



System i
Security
Secure Perspective

Version 6 Release 1





System i
Security
Secure Perspective

Version 6 Release 1

Note

Before using this information and the product it supports, read the information in “Notices,” on page 15.

This edition applies to version 6, release 1, modification 0 of IBM i5/OS (product number 5761-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

© Copyright International Business Machines Corporation 2007, 2008. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Secure Perspective	1
What's new for V6R1	1
Secure Perspective concepts	1
Policy-based security	1
Importing and exporting objects	2
Dictionary term creation	2
Domain configuration	3
Policy creation	3
Term mapping	3
Policy actions	4
Prediction of potential problems	4
Systems controlled by policy considerations	5
Prerequisites for installing Secure Perspective	7
Installing Secure Perspective	8
Installing Secure Perspective on i5/OS V5R4, or later	9

Installing Secure Perspective on i5/OS V5R3.	9
Installing Secure Perspective for Windows	11
Installing Secure Perspective agents	11
Writing effective security policies	12
Defining the policy	12
Implementing the policy	12
Managing the policy	13
Related information for Secure Perspective	13

Appendix. Notices	15
Programming Interface Information	16
Trademarks	17
Terms and conditions	17

Secure Perspective

Secure Perspective is a tool you can use to meet your security needs. You can use Secure Perspective to create and implement policies which can handle large amounts of data, prove security compliance in an audit, and close the gap between those who develop your security policy and those who implement it.

IBM Secure Perspective for i5/OS (5733-PS1) is a licensed program. It requires a license before you can use it.



What's new for V6R1

Read about new or significantly changed information for the Secure Perspective topic collection.

Miscellaneous updates have been made since the previous publication.

How to see what's new or changed

To help you see where technical changes have been made, the information center uses:

- The  image to mark where new or changed information begins.
- The  image to mark where new or changed information ends.

In PDF files, you might see revision bars (|) in the left margin of new and changed information.

To find other information about what's new or changed this release, see the Memo to users.

Secure Perspective concepts

To effectively use Secure Perspective to create security policies and to plan security measures for your system, you need to understand concepts about Secure Perspective.

Policy-based security

This topic describes the benefits of using Secure Perspective to create policy-based security.

With today's heightening security and compliance demands, securing the systems in an organization is no longer enough. Special attention must now be paid to securing the important data owned by an organization. Unfortunately, without a tool, the quantity of data to be secured becomes unmanageable to even the most technically knowledgeable policy makers. In addition, compliance is difficult to prove. What is needed is a simple way to state how systems must behave and the ability to monitor that behavior.

The Secure Perspective licensed program allows organizations to create enforceable security policies using natural language. The natural language approach defines an understandable security policy that is meaningful for all parties within a business. Additionally, natural language policies fit well in implementing requirements for chosen regulations. As a result, the policies can be created by business leaders who know how data assets should be protected without needing knowledge of where that information is stored. Data owners and system administrators can map terms from the policy to digital assets. The organization's policy can then be enforced with the click of a button. Also, Secure Perspective provides capabilities to automatically verify that a system is in compliance with stated policies. Quick changes to the security policy in response to an auditor's request can be applied instantly to computers within an organization, avoiding costly IT change processes.

Some of the benefits of Secure Perspective are as follows:

- Tools to create well-structured natural language security policies.
- Facilitators for the mapping of a policy to digital assets.
- Policy applications or compliance checks with a click of a button.
- Records of all policy application and compliance activity.
- The ability to see how applying a policy affects business processes.
- The ability to undo the application of a policy if undesired consequences occur.

In bridging the gap between natural language and system commands, Secure Perspective enables a unified process for organizations to manage their data security. As the business world adapts to heightening security demands, focusing effort and saving time becomes even more important. Secure Perspective is an effective tool in attaining these goals.

