IBM Security Identity Manager
Version 6.0

# *IBM Security Access Manager Adapter Installation and Configuration Guide*

SC27-4421-02

IBM Security Identity Manager
Version 6.0

# *IBM Security Access Manager Adapter Installation and Configuration Guide*

SC27-4421-02

**Note**
Before using this information and the product it supports, read the information in "Notices" on page 59.

**Edition notice**

**Note: This edition applies to version 6.0 of IBM Security Identity Manager (product number 5724-C34) and to all subsequent releases and modifications until otherwise indicated in new editions.**

# Contents

# Figures

# Tables

# Preface

## About this publication

The *IBM Security Access Manager Adapter Installation and Configuration Guide* provides the basic information that you can use to install and configure the IBM Security Access Manager Adapter, previously known as IBM Tivoli Access Manager Combo Adapter.

The IBM Security Access Manager Adapter enables connectivity between the IBM® Security Identity Manager Server and the IBM Security Access Manager Policy Server and its associated directory server.

## Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Identity Manager library."
- Links to "Online publications."
- A link to the "IBM Terminology website."

### IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation, see the online library (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm).

### Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

**IBM Security Identity Manager library**
The product documentation site (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm) displays the welcome page and navigation for the library.

**IBM Security Systems Documentation Central**
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

**IBM Publications Center**
The IBM Publications Center site ( http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

### IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

## Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

## Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

## Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix F, "Support information," on page 53 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

**Note:** The **Community and Support** tab on the product information center can provide additional support resources.

## Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

# Contents

# Figures

# Tables

# Chapter 1. Overview of the IBM Security Access Manager Adapter

An adapter is a program that provides an interface between a managed resource and the IBM Security Identity Manager Server.

Adapters might or might not be on the managed resource, and the IBM Security Identity Manager Server manages access to the resource by using your security system. Adapters function as trusted virtual administrators on the target operating system. They do such tasks as creating login IDs, suspending IDs, and do other functions that administrators normally run manually.

The IBM Security Access Manager Adapter uses the IBM Tivoli® Directory Integrator function to facilitate communication between the IBM Security Identity Manager Server and IBM Security Access Manager Server. The following sections provide information about the IBM Security Access Manager Adapter:



## Features of the adapter

The adapter automates various administrative tasks.

You can use the IBM Security Access Manager Adapter to automate the following account management tasks:

- Creating new users.
- Creating SSO credentials for users.
- Modifying users' SSO credentials and attributes.
- Changing user account passwords.
- Suspending, restoring, and deleting user accounts.
- Reconciling user, SSO credentials, and user attributes.
- Creating and deleting groups, and modifying their descriptions

## Architecture of the adapter

IBM Security Identity Manager communicates with the IBM Security Access Manager Adapter to administer IBM Security Access Manager user accounts.

You can do the following actions on an account:

- Add
- Delete
- Modify
- Change Password
- Restore
- Suspend
- Search for account information

The IBM Security Access Manager Adapter consists of IBM Tivoli Directory Integrator AssemblyLines. When an initial request is made by IBM Security Identity Manager server to the IBM Security Access Manager Adapter, the AssemblyLines are loaded into the IBM Tivoli Directory Integrator server. As a result, subsequent service requests do not require those same AssemblyLines to be reloaded.

The AssemblyLines use the IBM Tivoli Directory Integrator IBM Security Access Manager connector, LDAP connector, and IBM Security Access Manager User connector to undertake user management-related tasks on the directory server. It does these tasks remotely by using the login user ID and password of a user that has administrator privileges.

Figure 1 shows the various components that work together to complete user management tasks in an IBM Tivoli Directory Integrator environment.

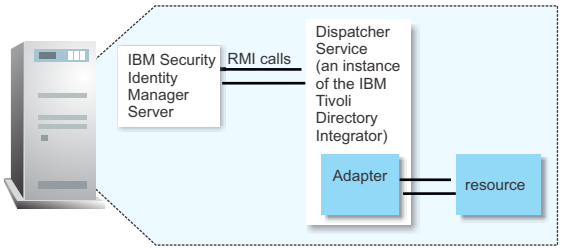


*Figure 1. The architecture of the IBM Security Access Manager Adapter*

For more information about IBM Tivoli Directory Integrator, see the *IBM Tivoli Directory Integrator: Getting Started Guide*.

## Supported configurations

The IBM Security Access Manager Adapter supports a number of different configurations and is designed to operate with IBM Security Identity Manager 6.0.

There are fundamental components of an IBM Security Access Manager Adapter environment:

- An IBM Security Identity Manager server
- An IBM Tivoli Directory Integrator server
- A compatible directory server
- The IBM Security Access Manager Adapter.

The IBM Security Access Manager Runtime for Java™ Environment must also be configured on the same Java Runtime Environment (JRE) as used by IBM Tivoli Directory Integrator.

The IBM Security Access Manager Adapter is both highly configurable and highly customizable. Support can extend only to the configuration of the adapter such as adding mapping for more attributes. Support cannot extend to customization by way of changes, additions, or modifications to its IBM Tivoli Directory Integrator Assembly Line scripts for example.

# Chapter 2. Installation planning for the IBM Security Access Manager Adapter

Installing and configuring the adapter involves several steps that you must complete in an appropriate sequence. Review the roadmaps before you begin the installation process.

## Preinstallation roadmap

Prepare the environment before you install the adapter.

Do the tasks that are listed in the following table.

*Table 1. Preinstallation roadmap*

| What to do | Where to find more information |
|---|---|
| Verify that the software and hardware requirements for the adapter that you want to install are met. | See "Prerequisites" on page 4. |
| Collect the necessary information for the installation and configuration. | See "Installation worksheet for the adapter" on page 4. |
| Obtain the installation software. | Download the software from Passport Advantage®. See "Software download" on page 5. |

## Installation roadmap

You must complete the necessary steps to install the adapter. The steps include completing post-installation configuration tasks and verifying the installation.

To install the adapter, complete the tasks that are listed in the following table:

*Table 2. Installation roadmap*

| What to do | Where to find more information |
|---|---|
| Install the adapter. | See "Installing the IBM Security Access Manager Adapter" on page 7. |
| Import the adapter profile. | See "Importing the adapter profile into the IBM Security Identity Manager Server" on page 10. |
| Create a service. | See "Creating an IBM Security Access Manager service" on page 11. |
| Configure the adapter. | See Chapter 6, "Customization of the IBM Security Access Manager Adapter," on page 21. |
| Verify the adapter profile installation. | See Chapter 8, "IBM Security Access Manager Adapter profile installation verification," on page 31. |

## Prerequisites

Verify that all of the prerequisites are met before you install the IBM Security Access Manager Adapter.

Table 3 identifies hardware, software, and authorization prerequisites to install the IBM Security Access Manager Adapter.

