user rights before you can open and use the Administrator Utility.

### Add a user to UVM

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

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

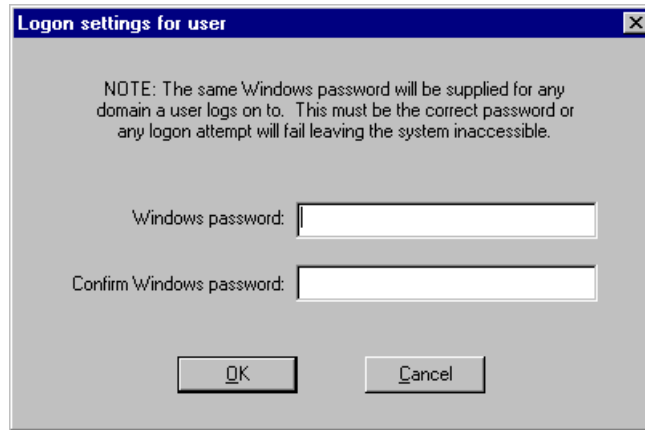


2. Type the hardware password and click **OK**. The Administrator Utility window opens.
3. Click the **User Authentication Setup** tab.
4. In the **Select a user** area, select a user name from the list. The user names in the list are defined by the user accounts created in the operating system.
5. In the **Add or reset selected user** area, type a new UVM passphrase for the selected user. For information on the rules for the UVM passphrase, see "Appendix B - Rules for the hardware password and the UVM passphrase," on page 69.
6. In the **Confirm UVM passphrase** field, type the passphrase again.



7. Click **Add or reset user**. A window opens that notifies you that the operation was successful. This operation created the client user encryption keys and assigned the UVM passphrase that you typed. Click **OK**.
8. Click **Windows logon settings**.

The logon settings window opens.



9. In the **Windows password** field, type the operating system password (the Windows password, not the UVM passphrase) associated with the user.  
**Note:** The same Windows password will be supplied for any domain on which the user logs on.
10. In the **Confirm Windows password** field, type the password again and click **OK**. A window opens that notifies you that the operation was successful. Click **OK**.

You have now added a user to UVM which created the user encryption keys for the client. To add another user, repeat the steps in this section.

**Note:** Notify the client users of the UVM passphrases that have been set. Users can change their UVM passphrases by using the Client Utility. For details, see “Using the Client Utility,” on page 46.

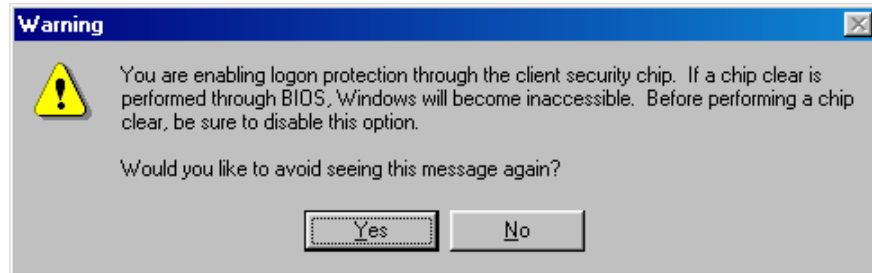
Now that you have added a user, you can set up additional security features provided by Client Security. You can do the following:

- Set up UVM protection for the operating system logon (see “Set up UVM protection for the operating system logon,” on page 18)
- Register user fingerprints with UVM (see “Register user fingerprints with UVM,” on page 18)
- Archive the user encryption keys that were created. See “Update the key archive,” on page 31 for more information.
- Set up and use the Client Security screen saver, see “Setting up the Client Security screen saver,” on page 45 for details.

### Set up UVM protection for the operating system logon

1. Select the **Use UVM protection** check box and the following window opens.

**Note:** The **Use UVM protection** check box is active if you have supplied the Windows logon password for the current user. If the check box is not available, go to step 8 on page 17 and complete the steps for providing the Windows logon password.



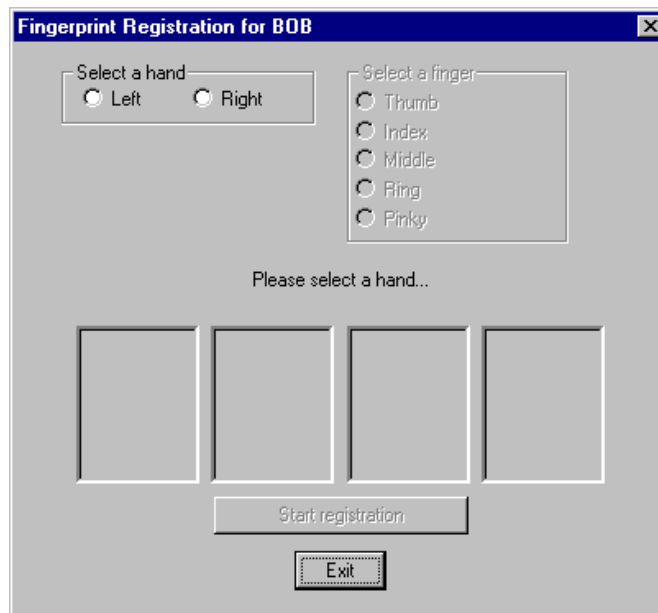
2. Click **Yes** or **No** to exit the warning window.

To activate UVM protection for the system logon, you must shut down and restart the computer. When the computer restarts, you will be prompted to log on to the computer. For details on using UVM protection, see "Using UVM protection for the system logon," on page 44.

**Note:** UVM protection for the system logon is not supported for clients running Windows 2000.

### Register user fingerprints with UVM

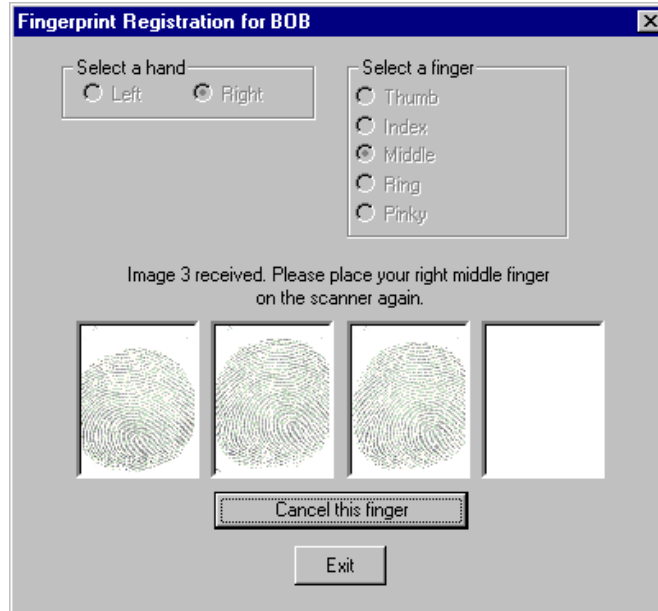
1. In the **Select a user** area, select a user name from the list.
2. Click **Register user's fingerprints**. The following window opens.



## Client Security Software

3. In the **Select a hand** area, click **Left** or **Right**.
4. In the **Select a finger** area, click to select the finger you will scan for prints, and click **Start registration**.
5. Place your finger on the UVM-aware fingerprint sensor and follow the on-screen instructions to scan four copies of your fingerprint. (The fingerprint registration program requires that four fingerprints be scanned.) You can click **Cancel this finger** at any time to cancel the scan of the finger you selected.

The window below shows that three fingerprints have been registered.



---

## Chapter 3 - Working with UVM policy

After you have added users to UVM, you must edit and save a security policy for each IBM client. The security policy provided by Client Security Software is called UVM policy, which combines the settings that you provided in Chapter 2 - Adding users to UVM with authentication requirements at the client level. UVM policy can be used to control the security policy of a client locally, or remotely across multiple clients.

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

- Each user must type a UVM passphrase and use fingerprint authentication to log on to the operating system. (Fingerprint authentication is optional.)
- Each user must type a UVM passphrase each time a digital certificate is acquired.
- Policy Director will control specific authentication objects as set in UVM policy.

**Note:** UVM policy sets the requirements for authentication objects for the IBM client and not for the individual user. Therefore, if you set UVM policy to require fingerprint for an authentication object (such as the operating-system logon), each user that is added to UVM must have registered their fingerprints to use that object. For details about adding a user, see “Chapter 2 - Adding users to UVM,” on page 14.

UVM policy is saved in a file named `globalpolicy.gvm`. To use UVM on remote clients, UVM policy can be saved on one IBM client and then copied to other clients. Using UVM policy on remote clients can save you the time it takes to set up UVM policy on a per client basis.

The sections in this chapter provide information about the following:

- Editing UVM policy for a local client and remote clients, and viewing the policy summary.
- Changing the password for the UVM-policy file. Each time you save `globalpolicy.gvm`, you can save the file with a new password.
- Giving Policy Director control of certain authentication objects.

---

## Editing a local UVM policy

You edit a local UVM policy and use it only on the client for which it was edited. If you installed Client Security in its default location, the local UVM policy is stored as `\Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm`.

You use the UVM-policy editor to edit and save a local UVM policy. The interface for the UVM-policy editor is provided in the Administrator Utility.

### Notes:

- Only a user who has been added to UVM can use the UVM-policy editor.
- If you set UVM policy to require fingerprint for an authentication object (such as the operating-system logon), each user that is added to UVM must have registered their fingerprints to use that object.
- If you save changes to the UVM policy, a window opens that asks for the admin private key. Type the admin private key and click **OK** to save your changes. If you provide an incorrect admin private key, your changes will not be saved.

