IBM* Client Security Solutions

Client Security Software Version 2.1 Administrator's Guide

IBM* Client Security Solutions

Client Security Software Version 2.1 Administrator's Guide

Contents

Preface

This guide contains information on setting up and using the security features provided with Client Security Software.

This guide is organized as follows:

″Chapter 1, "Introducing IBM Client Security Software",″ contains an overview of the software that are included in the software, and specific examples that can help you decide how to use Client Security Software.

″Chapter 2, "How to use Client Security Software",″ contains examples using the components provided by Client Security Software to set up the security features that IBM client users require.

″Chapter 3, "Adding users to UVM",″ contains instructions about setting up UVM protection for the operating-system logon, and for adding new users to User Verification Manager (UVM).

″Chapter 4, "After users have been added to UVM",″ contains information about editing and saving UVM policy for IBM clients.

″Chapter 5, "Working with UVM policy",″ contains instructions about setting up UVM protection for a Lotus Notes User ID.

″Chapter 6, "Using other features of the Administrator Utility",″ contains instructions about using Administrator Utility features.

″Chapter 7, "Instructions for the client user",″ contains instructions about different tasks that the client user performs when using Client Security Software. Instructions about using UVM logon protection, the Client Security screen saver, secure e-mail and the Client Utility are included.

″Chapter 8, "Troubleshooting",″ contains helpful information for overcoming known limitations and 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 security administrators who will:
- 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

This guide is also intended for Policy Director administrators who will use IBM SecureWay Policy Director to manage authentication objects provided in UVM policy. Policy Director administrators must be able to manage the following:

- The Policy Director object space
- The authentication, authorization, and credential acquisition processes
- The IBM Distributed Computing Environment (DCE)
- 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*. 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. You must install Client Security Software on an IBM client before you can use this guide. Instructions for installing the software are provided in the *Client Security Software Installation Guide*.

References to *Using Client Security with Policy Director*

References to *Using Client Security with Policy Director* are provided in this document. Security administrators who will use Policy Director to manage authentication objects for UVM policy should read *Using Client Security with Policy Director*.

References to the *Client Security User's Guide*

References to the *Client Security User's Guide* are provided in this document. Administrators can use this guide to set up and maintain UVM policy on IBM clients that use Client Security Software. After an administrator has set up user authentication and UVM security policy, a client user can read the *Client Security User's Guide* to learn how to use Client Security Software.

The User's Guide contains information about performing Client Security Software tasks, such as using UVM logon protection, setting up the Client Security screen saver, creating a digital certificate, and using the Client Utility.

Additional information

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

Chapter 1. Introducing IBM Client Security Software

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

Client Security Software applications and components

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

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

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

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

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

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

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

Public Key Infrastructure (PKI) features

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

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

- **Encryption key management for public key cryptography.** 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

1

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. How to use Client Security Software

Administrators can use the multiple components provided by Client Security Software to set up the security features that IBM client users require. Use the following examples to guide your thinking as you plan your Client Security policy and configuration. For example, Windows NT users can set up UVM protection for system logon which prohibits unauthorized users from logging onto the IBM client.

Example 1 - One Windows NT 4.0 client and one Windows XP client that both use Outlook Express

In this example, one IBM client (client 1) has Windows NT 4.0 and Outlook Express installed, the other client (client 2) has Windows XP and Outlook Express installed. There are three users who 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. It has also been established that both clients will require UVM protection for Windows NT logon. The administrator decided that the 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. Refer to the *Client Security Software Installation Guide* for details.
2. Install the UVM-aware fingerprint sensors and any associated software on each client.

   For information about UVM-aware products, go to http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html on the World Wide Web.
3. Set up user authentication with UVM for each client. See "Adding users to UVM" on page 8 for details. Do the following:
   a. 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.
   b. Set up UVM protection for the Windows logon for each client.
   c. Register user fingerprints. Because a policy will be set stating 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 15.
5. Restart each client to enable the UVM protection for the Windows logon.
6. Inform the users of the UVM passphrases that you have set for them and of the authentication requirements that you set in the UVM policy for the IBM client.

Users can now 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 Chapter 7, "Instructions for the client user" on page 29.
- Read the *Client Security User's Guide* to learn how to use the Client Utility.

Example 2 - Two Windows 2000 IBM clients that use Lotus Notes and the Client Security screen saver

In this example, the two IBM clients (client 1 and client 2) both have Windows 2000 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 clients will require UVM protection for the system logon, and will use the Client Security screen saver and UVM protection for Lotus Notes. The administrator decided a UVM policy for remote clients will be edited on client 1, and then 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.
2. Set up user authentication with UVM for each client. See "Adding users to UVM" on page 8 for details. Then, do the following:
   a. 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.
   b. 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 "Using UVM protection for Lotus Notes" on page 12.
4. Edit and save a UVM policy for remote clients on client 1, and then copy it 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 18.
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.