*Table 3. Prerequisites to install the adapter*

| Prerequisite | Description |
|---|---|
| Operating System | The IBM Security Access Manager Adapter can be used on any operating system that is supported by IBM Tivoli Directory Integrator. |
| Network Connectivity | TCP/IP network |
| System Administrator Authority | The person who completes the IBM Security Access Manager Adapter installation procedure must have system administrator authority to complete the steps. |
| IBM Tivoli Directory Integrator Server | Version 7.1 fix pack 5 or later<br><br>Version 7.1.1 |
| IBM Security Identity Manager server | Version 6.0 |
| IBM Security Identity Manager Adapter (also known as the RMI Dispatcher) | For IBM Tivoli Directory Integrator Server 7.1, obtain the dispatcher installer from the IBM Passport Advantage website: http://www-01.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm. |
| IBM Security Access Manager Java Runtime (previously known as IBM Tivoli Access Manager) | Corresponding version to the IBM Security Access Manager Server. The IBM Security Access Manager Adapter supports IBM Security Access Manager versions 6.0, 6.1 and 6.1.1. |

For information about the minimal system requirements and supported operating systems for IBM Tivoli Directory Integrator, refer to the *IBM Tivoli Directory Integrator: Administrator Guide*.

## Dispatcher installation verification

If this installation is the first adapter that is based on Tivoli Directory Integrator, you must install the Dispatcher before you install the adapter.

Install the Dispatcher on the IBM Tivoli Directory Integrator server where you want to install the adapter.

Obtain the Dispatcher installer from the IBM Passport Advantage website. For information about the Dispatcher installation, see the *Dispatcher Installation and Configuration Guide*.

## Installation worksheet for the adapter

Use the information from the adapter worksheet to install the adapter.

Table 4 identifies the information that you use to install the IBM Security Access Manager Adapter.

*Table 4. Required information to install the adapter*

| Required information | Description |
|---|---|
| Administrator account on the managed resource for running the IBM Security Access Manager Adapter. | An administrator account on the managed resource that has administrative rights. |
| IBM Security Access Manager Administrator account | An administrator account in IBM Security Access Manager with administrative rights. For example, sec_master. |
| Directory Service Administrator account | An administrative account on the underlying directory server of IBM Security Access Manager. This account must have enough access rights to manage IBM Security Access Manager directory accounts and group membership entries. |

## Software download

Download the software through your account at the IBM Passport Advantage website.

Go to IBM Passport Advantage.

See the *IBM Security Identity Manager Download Document* for instructions.

**Note:**

You can also obtain additional adapter information from IBM Support.

# Chapter 3. Installation and configuration of the IBM Security Access Manager Adapter

The following sections contain the information that you use to install and configure the adapter.



## Installing the IBM Security Access Manager Adapter

You must do several sequential tasks to install the adapter.

### Procedure

1. Configure JRTE against IBM Tivoli Directory Integrator Java Runtime Environment (JRE).
2. Configure IBM Tivoli Directory Integrator JRE into the IBM Security Access Manager secure domain.
3. Extract the IBM Security Access Manager Adapter compressed file (`Adapter-TamCombo-6.0.x.zip`) from the distribution package.
4. Install the IBM Security Access Manager Adapter Utilities Package.
5. Import the adapter profile into the IBM Security Identity Manager Server.

## Configuring the IBM Security Access Manager Run Time for Java System

The Java Run Time component (JRTE) must be installed on the same system where IBM Tivoli Directory Integrator Server and IBM Security Identity Manager Adapter are installed.

### About this task

For more information about installing the JRTE, see the *IBM Security Access Manager: Install Guide*.

To configure JRTE against IBM Tivoli Directory Integrator Server JRE, follow these configuration steps:

### Procedure

1. Start the IBM Security Access Manager configuration utility. Run the command `pdconfig`
2. Select **Access Manager Runtime for Java** from the list of installed packages.
3. Click **Configure**.
4. Select **Full** for configuration type and then click **Next**.
5. Specify the JRE path such as `C:\Program Files\ibm\TDI\V7.1\jvm\jre`. Then, click **Next**.
6. Specify **Host name**, **Port**, and **Domain**. Then, click **Next**.

7. Optionally enable Tivoli Common logging. Then, click **Finish**. A message that states that JRTE is successfully configured is shown on the screen.
8. Click **Close** to exit the utility.

### What to do next

For more information, see the *IBM Security Access Manager: Command Reference*.

## Configuring the IBM Security Access Manager Registry Direct API for Java System

You can use the Registry Direct API to improve the adapter performance.

### About this task

**Note:** To use the new Registry Direct API with IBM Security Access Manager 6.1, contact IBM Security Access Manager support. Obtain these items:

- A copy of the `com.tivoli.pd.rgy.jar` file from the IBM Security Access Manager 6.1.1 installation
- The instructions to install and configure the IBM Tivoli Directory Integrator Java Runtime environment.

To use the Registry Direct API for IBM Security Access Manager 6.1.1 or later:

### Procedure

Copy the `com.tivoli.pd.rgy.jar` file from IBM Security Access Manager installation directory to IBM Tivoli Directory Integrator JRE installation directory. On a Linux IBM Security Access Manager system, the `com.tivoli.pd.rgy.jar` file is typically at:

```
/opt/PolicyDirector/java/export/rgy
```

Copy this file to the following directory on the system where IBM Tivoli Directory Integrator is installed:

```
/opt/IBM/TDI/V7.1/jvm/jre/lib/ext
```

For more information, see Appendix D. Registry Direct Java API in the *IBM Security Access Manager: Administration Java Classes Development Reference*.

## Configuring the IBM Tivoli Directory Integrator Java Runtime Environment into the IBM Security Access Manager secure domain

To use IBM Security Access Manager security, the IBM Security Identity Manager adapter must be configured into your IBM Security Access Manager secure domain.

### About this task

IBM Security Access Manager provides a utility class `com.tivoli.pd.jcfg.SvrSslCfg` that can be used for configuration and unconfiguration tasks.

You must use the IBM Tivoli Directory Integrator JRE to run the utility.

For example, use the following command to configure IBM Tivoli Directory Integrator to use the IBM Security Access Manager policy server on `amserver.example.com`, with standard ports and default installation paths:

```
/opt/IBM/TDI/V7.1/jvm/jre/bin/java com.tivoli.pd.jcfg.SvrSslCfg
  -action config
  -admin_id sec_master
  -admin_pwd SEC_MASTER_PASSWORD
  -appsvr_id itdi_tam
  -port 1234
  -mode remote
  -policysvr amserver.example.com:7135:1
  -authzsvr amserver.example.com:7136:1
  -cfg_file /opt/IBM/TDI/V7.1/timsol/tam.conf
  -key_file /opt/IBM/TDI/V7.1/timsol/tam.ks
```

To use the new Registry Direct API reconciliation method for IBM Security Access Manager 6.1.1 or later, use the following command:

```
/opt/IBM/TDI/V7.1/jvm/jre/bin/java com.tivoli.pd.jcfg.SvrSslCfg
-action config
-admin_id sec_master
-admin_pwd SEC_MASTER_PASSWORD
-appsvr_id itdi_tam
-port 1234
-mode remote
-policysvr amserver.example.com:7135:1
-authzsvr amserver.example.com:7136:1
-cfg_file /opt/IBM/TDI/V7.1/timsol/tam.conf
-key_file /opt/IBM/TDI/V7.1/timsol/tam.ks
-ldap_mgmt true
-ldap_svrs ldapserver:389:readwrite:5
-ldap_ssl_enable false
```

The `tam.conf` file that is generated in this step is used in a later configuration process.

For more information about configuring IBM Security Access Manager Runtime for Java, see Appendix A. com.tivoli.pd.jcfg.SvrSslCfg in *IBM Security Access Manager: Authorization Java Classes Developer Reference* and Appendix D. Registry Direct Java API ("Installation and configuration") in *IBM Security Access Manager: Administration Java Classes Developer Reference*.

