IBM® Client Security
Solutions

Using Client Security Software Version 4.0 with Policy Director

IBM® Client Security
Solutions

Using Client Security Software Version 4.0 with Policy Director

First Edition (March 2002)

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 27 and Appendix D, “**Notices and Trademarks**” on page 33.

Contents

Preface

This guide contains helpful information on setting up Client Security Software for use with IBM SecureWay Policy Director (Policy Director).

This guide is organized as follows:

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

″Chapter 2, “Installing the Client Security component on a Policy Director server”,″ contains the prerequisites and instructions for installing Client Security support on your Policy Director server.

″Chapter 3, “Configuring IBM clients”,″ contains prerequisite information and instructions for configuring IBM clients to use the authentication services provided by Policy Director.

″Chapter 4, “Troubleshooting”,″ contains helpful information for solving problems you might experience while using the instructions provided in this guide.

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

″Appendix B, “Password and passphrase rules”,″ contains the rules for UVM passphrases and Security Chip passwords.

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

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

Who should read this guide

This guide is intended for enterprise administrators who will use Policy Director version 3.7 or version 3.8 to manage authentication objects set up by the User Verification Manager (UVM) security policy on an IBM client.

Administrators must be knowledgeable of the following concepts and procedures:

- Installation and management of the SecureWay Directory lightweight directory access protocol (LDAP)
- Installation and stup procedures for Policy Director Runtime Environment
- Management of the Policy Director object space

How to use this guide

Use this guide to set up Client Security support for use with Policy Director. This guide is a companion to the *Client Security Software Installation Guide*, *Client Security Software Administrator's Guide*, and *Client Security User's Guide*.

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

References to the *Client Security Software Installation Guide*

References to the *Client Security Software Installation Guide* are provided in this document. After you have set up and configured the Policy Director server and installed the Runtime Environment on the client, use the instructions in the *Client Security Software Installation Guide* to install Client Security Software on IBM clients. See Chapter 3, “Configuring IBM clients” on page 7 for more information.

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

References to the *Client Security Software Administrator’s Guide* are provided in this document. The *Client Security Software Administrator’s Guide* contains information on how to set up user authentication and the UVM policy for the IBM client. After you have installed Client Security Software, use the *Client Security Software Administrator’s Guide* to set up user authentication and the security policy. See Chapter 3, “Configuring IBM clients” on page 7 for more information.

Additional information

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

Chapter 1. Introducing IBM Client Security Software

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

Client Security Software applications and components

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

- **Administrator Utility:** The Administrator Utility is the interface an administrator uses to activate or deactivate the embedded Security Chip, and to create, archive, and regenerate encryption keys and passphrases. In addition, an administrator can use this utility to add users to the security policy provided by Client Security Software.
- **User Verification Manager (UVM):** Client Security Software uses UVM to manage passphrases and other elements to authenticate system users. For example, a fingerprint reader can be used by UVM for logon authentication. UVM software enables the following features:
  - **UVM client policy protection:** UVM software enables an administrator to set the client security policy, which dictates how a client user is authenticated on the system.
  - **UVM system logon protection:** UVM software enables an administrator to control computer access through a logon interface. UVM protection ensures that only users who are recognized by the security policy are able to access the operating system.
  - **UVM Client Security screen saver protection:** UVM software enables users to control access to the computer through a Client Security screen saver interface.
- **Client Utility:** The Client Utility enables a client user to change the UVM passphrase. On Windows NT, the Client Utility enables users to change Windows NT logon passwords to be recognized by UVM and to update key archives. A user can also create backup copies of digital certificates created with the IBM embedded Security Chip.

Public Key Infrastructure (PKI) features

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

- **Administrator control over client security policy.** Authenticating end users at the client level is an important security policy concern. Client Security Software provides the interface that is required to manage the security policy of an IBM client. This interface is part of the authenticating software User Verification Manager (UVM), which is the main component of Client Security Software.
- **Encryption key management for public key cryptography.** Administrators create encryption keys for the computer hardware and the client users with Client Security Software. When encryption keys are created, they are bound to the IBM embedded Security Chip through a key hierarchy, where a base level hardware key is used to encrypt the keys above it, including the user keys that are associated with each client user. Encrypting and storing keys on the IBM

embedded Security Chip adds an essential extra layer of client security, because the keys are securely bound to the computer hardware.

- **Digital certificate creation and storage that is protected by the IBM embedded Security Chip.** When you apply for a digital certificate that can be used for digitally signing or encrypting an e-mail message, Client Security Software enables you to choose the IBM embedded Security Chip as the cryptographic service provider for applications that use the Microsoft CryptoAPI. These applications include Internet Explorer and Microsoft Outlook Express. This ensures that the private key of the digital certificate is stored on the IBM embedded Security Chip. Also, Netscape users can choose IBM embedded Security Chips as the private key generators for digital certificates used for security. Applications that use the Public-Key Cryptography Standard (PKCS) #11, such as Netscape Messenger, can take advantage of the protection provided by the IBM embedded Security Chip.
- **A key archive and recovery solution.** An important PKI function is creating a key archive from which keys can be restored if the original keys are lost or damaged. Client Security Software provides an interface that enables you to establish an archive for keys and digital certificates created with the IBM embedded Security Chip and to restore these keys and certificates if necessary.
- **Right Click Encryption.** Right Click Encryption enables a client user to encrypt his files simply by clicking the right mouse button.