Policy creation

To reduce the time and risk involved in creating a security policy, take a systematic approach in the form of a precise process. Typically, the life cycle of a policy consists of the following steps:

- Authoring the statements
- Connecting to systems
- Predicting problems
- Applying the policy
- Checking for compliance

Secure Perspective facilitates each phase of this life cycle. For information on the process you can use to create security policies, see “Writing effective security policies” on page 12.

From a broad view, security is an organization-specific quality that can be difficult to measure. However, with a policy in place that governs everything that is enforced, the policy becomes the measure of an organization’s security. The policy, as crucial as it is, can only be as effective as its creation, implementation, and maintenance.

Importing and exporting objects

To effectively import and export objects, you need to understand the following concepts.

Secure Perspective allows for the importing and exporting of many different Secure Perspective objects, such as policies or term dictionaries in XML. This can be useful for environments where the policies are shared, but the underlying hardware and software implementations differ. For example, you can write a policy and term dictionary at the corporate level, and distribute them to branch offices. Importing and exporting allows the branch offices to map the resources to their specific environments. Importing and exporting also allows you to easily back up and restore your data.

Dictionary term creation

You can use natural language when creating policies using Secure Perspective. By creating a dictionary, you define the terms to use in your policies.

To make IT security policies easier to create, the set of terms used in a policy can be specified before any policy statements have been written. There are four types of terms: actors, actions, resources, and purposes. Each type of term is used in the policy statement in a different way.

Actor terms represent groups of users that should be given the same access rights. It is best if these terms represent abstract groups of users. Terms like *accountants* or *engineers* are good. Terms like *Members of the accounting department* are less abstract and create less useful security policies. Terms like *Jim Smith* or *my secretary* are too specific and should not be used. Terms for policies should address roles or positions within the organization instead of individuals.

Action terms represent ways in which users can interact with data. These can be terms like *view*, *read*, *update*, or *see*.

Resource terms represent groups of information. All of the objects in a resource have the same access rights. If a user is able to change one file of a resource, they can probably change all of the other files of the resource.

Purpose terms allow a statement to specify the possible reasons that a user might take an action. It is important to note that Secure Perspective cannot enforce these purposes. However, they might be important in constructing a sufficiently detailed security policy.

Domain configuration

To effectively configure the domain, you need to understand the following concepts.

Domain configuration provides the ability to define domains (systems) to secure by policy. Currently supported are i5/OS™, Microsoft® Windows®, and AIX® systems as well as DB2® databases on Linux®, UNIX®, and Windows.

For System i platforms you can also set up monitoring for terms to help in problem prediction.

Related reference

“Prediction of potential problems” on page 4

Use this information to predict future problems with your security policies. The problem prediction function of the Secure Perspective licensed program also allows you to predict if you will be denied access to any important business functions due to an incomplete policy or set of mappings.

Policy creation

To effectively create policies, you need to understand the following concepts.

Each policy is composed of policy statements. Each statement declares that an *actor* can take an *action* with respect to a *resource*. Optionally, the statement may specify that the actor can take the action only for a specific purpose. It is assumed that any user not given access to a resource by at least one policy statement should be denied access to that resource.

Policy statements can be entered or edited as text. The statements must have the format *Actors can action resource*. If a purpose is used for the statement, the format must be *Actors can action resource for the purposes of purpose*.

Each policy contains statements like:

Accountants can read and update accounting data.

Term mapping

To effectively map terms, you need to understand the following concepts.

Actor, action, and resource terms can be mapped to resources on the system. Actor terms can be mapped to user and group profiles. Actions can be defined in terms of the privileges on objects. Resources can be mapped to files, directories, tables, or other resources. Secure Perspective will change the security settings of any system object mapped to a resource to be in compliance with the policy.

Secure Perspective version 1 release 2 includes object filters. When mapping objects in System i, the **wildcard system object filter** allows you to map a term to a set of system resources that have a common naming convention. For instance, you can map the term *accountants* to a filter on the directory */acct_info/directory*. In this example, all the files in */acct_info/directory* with the first 4 characters *acct* are mapped to the *accountant* term even if the files were created after the filter was mapped.