## Installing the IBM Security Access Manager Adapter utilities package

The IBM Security Access Manager Adapter utilities package contains Java classes that are used by the IBM Security Access Manager Adapter assembly lines.

### Procedure

1. Copy `TAMComboUtils.jar` from the installation package to an appropriate IBM Tivoli Directory Integrator location:

   **Windows**

   IBM Tivoli Directory Integrator version 7.1:

   *ITDI_HOME*`\jars\connectors`

   **UNIX or Linux**

   IBM Tivoli Directory Integrator version 7.1:

   *ITDI_HOME*`/jars/connectors`

2. Restart the IBM Security Identity Manager Dispatcher service if it is already installed and running.

For information about starting and stopping the Dispatcher service, see the *Dispatcher Installation and Configuration Guide*.

## Adapter service start, stop, and restart

To start, stop, or restart the adapter, you must start, stop, or restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Tivoli Directory Integrator instance.

See the topic about starting stopping, and restarting the dispatcher service in the *Dispatcher Installation and Configuration Guide*.

## Importing the adapter profile into the IBM Security Identity Manager Server

An IBM Security Identity Manager adapter profile defines the types of resources that the IBM Security Identity Manager server can manage.

### About this task

In this case, the profile is used to create an IBM Security Access Manager Adapter service on the IBM Security Identity Manager Server.

You must import the adapter profile into the IBM Security Identity Manager Server before you use the IBM Security Access Manager Adapter.

Before you import the adapter profile, verify that the following conditions are met:

- The IBM Security Identity Manager server is installed and running.
- You have root or Administrator authority on the IBM Security Identity Manager Server.

The IBM Security Access Manager Adapter distribution package contains the following adapter profile:

**`itamprofile.jar`**

The `itamprofile.jar` profile is used when IBM Security Access Manager is configured against supported LDAP and Active Directory user registries, including Active Directory Application Mode (ADAM) or other supported user registries.

**Note:** For an IBM Security Identity Manager installation that uses Sun Directory Server, use `itamprofileSunDS.jar` to install the profile.

It extends IBM Security Identity Manager directory schema with:

- IBM Security Access Manager account attributes
- Attributes from the **`InetOrgPerson`** object class as define in *RFC 2798 "Definition of the inetOrgPerson LDAP Object Class"*
- Attributes that can be mapped to Active Directory attributes

See Table 7 on page 23.

To import the adapter profile, complete the following steps:

### Procedure

1. Log in to the IBM Security Identity Manager server by using an account that has the authority to do administrative tasks.
2. Import the adapter profile by using the **import** feature for your IBM Security Identity Manager product. Refer to the online help or the product documentation for specific instructions about importing the adapter profile.
3. Restart the IBM Security Identity Manager Dispatcher service.

### What to do next

If you receive an error that is related to the schema when you import the adapter profile, refer to the `trace.log` file for information about the error. The `trace.log` file location is specified by using the **`handler.file.fileDir`** property that is defined in the IBM Security Identity Manager `enRoleLogging.properties` file. The `enRoleLogging.properties` file is installed in the *`ISIM_HOME`*`\data` directory.

## Creating an IBM Security Access Manager service

After the adapter profile is imported on IBM Security Identity Manager, you must create a service so that IBM Security Identity Manager can communicate with the adapter.

### About this task

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter.

### Procedure

1. Log on to the IBM Security Identity Manager server with an account that has the authority to do administrative tasks.
2. In the My Work pane, click **Manage Services** and click **Create**.
3. On the Select the Type of Service page, select **IBM Security Access Manager profile**.
4. Click **Next** to display the adapter service form.
5. Complete the following fields on the service form:

   **SERVICE SETUP Tab**

   **Service name**
   Specify a name that defines this IBM Security Access Manager Adapter service on the IBM Security Identity Manager Server.

   **Description**
   Optionally, specify a description for this service.

   **IBM Tivoli Directory Integrator location**
   Specify the URL for the IBM Tivoli Directory Integrator instance. Valid syntax is `rmi://`*`ip-address`*`:`*`port`*`/ITDIDispatcher`, where *ip-address* is the IBM Tivoli Directory Integrator host and *port* is the port number for the RMI Dispatcher. You might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. For information about changing the port number, see the *RMI Dispatcher Installation and Configuration Guide*.

**Owner**
Optionally, specify the service owner

**Service prerequisite**
Optionally, specify the service prerequisite

**IBM SECURITY ACCESS MANAGER SETUP tab**

**IBM Security Access Manager API**
The IBM Security Access Manager Adapter has two methods for managing IBM Security Access Manager user accounts and groups:

**IBM Security Access Manager Administration API**
This method is designed to use the IBM Security Access Manager Administration Java API.

**IBM Security Access Manager Registry Direct API**
This method is designed to use with the IBM Security Access Manager Registry Direct Java API. Applicable only when IBM Security Access Manager version is 6.1 or later and when the directory server type is LDAP. This method provides optimal performance and supports high availability. For more detail, see Appendix C, "Performance optimization," on page 45.

**Enable GSO Support**
If checked, the adapter manages GSO-related account attributes and resource objects. When you manage GSO-related attributes and objects, the adapter uses the IBM Security Access Manager Administration API regardless of the value of the **IBM Security Access Manager API** field in the service form. This is because the Registry Direct API does not support GSO management.

**Use group cache on reconciliation**
Enabling this option causes the IBM Security Access Manager Adapter to use an internal cache for resolving the group membership information for the users. In some circumstances, this option might improve the reconciliation performance. For more detail, seeAppendix C, "Performance optimization," on page 45. Application only when **IBM Security Access Manager Registry Direct API** is selected as the reconciliation method.

**Reload group cache on each reconciliation**
Enabling this option causes the group cache to be reloaded on each reconciliation. For most cases, enable this option so the cache is up-to-date. In some circumstances, it might be useful to disable this option:

- Repeatedly running a full reconciliation for many users during testing.
- Environments in which the group membership information does not change or is irrelevant.

This option applies only when the **Use group cache on reconciliation** option is enabled.

**Reconciliation Page Size**
Optionally, apply only when you use IBM Security Access Manager Registry Direct API reconciliation.

If a page size other than 0 is specified, the IBM Security Access Manager Adapter uses **page mode** search to obtain user accounts information.

For more information, see Appendix A, "Reconciliation page size," on page 41.

**IBM Security Access Manager Admin User**
Specify the IBM Security Access Manager administrator account name (for example, `sec_master`). This account must have enough access rights to manage accounts.

**IBM Security Access Manager Admin User Password**
Specify the password for the IBM Security Access Manager administrator account.

**IBM Security Access Manager Config File**

Specify the file name and path for the configuration file that was created by using **SvrSslCfg** with the `–cfg_file` option during step "Configuring the IBM Tivoli Directory Integrator Java Runtime Environment into the IBM Security Access Manager secure domain" on page 8.

The example has this file path: `/opt/IBM/TDI/V7.1/timsol/tam.conf`.

**Add Account**
Specify the following options for adding IBM Security Access Manager user account:

**Create user entry in registry.**
Causes the adapter to create a user entry in the directory server registry with a specific DN. If the entry exists, requests for account provisioning fail.

**Import user entry from registry.**
Causes the adapter to reuse an existing user entry from the directory server registry. If an entry with a specified DN does not exist, the request fails.