Chapter 2. Installing the Client Security component on a Policy Director server

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

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

- Locally, using a policy editor that resides on the IBM client
- Throughout an enterprise, using Policy Director

Before Client Security can be used with Policy Director, the Client Security component of Policy Director must be installed. This component can be downloaded from the http://www.pc.ibm.com/ww/security/secdownload.html IBM Web site.

Prerequisites

Before a secure connection can be established between the IBM Client and the Policy Director server, the following components must be installed on the IBM Client:

- IBM Global Security Toolkit
- IBM SecureWay Directory Client
- Policy Director Runtime Environment

For detailed information about installing and using Policy Director, see the documentation that is provided on the http://www.tivoli.com/products/index/secureway_policy_dir/index.htm Web site.

Downloading and installing the Client Security component

The Client Security component is available as a free download from the IBM Web site. To download and install the Client Security component on the Policy Director server and IBM client, complete the following procedure:

1. Download PDCS.exe from the http://www.pc.ibm.com/ww/security/secdownload.html Web site.
2. Click the link for downloading Client Security Software, and then complete the registration form and questionnaire.

   PDCS.exe is available from the same IBM Web page that contains the Client Security Software code.
3. Run PDCS.exe to extract the following files:
   - **PD_Add_ClientSecurity.txt** This file is used to add the IBM Solutions object space, Client Security Actions, and individual ACL entries on the Policy Director server. The individual ACLs can be edited or removed, however, the IBM Solutions object space and Client Security Actions must not change.
   - **PD_Remove_ClientSecurity.txt** This file can be used to remove the OBject Space, Actions, and ACL entries created by the PD_Add_ClientSecurity.txt file.
   - **PDCS.conf** The Policy Director/Client Security configuration file (PDCS.conf) is used as the base configuration file.

Adding the Client Security components on the Policy Director server

The pdadmin utility is a command-line tool that an administrator can use to perform most Policy Director administration tasks. Multiple command execution enables an administrator to use a file that contains multiple pdadmin commands to perform a complete task or series of tasks. The communication between the pdadmin utility and the Management Server (pdmgrd) is secured over SSL. The pdadmin utility is installed as part of the Policy Director Runtime Environment (PDRTE) package.

The pdadmin utility accepts a filename argument that identifies the location of such a file, for example:

```
MSDOS>pdadmin [-a <admin-user >][-p <password >]<file-pathname >
```

The following command is an example of how to create the IBM Solutions object space, Client Security Actions, and individual ACL entries on the Policy Directory server:

```
MSDOS>pdadmin -a sec_master -p password C:\PD_Add_ClientSecurity.txt
```

Refer to the *Policy Director Base Administrator Guide* for more information about the pdadmin utility and its command syntax.

Establishing a secure connection between the IBM client and the Policy Director server

The IBM Client must establish its own authenticated identity within the Policy Director secure domain in order to request authorization decisions from the Policy Director Authorization Service.

A unique identity must be created for the application in the Policy Director secure domain. In order for the authenticated identity to perform authentication checks, the application must be a member of the remote-acl-users group. When the application wants to contact one of the secure domain services, it must first log in to the secure domain.

The svrsslcfg utility enables the IBM Client Security applications to communicate with the Policy Director Management Server and Authorization Server.

The svrsslcfg utility enables the IBM Client Security applications to communicate with the Policy Director Management server and the Authorization server.

The svrsslcfg utility performs the following tasks:

- Creates a user identity for the application. For example, DemoUser/HOSTNAME
- Creates an SSL key file for that user. For example, DemoUser.kdb and DemoUser.sth
- Adds the user to the remote-acl-users group

The following parameters are needed:

- **-f cfg_file** Configuration file path and name, use PDCS.conf
- **-d kdb_dir** The directory that is to contain the key ring database files for the server.
- **-n server_name** The actual Windows Username/UVM username of the intended IBM Client user.

- **-P admin_pwd** The Policy Director Administrator password.
- **-s server_type** Must be specified as remote.
- **-S server_pwd** The password for the newly created user. This parameter is required.
- **-r port_num** Set the listening port number for the IBM Client. This is the parameter specified in the Policy Director Runtime variable SSL Server Port for PD Management Server.

To establish a secure connection between the IBM client and the Policy Director server, complete the following procedure:

1. Create a directory and move the PDCS.conf file to the new directory.

   For example, `MSDOS> mkdir C:\PDCS MSDOS> move C:\PDCS.conf C:\PDCS\`
2. Run svrsslcfg to create the user.