You can edit term mappings, use mapping accelerators, or view a mapping summary for each individual system.

Policy actions

To effectively perform policy actions, you need to understand the following concepts.

Several policy actions are available: apply policy, check policy compliance, and problem prediction. Apply policy and check policy compliance are available for each system platform. Problem prediction is only available for System i.

- **Apply policy**

After a policy has been created and mappings made, the policy can be applied to the system. This changes the security settings of the system. Before the settings are changed, the current state of the changing objects is captured. The policy application can be undone and the old state restored.

- **Check policy compliance**

Check policy compliance allows you to monitor the compliance of a policy for a set of systems. This policy action accesses the target systems and compares their current state with one that is compliant with the policy. A report is generated and returned to you with clear policy violations and object-compliant summaries. These summaries are all archived by system in the event history.

Related reference

“Prediction of potential problems”

Use this information to predict future problems with your security policies. The problem prediction function of the Secure Perspective licensed program also allows you to predict if you will be denied access to any important business functions due to an incomplete policy or set of mappings.

Prediction of potential problems

Use this information to predict future problems with your security policies. The problem prediction function of the Secure Perspective licensed program also allows you to predict if you will be denied access to any important business functions due to an incomplete policy or set of mappings.

The problem prediction function allows you to simulate the application of a policy before you actually apply it. Based on past system use, the problem prediction function can report potential problems with your security policy. This function eases the adoption of a new policy by testing the policy before implementation by ensuring that all users have the correct authority and by finding potential points of unauthorized access to resources.

The problem prediction function is available only on System i. It works by capturing the history of past system use, and then analyzing the past use. Based on the analyzed data, it can then predict problems likely to occur with the application of the new policy. The tool reports these results.

For a description of how the process of using problem prediction can work on an unsecured system as part of developing a security policy, see the following example of the steps you can take in the security development process:

1. Turn on system auditing.
2. Allow the system to monitor itself for a given period.
3. Create the policy and mappings you plan to use on the system.
4. After the monitoring period, run the problem prediction function on the system.
5. Monitor the results to verify that the policy matches system use.
6. Adjust the policy and mappings to correct for any problems.
7. Apply the policy to the system.

Systems controlled by policy considerations

Consider this information before installing and using Secure Perspective.

AIX

Using Secure Perspective to control an AIX system gives policy-based resource access control over files. When applying a policy to an AIX system, the files mapped to resource terms are given new NFS4 access control lists (ACLs). When files are evaluated for their compliance with a policy, the ACL for each file is examined to determine if it grants the access specified by the policy. If the ACL is not of the NFS4 type, the compliance report indicates that the file might be out of compliance because the exact level of user access cannot be determined.

For AIX to secure a file using an NFS4 ACL, the file must reside in a JFS2 file system created with extended attributes version 2. However, when Secure Perspective removes the application of a policy, the previous ACL is restored, regardless of whether that ACL was of type AIXC or NFS4.

The Secure Perspective Agent for AIX must be installed on any AIX system that will be controlled by Secure Perspective. The agent installer can be found on CD 2 and must be installed by the root user.

System i

System i has no considerations.

Windows

The Secure Perspective agent for use with the Windows operating system must be installed on any Windows system that will be controlled by Secure Perspective. The agent installer can be found on the Secure Perspective installation CD 2, and must be installed by the administrator profile.

DB2

The DB2 system controller has a few unique characteristics that it is important to understand to make the best use of Secure Perspective. These are as follows:

1. Ability to control system-level authorities.
2. Unique behavior toward the user whose credentials are used to apply policy.
3. Retrieval only of users who have authority on the system.

DB2 characteristics

Consider these DB2 characteristics before installing and using Secure Perspective.

The database resource

When mapping terms on a DB2 system, notice the top-level resource object called database. If you do not want to affect system-level authorities when you apply a policy, do not map this object to a term. If you do want to affect system-level authorities when you apply a policy, then you must map this object to a term. However, be aware of the effect this will have on the system.