**Import or create user entry.**
Causes the adapter to check whether a user entry with a specific DN exists, and if so, this user entry is used. Otherwise, a new registry entry for the IBM Security Access Manager account is created.

**Delete user entry from Registry**
If this check box is checked, during the deletion of the IBM Security Access Manager account, the user entry is removed from the directory server registry. If the check box is left cleared, the user entry remains in the registry.

**Add group**
Specify one of the following options for adding IBM Security Access Manager groups:

**Create group entry**
Causes the adapter to create a group in the directory server registry with a specific DN. If the entry exists, the group cannot be created.

**Import group entry**
Causes the adapter to import an existing group entry from the directory server registry. Import fails if the entry with the DN specified does not exist.

**Delete group entry from registry**
If this check box is checked, during the deletion of the IBM Security Access Manager group, the group entry is removed from the directory server registry. If the check box is left cleared, the group entry remains in the registry.

**Synchronize IBM Security Access Manager password in SSO Lockbox**
If this check box is checked, during the password change operation, all of the account SSO credentials passwords are synchronized with the new account password.

**IBM Security Access Manager Domain Name**
Optionally, specify the IBM Security Access Manager Domain Name. If this field is left blank, the default IBM Security Access Manager runtime domain is used.

**DISPATCHER ATTRIBUTES Tab**

**Disable AL Caching**
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add operation, modify operation, delete operation, and test operation are not cached.

**AL FileSystem Path**
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Identity Manager. You can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system:

```
c:\Program Files\IBM\TDI\V7.1\profiles
```

or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system:

```
/opt/IBM/TDI/V7.1/profiles
```

**Max Connection Count**
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter `10` when you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. You can enter `0` in the **Max Connection Count** field. In this case, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

**On the Status and information tab**
The page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

**Last status update: Date**
Specifies the most recent date when the **Status and information** tab was updated.

**Last status update: Time**
Specifies the most recent time of the date when the **Status and information** tab was updated.

**Managed resource status**
Specifies the status of the managed resource that the adapter is connected to.

**Adapter version**
Specifies the version of the adapter that the IBM Security Identity Manager service uses to provision request to the managed resource.

**Profile version**
Specifies the version of the profile that is installed in the IBM Security Identity Manager server.

**TDI version**
Specifies the version of the Tivoli Directory Integrator on which the adapter is deployed.

**Dispatcher version**
Specifies the version of the Dispatcher.

**Installation platform**
Specifies summary information about the operating system where the adapter is installed.

**Adapter account**
Specifies the account that running the adapter binary file.

**Adapter up time: Date**
Specifies the date when the adapter started.

**Adapter up time: Time**
Specifies the time of the date when the adapter started.

**Adapter memory usage**
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also

- Verify the adapter log to ensure that the IBM Security Identity Manager test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify IBM Security Identity Manager service parameters for the adapter profile. You might verify the work station name or the IP address of the managed resource and the port.

6. Click **Finish**.

# Chapter 4. IBM Security Access Manager Adapter upgrade

Upgrading the adapter involves tasks, such as upgrading the connector, dispatcher, and the existing adapter profile.

To verify the required version of these adapter components, see the adapter release notes.

## Upgrading from adapter version 5.1.12 or older

To upgrade the adapter, you must remove the existing `TAMComboUtils.jar` file and install the new one.

### About this task

**Note:** The location to install the IBM Security Access Manager Adapter utilities JAR file is changed.

### Procedure

1. Remove the `TAMComboUtils.jar` from the *ITDI_HOME*`\jars\3rdparty\IBM\` directory.
2. Copy `TAMComboUtils.jar` from the installation package to the *ITDI_HOME*`\jars\connectors` directory.
3. Restart the IBM Security Identity Manager Dispatcher service if it is already installed and running.

   For information about starting and stopping the Dispatcher service, see the *Dispatcher Installation and Configuration Guide*.

## Profile upgrade

The IBM Security Access Manager Adapter distribution package now contains only one adapter profile `itamprofile.jar`. It is a merge of the existing `itamprofile.jar` and `itamprofileAD.jar` files.

Use this profile when IBM Security Access Manager is configured against a supported LDAP server, Active Directory, Active Directory Application Mode (ADAM), or other supported user registries.

**Note:** For an IBM Security Identity Manager installation that uses Sun Directory Server, use `itamprofileSunDS.jar` to install the profile.

To import the profile, see "Importing the adapter profile into the IBM Security Identity Manager Server" on page 10.

## Dispatcher upgrade

The new adapter package might require you to upgrade the Dispatcher.

Before you upgrade the dispatcher, verify the version of the dispatcher.

- If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.

- If the dispatcher version mentioned in the release notes is the same or earlier than the existing version, do not install the dispatcher.

The IBM Security Access Manager Adapter now supports the following dispatcher attributes:

- **Assembly Line File System Path**
- **Max Connection Count**
- **Disable Assembly Line Cache**

Upgrade your dispatcher to the latest version to support these new attributes.

# Chapter 5. Management of IBM Security Access Manager groups

You can manage IBM Security Access Manager groups by using the IBM Security Access Manager Adapter.



## Add Group

You can add a group by either creating one or importing an existing group. The **Add Group** configuration option is available on the IBM Security Access Manager Service form.

The adapter creates new groups with the default object classes as specified by the IBM Security Access Manager Java Administration API. You cannot specify custom object classes when you use the adapter to create a group. However, you can use the adapter to modify and delete IBM Security Access Manager groups with non-default object classes after they are imported.

When the adapter creates new groups it assigns them to the default group container, which is also specified by IBM Security Access Manager Java Administration API. By default, the adapter places new groups in the object space under `/Management/Groups`. You cannot specify a different group container when you use the adapter to create a group.

The parameters that are required on the IBM Security Identity Manager Add Group form are **group name** and **Distinguished Name (DN)**. You can also provide an optional **description**. The adapter does not support specifying a **Common Name(CN)** for the group, as the IBM Security Access Manager Java Administration API does not support this parameter. You cannot specify any other group attributes when you add a group.

## Modify Group

You can use the IBM Security Access Manager Adapter to modify the group description.

The **`description`** attribute that is managed by the IBM Security Access Manager Java Administration API is the only group attribute that the adapter can modify. You cannot use the adapter to modify any other attributes present in the group registry entry. These attributes can include the **`UID`**, **`CN`**, **`principal name`**, and attributes that form the **`Distinguished Name`**.

**Note:** In Active Directory, an existing description cannot be modified to an empty string. This condition is a known limitation in the IBM Security Access Manager Java Administration API. The description remains unchanged if you attempt to modify it to an empty string.

## Delete Group

You can use the adapter to delete IBM Security Access Manager groups.

If **Delete group entry from registry** is checked on the IBM Security Access Manager service form, then the entire group object is deleted from the registry. Otherwise, the group is removed from IBM Security Access Manager, but its registry object remains.

## Group Operation Notes

Group operations are logged in the IBM Tivoli Directory Integrator `ibmdi.log` log file.

If a group operation is not successful, review the log for more detailed information.

Also, dynamic groups are not supported.

# Chapter 6. Customization of the IBM Security Access Manager Adapter

You can use the configuration options to customize the IBM Security Access Manager Adapter.

The IBM Security Access Manager Adapter supports a standard set of attributes for default object classes that are used in IBM Security Access Manager servers. Because IBM Security Access Manager server requirements vary, you might customize or extend the IBM Security Access Manager Adapter schema to support more attributes or object classes.