   MSDOS> svrsslcfg -config -f C:\PDCS\PDCS.conf -d C:\PDCS\ -n <server_name> - s remote -S <server_pwd> -P <admin_pwd> -r 7135

   Note: Replace <server_name> with the intended UVM username and hostname of the IBM client.For example: –n DemoUser/MyHostName. The IBM Client Hostname can be found by typing “hostname” at the MSDOS prompt. The svrsslcfg utility will create a valid entry in the Policy Director server and provide a unique SSL key file for encrypted communication.
3. Run svrsslcfg to add the location of ivacld to the PDCS.conf file.

   By default, the PD Authorization server listens on port 7136. This can be verified by looking at the tcp_req_port parameter in the ivacld stanza of the ivacld.conf file on the Policy Director server. It is important that you get the ivacld host name correct. Use the pdadmin server list command to obtain this information. The servers are named: <server_name>-<host_name>. The following is an example of running pdadmin server list:

```
MSDOS> pdadmin server list ivacld-MyHost.ibm.com
```

The following command is then used to add a replica entry for the ivacld server displayed above. It is assumed that ivacld is listening on the default port 7136.

```
svrsslcfg -add_replica  -f <config file path> -h <host_name>
MSDOS>svrsslcfg -add_replica  -f C:\PDCS\PDCS.conf -h MyHost.ibm.com
```

Chapter 3. Configuring IBM clients

Before you can use Policy Director to control the authentication objects for IBM clients, you must configure each client by using the Administrator Utility, a component that is provided with Client Security Software. This section contains prerequisites and instructions for configuring IBM clients.

Prerequisites

Make sure the following software is installed on the IBM client in the following order:

1. **Microsoft Windows supported operating system.** You can use Policy Director to control the authentication requirements only for IBM clients running Windows NT Workstation 4.0 or Windows 2000.
2. **Client Security Software version 3.0 or later.** Install the software, and enable the IBM embedded Security Chip. Use the Administrator Utility to set up user authentication and edit the UVM security policy. For comprehensive instructions on installing and using Client Security Software, see the *Client Security Software Installation Guide* and the *Client Security Software Administrator's Guide*.

Configuring the Policy Director setup information

You can configure the Policy Director setup information by using the Administrator Utility, a software component that is provided by Client Security Software. The Policy Director setup information consists of the following settings:

- Selecting the full path to the Configuration File
- Selecting the Local Cache Refresh Interval

To configure the Policy Director setup information on the IBM client, complete the following procedure:

1. Click **Start > Programs > Client Security Software Utilities > Administrator Utility**.
2. Type the hardware password, and click **OK**.

   The Administrator Utility window opens. For complete information on using the Administrator Utility, see the *Client Security Software Administrator's Guide*.
3. In the Administrator Utility, click the **Configure Application Support and Policies** button.
4. Click the **Policy Configuration** button.
5. Under Policy Director Setup Information, select the full path to the PDCS.conf configuration file. For example, `C:\PDCS\PDCS.conf`
6. Click the **Apply** button.

Setting and using the local-cache feature

After Selecting the Policy Director configuration file, the local cache refresh interval can be set. A local replica of the security policy information as managed by Policy Director is maintained at the IBM client. You can schedule an automatic refresh of the local cache in increments of months (0-12) or days (0-30).

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

1. Click **Start > Programs > Client Security Software Utilities > Administrator Utility**.
2. Type the hardware password, and click **OK**.

   The Administrator Utility window opens. For complete information on using the Administrator Utility, see the *Client Security Software Administrator's Guide*.
3. Click the **Configure Application Support and Policies** button.
4. Click the **Policy Configuration** button.
5. Do one of the following:
   - To refresh the local cache, click **Refresh Local Cache**.
   - To set the automatic refresh rate, type the number of months (0-12) and days (0-30) in the fields provided, and click **Apply**. The local cache file expiration date will update to indicate when the next automatic refresh will take place.

     Note: Set a refresh interval of at least one day. This will greatly improve the performance of the Client Security operations that are protected by Policy Director.

Enabling Policy Director to control IBM client objects

UVM policy is controlled through a global policy file. The global policy file, called a UVM-policy file, contains authentication requirements for actions that are performed on the IBM client system, such as logging on to the system, clearing the screen saver, or signing e-mail messages.

Before you can enable Policy Director to control the authentication objects for an IBM client, use the UVM-policy editor to edit the UVM-policy file. The UVM-policy editor is part of the Administrator Utility.

Important: Enabling Policy Director to control an object gives object 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.

Editing a local UVM policy

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

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. Only a user who has been added to UVM can use the UVM-policy editor.

Note: If you set UVM policy to require fingerprints for an authentication object (such as the operating-system logon), users that are added to UVM must have their fingerprints registered to use that object.

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

1. Click the **Configure Application Support and Policies** button.
2. Under UVM Policy, click **Local Client**, and then click **Edit Policy**. The Global Policy Access Password window opens.
3. In the UVM Policy area, click **Local Client**, and then click **Edit Policy**.

   The Global Policy Access Password window opens.

4. 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 on the UVM-policy editor, see the *Client Security Software Administrator's Guide*.

5. On the Policy Selection page, select the UVM-policy file (globalpolicy.gvm) from the drop-down list.
6. Click the **Object Selection** tab, click **Action** or **Object type**, and select the object for which you want to assign authentication requirements.