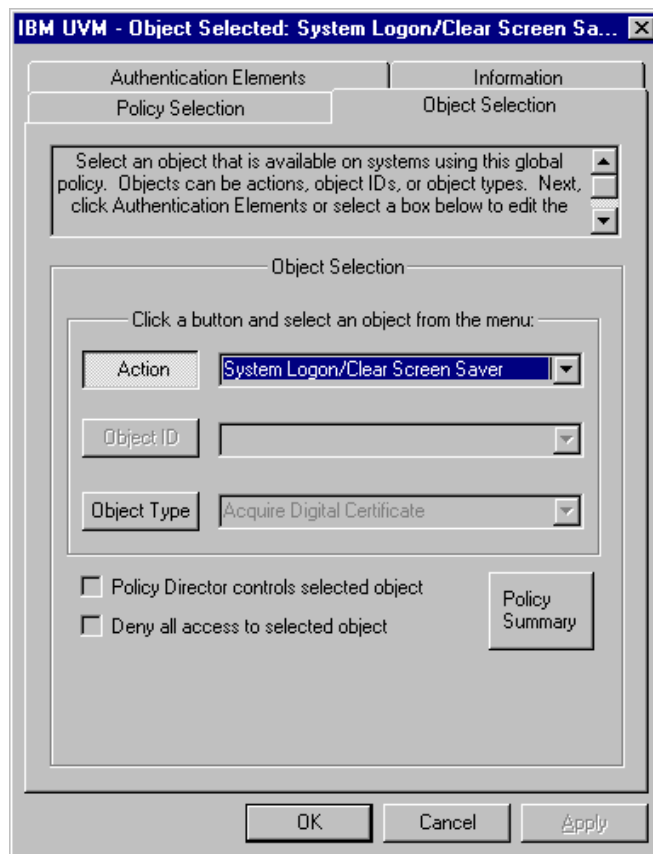
To start the UVM-policy editor:

1. Enter the Administrator Utility, and click the **Policy Setup** tab.
2. In the **UVM Policy** area, select **Local Client**, and then click **Edit UVM Policy**.
3. The Global Policy Access Password window opens. Type *password* and press Enter.

**Note:** The default access password for the UVM-policy file is the word *password*. After you edit the UVM policy, you can change the access password. For more information, see “Changing the password for a UVM-policy file,” on page 25.

4. On the **Policy Selection** page, select the UVM-policy file (`globalpolicy.gvm`) from the drop-down menu.
5. Click the **Object Selection** tab, then click **Action** or **Object type** and select the object for which you want to assign authentication requirements. Actions include System Logon/Clear Screen Saver and E-mail Decryption; an object type is Acquire Digital Certificate.

The following example shows that **System Logon/Clear Screen Saver** is selected.



For each object you select, do one the following:

- Click the **Authentication Elements** tab, and edit the settings for the available authentication elements that you want to assign to the object.
- Select **Policy Director controls selected object** to enable Policy Director to control the object you chose. You can select this option only if you want Policy Director to control the authentication elements for the IBM client. For more information, see *Using Client Security with Policy Director*.

**Important:** If you enable Policy Director to control the object, you are giving control to the Policy Director object space. If you do this, you must reinstall Client Security Software to re-establish local control over that object.

- Select **Deny all access to selected object** to deny access for the object you chose.

**Note:** While you are editing UVM policy, you can view the policy summary information by clicking on **UVM Policy Summary**. Also, you can click **Apply** to save your changes. If you click **Apply**, a window opens that prompts you for the admin private key. Type the admin private key and click **OK** to save your changes. If you provide an incorrect admin private key, your changes will not be saved.

6. Click the **Information** tab and type information for the system name, user details, and system and enterprise administrator details.

7. Click the **Policy Selection** tab and click the **UVM Policy** button. The **Save** and **Save as** become available. Do one of the following:
  - Click **Save** to save the policy file and follow the instructions on the screen.
  - To save the file with a new password, click **Save as** and see “Changing the password for a UVM-policy file,” on page 25 for information on changing to a new password.

**Note:** If you save your changes, a window opens that asks for the admin private key. Type the admin private key and click **OK** to continue. If you provide an incorrect admin private key, your changes will not be saved.
8. Click **OK** to save your changes and exit.

---

### Editing and using UVM policy for remote clients

To use UVM policy across multiple IBM clients, you can edit and save UVM policy for remote clients, and then you can copy the UVM-policy file to other IBM clients. If you installed Client Security in its default location, the remote UVM-policy file will be stored as `\Program Files\IBM\Security\UVM_Policy\remote\globalpolicy.gvm`. You must save the UVM-policy file once before the `\remote` subdirectory and its contents are created.

You use the UVM-policy editor to edit and save a UVM policy for remote clients. The interface for the UVM-policy editor is provided in the Administrator Utility.

#### Notes:

- Only a user who has been added to UVM can use the UVM-policy editor.
- If you set a UVM policy for remote clients to require fingerprint for an authentication object (such as the operating-system logon), each user that is added to UVM must have registered their fingerprints to use that object, and all remote clients that will use the policy must have a UVM-aware fingerprint sensor installed.
- If you save changes to the UVM policy, a window opens that asks for the admin private key. Type the admin private key and click **OK** to save your changes. If you provide an incorrect admin private key, your changes will not be saved.

To start the UVM-policy editor:

1. Enter the Administrator Utility, and click the **Policy Setup** tab.
2. In the **UVM Policy** area, select **Remote Clients**, and then click **Edit UVM Policy**.
3. The Global Policy Access Password window opens. Type *password* and press Enter.

**Note:** The default access password for the UVM-policy file is the word *password*. After you edit the UVM policy, you can change the access password. For more information, see “Changing the password for a UVM-policy file,” on page 25.

4. On the **Policy Selection** page, select the UVM-policy file (`globalpolicy.gvm`) from the drop-down menu.

5. Click the **Object Selection** tab, then click **Action** or **Object type** and select the object for which you want to assign authentication requirements. Actions include System Logon/Clear Screen Saver and E-mail Decryption; an object type is Acquire Digital Certificate.
  6. For each object you select, do one the following:
    - Click the **Authentication Elements** tab, and edit the settings for the available authentication elements that you want to assign to the object.
    - Select **Policy Director controls selected object** to enable Policy Director to control the object you chose. You can select this option only if you want Policy Director to control the authentication elements for the IBM client. For more information, see *Using Client Security with Policy Director*.

**Important:** If you enable Policy Director to control the object, you are giving control to the Policy Director object space. If you do this, you must reinstall Client Security Software to re-establish local control over that object.
    - Select **Deny all access to selected object** to deny access for the object you chose.
- Note:** While you are editing the UVM-policy file, you can view the policy summary information by clicking on **UVM Policy Summary**. Also, you can click **Apply** to save your changes. If you click **Apply**, a window opens that prompts you for the admin private key. Type the admin private key and click **OK** to save your changes. If you provide an incorrect admin private key, your changes will not be saved.
7. Click the **Information** tab and type information for the system name, user details, and system and enterprise administrator details.
  8. Click the **Remote Configuration** tab. Select the authentication elements that are available on the remote clients that will use this UVM policy.

**For Policy Director administrators:** If remote clients are enabled by Policy Director, select the **Policy Director enabled client** check box.
  9. Click the **Policy Selection** tab and click the **UVM Policy** button. The **Save** and **Save as** become available. Do one of the following:
    - Click **Save** to save the policy file.
    - To save the file with a new password, click **Save as** and see “Changing the password for a UVM-policy file,” on page 25 for information on changing to a new password.
- Note:** If you save your changes, a window opens that asks for the admin private key. Type the admin private key and click **OK** to continue. If you provide an incorrect admin private key, your changes will not be saved.
10. Click **OK** to save your changes and exit.
  11. Copy the following files to other remote IBM clients that will use this UVM-policy:
    - \IBM\Security\UVM\_Policy\remote\globalpolicy.gvm
    - \IBM\Security\UVM\_Policy\remote\globalpolicy.gvm.sig



**Notes:**

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

---

## **Changing the password for a UVM-policy file**

To protect the settings for UVM policy, you can change the access password for the UVM-policy file. Before you can edit the UVM-policy file, you must type the access password each time you enter the UVM-policy editor.

The following instructions assume that you have accessed the UVM-policy editor and that you are ready to save the UVM-policy file. For details, see “Editing a local UVM policy,” on page 21.

To change the password for the UVM-policy file:

1. Select a UVM-policy file (globalpolicy.gvm) and click the **UVM Policy** button.
2. Click **Save as** to save the file with a new password. The **Save as** window opens.
3. After you save the file, a window opens that asks you to verify that you want save the file with a new name. Click **OK**.
4. In the **Access Password** field, type the current password for the UVM-policy file and click **Change Password**.



5. In the **Access Password** field, type the current password and click **Change Password**.



The image shows a dialog box titled "Global Policy Access Password". At the top, there is a text area with the instruction: "Type old, new policy access passwords and verify policy access password, followed by <Enter>." Below this are three input fields: "Access Password", "New Password", and "Verify Password". A "Change Password" button is located between the "Access Password" and "New Password" fields. A "CANCEL" button is at the bottom of the dialog.

6. In the **New Password** field, type a new password.  
**Rules for the policy password:** The policy password can be any combination of alphanumeric characters less than 256 characters in length.
7. In the **Verify Password** field, type the new password again and press **Enter**. For the new password to take affect, you must press **Enter** after you type the password again in the **Verify Password** field.

---

## Chapter 4 - Setting up UVM protection for Lotus Notes

You can use Lotus Notes to communicate with other users in a variety of ways. For example, Notes users can send e-mail and share information through databases or spreadsheets.

To access Notes servers, each Notes user must have a User ID. The User ID is a file that uniquely identifies a Notes user, and it determines the access privileges that are assigned to a user. In Notes, you can set the User ID to be password protected so that a password is required each time a user logs on to Notes. To use the security features provided by Client Security, you can set up UVM protection for a User ID, so that a Notes user must type a UVM passphrase to access Notes or to change the password.

