IBM Security Identity Manager
Version 6.0

IBM DB2 Adapter Installation and Configuration Guide

SC27-5601-01

IBM Security Identity Manager
Version 6.0

IBM DB2 Adapter Installation and Configuration Guide

SC27-5601-01

Note
Before using this information and the product it supports, read the information in "Notices" on page 45.

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 DB2 Adapter Installation and Configuration Guide* provides the basic information that you can use to install and configure the IBM® Security Identity Manager IBM DB2 Adapter. The adapter enables connectivity between the IBM Security Identity Manager server and the managed resource.

IBM Security Identity Manager was previously known as Tivoli® Identity Manager.

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 D, "Support information," on page 39 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.

Chapter 1. Overview of the adapter

The IBM DB2 Adapter enables communication between the IBM Security Identity Manager server and the IBM DB2 (IBM DB2).

An adapter provides an interface between a managed resource and the IBM Security Identity Manager server. Adapters might reside on the managed resource. 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 platform. They perform tasks, such as creating, suspending, and restoring user accounts, and other administrative functions that are performed manually. The adapter runs as a service, independently of whether you are logged on to the IBM Security Identity Manager server.

Features of the adapter

The adapter automates the following user account management tasks.

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Suspending, restoring, and deleting user accounts

Architecture of the adapter

You must install the following components for the adapter to function correctly:

- Dispatcher
- Tivoli Directory Integrator connector
- IBM Security Identity Manager adapter profile

You need to install the Dispatcher and the adapter profile; however, the Tivoli Directory Integrator connector might already be installed with the base Tivoli Directory Integrator product.

Figure 1 describes the components that work together to complete the user account management tasks in a Tivoli Directory Integrator environment.

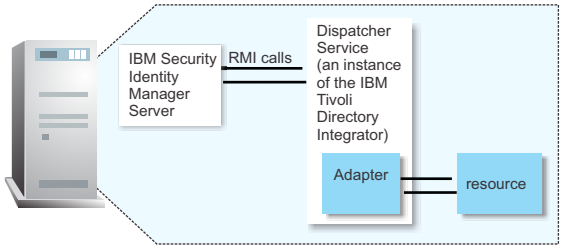

Figure 1. The architecture of the IBM DB2 Adapter

For more information about Tivoli Directory Integrator, see the *Quick Start Guide* in the IBM Security Identity Manager product documentation.

Supported configurations

There are two ways to configure the IBM DB2 Adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

There are fundamental components in each environment:

- The IBM Security Identity Manager server
- The IBM Tivoli Directory Integrator server
- The managed resource
- The adapter

The adapter must be installed directly on the server that runs the Tivoli Directory Integrator server.

Single server configuration

The IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the IBM DB2 Adapter are installed on one server to establish communication with the managed resource. The managed resource is installed on a different server as described Figure 2.

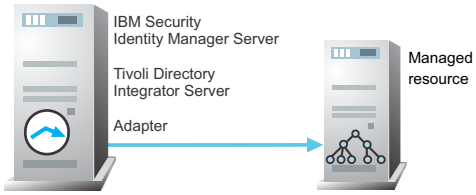

Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the IBM DB2 are installed on different servers. The Tivoli Directory Integrator server and the IBM DB2 Adapter are installed on the same server as described in Figure 3.

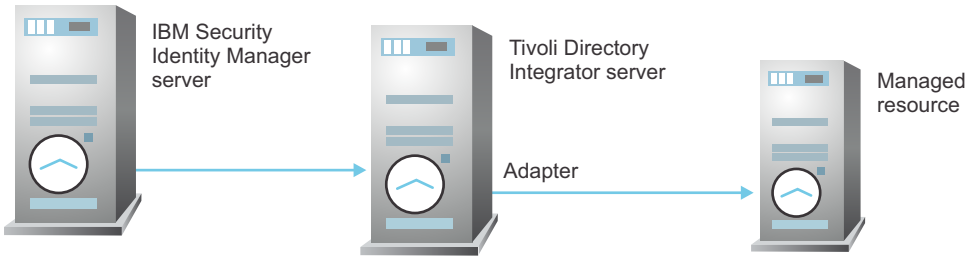

Figure 3. Example of multiple server configuration

Chapter 2. Adapter installation planning

Installing and configuring the adapter involves several steps that you must complete in the appropriate sequence.

