IBM® Client Security Solutions

Using Client Security with Policy Director

Client Security Software Version 1.2

June 2000

Before using this information and the product it supports, be sure to read "Appendix A - Notices and Trademarks," on page 18.

First Edition (June 2000)

Table of Contents

About this guide

The guide contains information to help you set up Client Security Software for use with IBM Tivoli® SecureWay® Policy Director (Policy Director).

The guide is organized as follows:

"Chapter 1 - Overview," contains an brief overview of Policy Director.

"Chapter 2 - 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 3 - Configuring IBM clients," contains prerequisite information and instructions for configuring IBM clients to use the authentication services provided by Policy Director.

"Chapter 4 - Troubleshooting," contains information that can help you if you experience problems 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 an enterprise administrator who plans to use Policy Director to manage the authentication objects set up by the User Verification Manager (UVM) security policy for an IBM client.

The administrator must be knowledgeable of the following:

- Installation and management of the IBM Distributed Computing Environment (DCE) and the IBM SecureWay Directory's lightweight directory access protocol (LDAP)
- Installation and set up 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 and all other documentation for Client Security Software are available for download from the following IBM Web site:

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

Compare 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 Policy Director server and installed NetSEAT client, use the instructions in the *Client Security Software Installation Guide* to install Client Security Software on IBM clients. See "Chapter 3 - Configuring IBM client," on page 9 for more information.

Compare to the Client Security Software Administrator's Guide

References to the *Client Security Software Administrator's Guide* are provided in this document. The *Client Security Software Administrator's Guide* contains information on how to set up user authentication and the UVM policy for the IBM client. After you have installed Client Security Software, use the *Client Security Software Administrator's Guide* to set up user authentication and the security policy. See "Chapter 3 - Configuring IBM client," on page 9 for more information.

Conventions used in this guide

IBM client is a term used to describe networked IBM computers that have the IBM embedded Security Chip and that are running Client Security Software.

Also, this guide uses several typeface conventions:

- ***Bold*** - Commands, keywords, authorization roles, and other information that you must use literally appear in ***bold***.
- *Italics* - Variables and values that you must provide appear in *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

A concern for computer security is authentication of the end user at the client level. Client Security Software provides the interface and software required to manage the security policy of an IBM client. This interface is part of the authenticating software User Verification Manager (UVM), the main component of Client Security Software.

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

- locally, through the use of a policy file that resides on the IBM client,
- or across an enterprise with Policy Director.

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

Policy Director concepts

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

Management Console, ACLs and Objects

The Management Console, a component of Policy Director, provides the central interface where you can add or delete users or groups and apply *access controls (ACLs)* to objects provided by Client Security Software, such as digital certificate access or acquisition, system logon, clearing the screen saver, and decryption of encrypted e-mail. You use the Management Console to select what authentication elements will be used as permissions for those objects. You use the Management Console Object Space management task panel to attach ACLs to objects or to remove ACLs from objects.

NetSEAT client

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. NetSEAT is a network support module that works seamlessly as a secure proxy for client applications by allowing end-to-end encryption for all client server traffic.

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 provided on the IBM Web site. After you install the component, *IBM Client Security Solutions* appears as a user-defined object in the object namespace of the Management Console.

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

Chapter 2 - 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.

If you install the Client Security component, the following two features are added to the Policy Director Management Console:

- 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 can install the Client Security component, Policy Director server version 3.0.1.87 or later must be installed. Also, make sure the following components are installed:

- 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 provided at the following Web address:

http://www.ibm.com/software/security/policy/library/

Download and install 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:

1. Download PDServer.exe from the following Web address:

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

   Click on the link for downloading Client Security Software, and then complete the registration form and questionnaire. PDServer.exe is available for download at the same IBM web page that hosts the Client Security Software code.

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

- ***setupPD.bat*** is the batch file that you will run on the server. This file is required for the installation.
- ***Security.txt*** 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*** 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 ivmgrd.conf 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 the ivmgrd.conf file.