   Examples of valid actions include System Logon, System Unlock, and E-mail Decryption; an example of an object type is Acquire Digital Certificate.
7. For each object that you select, select **Policy Director controls selected object** to enable Policy Director for that object.

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

   Note: While you are editing UVM policy, you can view the policy summary information by clicking **UVM Policy Summary**.
8. Click the **Information** tab, and type the system name, user details, and system and enterprise administrator details in the appropriate fields.
9. Click the **Policy Selection** tab, and click the **UVM Policy** button.
   - To save the policy file, click **Save** and follow the on-screen instructions.
   - To save the file with a new password, click **Save as** and follow the on-screen instructions.
10. Click **OK** to save your changes and exit.

Editing and using UVM policy for remote clients

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

Note: If you set a UVM policy for remote clients to require fingerprints for an authentication object (such as the operating-system logon), users that are added to UVM must have their fingerprints registered to use that object. Also, all remote clients that will use the policy must have UVM-aware fingerprint sensors installed.

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

1. Click the **Configure Application Support and Policies** button.
2. In the UVM Policy area, click **Remote Clients**, and then click **Edit Policy**.

   The Global Policy Access Password window opens.
3. 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.

4. On the Policy Selection page, select the UVM-policy file (globalpolicy.gvm) from the drop-down list.
5. Click the **Object Selection** tab, click **Action** or **Object type**, and select the object for which you want to assign authentication requirements.

   Examples of actions include System Logon, System Unlock, and E-mail Decryption; an example of an object type is Acquire Digital Certificate.
6. For each object that you select, click **Policy Director controls selected object** to enable Policy Director for the object.

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

   Note: While you are editing the UVM-policy file, you can view the policy summary information by clicking on UVM Policy Summary.
7. Click the **Information** tab, and type the system name, user details, and system and enterprise administrator details in the appropriate fields.
8. Click the **Remote Configuration** tab.
9. Select the authentication elements that are available on the remote clients that will use this UVM policy, and then select the **Policy Director enabled client** check box.
10. Click the **Policy Selection** tab, and click the **UVM Policy** button.
    - To save the policy file, click **Save** and follow the on-screen instructions.
    - To save the file with a new password, click **Save as** and follow the on-screen instructions.
11. Click **OK** to save your changes and exit.
12. 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:

1. If you install the Client Security Software in its default location, the root directory for the preceding files is \Program Files.
2. You must copy both files to the \IBM\Security\UVM_Policy\ directory path on remote clients.

Chapter 4. Troubleshooting

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

Administrator functions

This section contains information that an administrator might find helpful when setting up and using Client Security Software.

Setting an administrator password (NetVista)

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

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

Attention:

- In Windows XP, Windows NT, and Windows 2000, do not clear or disable the IBM embedded Security Chip when UVM logon protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.

  To disable UVM protection, open the Administrator Utility and clear the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before UVM protection is disabled.
- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

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

To set an administrator password:

1. Shut down and restart the computer.
2. When the Configuration/Setup Utility prompt appears on the screen, press **F1**.

   The main menu of the Configuration/Setup Utility opens.
3. Select **System Security**.
4. Select **Administrator Password**.
5. Type your password and press the down arrow on your keyboard.
6. Type your password again and press the down arrow.
7. Select **Change Administrator password** and press Enter; then press Enter again.
8. Press **Esc** to exit and save the settings.

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

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

Setting a supervisor password (ThinkPad)

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

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

Attention:

- In Windows XP, Windows NT, and Windows 2000, do not clear or disable the IBM embedded Security Chip when UVM logon protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.

  To disable UVM protection, open the Administrator Utility and clear the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before UVM protection is disabled.
- Do not clear or disable the IBM embedded Security Chip if UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

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

To set a supervisor password, complete the following procedure:

1. Shut down and restart the computer.
2. When the IBM BIOS Setup Utility prompt appears on the screen, press **F1**.

   The main menu of the IBM BIOS Setup Utility opens.
3. Select **Password**.
4. Select **Supervisor Password**.
5. Type your password and press Enter.
6. Type your password again and press Enter.
7. Click **Continue**.
8. Press F10 to save and exit.

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

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

Protecting the hardware password

You set a Security Chip password to enable the IBM embedded Security Chip for a client. After you set a Security Chip password, access to the Administrator Utility is

protected by this password. You should protect the Security Chip password to prohibit unauthorized users from changing settings in the Administrator Utility.

Clearing the IBM embedded Security Chip (NetVista)

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:

- 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 and clear the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before UVM protection is disabled.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

To clear the IBM embedded Security Chip, do the following:

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

Clearing the IBM embedded Security Chip (ThinkPad)

If you want to erase all user encryption keys from the IBM embedded Security Chip and clear the 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:

- 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 and clear the **Replace the standard Windows logon with UVM's secure logon** check box. You must restart the computer before UVM protection is disabled.
- When the IBM embedded Security Chip is cleared, all encryption keys and certificates stored on the chip are lost.