Review the roadmaps before you begin the installation process.

Preinstallation roadmap

Before you install the adapter, you must prepare the environment.

Prepare the environment by doing the tasks that are listed in Table 1.

Table 1. Preinstallation roadmap

Task	For more information
Obtain the installation software.	Download the software from Passport Advantage® website. See "Software download" on page 6.
Verify that your environment meets the software and hardware requirements for the adapter.	See "Prerequisites" on page 4.
Obtain and install the Dispatcher.	Download the software from Passport Advantage website. See "Software download" on page 6. Follow the installation instructions in the dispatcher download package.
Obtain the necessary information for the installation and configuration.	See "Installation worksheet for the adapter" on page 5.

Installation roadmap

To install the adapter, complete the tasks that are described in the roadmap.

Table 2. Installation roadmap

Task	For more information
Verify the Dispatcher installation.	See "Dispatcher installation verification" on page 7.
Install the adapter.	See "Installing the adapter" on page 7.
Import the adapter profile.	See "Importing the adapter profile into the IBM Security Identity Manager server" on page 8.
Verify the profile installation.	See "Adapter profile installation verification" on page 9.
Create an adapter user account.	See "Adapter user account creation" on page 9.
Create a service.	See "Creating an adapter service" on page 10.
Configure the adapter.	See "Adapter configuration" on page 13.

Prerequisites

Verify that your environment meets all the prerequisites before you install the adapter.

Table 3 identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the IBM Tivoli Directory Integrator server.

Table 3. Prerequisites to install the adapter

Prerequisite	Description
Tivoli Directory Integrator server	• Version 7.1 fix pack 5 or later • Version 7.1.1
IBM Security Identity Manager server	Version 6.0
IBM DB2	A system that runs the IBM DB2 with one of following versions: • IBM DB2 v9.5.x • IBM DB2 v9.7.x • IBM DB2 v10.1 • IBM DB2 v10.5
IBM DB2 JDBC Driver	JDBC Driver **Note:** The driver file names are: • `db2jcc.jar` • `db2jcc_license_cu.jar`
Network Connectivity	Install the adapter on a workstation that can communicate with the IBM Security Identity Manager service through the TCP/IP network.
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.
Tivoli Directory Integrator adapters solution directory	A Tivoli Directory Integrator adapters solution directory is a Tivoli Directory Integrator work directory for IBM Security Identity Manager adapters. See the *Dispatcher Installation and Configuration Guide*.
IBM DB2 Account, for example `db2admin`.	You must provide a IBM DB2 account and password for every IBM DB2 instance that the adapter manages. The IBM DB2 account must have the following IBM DB2 privileges: **DBADM** Database administrator authority **SECADM** Security administrator authority

Install the IBM DB2 Adapter and the appropriate IBM DB2 JDBC drivers on the same workstation as the Tivoli Directory Integrator.

For information about the prerequisites and supported operating systems for Tivoli Directory Integrator, see the *IBM Tivoli Directory Integrator 7.1: Administrator Guide*.

Installation worksheet for the adapter

The installation worksheet identifies the information that you need before installing the adapter.

Table 4. Required information to install the adapter

Required information	Description	Value

IBM Tivoli Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Tivoli Directory Integrator is automatically installed with your IBM Security Identity Manager product, the default directory path for Tivoli Directory Integrator is as follows:
		
		Windows:
		• For version 7.1:
		`drive\Program Files\IBM\TDI\V7.1`
		• For version 7.1.1
		`drive\Program Files\IBM\TDI\V7.1.1`
		
		UNIX:
		• For version 7.1:
		`/opt/IBM/TDI/V7.1`
		• For version 7.1.1:
		`/opt/IBM/TDI/V7.1.1`

Adapters solution directory	When you install the dispatcher, the adapter prompts you to specify a file path for the adapters solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at:
		
		Windows
		• For version 7.1:
		`drive\Program Files\IBM\TDI\V7.1\isimsoln`
		• For version 7.1.1:
		`drive\Program Files\IBM\TDI\V7.1.1\isimsoln`
		
		UNIX:
		• For version 7.1:
		`/opt/IBM/TDI/V7.1/isimsoln`
		• For version 7.1.1:
		`/opt/IBM/TDI/V7.1.1/isimsoln`

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. Adapter installation

All the adapters that are based on Tivoli Directory Integrator require the Dispatcher for the adapters to function correctly.