Lotus Notes version 4.5 or later is supported. Lotus Notes must be installed before you can set up UVM protection.

### Notes:

- You can set up UVM protection only for the current user ID of a Notes session. If you want to switch IDs for a Notes session you must disable UVM protection, log on to Notes and switch user IDs, and then reset the new User ID password for UVM.
- The cryptographic operations of the IBM embedded Security Chip do not replace any of the encryption features provided by the User ID file in Notes. For example, the public and private keys of the User ID file are not replaced by keys created with Client Security Software.

---

### Enable UVM protection for a User ID

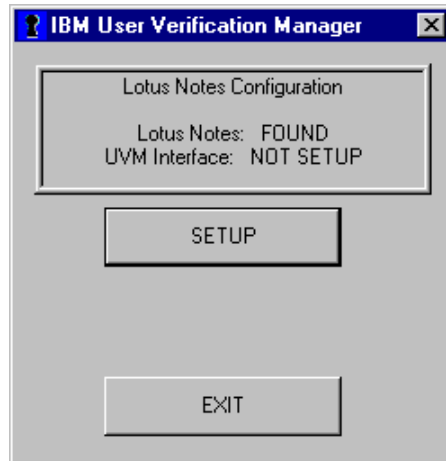
Before you can enable UVM protection for Notes, note the following:

- Notes must be installed on the IBM client
- a Notes User ID with a password must be setup
- the current user must be added to UVM

To set up UVM protection for Lotus Notes:

1. Click **Start > Programs > Client Security Software Utilities > Lotus Notes Configuration**. The Lotus Notes Configuration window opens.

## Client Security Software



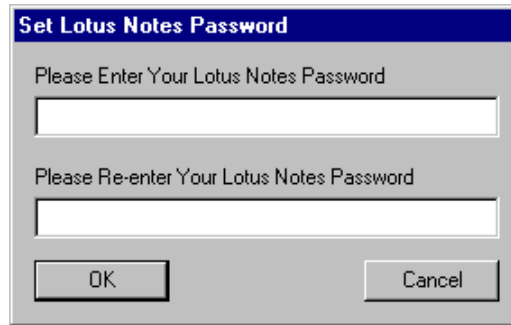
2. Click **Setup**. The following window opens and displays the current user ID associated with the Lotus Notes session. Click **Store Password**.



**Note:** If you have switched User IDs, the following window will open. You can click **Reset Password** to set up UVM protection for the new User ID.



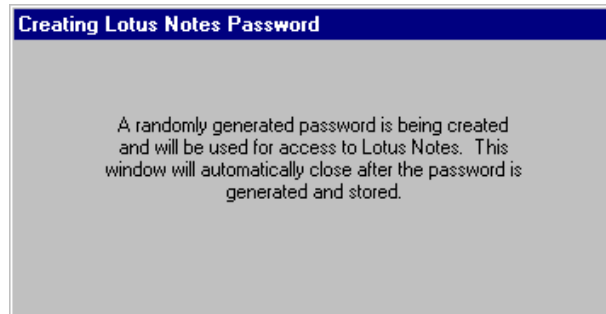
3. Type the Lotus Notes password associated with current user ID file, type it again to confirm it, and then click **OK**.



A windows opens that informs you to change the password in Lotus Notes. Click **OK**.

4. Click **Exit** on the Lotus Notes Configuration window. Next, open Notes and change your User ID password.

**Note:** If you change your Notes User ID password after you have enabled UVM protection, UVM will generate a random password for the User ID and the original password will be removed. The following window will open when you change your Notes User ID password.



5. Before you can use UVM protection for Lotus Notes, you must edit and save the UVM policy used for the client so that the Lotus Notes authentication objects are protected. See “Chapter 3 - Working with UVM policy,” on page 20 for more information about editing and saving UVM policy.

---

## **Disable UVM protection for a User ID**

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

1. Click **Start > Programs > Client Security Software Utilities > Lotus Notes Configuration**. The Lotus Notes Configuration window opens.



2. Click **Disable**.

If you click **Disable**, a window opens that provides a disable warning. Click **OK** to continue. The warning message is a notification that UVM and Notes integration is being disabled. If you want to reset the UVM and Notes integration in the future, use the Lotus Notes Configuration utility to reset the password with the User ID file.

**Note:** After you disable the password, you can remove the association between UVM and Notes integration by clicking **Remove password**. If you do this, you must request a new User ID file to use.

---

## Set up UVM protection for a switched User ID

If you want to switch from a User ID that has UVM protection enabled to another User ID, you must do the following:

1. Exit Notes.
2. Disable UVM protection for the current User ID, see “Disable UVM protection for a User ID,” on page 29 for details.
3. Enter Notes and switch User IDs, see your Lotus Notes documentation for information on switching User IDs.
4. If you want to set up UVM protection for the User ID that you have switched to, enter the Lotus Notes Configuration tool (provided by Client Security Software), and set up UVM protection, see “Enable UVM protection for a User ID,” on page 27.

---

## Chapter 5 - Using other features of the Administrator Utility

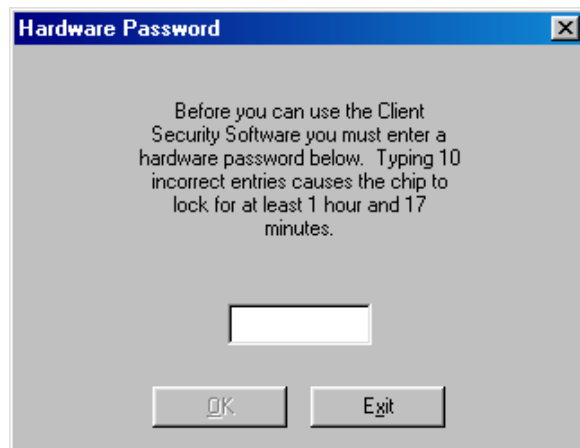
If you set up Client Security Software on IBM clients, you used the Administrator Utility to enable the IBM embedded Security Chip, set a hardware password, generate the hardware keys, and set up the security policy. This chapter provides instructions for using other features that the Administrator Utility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

**Note:** For Windows NT and Windows 2000 users, you must have administrator user rights assigned to your user ID to use the Administrator Utility.

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

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

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



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

---

### Update the key archive

When the key archive is first created, copies of all encryption keys are created. Reasons why updating the key archive might be necessary are if you create digital certificates and want to make copies of the private key stored on the IBM embedded Security Chip or if you want to move the key archive to another location.

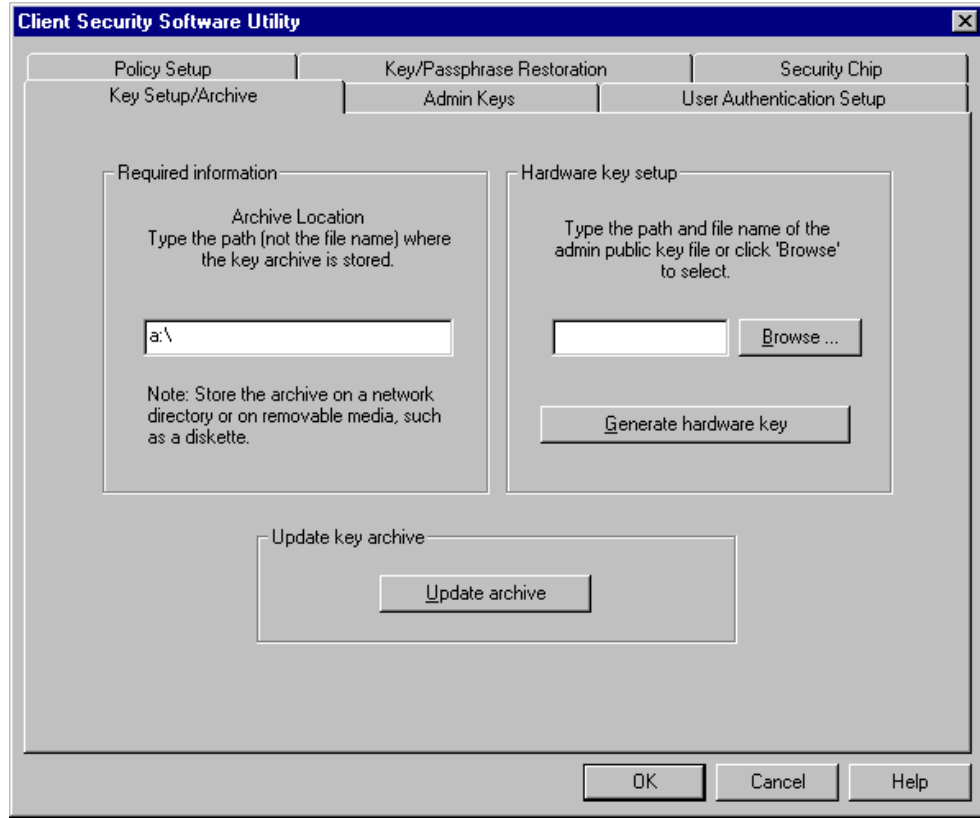
**Note:** The client user can also update the key archive by using the Client Utility. For more information, see "Using the Client Utility," on page 46.

To update the key archive:

1. Open the Administrator Utility.

## Client Security Software

2. Click the **Key Setup/Archive** tab.



3. In the **Required information** area, type the path (not the file name) where the key archive will be stored. Store the archive on a network directory or diskette.
4. Click **Update archive**. A window opens that notifies you that the operation was successful. Click **OK**.