To clear the IBM embedded Security Chip, do the following:

1. Shut down and restart the computer.
2. When the IBM BIOS Setup Utility prompt appears on the screen, press Fn.

Note: On some ThinkPad models, you might need to press the F1 key at power on to clear the security chip. Refer to the help message at IBM BIOS Setup Utility for details.

The main menu of the IBM BIOS Setup Utility opens.

3. Select **Security**.
4. Select **IBM TCPA Feature Setup**.
5. Select **Clear IBM TCPA Security Feature**.
6. Select **Yes**.
7. Press Enter to continue.
8. Press F10 to save and exit.

The Administrator Utility

The following section contains information to keep in mind when using the Administrator Utility.

Deleting users

When you delete a user from Windows XP, Windows NT, and Windows 2000, the user name is deleted from the list of users in the Administrator Utility.

Denying access to selected objects with Policy Director control

The **Deny all access to selected object** check box is not disabled when 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.

Known limitations

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

Using Client Security Software with Windows operating systems

All Windows operating systems have the following known limitation: If a client user that is enrolled in UVM changes his Windows user name, all Client Security functionality is lost. The user will have to re-enroll the new user name in UVM and request all new credentials.

Windows XP operating systems have the following known limitation: Users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. UVM will point to the former user name while Windows will only recognize the new user name. This limitation occurs even if the Windows user name was changed prior to installing Client Security Software.

Using Client Security Software with Netscape applications

Netscape opens after an authorization failure: If the UVM passphrase window opens, you must type the UVM passphrase and click **OK** before you can continue. If you type an incorrect UVM passphrase (or provide an incorrect fingerprint for a fingerprint scan), an error message is displayed. If you click **OK**, Netscape will open, but you will not be able to use the digital certificate generated by the IBM

embedded Security Chip. You must exit and re-enter Netscape, and type the correct UVM passphrase before you can use the IBM embedded Security Chip certificate.

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

- SHA-1
- MD5

IBM embedded Security Chip certificate and encryption algorithms

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

When sending e-mail from one Outlook Express (128-bit) client to another Outlook Express (128-bit) client: If you use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0 to send encrypted e-mail to other clients using Outlook Express (128-bit), e-mail messages encrypted with the IBM embedded Security Chip certificate can only use the 3DES algorithm.

When sending e-mail between an Outlook Express (128-bit) client and a Netscape client: An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm.

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

Using UVM protection for a Lotus Notes User ID

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

1. Exit Notes.
2. Disable UVM protection for the current User ID.
3. Enter Notes and switch User IDs. See your Lotus Notes documentation for information about switching User IDs.

   If you want to set up UVM protection for the User ID that you have switched to, proceed to step 4.
4. Enter the Lotus Notes Configuration tool provided by Client Security Software and set up UVM protection.

Client Utility limitations

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

Windows XP Professional

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

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

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

- Change their UVM passphrases
- Update the Windows password registered with UVM
- Update the key archive

These limitations are cleared after an administrator starts and exits the Administrator Utility.

Windows XP Home

Windows XP Home Limited Users will not be able to use the Client Utility in any of the following situations:

- Client Security Software is installed on an NTFS formatted partition
- The Windows folder is on an NTFS formatted partition
- The archive folder is on an NTFS formatted partition

Error messages

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

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

Troubleshooting charts

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

Installation troubleshooting information

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

Problem Symptom	Possible Solution
An error message is displayed during software installation	**Action**
A message is displayed when you install the software that asks if you want to remove the selected application and all of its components.	Click **OK** to exit the window. Begin the installation process again to install the new version of Client Security Software.
A message is displayed during installation stating that a previous version of Client Security Software is already installed.	Click **OK** to exit from the window. Do the following: 1. Uninstall the software. 2. Reinstall the software. **Note:** If you plan to use the same hardware password to secure the IBM embedded Security Chip, you do not have to clear the chip and reset the password.
Installation access is denied due to an unknown hardware password	**Action**
When installing the software on an IBM client with an enabled IBM embedded Security Chip, the hardware password for the IBM embedded Security Chip is unknown.	Clear the chip to continue with the installation.
An unattended installation will not start	**Action**
The SMBus device driver must be installed to perform an unattended installation.	Install the SMBus device driver and restart the installation.
An unattended installation ends prematurely	**Action**
No error messages are displayed during unattended installations.	Perform an attended installation to view any error messages that might be displayed.
The setup.exe file does not respond properly	**Action**
If you extract all files from the csec4_0.exe file into a common directory, the setup.exe file will not work properly.	Run the smbus.exe file to install the SMBus device driver, and then run the csec4_0.exe file to install the Client Security Software code.
An error message displays when you install a UVM-aware fingerprint sensor	**Action**
During installation of the DigitalPersona U.are.UPro fingerprint sensor, a message is displayed that asks you to do the following: 1. Attach the fingerprint sensor. 2. Wait for the red light to illuminate on the sensor. 3. Click **OK**. 4. Select **Yes, I want to restart my computer now** and click **Finish**. The system will restart.	No further action is required. The fingerprint sensor will install correctly.

