IBM® Client Security Solutions

Using Client Security with Policy Director

Client Security Software Version 2.0

July 2001

Before using this information and the product it supports, be sure to read "Appendix A - Notices and Trademarks," on page 19.

First Edition (July 2001)

Table of Contents

About this guide

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

This guide is organized as follows:

"Chapter 1 - Introducing IBM Client Security Software," contains an overview of the components that are included in Client Security Software.

"Chapter 2 – Policy Director Overview," contains a brief overview of Policy Director.

"Chapter 3 - Installing the Client Security component on the Policy Director server," contains the prerequisites and instructions for installing Client Security support on your Policy Director server.

"Chapter 4 - Configuring IBM clients," contains prerequisite information and instructions for configuring IBM clients to use the authentication services provided by Policy Director.

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

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

Who should read this guide

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

Administrators must be knowledgeable of the following concepts and procedures:

- Installation and management of the IBM Distributed Computing Environment (DCE) and the SecureWay Directory lightweight directory access protocol (LDAP)
- Installation and setup procedures for Policy Director and NetSEAT
- Management of the Policy Director object space

How to use this guide

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

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

References to the *Client Security Software Installation Guide*

References to the *Client Security Software Installation Guide* are provided in this document. After you have set up and configured the Policy Director server and installed the NetSEAT client, use the instructions in the *Client Security Software Installation Guide* to install Client Security Software on IBM clients. See "Chapter 4 - Configuring IBM clients," on page 12 for more information.

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

References to the *Client Security Software Administrator's Guide* are provided in this document. The *Client Security Software Administrator's Guide* contains information on how to set up user authentication and the UVM policy for the IBM client. After you have installed Client Security Software, use the *Client Security Software Administrator's Guide* to set up user authentication and the security policy. See "Chapter 4 - Configuring IBM clients," on page 12 for more information.

Additional information

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

Chapter 1 - Introducing IBM Client Security Software

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

Client Security Software applications and components

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

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

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

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

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

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

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

? **Right Click Encryption:** Right Click Encryption enables a client user to encrypt his files simply by clicking the right mouse button.

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**[1]. Administrators create encryption keys for the computer hardware and the client users with Client Security Software. When encryption keys are created, they are bound to the IBM embedded Security Chip through a key hierarchy, where a base level hardware key is used to encrypt the keys above it, including the user keys that are associated with each client user. Encrypting and storing keys on the IBM embedded Security Chip adds an essential extra layer of client security, because the keys are securely bound to the computer hardware.

? **Digital certificate creation and storage that is protected by the IBM embedded Security Chip**. When you apply for a digital certificate that can be used for digitally signing or encrypting an e-mail message, Client Security Software enables you to choose the IBM embedded Security Chip as the cryptographic service provider for applications that use the Microsoft? CryptoAPI. These applications include Internet Explorer and Microsoft Outlook Express. This ensures that the private key of the digital certificate is stored on the IBM embedded Security Chip. Also, Netscape users can choose IBM embedded Security Chips as the private key generators for digital certificates used for security. Applications that use the Public-Key Cryptography Standard (PKCS) #11, such as Netscape Messenger, can take advantage of the protection provided by the IBM embedded Security Chip.

? **A key archive and recovery solution**. An important PKI function is creating a key archive from which keys can be restored if the original keys are lost or damaged. Client Security Software provides an interface that enables you to establish an archive for keys and digital certificates created with the IBM embedded Security Chip and to restore these keys and certificates if necessary.

[1] Public key cryptography uses encryption keys that are issued in pairs. One is the public key; the other is the private key. Both keys are required to encrypt and decrypt information and are also used to identify and authenticate client users.

Chapter 2 – Policy Director Overview

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

This chapter discusses components of Policy Director that interact with the Client Security Software.

Policy Director concepts

Policy Director enables enterprise administrators to control the authentication elements that are used by IBM clients.

Management Console, access control lists, and objects

The Management Console, a component of Policy Director, provides the central interface that you use to add or delete users or groups and apply *access control lists (ACLs)* to objects that are provided by Client Security Software. Objects that are provided by Client Security Software include digital certificate access or acquisition, system logon, clearing the screen saver, and decryption of encrypted e-mail. The Management Console enables you to select which authentication elements will be used as permissions for those objects. The Management Console Object Space management task panel attaches or removes ACLs to and from objects.

NetSEAT client

NetSEAT client is a network-support module that works as a secure proxy for client applications by enabling end-to-end encryption of all client-server communications. To use Client Security Software with Policy Director, you must have NetSEAT client installed on the IBM client. Policy Director and IBM clients use the NetSEAT component to manage security policy.