The users can now 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 2000

Example 3 - Multiple Windows NT 4.0 IBM clients that are managed by Policy Director and that use Netscape for e-mail

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. In this example, multiple IBM clients have both Windows NT 4.0 and Netscape installed. All clients have NetSEAT client, a Policy Director component, installed. All clients using an LDAP server have LDAP client installed. 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.

Note: Although NetSEAT client can be installed on Windows 98 clients, you can use Policy Director in conjunction with Client Security software only on IBM clients running Windows NT 4.0.

In this example, 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 and all clients will require UVM protection for the Windows NT logon.

To set up client security, do the following:
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 http://www.ibm.com/pc/ww/ibmpc/security/secdownload.html on the World Wide Web.
4. Set up user authentication with UVM on each client. See "Adding users to UVM" on page 8 for details. Then, do the following:
   a. Add users to UVM by assigning them a UVM passphrase.
   b. Set up UVM protection for the Windows NT logon on each client.
   c. Register the fingerprints for each client user. 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 it 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 18.
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 the *Client Security Software Installation Guide*.

9. Use Policy Director to control the IBM Client Security Solutions objects that appear in the Policy Director Management Console.

10. Inform client users of the UVM passphrases that have been set and the policy that has been set for each client.

11. Advise client users to 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 a 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 3. Adding users to UVM

The following information is useful when adding users to UVM.

Authentication for client users

Authenticating end users at the client level is an important computer 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 file that resides on the IBM client
- Throughout an enterprise, using Policy Director

Hardware encryption keys are generated when you add the first user.

Elements of authentication

Elements of authentication (such as UVM passphrases or user fingerprints) are used to verify users to the IBM client. When you add a user to UVM, you will assign a UVM passphrase for the client user. The UVM passphrase, which can be up to 256 characters long, is the main authentication element used by UVM. When you assign a UVM passphrase, user encryption keys are created for that client user and stored in a single file that is managed by the IBM embedded Security Chip. If the IBM client uses a UVM-aware fingerprint sensor for authentication, you must register the user fingerprints with UVM.

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.** 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, see "UVM operating-system logon protection" on page 11 for important information.

  For information about using UVM protection, see "UVM operating-system logon protection" on page 11.
- **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 UVM operating-system logon protection" on page 11. You do not need to enable UVM protection for the system logon to use the Client Security screen saver.

Before you add users to UVM

When 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. Client Security Software works in conjunction with the security features provided by the operating system. The following list describes the programs or procedures you can use to add new users for the respective operating system.

7

Notes:

1. When you use the operating system software to add new users, the domain password for each new user must be the same.
2. After a user has been enrolled in UVM, do not change his Windows user name. If you do, you will have to re-enroll the new user name in UVM and request all new credentials.

- **Windows XP and 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.

  Note: Do not enroll users in UVM that previously had their Windows user name changed. UVM will point to the former user name while Windows will only recognize the new user name.

- **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 98, and Windows Millennium Edition.** New users can be added by typing a new user name and password in the logon application. In Windows 98, when you delete a user from the computer, the user name is not deleted from the list of users in the Administrator Utility. See the operating system documentation for more information.

  Attention:

  If you use the Microsoft Family Logon client for Windows 98, configure Microsoft Family Logon and use the operating-system software to create new users **before** you assign UVM passphrases for users and set 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.

  When 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.

Adding users to UVM

Windows XP, Windows 2000 Professional, and Windows NT users must log on with administrator rights to use the Administrator Utility.

To add users to UVM, complete the following procedure:

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

   The Enter the IBM Security Chip password message is displayed.
2. Type the IBM Security Chip password and click **OK**.

   The Administrator Utility window opens.
3. In the **Windows Users Not Enrolled in UVM** 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 or network.
4. Click **Enroll User**.

An IBM Security Subsystem Administrator Utility message is displayed.

5. Click **OK**.

   When you select to generate new keys, the Modify Client Security Key Configuration - IBM Security Subsystem Archive Keys window opens.

   Note: Before performing this task on a ThinkPad computer, you must disable the supervisor password.

6. Type the Key Storage Directory (Path) or click **Browse** to point to the storage directory, and click **Next**.

   A message is displayed indicating that the operation completed successfully.

7. Click **OK**.

   The Modify Client Security Key Configuration - ISS Key Setup/Archive window opens.

8. Type the Archive Location path or click **Browse** to point to the archive location, and click **Next**.

   Note: If a BIOS Administrator Password is enabled on the system, a password field is displayed. Type the BIOS Administrator password and press **Enter**.

   A message is displayed indicating that the operation completed successfully.

9. Click **OK**.

   The Modify Client Security User Configuration - User Authentication Setup window opens.

10. Type and confirm an initial UVM passphrase for the user, and click **Next**.

    A message is displayed indicating that the operation completed successfully.