**Note:** The adapter does not support modifying **UID**, **CN**, **principal name**, and attributes that form the Distinguished Name (DN).

## Customization of the IBM Security Access Manager Adapter profile

You can customize the adapter profile by enabling various user entry attributes for the default IBM Security Access Managerconfigurations.

### User entry attributes for default IBM Security Access Manager configurations

The adapter profile by default enables on the account form only IBM Security Access Manager attributes.

The attribute labels, names, and types are listed in Table 5.

*Table 5. Standard attributes supported by the IBM Security Access Manager Adapter*

| Name | Attribute name in schema | Schema | Note |
|---|---|---|---|
| User ID | eruid | Directory String | |
| User password | erpassword | Binary | |
| Password Last Changed | eritampwdlastchanged | Directory String | This attribute cannot be modified. |
| Distinguish Name | eritamdn | DN | |
| Full Name | cn | Directory String | |
| Last Name | sn | Directory String | |
| Description | description | Directory String | |
| Max number of failed logon | eritammaxfailedlogon | Integer | |
| Do Not Enforce Password Policy | eritamppolicy | Boolean | |
| Change Password on Next Login | eritampvalid | Boolean | |
| Single Signon Capability | eritamsinglesign | Boolean | |

*Table 5. Standard attributes supported by the IBM Security Access Manager Adapter (continued)*

| Name | Attribute name in schema | Schema | Note |
|---|---|---|---|
| Group Membership (multi-value attribute) | eritamgroupname | Directory String | |
| SSO Credentials (multi-value attribute) | eritamcred | Directory String | |
| Date of last access | erlastaccessdate | Directory String | |
| State of the account | eraccountstatus | Integer | |

The IBM Security Access Manager Adapter is designed to work with user entry attributes from object classes that are defined in the IBM Security Access Manager configuration. Typically for non-Active Directory configuration, the user entry object classes are **inetOrgPerson**, **organizationPerson** and **Person**. For Active Directory typical configuration, the user entry object class is **User**.

The adapter schema contains attributes from **inetOrgPerson**, **organizationPerson**, and **Person** object classes. These attributes are shown in Table 6.

*Table 6. The inetOrgPerson attributes supported by the IBM Security Access Manager Adapter*

| Attribute | Attribute | Attribute |
|---|---|---|
| BusinessCategory | homePostalAddress | PreferredLanguage |
| CarLicense | initials | RegisteredAddress |
| HomePhone | L | RoomNumber |
| DepartmentNumber | Mail | Secretary |
| preferreddeliverymethod | manager | UserPassword |
| DestinationIndicator | mobile | St |
| DisplayName | Pager | Street |
| EmployeeNumber | physicalDeliveryOfficeName | TelephoneNumber |
| EmployeeType | postalAddress | teletexTerminalIdentifier |
| FacsimileTelephoneNumber | postalCode | TelexNumber |
| GivenName | postOfficeBox | Title |

The adapter schema also contains attributes from the **User** object class. Table 7 on page 23 lists attributes from the **User** object class only. Some of these attributes have different names in the IBM Security Identity Manager Server schema and Windows Active Directory schema. The names mapping and attribute description are also shown in this table.

*Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter*

| Windows Active Directory Attribute | IBM Tivoli Directory Server Attribute | Description | Note |
|---|---|---|---|
| accountExpires | ntUserAcctExpires | Account expires on AD Account Tab | IBM Tivoli Directory Integrator does the advanced mapping to support this attribute. |
| c | c | Country/region on AD Address Tab | |
| co | co | Country/region on AD Address Tab | |
| company | company | Company on AD User Organization Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| countryCode | countryCode | Country/region on AD Address Tab | |
| department | department | Department on AD User Organization Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| displayName | displayName | Display name on AD General Tab | |
| facsimileTelephone Number | facsimileTelephone Number | Fax on AD Telephones Tab | |
| homeDirectory | NTUserHomeDir | Home folder: Local path/To on AD Profile Tab | IBM Tivoli Directory Integrator does the advanced mapping to support this attribute. |
| homeDrive | ntUserHomeDirDrive | Home folder: Connect on AD Profile Tab | IBM Tivoli Directory Integrator does the advanced mapping to support this attribute. |
| homePhone | homePhone | Home on AD Telephones Tab | |
| info | info | Notes® on AD Telephones Tab | |
| initials | initials | Initials on AD General Tab | |

*Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter (continued)*

| Windows Active Directory Attribute | IBM Tivoli Directory Server Attribute | Description | Note |
|---|---|---|---|
| ipPhone | ipPhone | IP phone on AD User Telephones Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| l | l | City on AD Address Tab | |
| mail | mail | Email on AD General Tab | |
| manager | manager | DN of manager on AD Organization Tab | |
| mobile | mobile | | |
| otherFacsimile TelephoneNumber | otherFacsimile TelephoneNumber | Fax Number (Others) on AD User Telephones Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| otherHomePhone | otherHomePhone | Home Phone (Others) on AD User Telephones Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| otherIpPhone | otherIpPhone | IP Phone Number (Others) on AD User Telephones Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |

*Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter (continued)*

| Windows Active Directory Attribute | IBM Tivoli Directory Server Attribute | Description | Note |
|---|---|---|---|
| otherMobile | otherMobile | Mobile Number (Others) on AD User Telephones Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| otherPager | otherPager | Pager Number (Others) on AD User Telephones Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| otherTelephone | otherTelephone | Phone Number (Others) on AD User General Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| pager | pager | Pager on AD Telephones Tab | |
| physicalDelivery OfficeName | physicalDelivery OfficeName | Office on AD General Tab | |
| postalCode | postalCode | Zip/Postal Code on AD Address Tab | |
| postOfficeBox | postOfficeBox | P.O. Box on AD Address Tab | |
| profilePath | profilePath | Profile path on AD User Profile Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |

*Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter (continued)*

| Windows Active Directory Attribute | IBM Tivoli Directory Server Attribute | Description | Note |
|---|---|---|---|
| sAMAccountName | sAMAccountName | User logon name (preWindows 2000) on AD User Account Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |
| scriptPath | ntUserScriptPath | Log on script on AD Profile Tab | IBM Tivoli Directory Integrator does the advanced mapping to support this attribute. |
| st | st | State/province on AD Address Tab | |
| streetAddress | streetAddress | Street on AD Address Tab | |
| telephoneNumber | telephoneNumber | Telephone number on AD General Tab | |
| title | title | Title on AD Organization Tab | |
| url | url | Web Page Address (Others) on AD General Tab | |
| userPrincipalName | userPrincipalName | User logon name on AD Account Tab | |
| userWorkstations | ntUserWorkstations | Log On To/Logon Workstations on AD Account Tab | IBM Tivoli Directory Integrator does the advanced mapping to support this attribute. |
| wWWHomePage | wWWHomePage | Web page on AD User General Tab | To support its management, this attribute is added to IBM Security Identity Manager's IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile. |

Attributes such as **userAccountControl**, non-modifiable attributes such as the **memberOf** and **logonHours** attribute are not supported. These attributes have INTEGER8 syntax; hence it would be difficult to manage them on the account form.

To manage any of the user entry attributes, complete the following steps:

1. Log in to IBM Security Identity Manager as an Administrator.

2. From the IBM Security Identity Manager GUI, go to **Configuration** and then **Form Customization**.
3. Expand **Account** and then select the **itamaccount** Account.
4. Select the tab where you want to place an attribute.
5. From the attribute list, double-click the attribute to add it to the account form.
6. Click **Save Form Template**.