The Secure Perspective model assumes that anyone who is not granted specific access to a mapped object by a policy should not have access to that object. That means that if the database object is mapped, all users who are not granted database-level authorities (including database administrator and connect authorities) by the policy will have those authorities revoked. If you have the database object mapped, make sure that the policy grants the appropriate users the correct authorities.

Checking compliance

Because the DB2 system controller handles system-level authorities, these authorities must be considered when checking compliance. Consider the following facts:

1. Users with database administrator authority have all privileges on all objects in the database, whether they are explicitly granted those privileges or not.
2. Users that do not have connect authority do not effectively have any privileges, even if they are explicitly granted privileges on specific objects.

These facts result in the following compliance check behaviors:

1. If a user with database administrator authority on the system is not granted database administrator authority by the policy, the compliance report will mark that user as having unauthorized access to all objects to which the policy does not explicitly give that user access.
2. If a user is granted database administrator authority in the policy, but does not actually have database administrator authority on the system, the compliance report will mark that user as being denied access to all the objects to which the user does not have actual access on the system.
3. If a user is not granted database administrator or connection authority by the policy, but has connection authority on the system, the compliance report marks the user as having unauthorized access to objects to which that user has access on the system. The compliance report does not mark the user as being denied access to objects to which the policy grants access, but the system does not grant access.
4. If a user does not have connection authority on the system, whether or not the policy grants that user connection authority, the compliance report marks that user as being denied access to all the objects to which the policy gives the user access. The compliance report does not mark the user as having unauthorized access to objects to which the system grants the user access, but the policy does not grant access.

User whose credentials are used

The DB2 system does not allow users to revoke authorities or privileges from themselves, and it sometimes does not allow users to grant authorities or privileges to themselves. Secure Perspective generates all statements that are necessary to fully implement the policy. Therefore, when you apply (or undo) a policy, you can expect failed statements relating to the user name that was used to authenticate to the database. These statements also fail if you logged into the database by using a command line with that username and attempted to run the statements there.

Users with no authority or privileges

Secure Perspective retrieves its information from the database catalog tables. This includes the retrieval of users and groups. Therefore, for the application to register a user or group as existing, an entry must exist where that user appears as a grantee in one of the following views:

- SYSCAT.DBAUTH
- SYSCAT.TABAUTH
- SYSCAT.COLAUTH
- SYSCAT.SCHEMAAUTH
- SYSCAT.INDEXAUTH
- SYSCAT.PACKAGEAUTH

If the user and group does not appear as a grantee in one of those places, then they do not appear on the **Actor** tab of the Term mappings display screen and cannot be mapped to any actor terms.

Related concepts

“Systems controlled by policy considerations” on page 5
Consider this information before installing and using Secure Perspective.

Prerequisites for installing Secure Perspective

This topic describes the prerequisite conditions necessary for installing Secure Perspective.

Before you begin installing Secure Perspective on the i5/OS® operating system, complete the following prerequisites:

1. If you plan to access Secure Perspective using Internet Explorer, ensure you have the Scalable Vector Graphics (SVG) plug-in.
2. Establish a 5250 session to the system where Secure Perspective (5733-PS1) will be installed.
3. Ensure you have a user profile with *ALLOBJ and *SECADM special authority.
4. Verify that the Developer Kit for Java™ (5761-JV1) has been installed on your system. Do the following:
 - a. On a command line, enter the command G0 LICPGM.
 - b. Select Option 10 (Display installed licensed programs).
 - c. Scroll the list and look for Developer Kit for Java (5761-JV1). If the product is not on your system, obtain the product and install it on your system.
5. Verify that IBM® HTTP Server for i5/OS (5761-DG1) has been installed on your system. Do the following:
 - a. On a command line, enter the command G0 LICPGM.
 - b. Select Option 10 (Display installed licensed programs).
 - c. Scroll the list and look for IBM HTTP Server for i5/OS (5761-DG1). If the product is not on your system, obtain the product and install it on your system.
6. Verify that your system has an active optical device. Do the following:
 - a. On a command line, enter the command WRKCFGSTS *DEV *OPT.
 - b. Ensure that you have devices varied on by verifying that the Status is Active. If the device is not varied on, type 1 under the Opt column to make the device active.
 - c. If no devices are listed, you have no optical devices connected to your system. After you have connected an optical device to the system, you can continue.
7. For i5/OS V5R4, or later, verify that all of the necessary PTFs and PTF group SF99114, PTF Group Level 6 or higher have been applied to your system.
 - To verify PTFs for i5/OS (5761-SS1), use the following command:
DSPPTF LICPGM(5761SS1) SELECT(*ALL)
Page down the lists of PTFs and verify that all of the following PTFs have been applied to your system:
 - SI26787
 - SI25516
 - SI22392
 - SI21743
 - SI21742
 - To verify PTFs for HTTP server (5761-DG1), use the following command:
DSPPTF LICPGM(5761DG1) SELECT(*ALL)
Page down the lists of PTFs and verify that all of the following PTFs have been applied to your system:
 - SI26881
 - SI26873