11. Click **OK**.

    The Modify Client Security User Configuration - Windows Logon Password window opens.

12. In the Windows Password field, type the operating system password associated with the user.

    Important: The system will supply the same Windows password for the user regardless of domain. Make sure the password you enter matches the user's current password. Failure to do so will result in the user being denied access to the system.

13. In the Confirm Windows Password field, type the operating system password associated with the user, and click **Next**.

    A message is displayed indicating that the operation completed successfully.

14. Click **OK**.

    The Modify Client Security User Configuration - UVM Enabled Devices window opens.

15. Click **Enroll Fingerprints**.

    The Fingerprint Registration window opens.

16. Select a hand and finger to be registered by clicking the appropriate radio buttons.

    The Fingerprint Registration window reflects your selections.

17. Click **Start registration**.

18. Place a finger on the UVM-aware fingerprint sensor and follow the on-screen instructions.

Each fingerprint must be scanned four times. Click **Cancel this finger** to cancel the fingerprint scan. A screen shows the fingerprints that are being stored. A screen will display after the fingerprints have been successfully registered.

19. Click **Exit** when finished registering fingerprints.

    The Modify Client Security User Configuration - Operation complete window opens.

20. Click **Finish**.

    This returns you to the Administrator Utility main window. You have now added a user to UVM, created user encryption keys for the client, and registered user fingerprints. To add other users, repeat this procedure.

21. After adding new users to UVM, inform them of the UVM passphrases that were set for them. Users can change their UVM passphrases by using the Client Utility. For details, see Chapter 7, "Instructions for the client user" on page 29.

Chapter 4. After users have been added to UVM

After users have been added to UVM, additional Client Security functions can be accomplished, such as the following:

- **Setting up UVM protection for the operating system logon.** See "Setting UVM operating-system logon protection" for more information.
- **Archiving user encryption keys.** See "Changing the key archive location" on page 21 for more information.
- **Setting up the Client Security screen saver.** See Chapter 7, "Instructions for the client user" on page 29 for more information.
- **Registering user fingerprints with UVM.** See "Registering user fingerprints with UVM" on page 12 for more information.

  If a UVM-aware fingerprint sensor is installed prior to adding users to UVM, fingerprint registration can be done at that time.

UVM operating-system logon protection

Windows operating systems include applications that provide logon protection. UVM protection is designed to work in parallel with those Windows logon applications. UVM system logon protection enhances the password feature provided with your operating system. For Windows XP Professional, Windows NT, and Windows 2000, the 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.

Setting UVM operating-system logon protection

Read the following information 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" in Chapter 8, "Troubleshooting" on page 37.
- 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 utilizing UVM logon protection.
- In Windows XP Professional, 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. For rules regarding the UVM passphrase, see Appendix B, "Password and passphrase rules" on page 55.

Setting up UVM operating-system logon protection

To set up UVM protection for your operating system, complete the following procedure:

1. Select the **Use UVM Protection for this Workstation instead of using Windows Logon Protection** check box.

   The **UVM Protection for this Workstation instead of using Windows Logon Protection** check box is activated when you supply the Windows logon password for the current user. If this check box is not available, return to the steps for providing the Windows logon password.

2. Click **Yes** or **No** to continue.

3. To activate UVM protection for the system logon, you must restart the computer.

When the computer restarts, you will be prompted to log on to the computer. For more information about UVM protection, see "UVM operating-system logon protection" on page 11.

Registering user fingerprints with UVM

When UVM policy has been edited to include fingerprint authentication, each user must register fingerprints with UVM.

To register user fingerprints with UVM, complete the following Administrator Utility procedure:

1. In the Windows Users Enrolled in UVM area, select a user name from the list.

2. Click **Edit User**.

   The Modify Client Security Key Configuration- Edit UVM User Attributes window is displayed.

3. Select **Register with UVM-aware device** and click **Next**.

   The Modify Client Security Key Configuration- UVM Enabled Devices window is displayed.

4. Click **Register user fingerprints**.

5. In the Select a hand area, click **Left** or **Right**.

6. In the Select a finger area, click to select the finger you will scan for prints, and click **Start registration**.

7. Place your finger on the UVM-aware fingerprint sensor and follow the on-screen instructions.

   You must scan each fingerprint four times. Click **Cancel this finger** to cancel the fingerprint scan. The screen displays the fingerprints that are being stored.

8. Specify another finger to register, or click **Exit** to finish.

Using UVM protection for Lotus Notes

UVM provides enhanced security protection for Lotus Notes users.

Enabling UVM protection for a Lotus Notes User ID

Before you can enable UVM protection for Lotus Notes, Notes must be installed on the IBM client, a Notes User ID and password must be established for the user, and the Notes user must be added to UVM.

To set up UVM protection for Lotus Notes, do the following:

1. Click **Start > Programs > IBM Client Security Software > Lotus Notes Configuration**.

   The Lotus Notes Configuration window opens.