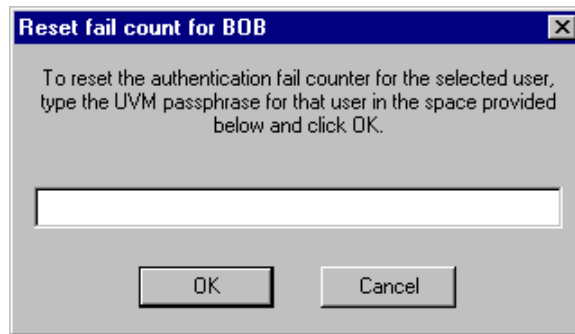
---

## Reset the authentication fail counter

To reset the authentication fail counter for a user:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **User Authentication Setup** tab.
3. In the **Select a user** area, select a user.
4. Click **Reset fail count**. The following window opens.





5. Type the UVM passphrase for the user selected and click **OK**. A window opens that notifies you that the operation was successful. Click **OK**.

---

## Changing information for Policy Director settings

The following information is intended for a security administrator who plans to use Policy Director to manage authentication objects for the UVM security policy. For more information, see *Using Client Security with Policy Director*.

### Editing Policy Director setup information

To configure the Policy Director setup information on the IBM client:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Policy Setup** tab.
3. Select **DCE** or **LDAP** for the server registry that you will use.
4. For each field related to the server registry you selected, enter the appropriate information.

### Refreshing the local cache

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

To set or refresh the local cache:

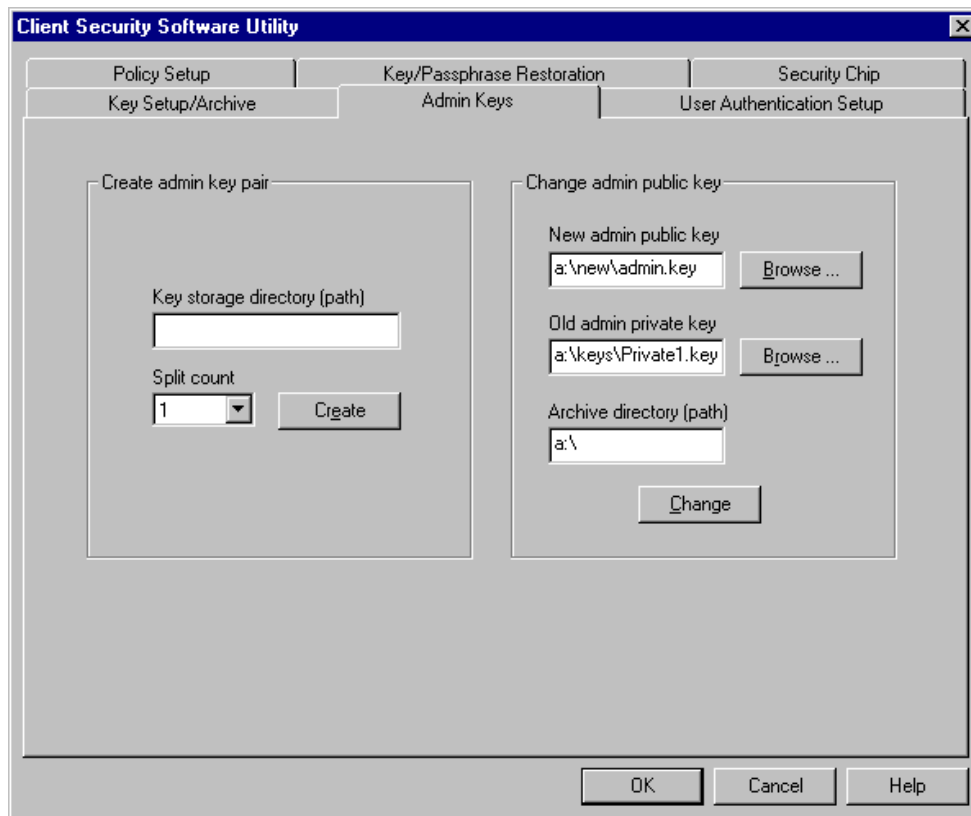
1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Policy Setup** tab.
3. Do one of the following:
  - To refresh the local cache, click **Refresh now**.
  - To set the refresh rate, type the number of months and days in the fields provided. The months and days values represent the amount of time between scheduled

## Change the admin public key

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

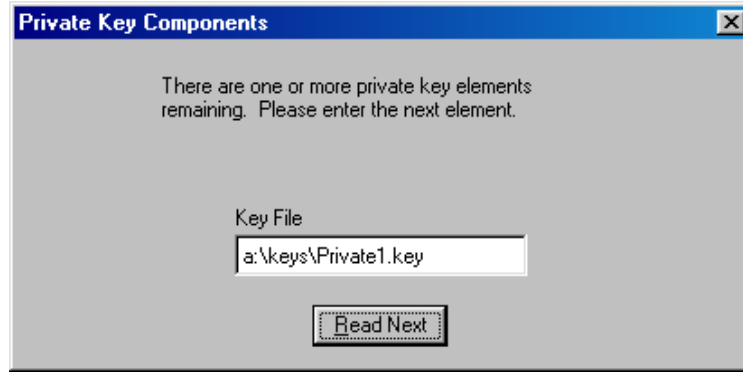
To change the admin public key:

1. Open the Administrator Utility; for details, see the instructions on page 31.
2. Click the **Admin Keys** tab.
3. In the **New admin public key** field, type the file name for the new admin public key, or click **Browse** to search for the file.



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

**Note:** If the admin private key was split into multiple files, a window opens that asks you to type in the location and name of each file. Click **Read Next** after you type each file name in the **Key File** field.



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

---

## **Restore keys**

When you restore keys, you are copying the most recent user key files from the key archive and storing them on the IBM embedded Security Chip of the computer. These copied user key files appear in the directory where they were previously stored on the computer, such as on a network directory or diskette.

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

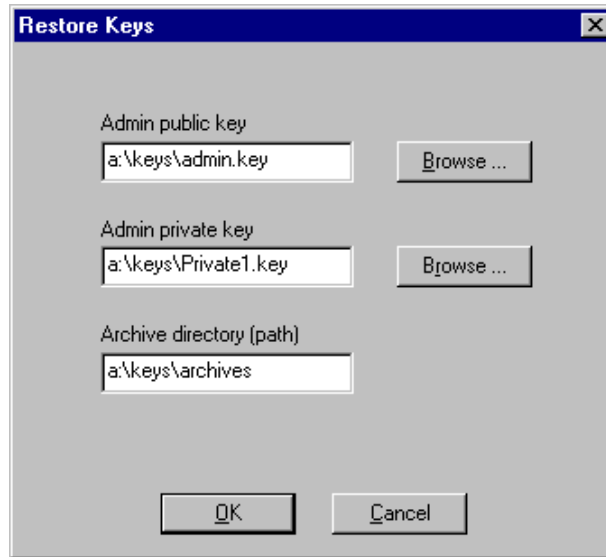
## **System board replacement**

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

You can perform the key restoration after you have enabled the new chip and set a hardware password. For details, see “Enabling the IBM embedded Security Chip and setting a hardware password,” on page 42.

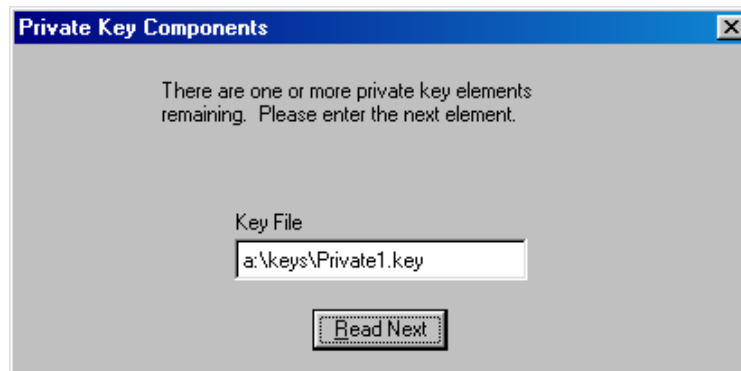
To restore keys after a system board replacement, do the following:

1. Open the Administrator Utility. The following window opens. The text in the fields are examples only.



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

**Note:** If the admin private key was split into multiple files, a window opens that asks you to type in the location and name of each file. Click **Read Next** after you type each file in the **Key File** field.