- SI26803
- SI22447
- SI22402
- SI22394
- To verify that the PTF group SF99114 (PTF Group Level 6 or higher) has been applied to your system, use the Work with PTF Groups (WRKPTFGRP) command:
WRKPTFGRP SF99114

If any of the PTFs or the PTF group is not on your system, obtain the PTF or group by using the SNDPTFORD command or by using IBM Fix Central.

Before you begin installing Secure Perspective on Windows, complete the following prerequisites:

1. Ensure you have DB2 Express version 8 installed.
2. Ensure you have Java version 1.5 or later installed.

Related tasks

“Installing Secure Perspective”

IBM Secure Perspective for i5/OS can be installed on systems running i5/OS V5R3, or later. Follow the instructions for the version of i5/OS that you have.

Related information

Ordering fixes using the Internet

Installing Secure Perspective

IBM Secure Perspective for i5/OS can be installed on systems running i5/OS V5R3, or later. Follow the instructions for the version of i5/OS that you have.

Before you begin installing Secure Perspective, complete the prerequisites in “Prerequisites for installing Secure Perspective” on page 7.

To install IBM Secure Perspective (5733-PS1) on i5/OS, complete the following steps:

1. Establish a 5250 session to the system on which you want to install Secure Perspective.
2. Sign on with a user profile that has *ALLOBJ and *SECADM special authorities.
3. Load the Secure Perspective product CD into an optical device drive connected to your system.
4. On the command line, type WRKOPTVOL. Note the name of the device for optical volume PS1.
5. Load the product onto the system, using the Restore Licensed Program (RSTLICPGM) command. In the following example, the optical device name is OPT01: RSTLICPGM LICPGM(5733PS1) DEV(OPT01).
6. On the Software License Agreement display screen, press F14 to accept the license agreement.
7. When the RSTLICPGM command is completed, you will a message that indicates a successful installation.
8. To verify the installation, do the following:
 - a. On a command line, type G0 LICPGM.
 - b. Select Option 10 (Display installed license programs).
 - c. Scroll through the list and look for 5733-PS1 Secure Perspective for i5/OS.
 - d. Press F3 to exit.

If you are installing on i5/OS V5R4, continue with the set up tasks in Installing Secure Perspective on i5/OS V5R4. If you are installing on i5/OS V5R3, continue with the set up tasks in Installing Secure Perspective on i5/OS V5R3. If you are installing on Windows, continue with the set up tasks in Installing Secure Perspective on Windows.

Related tasks

“Prerequisites for installing Secure Perspective” on page 7

This topic describes the prerequisite conditions necessary for installing Secure Perspective.

Installing Secure Perspective on i5/OS V5R4, or later

- | Use this procedure to complete the installation of Secure Perspective on systems running i5/OS V5R4, or
- | later.

Before starting this procedure, you must complete the procedures in “Installing Secure Perspective” on page 8.