   Note: The default path to ivmgrd.conf 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 Security.txt to the directory defined in ivmgrd.conf.
6. Run setupPD.bat on the Policy Director server with the *add* parameter. An example of the command is:

   `d:\temp\setupPD.bat add`

   Note: If you run setupPD.bat, 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 you were set will be cleared.

7. Stop and restart all Policy Director services.
8. Create users in Policy Directory that will use the Client Security object space.
9. Go to "Chapter 3 - Configuring IBM client," on page 9 to enable Policy Director to administer the authentication requirements for IBM clients.

Chapter 3 - Configuring IBM clients

Before you can use Policy Director to control the authentication objects for IBM clients, you must configure each client by using the Administrator Utility, a component 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 order shown below:

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 Windows 98 and Windows 95 clients, 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.
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*.

Configure the Policy Director setup information

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

- DCE host name
- LDAP host name
- LDAP port
- LDAP root DN name
- LDAP DN password
- LDAP SSL key file
- LDAP SSL key file DN
- LDAP SSL key file password

Notes:

- If an LDAP server is not used, the 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" for 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. Select ***DCE*** or ***LDAP*** for the server registry that you will use.
5. For each field related to the server registry you selected, enter the appropriate information.

Set and use 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 and day, 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 values represent the amount of time between scheduled refreshes.

Enable Policy Director to control IBM client objects

UVM policy is controlled through a single global policy file. The global 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: 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.

Editing a local UVM policy

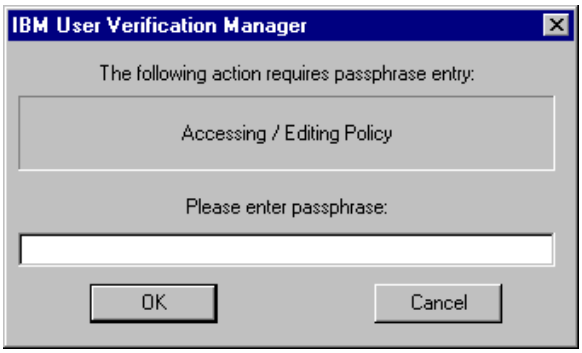
You edit a local UVM policy and use it only on the client for which it was edited. If you installed Client Security in its default location, the local UVM policy is stored as \Program Files\IBM\Security\UVM_Policy\globalpolicy.gvm.

Notes

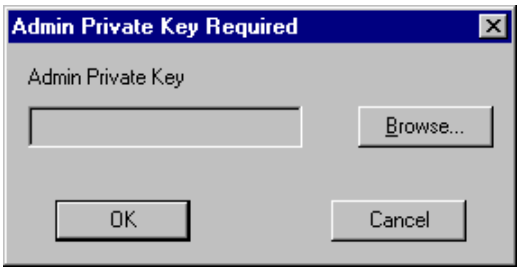
- If you set UVM policy to require fingerprint for an authentication object (such as the operating-system logon), each user that is added to UVM must have registered their fingerprints to use that object.
- The following instructions are also provided in the *Client Security Software Administrator's Guide*.

To start the UVM-policy editor:

1. Enter the Administrator Utility, and click the ***Policy Setup*** tab.
2. In the ***UVM Policy*** area, select ***Local Client***, and then click ***Edit UVM Policy***.
3. Do one of the following:
   - If the UVM passphrase verification window opens, type the UVM passphrase for the user currently logged on to the system and click ***OK***. The UVM passphrase window opens if this is the first time UVM policy has been edited on the current IBM client.



- If UVM policy has already been edited and saved on the current IBM client, type the admin private key, or click ***Browse*** to search for it, and click ***OK***. (After the initial edit of a policy file, a window opens that asks for the admin private key if you try to access the policy editor.)



