IBM Client Security Solutions

Client Security User's Guide

December 1999

Before using this information and the product it supports, be sure to read "Appendix B - Notices and Trademarks," on page 22.

First Edition (December 1999)

The following paragraph does not apply to the United Kingdom or any 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 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 publication 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.

This publication was developed for products and services offered in the United States of America. IBM may not offer the products, services, or features discussed in this document in other countries, and the information is subject to change without notice. Consult your local IBM representative for information on the products, services, and features available in your area.

Requests for technical information about IBM products should be made to your IBM reseller or IBM marketing representative.

Table of Contents

About this Guide

The guide contains information to help you use Client Security Software on IBM networked computers that have the IBM embedded Security Chip. Throughout this document, these computers are referred to as *IBM clients*.

The guide is organized as follows:

"Chapter 1 - Overview of IBM Client Security Software,"contains an overview of the components provided by Client Security Software.

"Chapter 2 - Using UVM logon protection," contains instructions for using UVM logon protection provided by Client Security Software. Instructions for users of Windows NT Workstation 4.0, Windows 98 and Windows 95 are provided.

"Chapter 3 - Setting up the Client Security screen saver," contains instructions on how to set up the Client Security screen saver.

"Chapter 4 - Using the Client Utility," contains information and instructions on how to change your UVM passphrase. Also, for Windows NT users, instructions for changing the Windows NT password is provided.

"Chapter 5 - Using secure e-mail and Web browsing," contains information about using Microsoft and Netscape applications with the cryptographic capabilities provided by Client Security Software.

"Chapter 6 - Troubleshooting," contains troubleshooting information associated with Client Security Software.

"Appendix A - Rules for the UVM passphrase," contains a description of the rules for the UVM passphrase.

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

How to use this guide

This guide is intended for Client Security end users (or client users). Client Security must be installed and set up on your computer before you can use the information in this guide.

Knowledge of using digital certificates and using logon and screen saver programs is required.

The information provided in this guide is also provided in the *Client Security Software Administrator's Guide*. The *Client Security Software Administrator's Guide* is intended for a security administrator who installs and sets up Client Security Software on IBM clients. For information about installing and setting up Client Security Software, contact your administrator.

Conventions used in this guide

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

- **Bold -** Commands, keywords, file names, authorization roles, and other information that you must use literally appear in **bold**.

- *Italics* - Variables and values that you must provide appear in *italic*s. Words and phrases that are emphasized also appear in *italic*s.
- `Monospace` **-** Code examples, output, and system messages appear in `monospace`.

Chapter 1 - Overview of IBM Client Security Software

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

- **User encryption key management with the IBM embedded Security Chip**. Encrypting and storing your user keys on the IBM embedded Security Chip adds an extra layer of client security, because the keys are securely bound to the computer hardware. A security administrator generates the hardware and user encryption keys for you.
- **Digital certificate creation and storage that is protected by the IBM hardware**. When you apply for a digital certificate that can be used for an e-mail application or a Web browser, Client Security Software enables you to choose the IBM embedded Security Chip as the cryptographic service provider associated with the certificate.
- **Access to the security policy of your computer:** A security administrator sets up the security policy for your computer and provides you with your User Verification Manager (UVM) passphrase. You use the UVM passphrase to authenticate yourself as a trusted user of the security policy for the computer.
- **A key archive and recovery solution**. Two important functions in a PKI are creating a key archive and then restoring keys from that archive when necessary. If the encryption keys for your computer are lost, the security administrator can restore them from a key archive.

What software is installed?

When Client Security Software is installed and set up on your computer, the following software components are installed:

- **Client Utility:** The Client Utility enables you to change your UVM passphrase and, for Windows NT users, your Windows NT logon password.
- **User Verification Manager (UVM):** UVM is software that enables an administrator to set the security policy for the computer. As a client user of that security policy, you can use your UVM passphrase for authentication when you use UVM logon protection, the Client Security screen saver, and when you create digital certificates with the IBM embedded Security Chip as the cryptographic service provider.
- **UVM logon protection:** The security administrator sets up UVM logon protection for the computer. UVM logon protection ensures that only those users who are recognized by the security policy of the computer are able to access the operating system. You use your UVM passphrase when you attempt to log on to the computer.
- **Client Security screen saver:** The Client Security screen saver enables you to control access to the computer through a screen saver interface. You use your UVM passphrase to bypass the screen saver and gain access to the computer.