To install Secure Perspective on i5/OS, complete the following steps:

1. If the *ADMIN HTTP server is running, end the server by typing the following on a command line:
ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN).
2. Restart the HTTP *ADMIN server by typing the following on a command line: STRTCPSVR
SERVER(*HTTP) HTTPSVR(*ADMIN).

The HTTP server must be restarted, so that it recognizes the Secure Perspective application.

3. Open a web browser. Both Mozilla Firefox and Internet Explorer are supported.
4. In the browser, navigate to your Secure Perspective home page. Your home page URL will have the following format: `http://fullyqualifiedmachinename:2001/SecurePerspective`. The `fullyqualifiedmachinename` is made up of the system name and its domain. For example, if your system name is *sysname* and your company domain is *mycompany.com*, the Secure Perspective home page address is `sysname.mycompany.com:2001/SecurePerspective`.

Installing Secure Perspective on i5/OS V5R3

Use this procedure to complete the installation of Secure Perspective on systems running on i5/OS V5R3.

Before starting this procedure, you must complete the procedures in “Installing Secure Perspective” on page 8.

To install Secure Perspective on i5/OS, complete the following steps:

1. Open the edit session with the following Edit File (EDTF) command:
EDTF STMF('/QIBM/ProdData/HTTPAdmin/conf/server.xml')
2. Add an entry for the Secure Perspective application to the webapps section of the file. Add the entry in the position of the Secure Perspective entry that appears in bold in the following example:

```
<!-- ===== webapps ===== -->
```

```
<Context path="/HTTPAdmin"
docBase="webapps/HTTPAdmin"
debug="0"
reloadable="false" >
</Context>
```

```
<Context path="SecurePerspective"
docBase="webapps/SecurePerspective"
debug="0"
reloadable="false" >
</Context>
```

```
<Context path="/mmconsole"
docBase="webapps/mmconsole"
debug="0"
reloadable="false" >
</Context>
```

3. Change the JASPER_LOG verbosityLevel value to WARNING. Make the change as shown in the following example:


```
<Logger name="JASPER_LOG"
  path="logs/jasper.log"
  verbosityLevel="WARNING" />
```

4. Press F3 (Exit) to save and exit the /QIBM/ProdData/HTTPAdmin/conf/server.xml edit session.
5. To change the JK plug-in for the Apache configuration file, open an edit session with the following command: EDTF STMF('/QIBM/ProdData/HTTPAdmin/conf/admin-ibm.conf').

You must change the Tomcat Web container file and the JK plug-in for the Apache configuration file so that it detects requests that need to be routed to the Tomcat engine.

6. To the Servlet engine directives section of the file, add the Secure Perspective Apache directives in the same position as the bold text in the following example:

```
#-----
# Servlet engine directives
#-----
LoadModule jk module
/QSYS.LIB/QHTTPSVR.LIB/QZTCJK.SRVPGM
JkWorkersFile
/QIBM/ProdData/HTTPAdmin/conf/workers.properties
JkLogFile /QIBM/UserData/HTTPAdmin/logs/jk.log
JkLogLevel error
JkMount /HTTPAdmin jni
JkMount /HTTPAdmin/* jni
JkMount /SecurePerspective jni
JkMount /SecurePerspective/* jni
JkMount /IPAdmin jni
JkMount /IPAdmin/* jni
```