Interaction with Client Security

Before you can use Client Security with Policy Director, you must install the Client Security component for Policy Director that is accessed from the http://www.pc.ibm.com/ww/security/secdownload.html Web site. After you install the component, IBM Client Security Solutions is displayed as a user-defined object in the object name space of the Management Console.

IBM Client Security Solutions is considered to be a system resource by Policy Director, because it is protected by ACLs that are attached to the object representations of IBM Client Security Solutions.

Chapter 3 - Installing the Client Security component on the Policy Director server

This chapter contains prerequisite information and instructions for installing the Client Security component on a Policy Director server.

The following features are added when the Client Security component is installed:

- The Client Security permission is added to the Management Console.
- IBM Client Security Solutions is added to the Object Space tree.

After the Client Security component is installed, you can add IBM client users to Policy Director.

Prerequisites

Before you install the Client Security component, make sure that the following components are installed:

- Policy Director server version 3.0.1.87 or later
- IBM Distributed Computing Environment (DCE) server
- IBM SecureWay Directory lightweight directory access protocol (LDAP) server (optional)
- Policy Director Base (IVBase)
- Management server (IVMgr)
- Authorization server (IVAcld)
- NetSEAT client
- Management Console

For detailed information about installing and using Policy Director, see the documentation that is provided on the http://www.pc.ibm.com/ww/security/securitychip.html Web site.

Downloading and installing the Client Security component

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

1. Download PDServer.exe from the http://www.pc.ibm.com/ww/security/secdownload.html Web site.

   Click the link for downloading Client Security Software, and then complete the registration form and questionnaire. PDServer.exe is available from the same IBM Web page that contains the Client Security Software code.

2. Run PDServer.exe to extract the following files:

   - **setupPD.bat** ? This is the batch file that you will run on the server. This file is required for the installation.

- ✍ **Security.txt** ? This is the map file that contains text that will be added to the object space tree. Do not edit this file. This file is required for the installation.
- ✍ **ivmgrd.conf.example** ? This file contains example text. Use this file as a reference for editing the ivmgrd.conf file on the server.

3. Log in to NetSEAT client.
4. In the Policy Director installation directory, edit the ivmgrd.conf file to define the Client Security object space with the Security.txt map file, and save the file. The following example, from ivmgrd.conf.example, shows the line that you must add to your ivmgrd.conf file.

   Note: The default path to the ivmgrd.conf file is \program files\ibm\policy director\ivmgrd\lib\ivmgrd.conf.

```
  .
  .
  .
#
# Application object spaces
#
# This section defines the third party application object spaces.
# Each entry has the following format:
#
#  <object-space-root> = <map-file>
#
# Some examples:
#  /Application Objects/MyApp = /usr/local/myapp/objectspace.conf
#  /Demo App = /opt/intraverse/lib/filemap.txt
#
[object-spaces]

/IBM Client Security Solutions = c:\mapfiles\Security.txt
  .
  .
  .
```

5. Copy the Security.txt file to the directory that is defined in the ivmgrd.conf file.
6. Run the setupPD.bat file on the Policy Director server with the `add` parameter. For example:

   ```
   d:\temp\setupPD.bat add
   ```

   Note: If you run the setupPD.bat file, all ACLs for Client Security will be cleared. For example, if you reinstall the Client Security component for Policy Director by running setupPD.bat, any ACLs that were set will be cleared.
7. Stop and restart all Policy Director services.
8. In Policy Director, create users (UVM user names) that will use the Client Security object space.

   Important: You must register UVM user names in Policy Director before configuring IBM clients.
9. Run DCE Director on the Policy Director server, and register the DCE login name. Next, add the DCE login name to the remote_acl_users group.

10. Go to "Chapter 4 - Configuring IBM clients," on page 12 for instructions on enabling Policy Director to administer the authentication requirements for IBM clients.

Chapter 4 - Configuring IBM clients

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

Prerequisites

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

1. Microsoft® Windows NT® Workstation 4.0. You can use Policy Director to control the authentication requirements only for IBM clients running Windows NT Workstation 4.0.
2. NetSEAT client. Although NetSEAT client can be installed on clients running Windows 98®, Client Security can be used only with IBM clients running Windows NT.
3. LDAP client (optional). Install LDAP client only if Policy Director is used with an LDAP server. Also, authorization server (IVAcld) must be installed on the client to support a Policy Director server LDAP registry.
4. Client Security Software version 1.2 or later. Install the software, and enable the IBM embedded Security Chip. Use the Administrator Utility to set up user authentication and edit the UVM security policy. For comprehensive instructions on installing and using Client Security Software, see the *Client Security Software Installation Guide* and the *Client Security Software Administrator's Guide*.