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

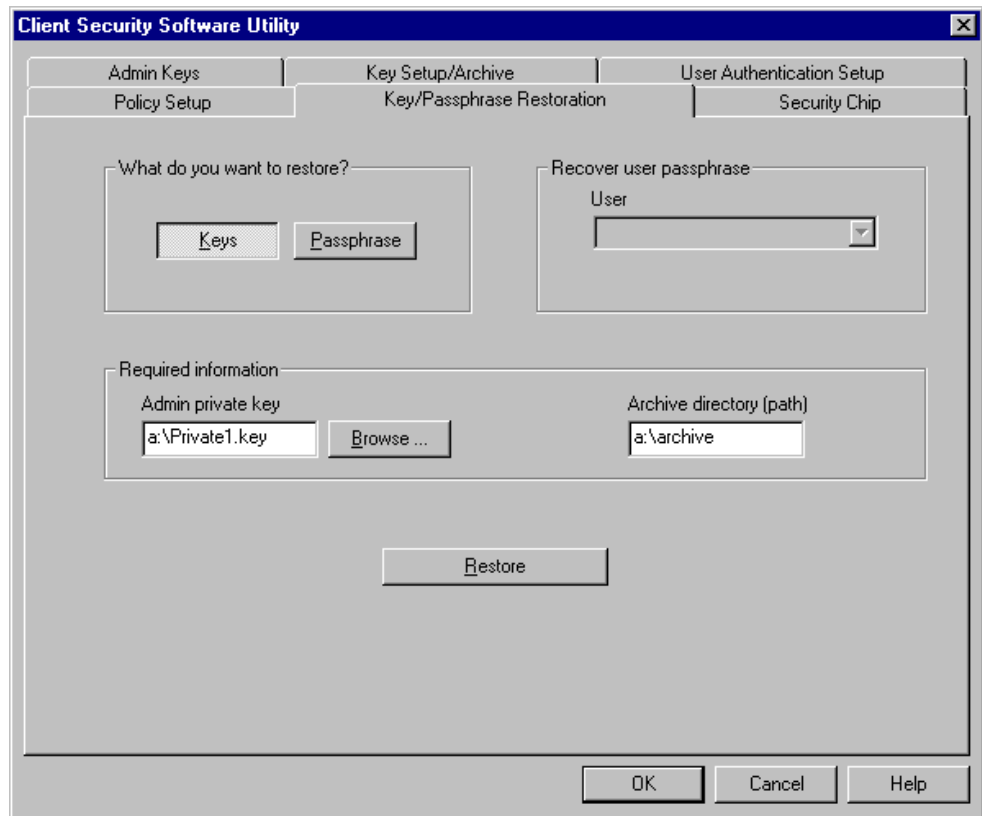
### Hard disk drive failure

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

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

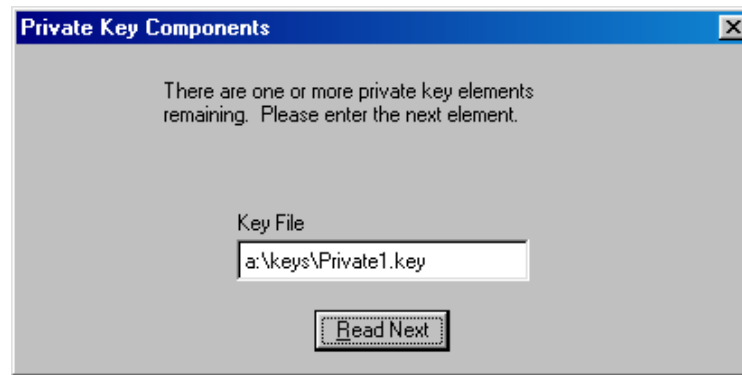
To restore user keys from a key archive:

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



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

**Note:** If the admin private key was split into multiple files, a window opens that asks you to type in the location and name of each file. Click **Read Next** after you type each file in the **Key File** field.



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

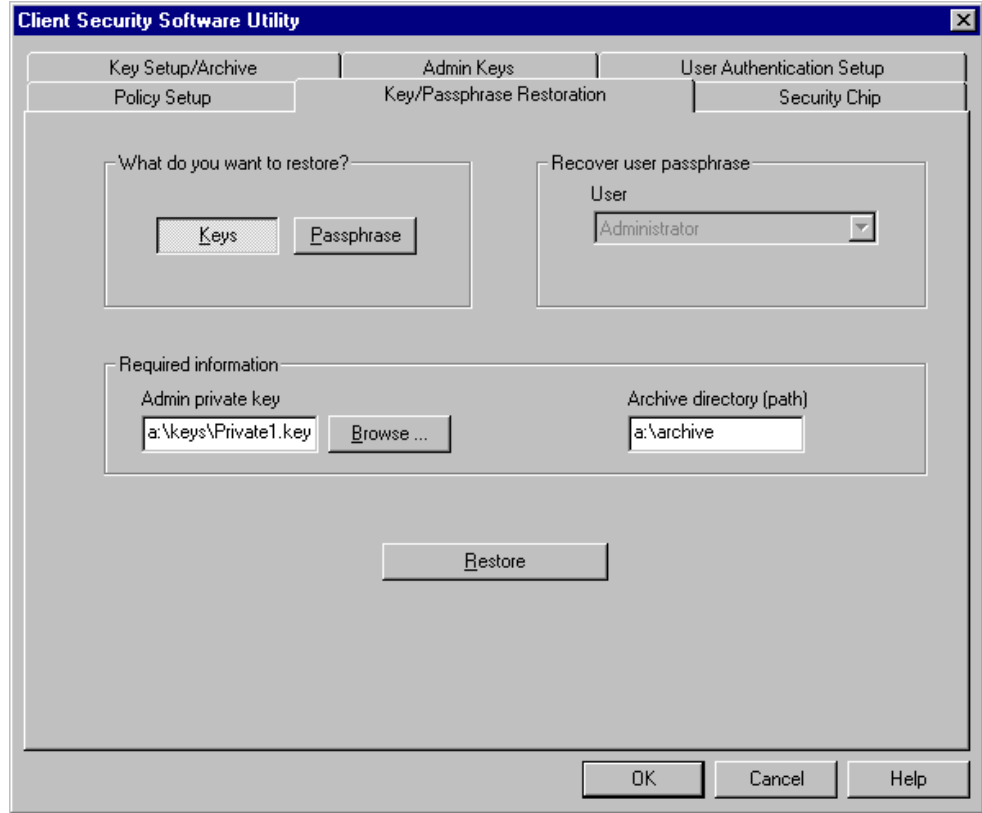
---

## Recover a UVM passphrase

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

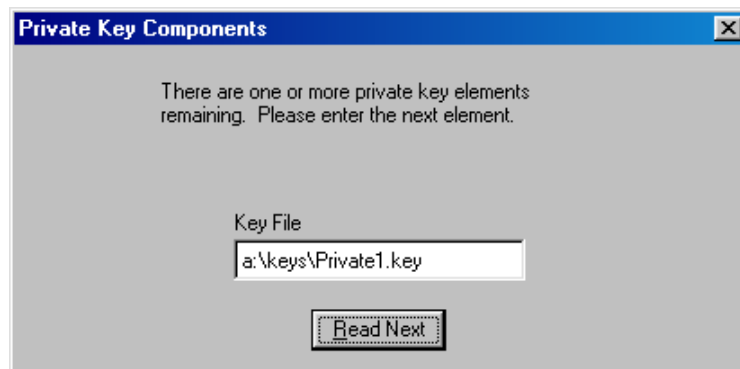
To recover the passphrase:

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



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

**Note:** If the admin private key was split into multiple files, a window opens that asks you to type in the location and name of each file. Click **Read Next** after you type each file in the **Key File** field.



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

## Change the hardware password

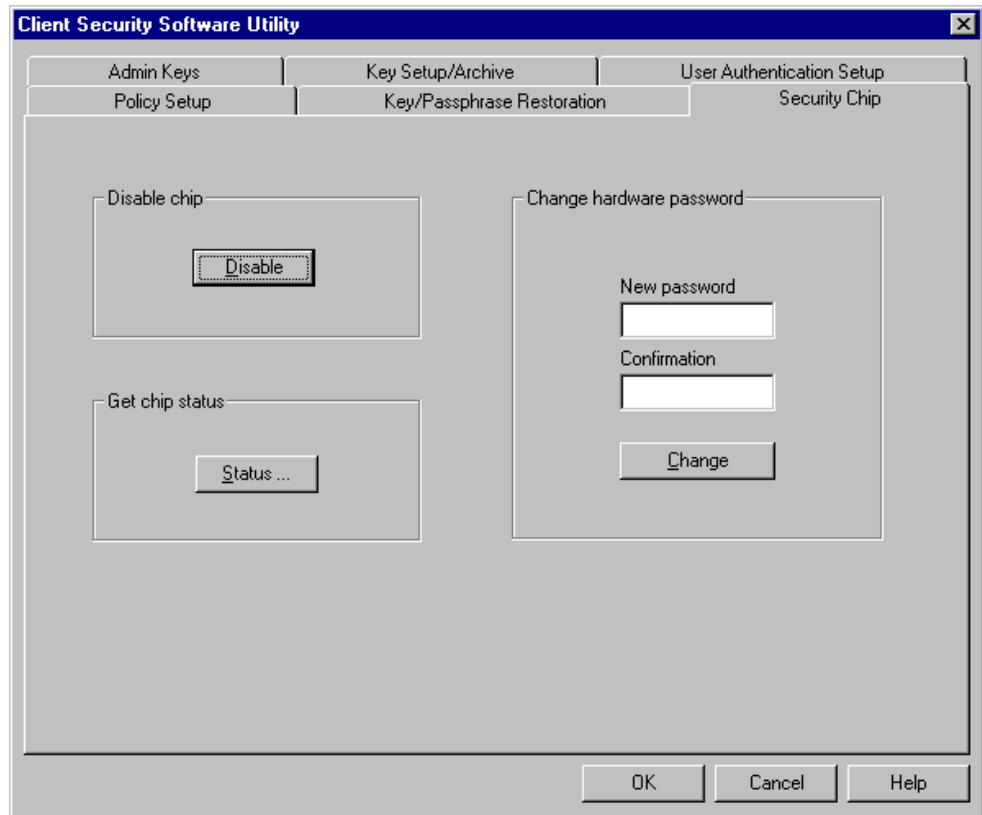
You must set a hardware password to enable the IBM embedded Security Chip. Access to the Administrator Utility is also protected by the hardware password.

**Notes:**

- For improved security, change the hardware password periodically. A password that remains unchanged for a long period of time can be more vulnerable to outside parties.
- For information on the rules of the hardware password, see “Appendix B - Rules for the hardware password and the UVM passphrase,” on page 69.

To change the hardware password:

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



4. In the **Confirmation** field, type the password again.
5. Click **Change**.

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



## Client Security Software

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

---

### View information about Client Security Software

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

- Encryption status of the embedded Security Chip
- Status on enablement of the IBM embedded Security Chip
- Version number of the firmware used with Client Security Software
- The validity of the hardware encryption keys

To view client security information:

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



4. Click **OK** to exit.

---

### Disable the IBM embedded Security Chip

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

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

To disable the embedded Security Chip:

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

3. In the **Disable Chip** area, click **Disable** and follow the on-screen instructions.

**Notes:**

- If your computer has Enhanced Security enabled, you might have to type the administrator password that was set in the Configuration/Setup Utility to disable the chip.
- To use the IBM embedded Security Chip and hardware encryption keys after the chip is disabled, the chip must be re-enabled. For more information, see “Enabling the IBM embedded Security Chip and setting a hardware password.”