## Customization of the adapter workflows to provide credentials password in clear text

The adapter form for the attribute **SSO Credentials** creates a composite **eritamcred** attribute value that is sent to the adapter.

The attribute has this format:

```
<Resource Name> (Web Resource OR Group Resource)|
<Resource Account Name>|<Resource Password Base64 encoded>;
```

To specify initial resource password in a workflow, you must implement base64 encoding of the password.

The following example shows that a resource called `WebRsrc1`, of type `Web Resource`, with resource user ID `resid1` and resource password `pwd01` . The password `pwd01` has base64-encoding:

```
WebRsrc1 (Web Resource)|resid1|cHdkMDE=
```

The adapter offers alternative format for this attribute that makes it possible to specify the resource password in clear text, by putting prefix {clear}:

```
<Resource Name> (Web Resource OR Group Resource)|
<Resource Account Name>|{clear}<Resource Password in clear text>
```

This example of a web resource credential has a resource password that is set to "changeMe" concatenated with their surname:

```
WebRsrc1 (Web Resource)|resid1|{clear}changeMe" + subject.getProperty("sn")
```

Alternatively, you can still choose to assign a constant, simple, human-readable resource password. Here is an example of a group resource credential:

```
GroupRsrc2 (Group Resource)|resid2|{clear}tempPwd
```

**Note:**

- Resource passwords that are prefixed with {clear} must not contain the pipe character (|).
- There is no space between the string {clear} and password.
- If the string {clear} is incorrectly typed, the base64encode method that is used in the adapter does not report an error. A corrupted password is set.

## Customizing the adapter to report corrupted or not well-formed accounts

The adapter user account attributes are the super set of IBM Security Access Manager user attributes and corresponding user registry attributes. During the reconciliation operation, the adapter merged those two sets of attributes into one.

### About this task

If directory server is corrupted, some accounts can be corrupted to the point that only account name can be retrieved. By default the adapter is designed to log the error in the dispatcher log file and continue reconciliation.

The behavior can be changed to force reconciliation to stop on first corrupted account event.

Follow these steps to enable this feature:

### Procedure

1. Extract the `itamprofile.jar` file by using the following command:
   ```
   jar -xvf itamprofile.jar
   ```
   **Note:** For an IBM Security Identity Manager installation that uses Sun Directory Server, use `itamprofileSunDS.jar`.
   Two directories are created:
   a. The directory `itamprofile` contains the adapter profile.
   b. The directory `META-INF` contains metadata for the JAR file.
2. Delete the `META-INF` directory. It is re-created by repackaging the adapter profile.
3. Under the `itamprofile` directory, in the `service.def`, change **`dispatcherParameter continueSearchOnMalformedAccount`** to `FALSE` for operation search. Use the following syntax:
   ```
   <dispatcherParameter name="continueSearchOnMalformedAccount">
   <default>FALSE</default>
   </dispatcherParameter>
   ```
4. Repackage the file by using the following command from a command prompt:
   ```
   jar -cvf itamprofile.jar itamprofile
   ```
5. Import the customized profile.
6. Restart the dispatcher.

### What to do next

For more information about how to customize adapter profile, see the *IBM Security Identity Manager Custom Adapter Developer's Guide*.

## Dispatcher configuration properties

Dispatcher configuration properties are set on the IBM Tivoli Directory Integrator.

For information about setting IBM Tivoli Directory Integrator configuration properties for the operation of the IBM Security Access Manager Adapter, see the *Dispatcher Installation and Configuration Guide*.

# Chapter 7. SSL authentication configuration for the IBM Security Access Manager Adapter

Secure communication requires that SSL authentication is used between the various components.

You must configure secure communication between:

- IBM Security Identity Manager and IBM Security Access Manager Adapter
- IBM Security Access Manager Adapter and Windows Active Directory

## SSL configuration for IBM Security Identity Manager and IBM Security Access Manager Adapter

When you configure Secure Sockets Layer (SSL) communication for the adapters that are based on IBM Tivoli Directory Integrator, you must configure SSL between WebSphere® Application Server and IBM Tivoli Directory Integrator.

You must configure the IBM Tivoli Directory Integrator to use SSL. You must also configure WebSphere to use SSL by using the default keystore and default truststore. For more WebSphere SSL configuration information, see the WebSphere online help available from the WebSphere Application Server Administrative Console.

For information about providing SSL communications between the IBM Security Identity Manager server and the IBM Tivoli Directory Integrator server, see the *Dispatcher Installation and Configuration Guide*.

# Chapter 8. IBM Security Access Manager Adapter profile installation verification

If the IBM Security Access Manager Adapter profile is not already installed on your system, you must import the adapter profile.

See "Importing the adapter profile into the IBM Security Identity Manager Server" on page 10 for information about importing the adapter profile.

After you install the adapter profile, verify that the adapter profile was successfully installed. If the adapter profile is not installed correctly, the adapter might not function as intended.

To verify that the adapter profile was successfully installed, complete the following steps.

- Create a service by using the IBM Security Access Manager Adapter profile.
- Open an account on the service.

You might not be able to create a service by using the IBM Security Access Manager Adapter profile or open an account on the service. In this case, the adapter profile is not installed correctly. You might import the adapter profile again.

# Chapter 9. IBM Security Access Manager Adapter troubleshooting

Troubleshooting is the process of determining why a product does not function as it is designed to function.

Use the information and techniques to identify and resolve problems that relate to the IBM Security Access Manager Adapter. There is also information about troubleshooting errors that might occur during run time.

## Techniques for troubleshooting problems

*Troubleshooting* is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

### What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

### Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not been fully tested together.

## When does the problem occur?

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you must look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

## Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being done?
- Does a certain sequence of events happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Just because multiple problems might occur around the same time, the problems are not necessarily related.

## Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of

tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications encounter the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix F, "Support information," on page 53.

## Reconciliation of supporting data

You can use search filters to limit the reconciliation of attributes such as **group names**.

The reconciliation of only **group names** is not currently supported. You can use a search filter to limit the attributes that are returned. For example:

```
(eritamgroup=pattern)
```

All supporting data can be reconciled by using the search filter in the reconciliation query. To reconcile supporting data only, the following search filter can be used:

```
(!(objectclass=eritamaccount))
```

Such a filter reconciles all non-account information.