2. Click **Setup**.

   A window opens and displays the current user ID associated with the Lotus Notes session.

3. Click **Store Password**.

   If you have switched User IDs, click **Reset Password** to set up UVM protection for the new User ID.

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

   A windows opens asking you to change the password in Lotus Notes.

5. Click **OK**.

6. Click **Exit** on the Lotus Notes Configuration window; then open Notes and change your User ID password.

   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.

7. 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 5, "Working with UVM policy" on page 15 for more information about editing and saving UVM policy.

Disabling UVM protection for a Lotus Notes User ID

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

1. Click **Start > Programs > IBM Client Security Software > Lotus Notes Configuration**.

   The Lotus Notes Configuration window opens.

2. Click **Disable**.

   When you click **Disable**, a warning message is displayed. The message is a notification that UVM and Notes integration is being disabled.

3. Click **OK**.

   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.

Setting up UVM protection for a switched Lotus Notes User ID

To switch from a User ID that has UVM protection enabled to another User ID, do the following:

1. Exit Lotus Notes.

2. Disable UVM protection for the current User ID. See "Disabling UVM protection for a Lotus Notes User ID" for details.

3. Enter Lotus Notes and switch User IDs. See your Lotus Notes documentation for information on switching User IDs.

4. 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 "Enabling UVM protection for a Lotus Notes User ID" on page 12.

Chapter 5. 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 ″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.

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 "Adding users to UVM" on page 8.

UVM policy is saved in a file named globalpolicy.gvm. To use UVM on remote clients, UVM policy must be saved on one IBM client and then copied to other clients. Using UVM policy on remote clients can save you time setting up UVM policy on other clients.

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. Use the UVM-policy editor to edit and save a local UVM policy. Only a user who has been added to UVM can use the UVM-policy editor.

When you save changes to the UVM policy, a message is displayed 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.

Authentication occurs based on what you select in the policy editor. For example, if you select ″No passphrase required after 1st used this way″ for Lotus Notes Logon, then whenever you logon to Lotus Notes it will ask for UVM authentication. Each time you access Lotus Notes after that, until you reboot or log off, the passphrase is not required.

When 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.

While you are editing UVM policy, you can view the policy summary information by clicking UVM Policy Summary. Also, you can click **Apply** to save your changes. When you click **Apply**, a message is displayed 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.

UVM policy objects

UVM policy objects enable you to establish different security policies for various user actions.

Valid UVM policy objects include the following:

System Logon - Clear Screen Saver
> This object controls authentication requirements necessary to log onto the system or to clear the Client Security screen saver.

Netscape - PKCS#11 Logon
> This object controls authentication requirements necessary when a PKCS#11 C_OpenSession call is received by the PKCS#11 module. Most users should leave this setting on ″No passphrase required after 1st used this way.″

Lotus Notes Logon
> This object controls authentication requirements necessary to log onto Lotus Notes.

Lotus Notes Change Password
> This object controls authentication requirements necessary to use UVM to generate a random Lotus Notes password.

Digital Signature (e-mail)
> This object controls authentication requirements necessary when you click the Sign button in Microsoft Outlook or Outlook Express.

Decryption (e-mail)
> This object controls authentication requirements necessary when you click the Decrypt button in Microsoft Outlook or Outlook Express.

Acquire Digital Certificate
> This object controls authentication requirements necessary to acquire a digital certificate.

File and Folder Protection
> This object controls authentication requirements necessary when right-click encryption and decryption has been selected.

Password Bank
> This object controls authentication requirements necessary when using a password that has been stored along with an application.

Entrust Logon
> This object controls authentication requirements necessary when Entrust issues a PKCS#11 C_OpenSession call to be received by the PKCS#11 module. Most users should leave this setting on ″No passphrase required after 1st used this way.″

Change Entrust Logon Password
> This object controls authentication requirements necessary to change the Entrust logon password. Entrust does this by issuing a PKCS#11

C_OpenSession call to be received by the PKCS#11 module. Most users should leave this setting on "No passphrase required after 1st used this way."

Starting the UVM-policy editor

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

1. Click the **Policy Configuration** button.
2. In the UVM Policy area, select **Local Client**, and then click **Edit UVM Policy**.

   The Global Policy Access Password window opens.
3. Type password and press Enter.

   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 19.
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 example of 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. 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.
7. Click the **Information** tab and type information for the system name, user details, and system and enterprise administrator details.
8. Click the **Policy Selection** tab and click the **UVM Policy** button.

   The **Save** and **Save as** buttons become available.
9. Do one of the following:
   - Click **Save** to save the policy file and follow the instructions on the screen.
   - Click **Save as** to save the file with a new password. See "Changing the password for a UVM-policy file" on page 19 for more information on changing a password.

     When you save your changes, a message is displayed 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.