- **Support for the Microsoft CryptoAPI:** Support for Microsoft CryptoAPI is built into Client Security Software. Defined by Microsoft, CryptoAPI is used as the default cryptographic service for Microsoft operating systems and applications. With built-in CryptoAPI support, Client Security Software enables you to use the cryptographic operations of the IBM embedded Security Chip when you create digital certificates for Microsoft applications.
- **Support for PKCS#11:** Defined by RSA Data Security Inc., PKCS#11 is used as the cryptographic standard for Netscape and other products. After you install the IBM embedded Security Chip PKCS#11 module, you can use the IBM embedded Security Chip when you generate a digital certificate for Netscape applications and other applications that use PKCS#11.
- **Administrator Utility:** The Administrator Utility is the administrator interface to the client security features. Access to the Administrator Utility is protected by a password that the administrator creates.

Additional information

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

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

http://www.pc.ibm.com/ww/intellistation/security/index.html

Chapter 2 - Using UVM logon protection

This chapter contains information about using UVM logon protection. Before you can use UVM logon protection, it must be enabled for the computer. For information on enabling UVM logon protection, contact your security administrator.

UVM logon protection enables you to control access to the operating system through a logon interface. The logon procedure can differ depending on which operating system is used, Windows NT Workstation 4.0 or Windows 98 and Windows 95.

Windows NT Users

For Windows NT, UVM logon protection replaces the Windows NT logon application, so that, if you try to unlock the computer, the UVM logon window opens instead of the Windows NT logon window.

Note: You can use also the UVM logon window to perform a Windows shut down of the computer. To shut down the computer, click **Shut Down** on the UVM logon window.

To unlock a computer that uses Windows NT and UVM logon protection:

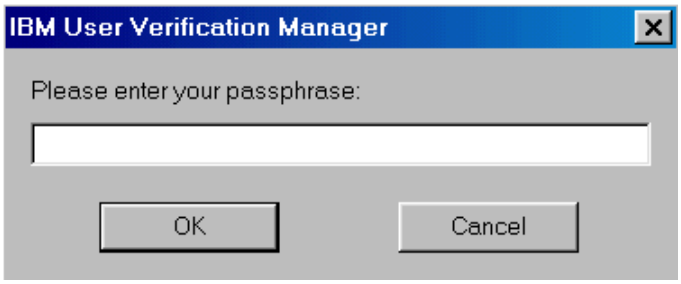
1. Press **Ctrl + Alt + Delete** to unlock the computer.

   The following UVM logon window opens.

2. Type your user name and the domain where you are logged on, and then click **Logon**.

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

The UVM passphrase window opens.



3. Type your UVM passphrase, and then click **OK** to access the operating system.

   If the UVM passphrase does not match the user name and domain entered, the UVM logon window opens again.

   If you type the correct UVM passphrase for the user name and domain entered, the logon is successful.

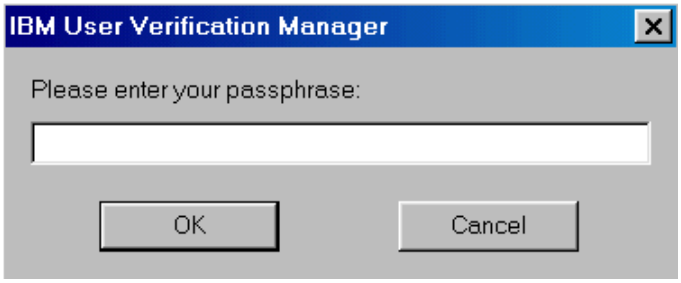
Windows 98 and Windows 95 Users

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

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

1. When the operating system logon window opens, type your user name and password information, and click **OK**.

   The UVM passphrase window opens.



2. Type your UVM passphrase (associated with the user name typed in the operating system logon), and then click **OK** to access the operating system.

   If you type the correct UVM passphrase, the computer unlocks.

If you type an incorrect UVM passphrase, the Client Security screen saver displays.[1]

[1] The Client Security screen saver may or may not be the selected screen saver for your computer. For Windows 98 and Windows 95, UVM logon protection uses the Client Security screen saver to secure the logon.