## Runtime problems

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Runtime Problems and corrective actions are described in the following table:

*Table 8. Runtime Problems*

| Problem | Corrective Action |
|---|---|
| Reconciliation does not return all IBM Security Access Manager accounts. It returns 500 or 2048 accounts only. | The default settings for LDAP and IBM Security Access Manager have constraints on the search size limit. The best practice is as follows:<br>1. Modify the IBM Tivoli Directory Server configuration file, `slapd32.conf` for LDAP 5.2 or `ibmslap.conf` for LDAP 6.0. This file is in the `etc` directory of the IBM Tivoli Directory Server. Set the **`ibm-slapdSizeLimit`** variable to 0 (no limit).<br>2. Modify the IBM Security Access Manager LDAP `ldap.conf` configuration file in the `etc` directory of the IBM Security Access Manager Policy Server. Set the **`max-search-size`** variable to greater than 2048 (the default setting). Setting the **`max-search-size`** to 0 means that the search size is unlimited.<br>3. Modify the IBM Security Access Manager configuration file, `pd.conf`, in the `etc` directory of the IBM Security Access Manager Policy Server. Set the **`ssl-v3-timeout`** variable to 84600 (the maximum setting) and set the **`ssl-io-inactivity`** variable to 0 (no limit).<br><br>For ADAM only:<br><br>Change the **`MaxResultSetSize`** and the **`MaxPageSize`** attribute to increase the search size limit on ADAM by using **`dsmgmt`**. The following example demonstrates setting the value of **`MaxResultSetSize`** and **`MaxPageSize`** to 200000 with the **ADAM Tools Command Prompt**:<br>`C:\WINDOWS\ADAM>dsmgmt`<br>`dsmgmt: LDAP Policies`<br>`ldap policy: Connections`<br>`server connections: Connect to server localhost:389`<br>`Binding to localhost:389 ...`<br>`Connected to localhost:389 using credentials`<br>`of locally logged on user.`<br>`server connections: Quit`<br>`ldap policy: Show Values`<br>`ldap policy: Set MaxResultSetSize to 200000`<br>`ldap policy:Set MaxPageSize to 200000`<br>`ldap policy:Commit Changes`<br><br>For more information, see the ADAM Help. |

*Table 8. Runtime Problems (continued)*

| Problem | Corrective Action |
|---|---|
| Reconciliation does not return all IBM Security Access Manager accounts. Reconciliation is successful but some accounts are missing. | For the adapter to reconcile many accounts successfully, you can increase the WebSphere JVM memory. The following steps must be completed on the WebSphere host computer: **Note:** Do not increase the JVM memory to a value higher than the System memory.<br>1. Log in to the WebSphere Administrative Console.<br>2. Expand **Servers** in the left menu and select **Application Servers**.<br>3. A table displays the names of known application servers on your system. Click the link for your primary application server.<br>4. Select **Process Definition** from within the **Configuration** tab.<br>5. Select the **Java Virtual Machine** property.<br>6. Enter a new value for the **Maximum Heap Size**. The default value is 256 MB.<br>The allocated JVM memory might not be large enough. In this case, an attempt to reconcile many accounts by using the IBM Security Access Manager adapter results in log file errors. The reconciliation process is not completed successfully. The adapter log files contain entries that state `ErmPduAddEntry failed`. The *`WebSphere_install_dir`*`/logs/itim.log` file contains `java.lang.OutOfMemoryError` exceptions. |
| The reconciliation of large numbers of IBM Security Access Manager accounts times out | During the reconciliation of large numbers of IBM Security Access Manager accounts (in the hundreds of thousands or millions), initialization of the reconciliation might take some time. This delay is hardware and performance-tuning dependent. Problems might occur as a result of timeout issues if you have IBM Tivoli Directory Server and DB2®configured against your IBM Security Access Manager Policy Server. Refer to the IBM Tivoli Directory Server user guides for information about configuring the **`ibm-slapdIdleTimeOut`** value in the `ibmslapd.conf` file. As a guideline, this value can be increased to greater than 10,000 for the reconciliation of approximately 5 million accounts. |

*Table 8. Runtime Problems (continued)*

| Problem | Corrective Action |
|---|---|
| A search filter with an asterisk character returns more accounts that expected | A Search Filter can be specified for the IBM Security Access Manager reconciliation query. You can provide an LDAP filter in the Query page to specify a subset of accounts only (no supporting data) to be included in the reconciliation.<br><br>Both the IBM Security Access Manager Administration API and Registry Direct API reconciliation methods support IBM Security Access Manager user account filtering. A subset of user accounts might be required. In this case, a Search Filter can be supplied that conforms to the IBM Security Access Manager pattern that was used to list User accounts.<br><br>For example, a Search Filter to reconcile a subset of IBM Security Access Manager User accounts that include `JaneDoe`, `JonDoe` and `JimDolt` might be: `(eruid=J*Do*)`. The pattern for the **`eruid`** attribute is interpreted as a literal string. The asterisk (*) character, which is interpreted as a metacharacter that matches zero or more characters is the exception. Asterisks can be at the beginning, in the middle, or at the end of the pattern, and the pattern can contain multiple asterisks. |
| Enabling the option **Do not reconcile SSO credentials** removes all credentials IBM Security Identity Manager registry. | Selecting this check box removes any current account credentials from IBM Security Identity Manager registry after first successful reconciliation. The IBM Security Identity Manager considers any non-returned credential to mean that the credential no longer exists for the account.<br><br>However, it is possible to retain any credentials that were reconciled previously by excluding the **`SSO credentials`** attribute from the reconciliation query. |
| The **Test** operation failed. | During a test of the IBM Security Access Manager service, the following message might be observed:<br><br>`CTGIMT605E An error occurred while processing the CTGIMT401E An error occurred while starting the tamTest_TAMCombo on my_server-requestid_4329bac6-28ad-11b2-d8dc-00000930ab5b agent. Error: java.lang.NoClassDefFoundError: com/tivoli/pd/jutil/PDException operation on the IBM Tivoli Directory Integrator server. Error: {1}`<br><br>This error might be because of either of the following reasons:<br>• The IBM Tivoli Directory Integrator JVM is not configured with IBM Security Access Manager.<br>• The Dispatcher was not stopped and restarted to pick up the change.<br><br>Ensure that the IBM Security Access Manager Runtime for Java is installed and configured correctly. Alternatively, restart the Dispatcher as described in the *Dispatcher Installation and Configuration Guide*. |

# Chapter 10. Uninstalling the IBM Security Access Manager Adapter

Uninstalling the adapter requires the removal of the JAR file and the removal of the adapter profile from IBM Security Identity Manager.

## About this task

**Note:** The Dispatcher component must be installed on your system in order for adapters to function correctly in an IBM Tivoli Directory Integrator environment. If you delete the adapter profile for the IBM Security Access Manager Adapter, do not uninstall the Dispatcher.

## Procedure

1. Stop the adapter service.
2. Remove the `TAMComboUtils.jar` file.
3. Start the adapter service.
4. Delete the IBM Security Access Manager profile from IBM Security Identity Manager server. For more specific information about removing a service profile, see the online help or the IBM Security Identity Manager product documentation.

# Appendix A. Reconciliation page size

Page mode causes the directory server to return a specific number of entries in multiple chunks instead of all entries in a single chunk. The chunks are also called pages.

Not all directory servers support this option. Verify whether your directory server supports Page Mode before you use this option.

If your directory service supports Page Mode, use the **SearchResultSetSize** value of the Dispatcher **itim_listener.properties** file for this value.

To locate this value, see the *Dispatcher Installation and Configuration Guide*.

# Appendix B. Enabling last login information

For IBM Security Access Manager version 6.1.1 or above, the adapter now supports reconciling the last login information for determining dormant accounts.

## About this task

To enable this feature, all IBM Security Access Manager servers must be configured to record the last login information. For more information about login information and dormant accounts, see the IBM Security Access Manager documentation.

## Procedure

- In `webseald.conf`, ensure that the following parameter is set:

  ```
  enable-last-login = yes
  ```

- Configure the IBM Security Access Manager Policy Server to return the last login information. For example, in `ivmgrd.conf`, set the following parameter:

  ```
  provide-last-login = yes
  ```

# Appendix C. Performance optimization

Modifying the settings for the Dispatcher, the directory server, reconciliation, and group caching might improve the performance of the system.