Administrator Utility troubleshooting information

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

Problem Symptom	Possible Solution
The Next button is unavailable after entering and confirming your UVM passphrase in the Administrator Utility	**Action**
On systems running Windows NT, Windows 2000, or Windows XP, when you add users to UVM, the **Next** button might not be available after you enter and confirm your UVM passphrase in the Administrator Utility.	Click the **Information** item on the Windows Task Bar and continue the procedure.
An error message displays when you attempt to edit local UVM policy	**Action**
When you edit the local UVM policy, an error message might display if no users are enrolled in UVM.	Add a user to UVM before attempting to edit the policy file.
An error message displays when you change the admin public key	**Action**
When you clear the embedded Security Chip and then restore the key archive, an error message might display if you change the admin public key.	Add the users to UVM and request new certificates, if applicable.
An error message displays when you attempt to recover a UVM passphrase	**Action**
When you change the admin public key and then attempt to recover a UVM passphrase for a user, an error message might display.	Do one of the following: • If the UVM passphrase for the user is not needed, no action is required. • If the UVM passphrase for the user is needed, you must add the user to UVM, and request new certificates, if applicable.
An error message displays when you try to save the UVM-policy file	**Action**
When you attempt to save a UVM-policy file (globalpolicy.gvm) by clicking **Apply** or **Save**, an error message might display.	Exit the error message, edit the UVM-policy file again to make your changes, and then save the file.
An error message displays when you try to open the UVM-policy editor	**Action**
When the current user (logged on to the operating system) has not been added to UVM, the UVM-policy editor will not open.	Add the user to UVM and open the UVM-policy editor.
An error message displays when you are using the Administrator Utility	**Action**
When you are using the Administrator Utility, the following error message might display: A buffer I/O error occurred while trying to access the Client Security chip. This might be corrected by a reboot.	Exit the error message and restart your computer.
A disable chip message is displayed when change the Security Chip password	**Action**

Problem Symptom	Possible Solution
When you attempt to change the Security Chip password, and you press Enter or Tab > Enter after you type the confirmation password, the Disable chip button will be enabled and a disable chip confirmation message is displayed.	Do the following: 1. Exit from the disable chip confirmation window. 2. To change the Security Chip password, type the new password, type the confirmation password, and then click **Change**. Do not press Enter or Tab > Enter after you type the confirmation window.

Client Utility troubleshooting information

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

Problem Symptom	Possible Solution
Limited Users are unable to perform certain Client Utility functions in Windows XP Professional	**Action**
Windows XP Professional Limited Users might not be able to perform the following Client Utility tasks: • Change their UVM passphrases • Update the Windows password registered with UVM • Update the key archive	These limitations are cleared after an administrator starts and exits the Administrator Utility.
Limited Users are unable to use the Client Utility in Windows XP Home	**Action**
Windows XP Home Limited Users will not be able to use the Client Utility in any of the following situations: • Client Security Software is installed on an NTFS formatted partition • The Windows folder is on an NTFS formatted partition • The archive folder is on an NTFS formatted partition	This is a known limitation with Windows XP Home. There is no solution to this problem.

ThinkPad-specific troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Client Security Software on ThinkPad computers.

Problem Symptom	Possible Solution
An error message is displayed when attempting a Client Security administrator function	**Action**

Problem Symptom	Possible Solution
The following error message is displayed after trying to perform a Client Security administrator function: ERROR 0197: Invalid Remote change requested. Press <F1> to Setup	The ThinkPad supervisor password must be disabled to perform certain Client Security administrator functions. To disable the supervisor password, do the following: 1. Press F1 to access the IBM BIOS Setup Utility. 2. Enter the current supervisor password. 3. Enter a blank new supervisor password, and confirm a blank password. 4. Press Enter. 5. Press F10 to save and exit.
Different UVM-aware fingerprint sensor does not work properly	**Action**
The IBM ThinkPad computer does not support the interchanging of multiple UVM-aware fingerprint sensors.	Do not switch fingerprint sensor models. Use the same model when working remotely as when working from a docking station.

Microsoft troubleshooting information

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

Problem Symptom	Possible Solution
Client Security does not work properly for a user enrolled in UVM	**Action**
The enrolled client user might have changed his Windows user name. If that occurs, all Client Security functionality is lost.	Re-enroll the new user name in UVM and request all new credentials.
Note: In Windows XP, users enrolled in UVM that previously had their Windows user name changed will not be recognized by UVM. This limitation occurs even if the Windows user name was changed prior to installing Client Security Software.	
Problems reading encrypted e-mail using Outlook Express	**Action**
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient. **Note:** To use 128-bit Web browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility.	Verify the following: 1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.
Problems using a certificate from an address that has multiple certificates associated with it	**Action**