Chapter 3 - Setting up the Client Security screen saver

This section contains information about setting up the Client Security screen saver. The Client Security screen saver is one of the software components that is automatically installed by Client Security Software. Before you can use the Client Security screen saver, at least one user must exist on the security policy of your computer. Contact your security administrator for information about adding new users to the security policy for your computer.

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.

To set up the Client Security screen saver:

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

If the Client Security is activated, press any key or move the mouse to access the UVM passphrase window. Type your UVM passphrase and click **OK** to access the desktop.

Note: If the IBM embedded Security Chip is disabled or all users are removed from the security policy for your computer, the Client Security screen saver is unavailable for use. See the security administrator for more information.

Chapter 4 - Using the Client Utility

The Client Utility enables you to change the following:

- **UVM passphrase**. Your UVM passphrase authenticates you as a trusted user to the security policy of the computer. To improve security, you can periodically change your UVM passphrase. Also, the UVM can be longer and more unique than traditional passwords.
- **Windows NT logon settings**.[2] If you change your Windows NT password with the User Manager program, you must also change the password by using the Client Utility.

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

To change the UVM passphrase or Windows NT password for the user currently logged on to the system:

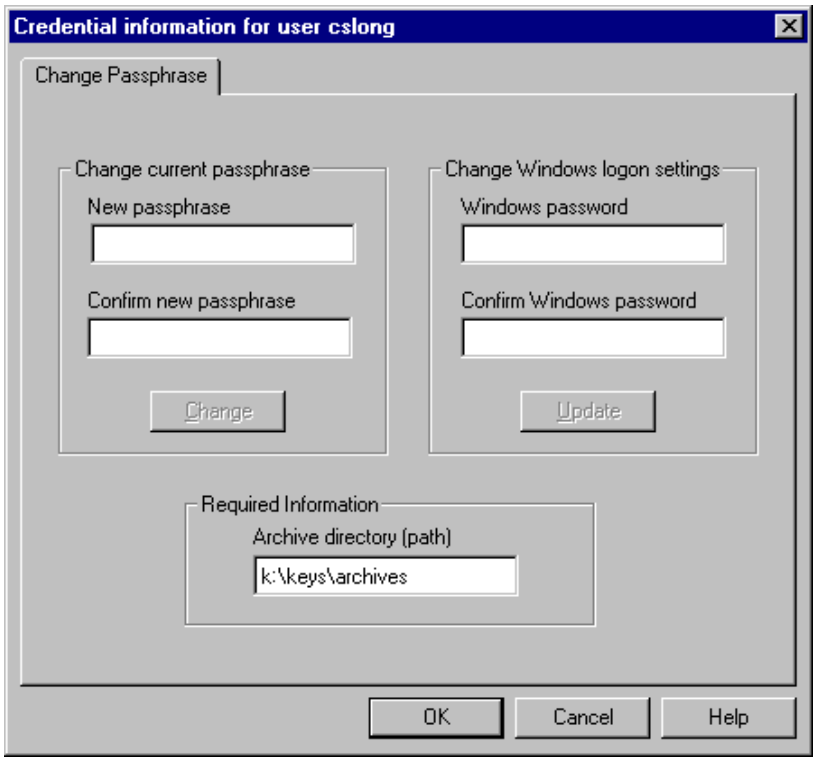
1. Click **Start → Programs → Client Security Software Utilities→ Client Utility**.

   The following 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.

[2] Changing the Windows logon password is applicable for users of Windows NT only.



3. In the **Required information** area, type the path to the key archive that was set up for you. Contact your security administrator for the location of the key archive.
4. Do one of the following:
   - To change the UVM passphrase, in the **Change current passphrase** area, type a new passphrase in the **New passphrase** field. Next, type the passphrase again in the **Confirm new passphrase** field, and then click **Change**. For information on the rules for the UVM passphrase, see "Appendix A - Rules for the UVM passphrase," on page 21.
   - To change the Windows NT logon password, in the **Windows password** field, type a new Windows NT password. Next, type the new password again in the **Confirm Windows password** field, and then click **Update**. For rules on the Windows NT logon password, see the operating system documentation.
5. Click **OK** to exit.