## Dispatcher tuning

You can modify the setting on the Dispatcher to optimize the performance.

For reconciling many entries, the following Dispatcher tuning settings are suggested for optimal performance:

- Edit `itim_listener.properties` in the IBM Tivoli Directory Integrator installation directory to set **`SearchResultSetSize`** to a larger value. For example, `SearchResultSetSize=1000`.

  This setting reduces the number of times that IBM Security Identity Manager server must contact the adapter to fetch a subset of entries. Increasing this value causes IBM Security Identity Manager server and the adapter to use more memory during reconciliation. You might also increase the JVM heap size for the Dispatcher and IBM Security Identity Manager server.
- Increase the JVM heap size for Dispatcher. For example, on Windows edit the `ibmdiservice.props` file in the adapter `timsol` directory. Set the following property: `jvmcmdoptions=-Xms1024M –Xmx1024M`

  On UNIX systems, edit the IBM Tivoli Directory Integrator server start script. For example, `/opt/IBM/TDI/V7.1/ibmdirsrv`. Modify the Java command line:

  ```
  "$JRE_PATH/java" -Xms1024M -Xmx1024M -cp "/opt/IBM/TDI/V7.1/jars/3rdparty/
  IBM/db2jcc_license_c.jar" "-Dlog4j.configuration=file:etc/log4j.properties"
  -jar "/opt/IBM/TDI/V7.1/IDILoader.jar" com.ibm.di.server.RS "$@"
  ```

The Dispatcher must be restarted after these changes are made.

See the *Dispatcher Installation and Configuration Guide*.

## Directory server performance tuning

Reconciliations retrieve a large amount of data from the IBM Security Access Manager user registry. The reconciliation performance of IBM Security Access Manager Adapter depends on the performance of the user registry.

To achieve the optimal performance, it is suggested that all documented performance tuning settings for the IBM Security Access Manager user registry be implemented.

For example, for IBM Tivoli Directory Server:

- Increase the **`search result size limit`** to be greater than the total number of entries that are required to be reconciled. For example, edit the `ibmslapd.conf` file to set the following parameter:

  ```
  ibm-slapdSizeLimit: 0
  ```
- Run **`runstat`** to help DB2 optimizer to determine the optimal accesses to the database.
- Run **`reorgchk`** and **`reorg`** to defragment the DB2 table spaces.

- Enable group members cache. If enough memory exists, set the maximum number of groups to the total number of groups. Set the maximum number of members to the number of members of the largest group. The first reconciliation is slower because it populates the cache.

The tests show that applying the preceding performance tuning settings improves the reconciliation performance especially for many users and groups with many members. This document does not describe all the performance tuning parameters for each user registry that is supported by IBM Security Access Manager. Review and configure all performance parameters to improve the general performance of the IBM Security Access Manager environment and any client that relies on it.

See these publications:

- *IBM Tivoli Directory Server: Performance Tuning and Capacity Planning Guide*
- *IBM Tivoli Directory Server: Administration Guide*
- *IBM Security Access Manager: Performance Tuning Guide*
- Vendor-specific documentation for other user registries that are supported by IBM Security Access Manager

## Reconciliation method

Several reconciliation methods exist. Depending on your system, the method that you choose, might affect the performance during reconciliation.

*Table 9. Reconciliation methods*

| IBM Security Access Manager API used | Menu selection |
|---|---|
| Administration API | IBM Security Access Manager Administration API |
| Registry Direct API | IBM Security Access Manager Registry Direct API |

For IBM Security Access Manager 6.1 and later, use **Registry Direct API** when the IBM Security Access Manager user registry is an LDAP server. These factors improve performance:

- Use of the **ibm-allgroups** attribute for IBM Tivoli Directory Server.
- Direct access to the user registry instead of using the IBM Security Access Manager Policy Server.
- Use of multiple directory server replicas.

## Group cache

Enabling the group cache for **Registry Direct API** reconciliation results in some performance improvement when there are many users and many small or empty groups.

When there are few groups or when the group cache is used within IBM Tivoli Directory Server, the benefit of using the adapter group cache is negligible. In addition, when there are groups with many members (for example, over 50000) using the group cache can negatively affect the reconciliation performance. The cache must be repopulated at the start of each reconciliation.

The group cache stores an internal representation of all users' group membership information. It requires a significant amount of memory. For 1 million users each belonging to 100 groups, approximately 1 GB of extra memory and JVM heap might be required for the adapter.

# Appendix D. High availability support

Support for high availability is provided by the Access Manager Registry Direct API, which eliminates the dependency on the IBM Security Access Manager policy server.

You can configure the Registry Direct API against multiple directory servers for failover as well as load balancing. Due to limitations in Registry Direct API, high availability is not supported for:

- Active Directory and Domino user registries
- IBM Security Access Manager Adapter versions older than version 6.1 fix pack 6
- GSO management, including the lifecycle management of GSO enabled accounts

For more information about configuring Registry Direct API, see Appendix D that describes Registry Direct Java API installation and configuration in version 6.1.1 of the *IBM Tivoli Access Manager for e-business: Authorization Java Classes Developer Reference*.

# Appendix E. Definitions for ITDI_HOME and ISIM_HOME directories

*ITDI_HOME* is the directory where Tivoli Directory Integrator is installed.
*ISIM_HOME* is the directory where IBM Security Identity Manager is installed.

*ITDI_HOME*

This directory contains the jars/connectors subdirectory that contains files for the adapters.

**Windows**

*drive*\Program Files\IBM\TDI*ITDI_VERSION*

For example the path for version 7.1:

C:\Program Files\IBM\TDI\V7.1

**UNIX**

/opt/IBM/TDI/*ITDI_VERSION*

For example the path for version 7.1:

/opt/IBM/TDI/V7.1

*ISIM_HOME*

This directory is the base directory that contains the IBM Security Identity Manager code, configuration, and documentation.

**Windows**

*path*\IBM\isim

**UNIX**

*path*/IBM/isim

# Appendix F. Support information

You have several options to obtain support for IBM products.



## Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

### About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

### Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).

   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
2. Find the content that you need by using the IBM Support Portal.

   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports).
   - IBM Security Identity Manager Support website.
   - IBM Redbooks®.
   - IBM support communities (forums and newsgroups).
4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.
5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to

include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

**Tip:** Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

## Obtaining a product fix

A product fix might be available to resolve your problem.

### About this task

You can get fixes by following these steps:

### Procedure

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the *Fix Central Site*. See http://www.ibm.com/support/fixcentral/.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.

## Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

### Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

### Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):

     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.

     a. Download and install the ISA tool from the ISA website. See http://www.ibm.com/software/support/isa/.
     b. Open ISA.

c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.

- Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

## Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

# Appendix G. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

## Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

## Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

## Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

## IBM and accessibility

See the IBM Human Ability and Accessibility Center For more information about the commitment that IBM has to accessibility.

# 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.

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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
2Z4A/101
11400 Burnet Road
Austin, TX 78758 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.

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 measurement 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. 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 IBM's application programming interfaces.

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

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

© (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 in softcopy form, the photographs and color illustrations might not be displayed.

## Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a 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.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.


Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

## Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled "Cookies, Web Beacons and Other Technologies and Software Products and Software-as-a Service".

# Index

## R



## S



## T



## U



## V



## W

Printed in USA

SC27-4421-02