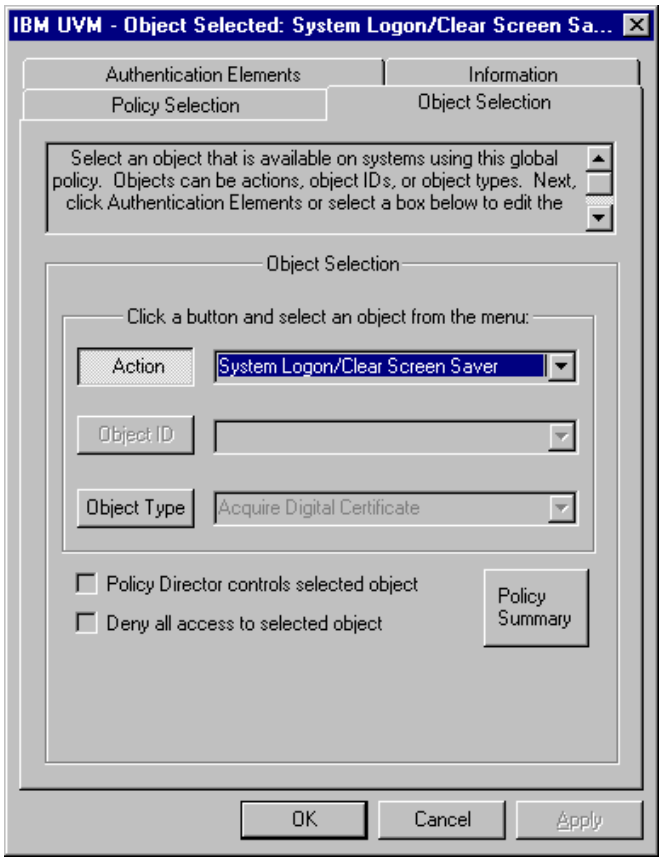
4. The Global Policy Access Password window opens. Type *password* and click ***OK***.

   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.

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

6. Click the ***Object Selection*** tab, then click ***Action*** or ***Object type*** and select the object for which you want to assign authentication requirements. Actions include System Logon/Clear Screen Saver and E-mail Decryption; an object type is Acquire Digital Certificate.

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



7. For each object 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***.

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

9. Click the ***Policy Selection*** tab and click the ***Global Policy*** button. The ***Save*** and ***Save as*** become available. Do one of the following:

   - Click ***Save*** to save the policy file.

- To save the file with a new password, click ***Save as*** and follow the on-screen instructions.

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

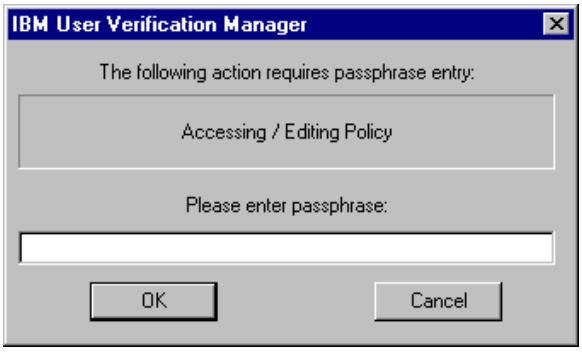
Editing and using UVM policy for remote clients

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

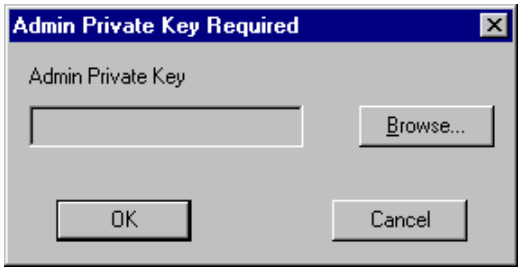
Note: If you set a UVM policy for remote clients to require fingerprint for an authentication object (such as the operating-system logon), each user that is added to UVM must have registered their fingerprints to use that object, and all remote clients that will use the policy must have a UVM-aware fingerprint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

To start the UVM-policy editor:

1. Enter the Administrator Utility, and click the ***Policy Setup*** tab.
2. In the ***UVM Policy*** area, select ***Remote Clients***, and then click ***Edit UVM Policy***.
3. Do one of the following:
   - If the UVM passphrase verification window opens, type the UVM passphrase for the user currently logged on to the system and click ***OK***. The UVM passphrase window opens if this is the first time the UVM-policy file has been edited on the current IBM client.