Chapter 5 - Using secure e-mail and Web browsing

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

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

Tips for using Client Security Software with Microsoft applications

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

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

Notes:

- Client Security Software Version 1.0 supports the use of the 40-bit version of Internet Explorer. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256 bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see your security administrator.
- For information about known limitations when using Client Security Software with Microsoft applications and troubleshooting information, see “Known limitations,” on page 19 and “Troubleshooting charts,” on 19.

Obtain a digital certificate

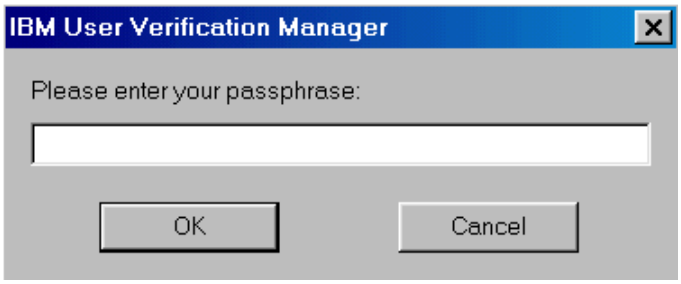
When you use a certificate authority to create a digital certificate to be used with Microsoft applications, you will be prompted to choose a cryptographic service provider (CSP) for the certificate.

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

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

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

After you select **IBM embedded Security Chip CSP** as the CSP, the UVM component in Client Security Software prompts you for the UVM passphrase. The following window opens, and you must type the UVM passphrase and click **OK** before you can continue.



Update the key archive

After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive by using the Administrator Utility. For details, see your security administrator.

Use the digital certificate

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

In Microsoft e-mail applications, after you create the digital certificate and use it to sign an e-mail message, the UVM passphrase window opens the first time you digitally sign an e-mail message. You must type the UVM passphrase and click **OK** before you can continue.

Tips for using Client Security Software with Netscape applications

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

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

Notes:

- Client Security Software Version 1.0 supports the use of the 40-bit version of Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256 bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see your security administrator.

- For information about known limitations when using Client Security Software with Netscape applications and troubleshooting information, see "Known limitations," on page 19 and "Troubleshooting charts," on 19.

Install the IBM embedded Security Chip PKCS#11 module

Before you can use a digital certificate, you must install the IBM embedded Security Chip PKCS#11 module onto the computer. Because the installation of the IBM embedded Security Chip PKCS#11 module requires a UVM passphrase, you must add at least one user to the security policy for the computer. You add a user by using the Administrator Utility. For details, see your security administrator.

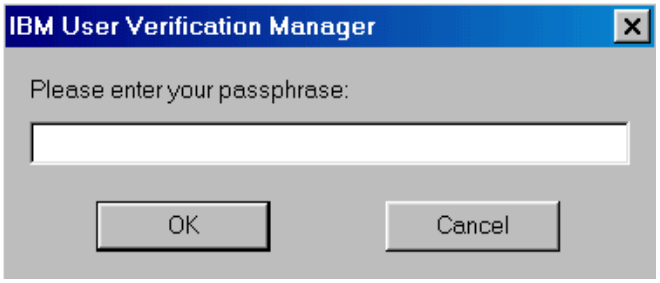
To install the IBM embedded Security Chip PKCS#11 module, do one of the following:

- If Netscape was installed on the computer before Client Security Software was installed, you can use the Windows Start menu to add the IBM embedded Security Chip module.
- If Netscape was installed on the computer after Client Security Software was installed, you must locate the install file in the C:\Program Files\IBM\Security directory and install it from there.

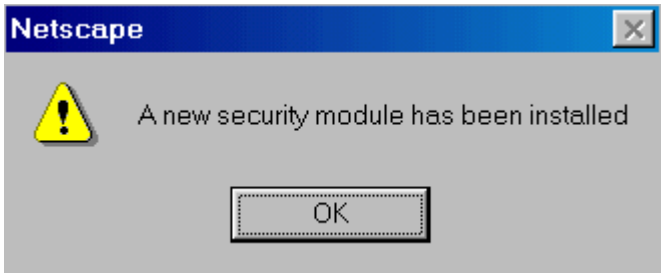
To install the module from the Windows Start menu:

1. Click **Start → Programs → Client Security Software Utilities→ Add IBM Embedded Security Chip Module**. The following window opens.