---

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

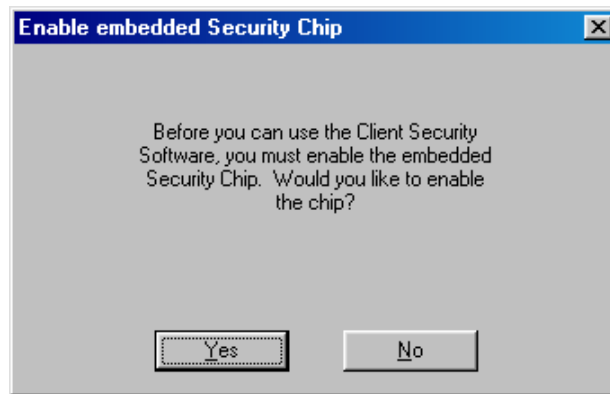
If you need to enable the IBM embedded Security Chip after the software has been installed, you can use the Administrator Utility to reset the hardware password and to set up new encryption keys.

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

To enable the chip and set a hardware password:

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

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



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

**Note:** If your computer has Enhanced Security enabled, you might have to type the administrator password that was set in the Configuration/Setup Utility to enable the chip.

2. Click **OK** to restart the computer
3. From the Windows desktop of the IBM client, click **Start > Programs > Client Security Software Utilities > Administrator Utility**.

## Client Security Software

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



The dialog box has a title bar with the text "New Password" and a close button (X). The main text reads: "The hardware has not been configured or has been cleared. A new password is required at this time. Please enter and confirm a new hardware password below." Below the text are two input fields: "New Password" and "Confirm". At the bottom are two buttons: "OK" and "Cancel".

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

---

## Chapter 6 - Instructions for the client user

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

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

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

---

### Using UVM protection for the system logon

This section contains information about using UVM protection the system logon. Before you can use UVM protection, it must be enabled for the computer. For more information, see "Set up UVM protection for the operating system logon," on page 18.

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

#### Windows NT

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

After UVM protection is enabled for the computer, the UVM logon interface will open each time you start the computer.

Also, if the computer is already running, you can press **Ctrl + Alt + Delete** to access the UVM logon interface. You can perform the following tasks:

- click **Shut down** to shut down the computer
- click **Lock Workstation** to lock the computer (see below for information on unlocking the computer)
- click **Task Manager** to open Task Manager
- click **Logoff** to log off the current user

To unlock a client that runs Windows NT and uses UVM protection:

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

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

3. Type your UVM passphrase, and then click **OK** to access the operating system. If fingerprint authentication is required by the UVM policy, a window opens that prompts you for a fingerprint scan.

### Windows 98 and Windows 95

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

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

1. If the operating system logon window opens, type the user name and password information, and click **OK**. The UVM passphrase window opens.
2. Type the UVM passphrase associated with the user name typed in the operating system logon, and then click **OK** to access the operating system. If a fingerprint scan is required, a window opens that prompts for a fingerprint scan.

If all the authentication requirements set in the UVM policy are met, the computer unlocks. If not, the Client Security screen saver displays, and then the UVM passphrase window opens again.<sup>3</sup>

---

### Setting up the Client Security screen saver

This section contains information about setting up the Client Security screen saver. The Client Security screen saver is one of the software components that is automatically installed by Client Security Software. Before you can use the Client Security screen saver, you must add at least one user to the security policy of the computer with the Administrator Utility. For details, follow the steps in “Chapter 2 - Adding users to UVM,” on page 14.

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

To set up the Client Security screen saver:

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

If the Client Security is activated, press any key or move the mouse to unlock the screen saver. Type your UVM passphrase or provide fingerprint scans to access the desktop.

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

---

<sup>3</sup> The Client Security screen saver may or may not be the selected screen saver for your computer. For Windows 98 and Windows 95, UVM logon protection uses the Client Security screen saver to secure the logon.

---

## **Using the Client Utility**

The Client Utility lets you or the client user change the following:

- **Change UVM passphrase.** To improve security, you can periodically change the UVM passphrase for a client user.
- **Update Windows logon settings.**<sup>4</sup> If you change the Windows NT password for a client user with the User Manager program, you must also change the password by using the Client Utility. Note that if you use the Administrator Utility to change the Windows logon password for a user, all user encryption keys previously created for that user will be deleted, and the associated digital certificates will become invalid.
- **Update the key archive.** If you create digital certificates and want to make copies of the private key stored on the IBM embedded Security Chip, or if you want to move the key archive to another location, update the key archive.
- **Register user fingerprints.** If you want to use a UVM-aware fingerprint sensor (or scanner) for authentication, you can register your fingerprints with UVM.

**Note:** Before you can register fingerprints with UVM, a fingerprint scanner must be attached to the IBM client system. For instructions on how to attach and use the fingerprint scanner, refer to the documentation provided by the hardware vendor.

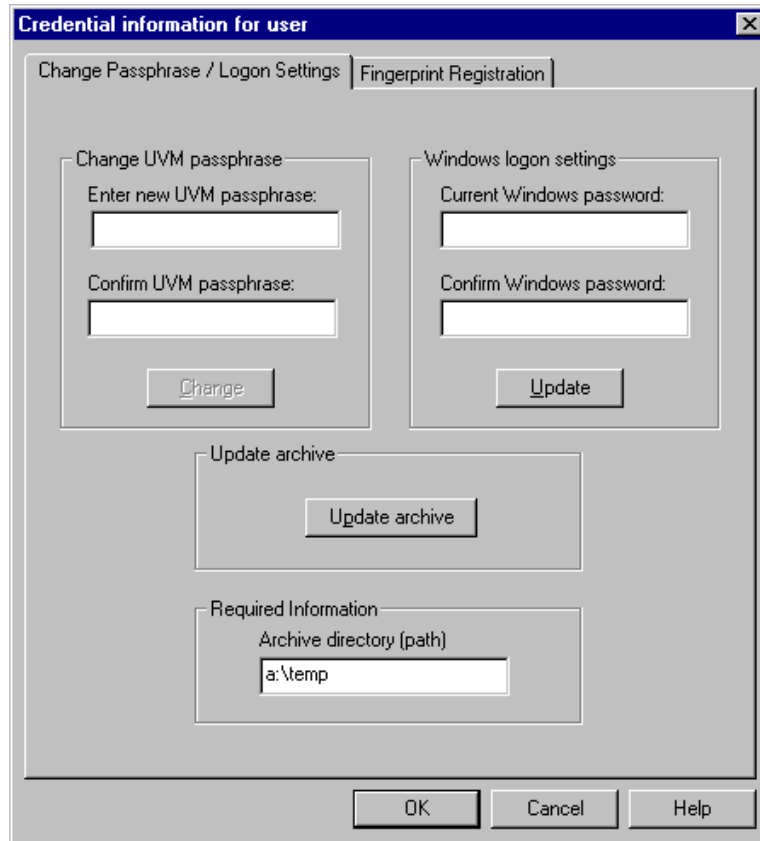
To use the Client Utility:

1. Click **Start > Programs > Client Security Software Utilities > Client Utility**. The UVM passphrase window opens.
2. Type the UVM passphrase for the client user who requires a UVM passphrase or Windows NT password change, and click **OK**.

The following window opens.

---

<sup>4</sup> Changing the Windows logon password is applicable for users of Windows NT only.



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

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

4. Do one of the following:
  - To change the UVM passphrase, in the **Change current passphrase** area, type a new passphrase in the **New passphrase** field. Next, type the passphrase again in the **Confirm new passphrase** field, and then click **Change**. For information on the rules for the UVM passphrase, see “Appendix B - Rules for the hardware password and the UVM passphrase,” on page 69.
  - To change the Windows NT logon password, in the **Windows password** field, type a new Windows NT password. Next, type the new password again in the **Confirm Windows password** field, and then click **Update**. For rules on the Windows NT logon password, see the operating system documentation.

**Note:** Only change Windows logon information in User Manager for the user currently logged on.

## Client Security Software

- To update the key archive, click **Update archive**; then click **OK** on the window that opens and notifies you that the operation was successful.
  - To register user fingerprints, click **Fingerprint Registration** and follow the instructions. For more information, see steps 3 through 5 for “Register user fingerprints with UVM,” on page 18.
5. Click **OK** to exit.

---

## Using secure e-mail and Web browsing

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

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

### Tips for using Client Security Software with Microsoft applications

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

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

#### Notes:

- To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see “View information about Client Security Software,” on page 41.
- For information about known limitations when using Client Security Software with Microsoft applications and troubleshooting information, see “Known limitations,” on page 55 and “Troubleshooting charts,” on 57.

#### ▪ Obtain a digital certificate

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

To use the cryptographic capabilities of the IBM embedded Security Chip for your Microsoft applications, make sure you select **IBM embedded Security Chip CSP** as your CSP when you obtain your digital certificate. This ensures that the



## Client Security Software

private key of the digital certificate is stored on the IBM embedded Security Chip.

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

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



The image shows a dialog box titled "Select a Cryptographic Service Provider:". Inside the dialog, there is a label "CSP:" followed by a dropdown menu that currently displays "IBM embedded Security Chip CSP". Below the dropdown menu, there is a checked checkbox with the text "Enable strong private key protection".

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

- **Update the key archive**

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

- **Use the digital certificate**

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

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

### Tips for using Client Security Software with Netscape applications

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

For details on how to use the security settings for Netscape applications, see the documentation provided by Netscape.

#### Notes:

- To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see "View information about Client Security Software," on page 41.