- If UVM policy has already been edited on the current IBM client, type the admin private key, or click ***Browse*** to search for it, and click ***OK***. (After the initial edit of a policy file, a window opens that asks for the admin private key if you try to access the policy editor.)



4. The Global Policy Access Password window opens. Type *password* and click ***OK***.

   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.

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

6. Click the ***Object Selection*** tab, then click ***Action*** or ***Object type*** and select the object for which you want to assign authentication requirements. Actions include System Logon/Clear Screen Saver and E-mail Decryption; an object type is Acquire Digital Certificate.

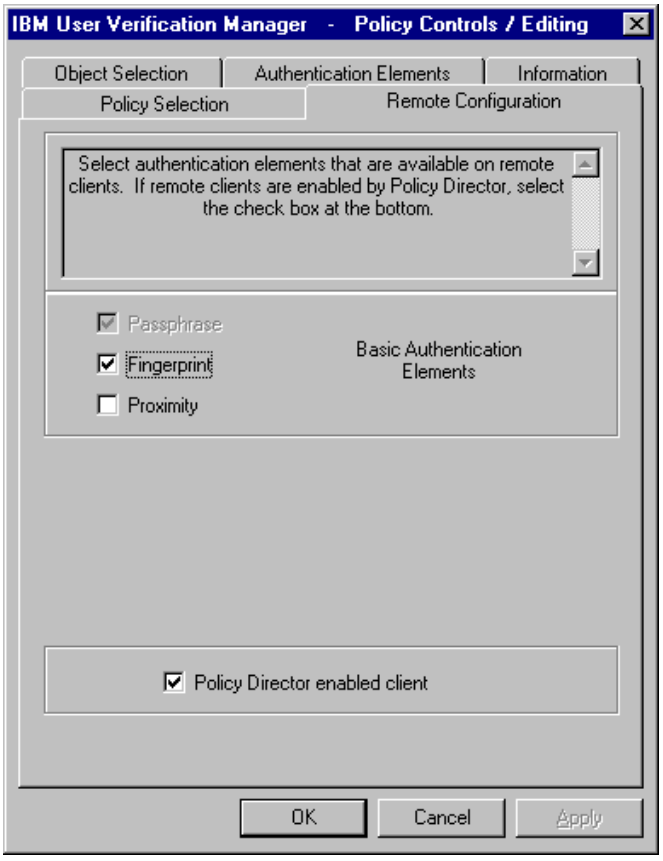
7. For each object you select, click ***Policy Director controls selected object*** to enable Policy Director for the object.

   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***.

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

9. 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.



10. Click the ***Policy Selection*** tab and click the ***Global Policy*** button. The ***Save*** and ***Save as*** become available. Do one of the following:
    - Click ***Save*** to save the policy file.
    - To save the file with a new password, click ***Save as*** and follow the on-screen instructions.
11. Click ***OK*** to save your changes and exit.
12. Copy the following files to other remote IBM clients that will use this UVM-policy:
    - \IBM\Security\UVM_Policy\remote\globalpolicy.gvm
    - \IBM\Security\UVM_Policy\remote\globalpolicy.gvm.sig

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

Chapter 4 - Troubleshooting

The following troubleshooting charts contain information that might be helpful if you experience problems using Client Security with Policy Director.

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

After installing the Client Security component, all ACLs for the Client Security namespace are cleared.	***Action***
If you re-install 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.

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 U.S., other countries, or both.

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

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

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