7. Press F3 (Exit) to save and exit the /QIBM/ProdData/HTTPAdmin/conf/admin-ibm.conf edit session.
8. Create the /QIBM/UserData/HTTPAdmin/work directory with the following command:
MKDIR DIR('/QIBM/UserData/HTTPAdmin/work') DTAAUT(*RX)
9. Grant the QTMHHTTP profile access to the directory you just created with the following command:
CHGAUT OBJ('/QIBM/UserData/HTTPAdmin/work')USER(QTMHHTTP)DTAAUT(*RWX)
10. Change the owner of the directory to QSYS with the following Change Owner (CHGOWN) command:
CHGOWN OBJ('/QIBM/UserData/HTTPAdmin/work') NEWOWN(QSYS)
11. Add the tools.jar for the Java Runtime Environment (JRE) 1.4 to the server's classpath for the Jasper compiler. To do this, open an edit session with the following Edit File (EDTF) command:
EDTF STMF('/QIBM/ProdData/HTTPAdmin/conf/workers.properties')
12. Add the following line to the worker.jni.class_path list:
worker.jni.class_path=/QIBM/ProdData/java400/jdk14/lib/tools.jar
13. If the *ADMIN HTTP server is running, end the server by typing the following command:
ENDTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
14. Restart the HTTP *ADMIN server by typing the following command:
STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
The HTTP server must be restarted, so that it recognizes the Secure Perspective application.
15. Open a Web browser session. Mozilla Firefox, Version 1.5 and later, and Internet Explorer, Version 6 and later, are supported. If you are using Internet Explorer, the Scalable Vector Graphics (SVG) plug-in is required.
16. In the browser, navigate to your Secure Perspective home page. Your home page URL will have the following format: http://fullyqualifiedmachinename:2001/SecurePerspective. The fullyqualifiedmachinename is made up of the system name and its domain. For example, if your system name is sysname and you company domain is mycompany.com, the Secure Perspective home page address is sysname.mycompany.com:2001/SecurePerspective.

Installing Secure Perspective for Windows

Use this procedure to complete the installation of Secure Perspective on systems running the Windows operating system.

Before starting this procedure, you must complete the procedures in “Installing Secure Perspective” on page 8.

The Windows installer can be found on CD 1 and must be installed by the administrator profile.

To install Secure Perspective for use with Windows, do the following:

1. Log on to the workstation using the administrator profile.
2. Insert Secure Perspective installation CD 1 into the workstation’s optical device drive.
3. Follow the steps of the installation wizard on the CD.

Installing Secure Perspective agents

Use this procedure to install the AIX agent or the Windows agent.

To install the AIX agent, do the following:

1. Log on to the workstation using the root user ID.
2. Insert Secure Perspective installation CD 2 into the workstation’s optical device drive.
3. Start the AIX agent installer.
4. Follow the directions of the installation wizard.

To install the Windows agent, do the following:

1. Log on to the workstation using the administrator user profile.
2. Insert Secure Perspective installation CD 2 into the workstation’s optical device drive.
3. Start the Windows agent installer.
4. Follow the directions of the installation wizard.

Prerequisites for installing Secure Perspective agents

Use this information to ensure all necessary conditions are met before you install Secure Perspective agents.

AIX

- Install the AIX agent with the root user name and password.
- Install Java Runtime Environment (JRE) version 1.5, or later.

DB2

Ensure that JDBC port 50000 is open for remote DB2 commands.

System i

- The system must have i5/OS version 5 release 3, or later, installed.
- The system must have IBM Toolbox for Java toolbox.

Windows

- You must install the Windows agent with the administrator profile.
- You must install Java Runtime Environment (JRE) version 1.5, or later.

Writing effective security policies

Use this topic to gain information about how to write security policies.

When writing a security policy, you should follow a process. This way, you can:

- Ensure your policy is thorough.
- Repeat the process easily.
- Reduce risk.

Writing effective security policies is a three-step process: defining the policy, implementing the policy, and managing the policy. The following information explains these steps in more detail.

Defining the policy

Use this topic to help you gather the information you need to define an effective security policy.

When you define a policy, consider the following elements:

- Objectives, or what you want to accomplish with your security policy.
- Scope, or who and what your security policy should cover. Your policy should state who can perform an action, not who cannot perform it.
- Data, or what needs to be secured.