## Client Security Software

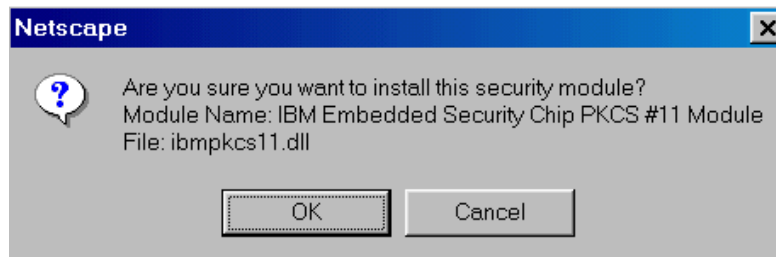
- For information about known limitations when using Client Security Software with Netscape applications and troubleshooting information, see “Known limitations,” on page 55 and “Troubleshooting charts,” on 57.

### ▪ Install the IBM embedded Security Chip PKCS#11 module

Before you can use a digital certificate, you must install the IBM embedded Security Chip PKCS#11 module onto the computer. Because the installation of the IBM embedded Security Chip PKCS#11 module requires a UVM passphrase, you must add at least one user to the security policy for the computer. For details, see “Chapter 2 - Adding users to UVM,” on page 14.

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

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



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

### ▪ Using the PKCS#11 logon protection

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

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

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

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



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

- **Update the key archive**

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

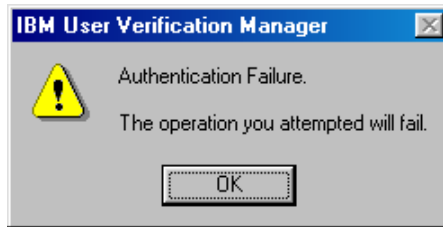
- **Use the digital certificate**

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

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

**Note:** If you do not meet the authentication requirements set by the UVM policy, the following window opens.

## Client Security Software



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

---

## Chapter 7 - Troubleshooting

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

---

### Administrator tips

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

#### Set an administrator password in the Configuration/Setup Utility

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

- Change the hardware password (for the IBM embedded Security Chip)
- Enable or disable the IBM embedded Security Chip
- Clear the IBM embedded Security Chip (see the Attention box below for important information about clearing the security chip)

#### Attention

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

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

To set an administrator password:

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

## Client Security Software

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

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

### Protect the hardware password

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

### Clearing the IBM embedded Security Chip

If you want 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 a user clears the IBM embedded Security Chip, all encryption keys and certificates stored on the chip will be lost and the contents of the hard disk could become unusable.
- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk will become unusable, and you must re-format the hard disk drive and reinstall all software. To clear UVM protection, open the Administrator Utility, click the **Key Setup/Archive** tab, and clear the **UVM protection** check box. You must shut down and restart the computer before UVM 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 opens.
3. Select **System Security**.
4. Select **IBM Embedded Security Chip**.
5. Select **Clear IBM Security Chip**.
6. Select **Yes** for Clear IBM Security Chip.
7. Press Esc to continue.
8. Press Esc to exit and save the settings.

---

## Known limitations

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

### Client Security Software and Netscape

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



Click **OK** to continue. Although Netscape opens, you will not be able to use the digital certificate generated by the IBM embedded Security Chip. You must exit and re-enter Netscape, and type the correct UVM passphrase before you can use the IBM embedded Security Chip certificate.

**Algorithms do not display:** All hashing algorithms supported by the IBM embedded Security Chip PKCS#11 module are not selected if the module is viewed in Netscape. The following algorithms are supported by the IBM embedded Security Chip PKCS#11 module, but are not identified as being supported when viewed in Netscape:

- SHA-1
- MD5

### IBM embedded Security Chip certificate and encryption algorithms

The following information is provided to help identify issues about the encryption algorithms that can be used with the IBM embedded Security Chip certificate. See Microsoft or Netscape for current information about the encryption algorithms used with their e-mail applications.

- **When sending e-mail from one Outlook Express (128-bit) client to another Outlook Express (128-bit) client:** If you use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0 to send encrypted e-mail to other clients using Outlook Express (128-bit), e-mail messages encrypted with the IBM embedded Security Chip certificate can only use the 3DES algorithm.
- **When sending e-mail between an Outlook Express (128-bit) client and a Netscape client:** An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm.
- **Some algorithms might not be available for selection in the Outlook Express (128-bit) client:** Depending on how your version of Outlook

## Client Security Software

Express (128-bit) was configured or updated, some RC2 algorithms and other algorithms might not be available for use with the IBM embedded Security Chip certificate. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.

### Administrator Utility

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

**The Deny all access to selected object check box is not disabled if Policy Director control is selected:** In the UVM-policy editor, if you select **Policy Director controls selected object** to enable Policy Director to control an authentication object, the **Deny all access to selected object** check box is not disabled. Although the **Deny all access to selected object** check box remains active, it cannot be selected to override Policy Director control.

### UVM protection for a Lotus Notes User ID

**UVM protection does not operate if you switch User IDs within a Notes session:** You can set up UVM protection only for the current user ID of a Notes session. If you want to switch from a User ID that has UVM protection enabled to another User ID, you must do the following:

1. Exit Notes.
2. Disable UVM protection for the current User ID, see "Disable UVM protection for a User ID," on page 29 for details.
3. Enter Notes and switch User IDs, see your Lotus Notes documentation for information about switching User IDs. If you want to set up UVM protection for the User ID that you have switched to, proceed to step 4.
4. Enter the Lotus Notes Configuration tool provided by Client Security Software and set up UVM protection, see "Enable UVM protection for a User ID," on page 27.

### Event log error messages

**Error messages related to Client Security Software are generated in the event log:** Client Security Software uses a device driver that might generate error messages in the event log. The errors associated with these messages do not affect the normal operation of your computer.

### Error messages if access to an authentication object is denied

**UVM invokes error messages that are generated by the associated program if access is denied for an authentication object:** If UVM policy is set to deny access for an authentication object, for example e-mail decryption, the message stating that access has been denied will vary depending on what software is being used. For example, an error message from Outlook Express that states access is denied to an authentication object will differ from a Netscape error message that states that access was denied.



---

## Troubleshooting charts

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

### Client Security Software and Microsoft applications

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security Software with Microsoft applications.

---

Problems reading encrypted e-mail using Outlook Express	Action
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.	<p>Verify the following:</p> <ol style="list-style-type: none"><li>1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses.</li><li>2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.</li></ol> <p><b>Note:</b> To use 128-bit Web browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see “View information about Client Security Software,” on page 41.</p>

---

<b>Problems using a certificate from an e-mail address that has multiple certificates associated with it</b>	<b>Action</b>
Outlook Express can list multiple certificates associated with a single e-mail address and some of those certificates can become invalid. A certificate can become invalid if the private key associated with the certificate no longer exists on the IBM embedded Security Chip of the sender's computer where the certificate was generated.	Ask the recipient to resend his digital certificate; then select that certificate in the address book for Outlook Express.
<b>Failure message when trying to digitally sign an e-mail message</b>	<b>Action</b>
If the composer of an e-mail message tries to digitally sign an e-mail message when the composer does not yet have a certificate associated with his or her e-mail account, an error message displays.	Use the security settings in Outlook Express to specify a certificate to be associated with the user account. See the documentation provided for Outlook Express for more information.
<b>Outlook Express (128 bit) encrypts e-mail messages with the 3DES algorithm only</b>	<b>Action</b>
When sending encrypted e-mail between clients that use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0, only the 3DES algorithm can be used.	To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see "View information about Client Security Software," on page 41.  Also, see Microsoft for current information on the encryption algorithms used with Outlook Express.

<b>Outlook Express clients return e-mail messages with a different algorithm</b>	<b>Action</b>
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm.  See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
<b>Error message when trying to use a certificate in Outlook Express that has been restored after a hard disk drive failure</b>	<b>Action</b>
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, do one of the following <ul style="list-style-type: none"><li>▪ obtain new certificates</li><li>▪ register the certificate authority again in Outlook Express</li></ul>
<b>Outlook Express does not update the encryption strength associated with a certificate sent from Netscape Messenger.</b>	<b>Action</b>
If a sender selects the encryption strength in Netscape and sends a signed e-mail message to a client using Outlook Express with Internet Explorer 4.0 (128-bit), the encryption strength of the returned e-mail might not match.	Delete the associated certificate from the address book in Outlook Express. Open the signed e-mail again and add the certificate to the address book in Outlook Express.

<b>In Outlook Express, the error decryption message displays.</b>	<b>Action</b>
<p>You can open a message in Outlook Express if you double-click it. In some instances, if you double-click an encrypted message too quickly, an error decryption message appears.</p> <p>Also, a decryption error message might display in the preview pane, if you select an encrypted message.</p>	<p>If you attempted to open an e-mail message and the decryption error message appears, close the message, and then open the encrypted e-mail message again.</p> <p>If the error message appears in the preview pane, no action is required.</p>
<b>An error message displays if you click the Send button twice when you are trying to send an encrypted e-mail message.</b>	<b>Action</b>
<p>When using Outlook Express, if you click the send button twice to send an encrypted e-mail message, an error message displays stating that the message could not be sent.</p>	<p>Close this error message and click the Send button once.</p>
<b>Error message when requesting a certificate from a certificate authority in Internet Explorer.</b>	<b>Action</b>
<p>If you are using Internet Explorer, you might receive an error message if you request a certificate that uses the IBM embedded Security Chip CSP.</p>	<p>Request the digital certificate again.</p>
<b>Authentication fails at logon for Windows 98 clients.</b>	<b>Action</b>
<p>Windows 98 clients with UVM protection might experience an authentication error if they try to log on.</p>	<p>Shut down and restart the computer.</p>

### Client Security Software and Netscape

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security Software with Netscape applications.