2. Click **OK**. The UVM passphrase window opens.



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



4. Click **OK**.

To install module from the C:\Program Files\IBM\Security directory:

1. In Netscape, click File → Open page.
2. Type C:\Program Files\IBM\Security\pkcs11.html

Select IBM embedded Security Chip when generating a digital certificate

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

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

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

Update the key archive

After you create a digital certificate, back up the certificate by updating the key archive. You can update the key archive by using the Administrator Utility. For details, see your security administrator.

Use the digital certificate

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

After you have installed the IBM embedded Security Chip PKCS#11 module, the UVM passphrase window opens each time you run Netscape. This is the only time the UVM passphrase window opens when you are using Netscape for sending and receiving secure e-mail or Web browsing. If the UVM passphrase window opens, you must type the UVM passphrase and click **OK** before you can continue.

Chapter 6 - Troubleshooting

This chapter provides known limitations and troubleshooting information that is helpful for identifying or solving problems.

Known limitations

This section provides information about known limitations of Client Security Software.

Netscape

All algorithms that supported by the IBM embedded Security Chip PKCS#11 module are not checked when the module is viewed. The following algorithms are supported by the IBM embedded Security Chip PKCS#11 module, but are not identified as being supported:

- SHA-1
- MD5

Troubleshooting charts

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

Encrypted e-mail

Problems reading encrypted e-mail using Outlook Express or Netscape	Action
Encrypted e-mail cannot be decrypted because of the differences in encryption strengths of the Web browsers used by the sender and recipient.	Verify the following: 1. The encryption strength for the Web browser the sender uses is compatible with the encryption strength of the Web browser 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. **Note:** Client Security Software Version 1.0 supports the use of 40-bit Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256 bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see your security administrator.

Microsoft

Outlook Express encrypts email messages with the 3DES encryption algorithm only	Action
When Outlook Express is used with the 128-bit version of Internet Explorer 4.0 or 5.0, e-mail messages can only be encrypted with 3DES. All other encryption algorithms are not supported.	Verify that you are using the 128-bit version of Internet Explorer 4.0 or 5.0. If you are using one of these browsers and you want to use an encryption algorithm other than 3DES, you must use the 40-bit version of Internet Explorer. **Note:** Client Security Software Version 1.0 supports the use of 40-bit Web browsers. To use 128-bit browsers with Client Security Software, the IBM embedded Security Chip must support 256 bit encryption. You can find out the encryption strength provided by Client Security Software in the Administrator Utility. For details, see your security administrator.

Netscape

Digital certificates with a signed e-mail from the same sender are not replaced within Netscape	Action
When a digitally signed e-mail is received more than once by the same sender, the first digital certificate associated with the e-mail is not overwritten within Netscape.	Delete the first e-mail; then re-open the second e-mail.

Appendix A - Rules for the UVM passphrase

This appendix contains the rules for the UVM passphrase. To improve security, the UVM passphrase is longer and can be more unique than a traditional password.

The following table describes the rules for the UVM passphrase.

Length	The passphrase can be up to 256 characters long.
Characters	The passphrase can contain any combination of characters that the keyboard produces, including spaces and nonalphanumeric characters.
Properties	The UVM passphrase is different from a password that you might use to log on to an operating system. The user passphrase can be used in conjunction with other authenticating devices, such as a fingerprint reader or a smart card.
Incorrect attempts	If you incorrectly type the UVM passphrase multiple times during a session, the computer will not lock up.

Appendix B - Notices and Trademarks

This appendix gives legal notice of IBM product availability, patents, and patents pending, as well as trademark information.

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available to all countries in which IBM operates. Any reverence 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. Subject to IBM's valid intellectual property and other legally protectable rights, any functionally equivalent and verification of operation in conjunction with other products, except those expressly designated by IBM, are the responsibility of the user.

IBM may have patents or pending patent applications covering subject matter 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
N. Castle Drive
Armonk, NY 10504-1785
U.S.A.

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.

Trademarks

IBM is a trademark of IBM Corporation in the U.S., other countries, or both.

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

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