Configuring the Policy Director setup information

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

- Distributed Computing Environment (DCE) host name
- Lightweight Directory Access Protocol (LDAP) host name
- LDAP port
- LDAP root distinguished name (DN)
- LDAP DN password
- LDAP Secure Sockets Layer (SSL) key file
- LDAP SSL key file DN
- LDAP SSL key file password

Notes:

- If an LDAP server is not used, LDAP settings are not required.
- If the Policy Director setup information is not accessible, NetSEAT client is not installed on the IBM client. See "Prerequisites" on page 12 for more information.

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

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

   Note: For complete information on using the Administrator Utility, see the *Client Security Software Administrator's Guide*.
3. In the Administrator Utility, click the **Policy Setup** tab.
4. Click **DCE** or **LDAP** for the server registry that you will use.
5. Type the appropriate information in each field related to the server registry that you selected.

Setting and using the local-cache feature

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

To set or refresh the local cache:

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

   Note: For complete information on using the Administrator Utility, see the *Client Security Software Administrator's Guide*.
3. In the Administrator Utility, click the **Policy Setup** tab.
4. 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 represents the amount of time between scheduled refreshes.

Enabling Policy Director to control IBM client objects

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

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

Important: Enabling Policy Director to control an object gives object control to the Policy Director object space. If you do this, you must reinstall Client Security Software to re-establish local control over that object.

Editing a local UVM policy

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.

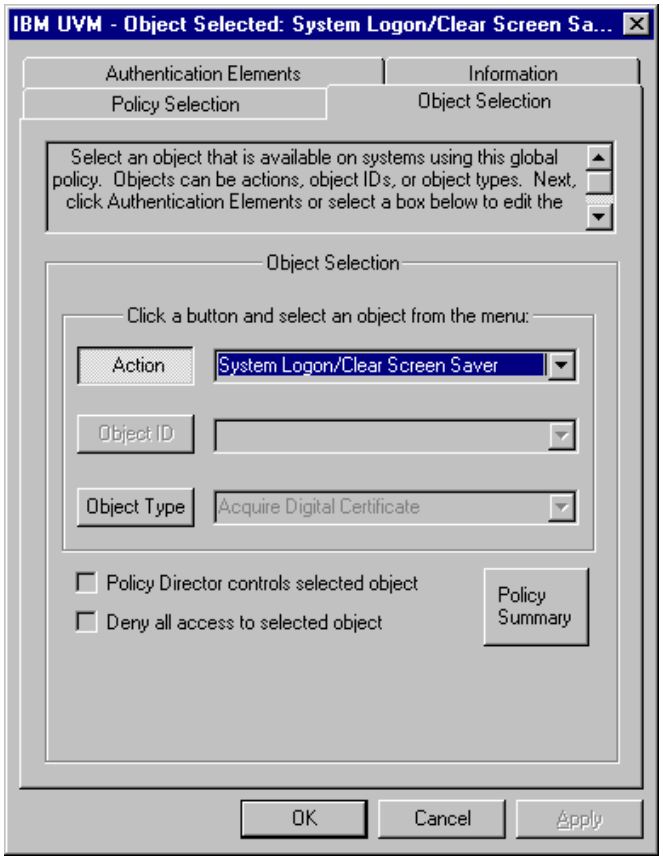
Note: If you set UVM policy to require fingerprints for an authentication object (such as the operating-system logon), users that are added to UVM must have their fingerprints registered to use that object.

To start the UVM-policy editor:

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

   Note: The default access password for the UVM-policy file is the word `password`. After you edit the UVM policy, you can change the access password. For complete information on the UVM-policy editor, see the *Client Security Software Administrator's Guide*.
4. On the **Policy Selection** page, select the UVM-policy file (globalpolicy.gvm) from the drop-down list.
5. Click the **Object Selection** tab, click **Action** or **Object type,** and select the object for which you want to assign authentication requirements. Actions include System Logon / Clear Screen Saver and E-mail Decryption; an object type is Acquire Digital Certificate.

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



6. For each object that you select, select **Policy Director controls selected object** to enable Policy Director for that object.

   Important: If you enable Policy Director to control 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.

   Note: While you are editing UVM policy, you can view the policy summary information by clicking **UVM Policy Summary**.

7. Click the **Information** tab, and type the system name, user details, and system and enterprise administrator details in the appropriate fields.

8. Click the **Policy Selection** tab, and click the **UVM Policy** button. To save the policy file, click **Save**, and follow the on-screen instructions. To save the file with a new password, click **Save as**, and follow the on-screen instructions.