<b>Problems reading encrypted e-mail</b>	<b>Action</b>
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.	<p>Verify the following:</p> <ol style="list-style-type: none"><li>1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses.</li><li>2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.</li></ol> <p><b>Note:</b> To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see "View information about Client Security Software," on page 41.</p>
<b>Failure message when trying to digitally sign an e-mail message when using Netscape Messenger</b>	<b>Action</b>
If the IBM embedded Security Chip certificate has not been selected in Netscape Messenger, and a composer of an e-mail message tries to sign the message with the certificate, an error message displays.	Use the security settings in Netscape Messenger to select the certificate. When Netscape Messenger is open, click the security icon on the toolbar and the Security Info window opens. Click <b>Messenger</b> in the left panel and then select the IBM embedded Security Chip certificate. See the documentation provided by Netscape for more information.

<b>An e-mail message sent from Netscape Messenger to Outlook Express is returned to the Netscape client with a different algorithm</b>	<b>Action</b>
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm.  See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
<b>Unable to use the digital certificate generated by the IBM embedded Security Chip</b>	<b>Action</b>
The digital certificate generated by the IBM embedded Security Chip is not available for use.	Verify that the correct UVM passphrase was typed when Netscape was opened. If you type the incorrect UVM passphrase, an error message displays stating an authentication failure. If you click <b>OK</b> , Netscape opens, but you will not be able to use the certificate generated by the IBM embedded Security Chip. You must exit and re-open Netscape, and then type the correct UVM passphrase.
<b>New digital certificates from the same sender are not replaced within Netscape</b>	<b>Action</b>
If a digitally signed e-mail is received more than once by the same sender, the first digital certificate associated with the e-mail is not overwritten.	If you receive multiple e-mail certificates, only one certificate is the default certificate. Use the security features in Netscape to delete the first certificate, and then re-open the second certificate or ask the sender to send another signed e-mail.

<b>Cannot export the IBM embedded Security Chip certificate</b>	<b>Action</b>
The IBM embedded Security Chip certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up certificates.	Go to the Administrator Utility or Client Utility to update the key archive. If you update the key archive, copies of all the certificates associated with the IBM embedded Security Chip are created.
<b>Error message when trying to use a certificate in Netscape that has been restored after a hard disk drive failure</b>	<b>Action</b>
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, obtain a new certificate.
<b>Netscape agent opens and causes Netscape to fail</b>	<b>Action</b>
Netscape agent opens and closes Netscape.	Turn off the Netscape agent.
<b>Netscape delays if you try to open it</b>	<b>Action</b>
If you add the IBM embedded Security Chip PKCS#11 module and then open Netscape, a short delay will occur before Netscape opens.	No action is required. This tip is for informational purposes only.

**Obtaining a digital certificate**

The following troubleshooting information might be helpful if you experience problems obtaining a digital certificate.

---

<b>UVM passphrase window or fingerprint authentication window displays multiple times during a digital certificate request.</b>	<b>Action</b>
The UVM security policy dictates that a user provides the UVM passphrase or fingerprints before a digital certificate can be acquired. If the user tries to acquire a certificate, the authentication window that asks for the UVM passphrase or fingerprint scan displays more than once.	Type your UVM passphrase or scan your fingerprint each time the authentication window opens.

---

<b>A VBScript or JavaScript error message displays.</b>	<b>Action</b>
If you request a digital certificate, an error message related to VBScript or JavaScript might display.	Restart the computer, and obtain the certificate again.

---

**Client Security Software and Lotus Notes**

The following troubleshooting information might be helpful if you experience problems with using Lotus Notes with Client Security Software.

---

<b>An error message displays if you attempt to change the Notes password and you are using Client Security Software</b>	<b>Action</b>
Changing the Notes password when using Client Security Software might display in an error message.	Retry the password change. If this does not work, restart the client.

---



<b>An error message displays after the randomly-generated password is created by Client Security Software</b>	<b>Action</b>
<p>An error message might display if you do the following:</p> <ol style="list-style-type: none"> <li>1. Use the Lotus Notes Configuration tool to set UVM protection for a Notes ID</li> <li>2. Open Notes and use the function provided by Notes to change the password for Notes ID file</li> <li>3. Close Notes immediately after you change the password.</li> </ol>	<p>Click <b>OK</b> to close the error message.</p> <p>No action is required. Contrary to the error message, the password has changed. The new password is a randomly-generated password created by Client Security Software, specifically UVM. The Notes ID file is now encrypted with the randomly-generated password, and the user does not need a new User ID file.</p> <p>If the end user changes the password again, UVM will generate a new random password for the Notes ID.</p>

**Administrator Utility**

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

<b>An error message displays after a key restoration and the admin public key is changed.</b>	<b>Action</b>
<p>If you clear the embedded Security Chip and then restore the key archive, an error message might display if you change the admin public key.</p>	<p>Add the users to UVM and request new certificates, if applicable.</p>
<b>An error message displays after the admin public key is changed and you attempt to recover a UVM passphrase.</b>	<b>Action</b>
<p>If you change the admin public key and then attempt to recover a UVM passphrase for a user, an error message might display.</p>	<p>Do one of the following:</p> <ul style="list-style-type: none"> <li>▪ If the UVM passphrase for the user is not needed, no action is required.</li> <li>▪ If the UVM passphrase for the user is needed, you must add the user to UVM, and request new certificates, if applicable.</li> </ul>

<p><b>An error message displays if you try to save the UVM-policy file.</b></p>	<p><b>Action</b></p>
<p>If you attempt to save a UVM-policy file (globalpolicy.gvm) by clicking Apply or Save, an error message might display.</p>	<p>Exit the error message, edit the UVM-policy file again to make your changes, and then save the file.</p>
<p><b>An error message displays if you try to open the UVM-policy editor.</b></p>	<p><b>Action</b></p>
<p>If the current user (logged on to the operating system) has not been added to UVM, the UVM-policy editor will not open.</p>	<p>Add the user to UVM and open the UVM-policy editor.</p>
<p><b>An error message displays while you are using the Administrator Utility.</b></p>	<p><b>Action</b></p>
<p>If you are using the Administrator Utility, the following error message might display:</p> <p>A buffer I/O error occurred while trying to access the Client Security chip. This might be corrected by a reboot.</p>	<p>Exit the error message, and shut down and restart your computer.</p>
<p><b>A disable chip window opens if you attempt to change the hardware password.</b></p>	<p><b>Action</b></p>
<p>If you attempt to change the hardware password, and you press <b>Enter</b> or <b>Tab &gt; Enter</b> after you type the confirmation password, the Disable chip button will be enabled and a disable chip confirmation window opens.</p>	<p>Do the following:</p> <ol style="list-style-type: none"> <li>1. Exit from the disable chip confirmation window.</li> <li>2. To change the hardware password, type the new password, type the confirmation password, and then click <b>Change</b>. Do not press <b>Enter</b> or <b>Tab &gt; Enter</b> after you type the confirmation window.</li> </ol>

**UVM-aware devices**

The following troubleshooting information might be helpful if you experience problems when using UVM-aware devices.

---

<b>A UVM-aware device stops working properly</b>	<b>Action</b>
If you disconnect a UVM-aware device from a Universal Serial Bus (USB) port, and then connect the device to the USB port again, the device might not work properly.	Restart the computer after the device has been connected to the USB port.

---

---

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

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

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

## Appendix B - Rules for the hardware password and the UVM passphrase

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

The following table describes the rules for the hardware password.

### *Hardware password rules*

Length	The password must be exactly eight characters long.
Characters	The password must contain alphanumeric characters only. A combination of letters and numbers is allowed.
Properties	You set the hardware password to enable the IBM embedded Security Chip in the computer. The hardware password must also be typed each time you access the Administrator Utility.
Incorrect attempts	If you incorrectly type the password 10 times, the computer locks for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly 10 more times, the computer locks up for 2 hours and 34 minutes. The time the computer is disabled doubles each time you incorrectly type the password 10 times.

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

The following table describes the rules for the UVM passphrase.

### **UVM passphrase rules**

Length	The passphrase can be up to 256 characters long.
Characters	The passphrase can contain any combination of characters that the keyboard produces, including spaces and nonalphanumeric characters.
Properties	The UVM passphrase is different from a password that you might use to log on to an operating system. The 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 not lock up. There is no limit on the number of incorrect attempts.

---

## Appendix C - Rules for using UVM protection for system logon

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

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

For Windows 95 and Windows 98, UVM protection uses the Client Security screen saver to secure the logon.

UVM protection for the system logon is not supported for clients running Windows 2000.

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

- Do not clear the IBM embedded Security Chip while UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software. For more information, see “Administrator tips,” on page 53.
- If you use the Microsoft Family Logon client for Windows 95 or Windows 98, configure Microsoft Family Logon before you assign UVM passphrases for users and before you set and use UVM protection. See the Attention box on page 15 for more information.
- If you clear the **Use UVM protection** check box in the Administrator Utility, the system returns to the Windows logon process without UVM logon protection.
- In Windows NT, you have the option of specifying the maximum number of attempts allowed for typing the correct password for the Windows NT logon application. This option does not apply to UVM logon protection. There is no limit that you can set for the number of attempts allowed for typing the UVM passphrase. For rules on the UVM passphrase, see “Appendix B - Rules for the hardware password and the UVM passphrase,” on page 69.

---

## Appendix D - Notices and Trademarks

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

---

### Notices

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

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

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

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

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

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

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

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

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

## **Client Security Software**

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

---

### **Trademarks**

IBM, NetVista, and SecureWay are trademarks of IBM Corporation in the U.S., other countries, or both.

Lotus Notes is a registered trademark of Lotus Development Corporation.

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

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

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

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