Problem Symptom	Possible Solution
Outlook Express can list multiple certificates associated with a single e-mail address and some of those certificates can become invalid. A certificate can become invalid if the private key associated with the certificate no longer exists on the IBM embedded Security Chip of the sender's computer where the certificate was generated.	Ask the recipient to resend his digital certificate; then select that certificate in the address book for Outlook Express.
Failure message when trying to digitally sign an e-mail message	**Action**
If the composer of an e-mail message tries to digitally sign an e-mail message when the composer does not yet have a certificate associated with his or her e-mail account, an error message displays.	Use the security settings in Outlook Express to specify a certificate to be associated with the user account. See the documentation provided for Outlook Express for more information.
Outlook Express (128 bit) only encrypts e-mail messages with the 3DES algorithm	**Action**
When sending encrypted e-mail between clients that use Outlook Express with the 128-bit version of Internet Explorer 4.0 or 5.0, only the 3DES algorithm can be used.	To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 56-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. See Microsoft for current information on the encryption algorithms used with Outlook Express.
Outlook Express clients return e-mail messages with a different algorithm	**Action**
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
Error message when using a certificate in Outlook Express after a hard disk drive failure	**Action**
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, do one of the following: • obtain new certificates • register the certificate authority again in Outlook Express
Outlook Express does not update the encryption strength associated with a certificate	**Action**

Problem Symptom	Possible Solution
When a sender selects the encryption strength in Netscape and sends a signed e-mail message to a client using Outlook Express with Internet Explorer 4.0 (128-bit), the encryption strength of the returned e-mail might not match.	Delete the associated certificate from the address book in Outlook Express. Open the signed e-mail again and add the certificate to the address book in Outlook Express.
An error decryption message displays in Outlook Express	**Action**
You can open a message in Outlook Express by double-clicking it. In some instances, when you double-click an encrypted message too quickly, a decryption error message appears.	Close the message, and open the encrypted e-mail message again.
Also, a decryption error message might display in the preview pane when you select an encrypted message.	If an error message appears in the preview pane, no action is required.
An error message displays when you click the Send button twice on encrypted e-mails	**Action**
When using Outlook Express, if you click the send button twice to send an encrypted e-mail message, an error message displays stating that the message could not be sent.	Close the error message and click the **Send** button once.
An error message displays when you requesting a certificate	**Action**
When using Internet Explorer, you might receive an error message if you request a certificate that uses the IBM embedded Security Chip CSP.	Request the digital certificate again.

Netscape application troubleshooting information

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

Problem Symptom	Possible Solution
Problems reading encrypted e-mail	**Action**
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient. **Note:** To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. If the IBM embedded Security Chip supports 256-bit encryption, you must use a 40-bit Web browser. You can find out the encryption strength provided by Client Security Software in the Administrator Utility.	Verify the following: 1. The encryption strength for the Web browser that the sender uses is compatible with the encryption strength of the Web browser that the recipient uses. 2. The encryption strength for the Web browser is compatible with the encryption strength provided by the firmware of Client Security Software.
Failure message when trying to digitally sign an e-mail message	**Action**
When the IBM embedded Security Chip certificate has not been selected in Netscape Messenger, and the writer of an e-mail message tries to sign the message with the certificate, an error message displays.	Use the security settings in Netscape Messenger to select the certificate. When Netscape Messenger is open, click the security icon on the toolbar. The Security Info window opens. Click **Messenger** in the left panel and then select the **IBM embedded Security Chip certificate**. See the documentation provided by Netscape for more information.
An e-mail message is returned to the client with a different algorithm	**Action**
An e-mail message encrypted with the RC2(40), RC2(64), or RC2(128) algorithm is sent from a client using Netscape Messenger to a client using Outlook Express (128-bit). A returned e-mail message from the Outlook Express client is encrypted with the RC2(40) algorithm.	No action is required. An RC2(40), RC2(64), or RC2(128) encryption request from a Netscape client to an Outlook Express (128-bit) client is always returned to the Netscape client with the RC2(40) algorithm. See Microsoft for current information on the encryption algorithms used with your version of Outlook Express.
Unable to use a digital certificate generated by the IBM embedded Security Chip	**Action**
The digital certificate generated by the IBM embedded Security Chip is not available for use.	Verify that the correct UVM passphrase was typed when Netscape was opened. If you type the incorrect UVM passphrase, an error message displays stating an authentication failure. If you click **OK**, Netscape opens, but you will not be able to use the certificate generated by the IBM embedded Security Chip. You must exit and re-open Netscape, and then type the correct UVM passphrase.
New digital certificates from the same sender are not replaced within Netscape	**Action**
When a digitally signed e-mail is received more than once by the same sender, the first digital certificate associated with the e-mail is not overwritten.	If you receive multiple e-mail certificates, only one certificate is the default certificate. Use the security features in Netscape to delete the first certificate, and then re-open the second certificate or ask the sender to send another signed e-mail.
Cannot export the IBM embedded Security Chip certificate	**Action**
The IBM embedded Security Chip certificate cannot be exported in Netscape. The export feature in Netscape can be used to back up	Go to the Administrator Utility or Client Utility to update the key archive. When you update the key archive, copies of all the certificates

Digital certificate troubleshooting information

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

Problem Symptom	Possible Solution
UVM passphrase window or fingerprint authentication window displays multiple times during a digital certificate request	**Action**
The UVM security policy dictates that a user provide the UVM passphrase or fingerprint authentication before a digital certificate can be acquired. If the user tries to acquire a certificate, the authentication window that asks for the UVM passphrase or fingerprint scan displays more than once.	Type your UVM passphrase or scan your fingerprint each time the authentication window opens.
A VBScript or JavaScript error message displays	**Action**
When you request a digital certificate, an error message related to VBScript or JavaScript might display.	Restart the computer, and obtain the certificate again.