To help you define the objectives, scope, and data of your security policy, use the following tips:

1. Before defining your security policy, assemble all of the people who are stakeholders in the security of your business. These people will want to contribute to the definition of your security policy. These can include the following types of people:
 - Business leaders
 - Data owners
 - System administrators
 - Legal analysts
 - Internal auditors
2. Identify the regulations and practices that influence your security needs. This information can come from the following types of sources:
 - Government or industry regulations or standards.
 - Requirements of the stakeholders in the security of your business.
 - Possible threats to your security.
3. Identify the assets your security policy must control. The following types of sources can help you identify your assets:
 - The regulations that need to be followed.
 - The types of data you use in your business, such as sales data or shipping data.
 - The points at which data is created, accessed, or deleted.
4. Identify the various roles individuals play as they interact with the data protected by your security policy. To help identify these roles, determine the following:
 - The types of individuals who are interacting with the data assets.
 - The nature of the interactions between the individuals and the assets.

Implementing the policy

After you have defined your needs for a security policy, you can use Secure Perspective to implement that policy. Use the tips in this topic to help you get started writing a security policy with Secure Perspective.

To implement a security policy, do the complete the following actions:

- Enter the data types that you identified into Secure Perspective as **Resources**.
- Enter the roles that you identified into Secure Perspective as **Actors**.
- Enter the data interactions that you identified into Secure Perspective as **Actions**.

You can use the following steps as guidelines for using Secure Perspective to write and apply a security policy.

1. Create clear, meaningful policy statements.
2. Identify the systems that contain relevant data that need to be connected to the controlling system. On Secure Perspective, add these machines to the **system configuration list**.
3. Connect policy terms to digital assets. Be aware of the file system's hierarchy and how this affects users' access to files within directories. In Secure Perspective, map resources to data assets, actors to user profiles, and actions to system actions.
4. Check current compliance. You may need to make adjustments on your system if it fails to comply with your policy. After applying patches or fixes, you might want to run a compliance check.
5. Use problem prediction to determine whether your current processes could be affected by the application of your security policy. You may need to modify your policy if it interferes with essential system procedures.
6. Use Secure Perspective to apply the policy. You can read the report for details and investigate any questionable failures. Undo the policy and make adjustments as necessary.

Restriction: Secure Perspective uses authorization lists to secure objects. The maximum number of files and members that can be secured by a single resource term is 2 097 104. If you apply a policy when more than 2 097 104 items (files added to the sum of the members in those files) are mapped to a term, the application of the policy will fail. An error message is shown on the display screen. Alternatively, you can divide the objects mapped to the term to two or more terms, modify the policy accordingly, and apply the policy again.

Managing the policy

Use Secure Perspective to continue to manage the security policy you have defined and implemented for your business. The tips in this topic can help you determine a process for managing your security policy.

1. Maintain security compliance by establishing a schedule for routine compliance checks. You may want to check compliance after such events as the application of fixes, system configuration changes, large additions of new assets, or large additions of new user profiles.
2. Establish how often you should revisit the policy to maintain currency with security standards.
3. Create a request procedure to follow if a particular user needs access to an asset or needs to belong to a different type of actor. Such requests should require a security manager's approval and require identity verification.
4. Limit administrative rights for the policy to security officers and system administrators. In Secure Perspective, the existing administrative users of the tool can assign administrative rights to others.
5. In case the system unexpectedly locks up, you can use the export function of Secure Perspective to export the dictionary and policy after changes. Use the import function to restore them.
6. In case of internal or external audits, you may want to save the printable summaries of the policy application or compliance check reports. Keep the summaries in a safe location other than the system running Secure Perspective.

Related information for Secure Perspective

Listed here are the Web sites and information center topics that relate to the Secure Perspective topic.

Secure Perspective updates and fixes

- Fix Central has the most recent fixes for Secure Perspective installed on the System i platform.

- IBM Secure Perspective has the most recent updates and fixes for Secure Perspective installed on Windows and for Secure Perspective agents.

Other information

- Planning and setting up system security describes how to plan, set up, and use your system security.
- Intrusion detection describes how to prevent intrusions that come from the TCP/IP network.

Appendix. 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 grant 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) 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

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
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, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This Secure Perspective publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM Secure Perspective.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
i5/OS
IBM
IBM (logo)
System i

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.



Printed in USA