Editing and using UVM policy for remote clients

To use UVM policy across multiple IBM clients, edit and save UVM policy for a remote client, and then copy the UVM-policy file to other IBM clients. If you install 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 before the \remote subdirectory and its contents are created.

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

When you save changes to the UVM policy, a message is displayed that requests 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.

When you set a UVM policy to require remote clients to provide a fingerprint for an authentication object (such as the operating-system logon), each user must have fingerprints registered to use that object. All remote clients that will use the policy must have UVM-aware fingerprint sensors installed.

While you are editing the UVM-policy file, you can view the policy summary information by clicking **UVM Policy Summary**. Also, you can click **Apply** to save your changes. If you click **Apply**, a message is displayed 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.

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

1. Click the **Policy Configuration** button.
2. In the UVM Policy area, select **Remote Clients**, and click **Edit UVM Policy**.

   The Global Policy Access Password window opens.
3. Type `password` and press Enter.

   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 19.
4. On the Policy Selection page, select the UVM-policy file (globalpolicy.gvm) from the drop-down menu.
5. Click the **Object Selection** tab, 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 example of 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. 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 to the chosen object.
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** buttons become available.
10. Do one of the following:
    - Click **Save** to save the policy file.
    - Click **Save as** to save the file with a new password. See "Changing the password for a UVM-policy file" for information on changing passwords.

    When you save your changes, a message is displayed that asks for the admin private key.
11. Type the admin private key and click **OK** to continue.

    If you provide an incorrect admin private key, your changes will not be saved.
12. Click **OK** to save your changes and exit.
13. 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

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 \IBM\Security\UVM_Policy\ directory path on the remote clients.

Changing the password for a UVM-policy file

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

The following instructions assume that you have accessed the UVM-policy editor and that you are ready to save the UVM-policy file.

To change the password for the UVM-policy file, complete the following procedure:
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. After you save the file, a message is displayed that asks you to verify that you want save the file with a new name.
3. Click **OK**.
4. In the Access Password field, type the current password for the UVM-policy file and click **Change Password**.
5. In the New Password field, type a new password.

   The policy password can be any combination of alphanumeric characters up to 255 characters in length.
6. In the Verify Password field, type the new password again and press Enter.

Chapter 6. Using other features of the Administrator Utility

When you set up Client Security Software on IBM clients, you use the Administrator Utility to enable the IBM embedded Security Chip, set a Security Chip password, generate the hardware keys, and set up the security policy. This section provides instructions for using other Administrator Utility functions.

To open the Administrator Utility, complete the following procedure:

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

   Because access to the Administrator Utility is protected by the Security Chip password, a message is displayed that asks you to type the Security Chip password.

2. Type the Security Chip password and click **OK**.

Changing the key archive location

When the key archive is first created, copies of all encryption keys are created and saved to the location specified at installation.

Note: The client user can also change the key archive location using the Client Utility. For more information, see Chapter 7, "Instructions for the client user" on page 29.

To change the key archive location, complete the following Administrator Utility procedure:

1. Click the **Key Configuration** button.
2. Click the **Change the archive location** radio button.

   The Modify Client Key Configuration- New Key Archive Location screen is displayed.
3. Type the new path, or click **Browse** to select the path.
4. Click **Next**.
5. Click **Finish**.

Changing the archive key pair

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

To change the archive key pair, complete the following Administrator Utility procedure:

1. Click the **Key Configuration** button.

   The Modify Client Security Key Configuration screen is displayed.
2. Click the **Change IBM Security Subsystem Archive keypair** radio button.

   The Modify Client Security Key Configuration - New UVM Administrator Public Key File window opens.
3. In the New ISS Archive Public Key File field, type the file name for the new archive key pair. You can also click **Browse** to search for the file, or click **Create** to generate a new archive key pair.

Notes:

    a. Before performing this task on a ThinkPad computer, you must disable the supervisor password.

    b. Make sure you create the new admin public key in a location other than that which contains the Old ISS Archive Private Key file.

4. In the Old ISS Archive Private Key File field, type the file name for the archive key pair, or click **Browse** to search for the file.

5. In the Archive Directory (Path) field, type the path where the key archive is stored, or click **Browse** to select the path.

6. Click **Next**.

    Note: If the archive key pair was split into multiple files, a message is displayed 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. Click **OK**.

Restoring keys

You might need to restore keys if you have replaced a system board or a failed hard disk drive. 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. 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.

Note: Before performing this task on a ThinkPad computer, you must disable the supervisor password.

Restoring the encryption keys from archive

If you replace the system board in your computer with a system board that contains 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 perform the key restoration after you have enabled the new chip and set a Security Chip password. For details, see "Enabling the IBM embedded Security Chip and setting a Security Chip password" on page 26.

To restore keys after a system board replacement, complete the following Administrator Utility procedure:

1. Click the **Key Configuration** button.

2. Click the **Restore IBM Security Subsystem keys from archive**, and click **Next**.

3. In the Archive Directory (Path) field, type the path and file name of the admin public key, or click **Browse** to search for the file.