9. Click **OK** to save your changes and exit.

Editing and using UVM policy for remote clients

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

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

To start the UVM-policy editor:

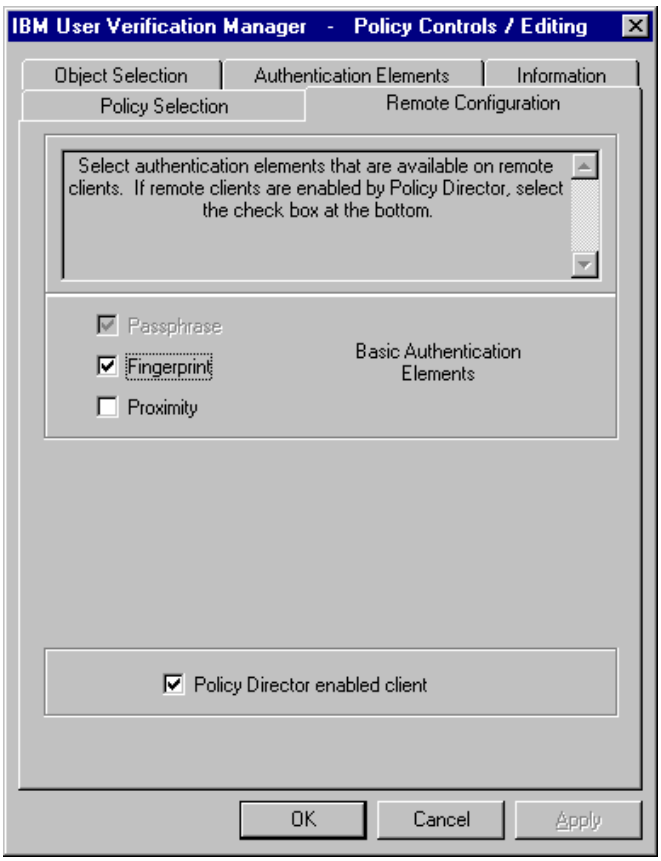
1. Start the Administrator Utility, and click the **Policy Setup** tab.
2. In the **UVM Policy** area, click **Remote Clients**, and then click **Edit Policy**.
3. The Global Policy Access Password window opens. Type *password* and press **Enter**.

   Note: The default access password for the UVM-policy file is the word *password*. After you edit the UVM policy, you can change the access password.
4. On the **Policy Selection** page, select the UVM-policy file (globalpolicy.gvm) from the drop-down list.
5. Click the **Object Selection** tab, click **Action** or **Object type,** and select the object for which you want to assign authentication requirements. Actions include System Logon / Clear Screen Saver and E-mail Decryption; an object type is Acquire Digital Certificate.
6. For each object that you select, click **Policy Director controls selected object** to enable Policy Director for the object.

   Important: If you enable Policy Director to control 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.

   Note: While you are editing the UVM-policy file, you can view the policy summary information by clicking on **UVM Policy Summary**.
7. Click the **Information** tab, and type the system name, user details, and system and enterprise administrator details in the appropriate fields.

8. Click the **Remote Configuration** tab. Select the authentication elements that are available on the remote clients that will use this UVM policy, and then select the **Policy Director enabled client** check box.



9. Click the **Policy Selection** tab, and click the **UVM Policy** button. To save the policy file, click **Save**, and follow the on-screen instructions. To save the file with a new password, click **Save as**, and follow the on-screen instructions.
10. Click **OK** to save your changes and exit.
11. Copy the following files to other remote IBM clients that will use this UVM-policy:

    ✍ \IBM\Security\UVM_Policy\remote\globalpolicy.gvm

    ✍ \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

    Notes:

    ✍ If you installed the Client Security Software in its default location, the root directory for the preceding files is \Program Files.

    ✍ You must copy both files to the \IBM\Security\UVM_Policy\ directory path on the remote clients.

Chapter 5 - Troubleshooting

Following is a list of possible problems and suggested actions that you can take to solve the problems.

Problem	Action
On the **Policy Setup** page in the Administrator Utility, the settings for Policy Director setup and the local cache setup are not accessible.	Install NetSEAT client. If NetSEAT client is not installed on the IBM client, the Policy Director settings on the **Policy Setup** page will not be available.

Problem	Action
After installing the Client Security component, all ACLs for the Client Security name space are cleared.	If you reinstall the Client Security component on the Policy Director server, any ACLs that have been set will be cleared. No action is required. This note is for informational purposes only.

Problem	Action
After configuring the Policy Director server, a user's control is valid for both the user and the group.	When configuring the Policy Director server, if you define a user to a group, the user's control is valid if *Traverse bit* is on for both the user and the group. No action is required. This note is for informational purposes only.

Appendix A - 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.