Policy Director troubleshooting information

The following troubleshooting information might be helpful if you experience problems when using Policy Director with Client Security Software.

Problem Symptom	Possible Solution
Local policy settings do not correspond to those on the server	**Action**
Policy Director allows certain bit configurations that are not supported by UVM. Consequently, local policy requirements can override settings made by an administrator when configuring the PD server.	This is a known limitation.
Policy Director setup settings are not accessible	**Action**
Policy Director setup and local cache setup settings are not accessible on the Policy Setup page in the Administrator Utility.	Install the Policy Director runtime Environment. If the Runtime Environment is not installed on the IBM client, the Policy Director settings on the Policy Setup page will not be available.
A user's control is valid for both the user and the group	**Action**
When configuring the Policy Director server, if you define a user to a group, the user's control is valid for both the user and the group if **Traverse bit** is on.	No action is required.

Lotus Notes troubleshooting information

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

Problem Symptom	Possible Solution
After enabling UVM protection for Lotus Notes, Notes is not able to finish its setup	**Action**
Lotus Notes is not able to finish setup after UVM protection is enabled using the Administrator Utility.	This is a known limitation. Lotus Notes must be configured and running before Lotus Notes support is enabled in the Administrator Utility.
An error message displays when you try to change the Notes password	**Action**
Changing the Notes password when using Client Security Software might display in an error message.	Retry the password change. If this does not work, restart the client.
An error message displays after you randomly-generate a password	**Action**
An error message might display when you do the following: • Use the Lotus Notes Configuration tool to set UVM protection for a Notes ID • Open Notes and use the function provided by Notes to change the password for Notes ID file • Close Notes immediately after you change the password	Click **OK** to close the error message. No other action is required. Contrary to the error message, the password has changed. The new password is a randomly-generated password created by Client Security Software. The Notes ID file is now encrypted with the randomly-generated password, and the user does not need a new User ID file. If the end user changes the password again, UVM will generate a new random password for the Notes ID.

Encryption troubleshooting information

The following troubleshooting information might be helpful if you experience problems when encrypting files using Client Security Software 3.0 or later.

Problem Symptom	Possible Solution
Previously encrypted files will not decrypt	**Action**
Files encrypted with previous versions of Client Security Software do not decrypt after upgrading to Client Security Software 3.0 or later.	This is a known limitation. You must decrypt all files that were encrypted using prior versions of Client Security Software *before* installing Client Security Software 3.0 or later. Client Security Software 3.0 cannot decrypt files that were encrypted using prior versions of Client Security Software because of changes in its file encryption implementation.

UVM-aware device troubleshooting information

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

Problem Symptom	Possible Solution
A UVM-aware device stops working properly	**Action**
When you disconnect a UVM-aware device from a Universal Serial Bus (USB) port, and then reconnect the device to the USB port, the device might not work properly.	Restart the computer after the device has been reconnected to the USB port.

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

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

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

Appendix B. Password and passphrase rules

This appendix contains information regarding rules pertaining to various system passwords.

Hardware password rules

The following rules pertain to the hardware password:

Length
The password must be exactly eight characters long.

Characters
The password must contain alphanumeric characters only. A combination of letters and numbers is allowed. No exceptional characters, like space, !, ?, %, are allowed.

Properties
Set the Security Chip password to enable the IBM embedded Security Chip in the computer. This password must be typed each time you access the Administrator Utility.

Incorrect attempts
If you incorrectly type the password ten times, the computer locks up for 1 hour and 17 minutes. If after this time period has passed, you type the password incorrectly ten more times, the computer locks up for 2 hours and 34 minutes. The time the computer is disabled doubles each time you incorrectly type the password ten times.

UVM passphrase rules

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

The following rules pertain to the UVM passphrase:

Length
The passphrase can be up to 256 characters long.

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

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

Incorrect attempts
If you incorrectly type the UVM passphrase multiple times during a session, the computer will 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 XP, Windows NT, and Windows 2000, UVM logon interface replaces the operating system logon, so that the UVM logon window opens each time a user tries to log on to the system.

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

- Do not clear the IBM embedded Security Chip while UVM protection is enabled. If you do, the contents of the hard disk become unusable, and you must re-format the hard disk drive and reinstall all software.
- If you clear the **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** check box in the Administrator Utility, the system returns to the Windows logon process without UVM logon protection.
- In Windows XP, Windows NT, and Windows 2000, 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.

Appendix D. Notices and Trademarks

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

Notices

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

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

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

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

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

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

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

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

Trademarks

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

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

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

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

Printed in U.S.A.