4. In the ISS Archive Private Key File field, type the path and file name of the admin private key, or click **Browse** to search for the file.

5. Click **Next**.

    A message is displayed that notifies you that the operation was successful.

Note: If the admin private key was split into multiple files, a message is displayed 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. Click **OK**.
7. Click **Finish**.

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 have been stored.

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

Note: Before performing this task on a ThinkPad computer, you must disable the supervisor password.

To restore user keys from a key archive, complete the following Administrator Utility procedure:

1. Click the **Key Configuration** button.
2. Click the **Restore IBM Security Subsystem keys from archive** radio button.

   The Modify Client Security Key Configuration - Restore All IBM Security Subsystem Keys window opens.
3. In the Archive Directory (Path) field, type the path for the admin public key, or click **Browse** to locate the file.
4. In the ISS Archive Private Key File field, type the path and file name for the admin private key, or click **Browse** to locate the file.
5. Click **Next**.

   A message is displayed that notifies you that the operation was successful.

   Note: If the admin private key was split into multiple files, a message is displayed that asks you to type the location and name of each file. Click **Read Next** after you type each file in the Key File field.
6. Click **OK**.
7. Click **Finish**.

Resetting the authentication fail counter

To reset the authentication fail counter for a user, complete the following Administrator Utility procedure:

1. In the Windows users enrolled in UVM area, select a user.
2. Click **Reset Fail Count**.
3. Type the UVM passphrase for the user selected and click **OK**.

   A message is displayed that notifies you that the operation was successful.
4. Click **OK**.

Changing Policy Director setting information

The following information is intended for security administrators who plan 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 Policy Director setup information on the IBM client, complete the following Administrator Utility procedure:

1. Click the **Policy Configuration** button.
2. Select DCE or LDAP for the server registry that you will use.
3. For each field related to the selected server registry, 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, complete the following Administrator Utility procedure:

1. Click the **Policy Configuration** button.
2. 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 value represent the amount of time between scheduled refreshes.

Recovering 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 can be changed by the client user, the Administrator Utility provides a way to recover the passphrase.

To recover the passphrase, complete the following Administrator Utility procedure:

1. Select a user from the Windows Users Enrolled in UVM field.
2. Click the **Recover Passphrase** button.

   The Recover Passphrase window opens.
3. In the IBM Security Subsystem Key Archive field, type the path and file name for the admin public key, or click **Browse** to locate the file.
4. In the IBM Security Subsystem Archive Private Key file field, type the path and file name for the admin private key.
5. Click **OK**.

   A message is displayed that shows you the UVM passphrase for the user.

If the admin private key was split into multiple files, a message is displayed 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.

Changing the IBM Security Chip password

You must set a Security Chip password to enable the IBM embedded Security Chip. Access to the Administrator Utility is also protected by the Security Chip password. For improved security, change the Security Chip 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 Security Chip password, see Appendix B, "Password and passphrase rules" on page 55.

To change the Security Chip password, complete the following Administrator Utility procedure:

1. Click the **Chip Settings** button.

   The Modify IBM Security Chip Settings screen is displayed.
2. Click **Change chip password**.

   The Change IBM Security Chip password widow opens.
3. In the New password field, type the new password.
4. In the Confirmation field, type the password again.
5. Click **OK**.

   A message is displayed that notifies you that the operation was successful.

   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.
6. Click **OK**.

Viewing 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:

- The encryption status of the embedded Security Chip
- The status of the IBM embedded Security Chip
- The version number of the firmware used with Client Security Software
- The validity of the hardware encryption keys

To view client security information, complete the following Administrator Utility procedure:

1. Click the **Chip Settings** button.

   The Modify IBM Security Chip Settings window opens containing information about the software and IBM Security Chip status.
2. Click **Refresh** to verify the status.
3. Click **Close** to exit.

Disabling the IBM embedded Security Chip

The Administrator Utility provides a way to disable the IBM embedded Security Chip. Because the Security Chip password is required to start the Administrator Utility and disable the chip, protect the Security Chip password to prohibit unauthorized users from disabling the chip.

Important: 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 and click the **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** check box. You must restart the computer before UVM protection for the system logon is disabled.

Note: Before performing this task on a ThinkPad computer, you must disable the supervisor password.

To disable the embedded Security Chip, complete the following Administrator Utility procedure:

1. Click the **Chip Settings** button.
2. Click the **Disable Chip** button and follow the on-screen instructions.
3. 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.

Enabling the IBM embedded Security Chip and setting a Security Chip 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 Security Chip password and to set up new encryption keys.

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

Note: Before performing this task on a ThinkPad computer, you must disable the supervisor password.

To enable the chip and set a Security Chip password, complete the following procedure:

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

   A message is displayed that asks you to enable the IBM embedded Security Chip for the IBM client.

2. Click **Yes**.

   A message is displayed that asks you to restart the computer. You must restart the computer before the IBM embedded Security Chip will be enabled. If your computer has Enhanced Security enabled, you might need to type the administrator password that was set in the Configuration/Setup Utility to enable the chip.

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

4. From the Windows desktop, click **Start > Programs > IBM Client Security Software > Administrator Utility**.

   Because access to the Administrator Utility is protected by the Security Chip password, a message is displayed that asks you to type the Security Chip password.

5. Type a new Security Chip password in the New password field, and then type it again in the Confirmation field.

6. Click **OK**.

Enabling Entrust support

The IBM Embedded Security Chip works with Client Security Software to enhance Entrust security features. Enabling Entrust support on a computer with Client Security Software transfers Entrust software security functions to the IBM Security Chip.

Client Security Software will automatically enable Entrust support; however, if the entrust.ini file is not in the usual path, a dialog opens for the user to browse for the entrust.ini file. After the user locates and selects the file, Client Security can enable Entrust support. After clicking the Enable Entrust Support button, reboot is necessary before Entrust will make use of the IBM Embedded Security Chip.

To enable Entrust support, complete the following procedure:

1. Click **Start > Programs > IBM Client Security Software > Enable Entrust Support**.

   The IBM Client Security Entrust Support screen is displayed with a message indicating Entrust support is disabled.

2. Click **Enable Entrust Support**.

   The IBM Client Security Entrust Support screen is displayed. The message on the screen is changed to reflect that Entrust support is enabled.

   Note: You must restart the computer for the changes to take effect.

   If the entrust.ini file is not in the usual path, the Entrust INI File Path window opens.

3. Click **Browse** to search for the entrust.ini file.

   The Open window is displayed.

4. Select the file and click **Open**.

   The Entrust INI File Path window opens with the file path displayed in the field.

5. Click **OK**.

   The IBM Client Security Entrust Support screen is displayed with a message indicating that Entrust support is enabled.

Chapter 7. Instructions for the client user

This section 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 logon protection for Windows XP, Windows NT, and Windows 2000 Professional systems. Before you can use UVM protection, it must be enabled for the computer.

UVM protection enables you to control access to the operating system through a logon interface. UVM logon protection replaces the Windows logon application, so that, when a user unlocks the computer, the UVM logon window opens instead of the Windows logon window. After UVM protection is enabled for the computer, the UVM logon interface will open each time you start the computer.

When the computer is running, you can access the UVM logon interface by pressing **Ctrl + Alt + Delete** to shut down or lock the computer, or to open the Task Manager or log off the current user.

To unlock a Windows XP, Windows NT, or Windows 2000 Professional client that uses UVM protection, do the following:

1. Press **Ctrl + Alt + Delete** to access the UVM logon interface.
2. Type your user name and the domain you are logged onto, 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 click **OK** to access the operating system. If fingerprint authentication is required by the UVM policy, a message is displayed that prompts you for a fingerprint scan.

   Note: Depending on the UVM policy authentication requirements for the client, further authentication processes might also be required.

The Client Security screen saver

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.

Setting up the Client Security screen saver

This section contains information about setting up the Client Security screen saver. Before you can use the Client Security screen saver, at least one user must be registered on the security policy of your computer.

To set up the Client Security screen saver, do the following:

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**.

Client Security screen saver behavior

The behavior of the Client Security screen saver differs depending on UVM Administrator Utility and Windows screen saver settings. In Windows XP, Windows NT, and Windows 2000, the system checks Windows settings first, and then the UVM Administrator Utility settings. Consequently, the screen saver only locks if the **Password protected** checkbooks has been selected on the Windows screen saver settings tab.

If this box has been selected, the system requires either the Windows password or the UVM passphrase, depending upon whether the **Use UVM Logon Protection** checkbox has been selected in the Administrator Utility. If it has been selected, the system requires the UVM passphrase. If it has not been selected, the system requires the Windows password.

Also, other authentication requirements might have been set in the security policy for the computer; therefore, further authentication might still be required. For example, you might have to scan your fingerprints to unlock the computer.

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

The Client Utility

The Client Utility enables the client user to perform various security maintenance tasks that do not require administrator access.

Client Utility features

The Client Utility enables the client user to do the following:

- **Change the UVM passphrase.** To improve security, you can periodically change the UVM passphrase.
- **Update Windows logon settings.** When you change the Windows XP or Windows NT password for a client user with the User Manager program, you must also change the password by using the Client Utility. If an administrator uses 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.

  Note: Changing the Windows logon password is applicable for users of Windows XP, Windows NT, and Windows 2000 only.

- **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.

- **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.

Client Utility Windows XP 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

Using the Client Utility

To use the Client Utility, do the following:

1. Click **Start > Programs > IBM Client Security Software > 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.
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**.
   - To change the Windows XP or Windows NT logon password, in the **Windows password** field, type a new Windows NT password. Next, type the new password again in the **Confirm Windows password** field, and then click **Update**. For rules on the Windows NT logon password, see the operating system documentation.

     > **Note:** Only change Windows logon information in User Manager for the user currently logged on.
   - To update the key archive, click **Update archive**; then click **OK** on the window that notifies you that the operation was successful.
   - To register user fingerprints, click the **Fingerprint Registration** tab; then click the **Click to launch fingerprint registration** button. In the radio boxes, select the hand and finger you will scan for prints, and click **Start registration**. Then, place the selected finger on the fingerprint reader and follow the on-screen instructions to scan four copies of your fingerprint. When you have finished scanning your fingerprints, click **Exit**.

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 (also called a 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.

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.

Note: To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256-bit encryption. The encryption strength provided by Client Security Software is found in the Administrator Utility.

Obtaining a digital certificate for Microsoft applications

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 Subsystem CSP** as your cryptographic service provider when you obtain your digital certificate. This ensures that the private key of the digital certificate is stored on the IBM 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.

After you select **IBM embedded Security Subsystem 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.

Updating the key archive for Microsoft applications

After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive using the Administrator Utility.

Using the digital certificate for Microsoft applications

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.

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.

Note: To use 128-bit browsers with Client Security Software, the IBM embedded
Security Chip must support 256-bit encryption. The encryption strength
provided by Client Security Software is found in the Administrator Utility.

Installing the IBM embedded Security Chip PKCS#11 module for Netscape applications

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.

To install the IBM embedded Security Chip PKCS#11 module, complete the
following steps:

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 >
     IBM Client Security Software > Add IBM Embedded Security Subsystem
     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.

   The UVM passphrase window opens.
2. Type the UVM passphrase and click **OK**.

   A message is displayed asking if you are sure you want to install this security
   module.
3. Click **OK**.

   A message is displayed that notifies you that the module was installed.
4. Click **OK**.

Using the PKCS#11 logon protection for Netscape applications

When PKCS#11 logon protection is set up 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.

Selecting the IBM embedded Security Chip to generate a digital certificate for Netscape applications

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 be asked to select the card or database
you wish to generate your key in, select **IBM embedded Security Subsystem**.

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

Updating the key archive for Netscape applications

After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive using the Administrator Utility.

Using the digital certificate for Netscape applications

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.

If you do not meet the authentication requirements set by the UVM policy, an error message is displayed. When you click **OK** on this message, Netscape will open, but you will not be able to use the digital certificate generated by the IBM embedded Security Chip until you restart Netscape and provide the correct UVM passphrase, fingerprints, or both.

Chapter 8. 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 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 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 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 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 without moving a jumper on the system board. 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 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 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 **Use UVM Logon Protection for this Workstation instead of using Windows Logon Protection** 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 F1. The main menu of the IBM BIOS Setup Utility opens.
3. Select **Config**.
4. Select **IBM Security Chip**.
5. Select **Clear IBM Security Chip**.
6. Select **Yes**.
7. Press Enter to continue.
8. Press F10 to save and exit.

The Administrator Utility

The following section contains general information to keep in mind when using the Administrator Utility, as well as troubleshooting information that might be helpful if you experience problems using the Administrator Utility.

Administrator Utility information

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.

When you delete a user from Windows 98, the user name is **not** 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.

Windows 98 and Windows Millennium operating systems have known security limitations: Operating systems derived for the Windows NT kernel adhere to more stringent security standards than operating systems derived from the Windows 9X kernel. Consequently, operating systems derived from the 9X kernel are not as secure, and some Client Security Software features might behave differently. For example, Windows 9X-based operating systems do not report suspend or resume events to the screen saver. Therefore, the Client Security screen saver might not provide the same level of security as it does under NT-based operating systems.

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 csec21.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 csec21.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
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**
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 on Client Security reboot	**Action**
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.

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
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.

Problem Symptom	Possible Solution
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**
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 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.
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**

Problem Symptom	Possible Solution
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 certificates.	Go to the Administrator Utility or Client Utility to update the key archive. When you update the key archive, copies of all the certificates associated with the IBM embedded Security Chip are created.
Error message when trying to use a restored certificate after a hard disk drive failure	**Action**
Certificates can be restored by using the key restoration feature in the Administrator Utility. Some certificates, such as the free certificates provided by VeriSign, might not be restored after a key restoration.	After restoring the keys, obtain a new certificate.
Netscape agent opens and causes Netscape to fail	**Action**
Netscape agent opens and closes Netscape.	Turn off the Netscape agent.
Netscape delays if you try to open it	**Action**
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 is for informational purposes only.

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.

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
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.

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. For more information, see ″Administrator tips,″ on page 60.
- 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. For rules on the UVM passphrase, see ″Appendix B - Rules for the Security Chip password and the UVM passphrase,″ on page 75.

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.

IBM ®