If the Dispatcher is installed from a previous installation, do not reinstall it unless there is an upgrade to the Dispatcher. See "Dispatcher installation verification."

After verifying the Dispatcher installation, you might install the Tivoli Directory Integrator connector. Depending on your adapter, the connector might already be installed as part of the Tivoli Directory Integrator product and no further action is required.

Dispatcher installation verification

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

You must install the dispatcher on the same Tivoli Directory Integrator server where you want to install the adapter.

Obtain the dispatcher installer from the IBM Passport Advantage website, http://ww.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm. For information about Dispatcher installation, see the *Dispatcher Installation and Configuration Guide*.

Installing the adapter

Take these steps to install the adapter.

Before you begin

Ensure that you do the following tasks:

- Verify that your site meets all the prerequisite requirements. See "Prerequisites" on page 4.
- Obtain a copy of the installation software. See "Software download" on page 6.
- Obtain system administrator authority. See "Prerequisites" on page 4.

About this task

The adapter uses the IBM Tivoli Directory Integrator JDBC connector. This connector is available with the base Tivoli Directory Integrator product. Because the Tivoli Directory Integrator JDBC connector is already installed, you need to install only the Dispatcher. See "Dispatcher installation verification."

To install the Dispatcher, see the *IBM Security Dispatcher Installation and Configuration Guide*.

What to do next

After you finish the adapter installation, do the following tasks:

1. Import the adapter profile. See "Importing the adapter profile into the IBM Security Identity Manager server."
2. Create a user account for the adapter on IBM Security Identity Manager. See "Adapter user account creation" on page 9.

IBM DB2 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

You can create a service on the IBM Security Identity Manager server and establish communication with the adapter.

Before you begin

Before you can create an adapter service, the IBM Security Identity Manager server must have an adapter profile to recognize the adapter. The files that are packaged with the adapter include the adapter profile JAR file. You can import the adapter profile as a service profile on the server with the Import feature of IBM Security Identity Manager.

The JAR file includes all the files that are required to define the adapter schema, account form, service form, and profile properties. You can extract the files from the JAR file to modify the necessary files and package the JAR file with the updated files.

Before you begin to 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 IBM Security Identity Manager.

About this task

An adapter profile defines the types of resources that the IBM Security Identity Manager server can manage. Use the profile to create an adapter service on IBM Security Identity Manager server and establish communication with the adapter.

To import the adapter profile, take the following steps:

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to do administrative tasks.
2. In the My Work pane, expand **Configure System** and click **Manage Service Types**.

3. On the Manage Service Types page, click **Import** to display the Import Service Types page.
4. Specify the location of the JAR file in the **Service Definition File** field by doing one of the following tasks:
   - Type the complete location of where the file is stored.
   - Use **Browse** to navigate to the file.
5. Click **OK**.

   Note: If you import the adapter profile and receive an error that is related to the schema, see 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.
6. Restart IBM Security Identity Manager for the change to take effect.

Adapter profile installation verification

After you install the adapter profile, verify that the installation was successful.

An unsuccessful installation:

- Might cause the adapter to function incorrectly.
- Prevents you from creating a service with the adapter profile.

To verify that the adapter profile is successfully installed, create a service with the adapter profile. For more information about creating a service, see "Creating an adapter service" on page 10.

If you are unable to create a service with the adapter profile or open an account on the service, the adapter profile is not installed correctly. You must import the adapter profile again.

Adapter user account creation

You must create a user account for the adapter on the managed resource. Provide the account information when you create a service for the adapter on IBM Security Identity Manager.

For more information about creating a service, see "Creating an adapter service" on page 10.

The accounts must be able to remotely connect to the IBM DB2 and must have sufficient privileges to administer IBM DB2 users. Table 5 lists the required privileges that the user account must have to administer IBM DB2 users.

Table 5. Required privileges and their descriptions

Privilege	Description
DBADM	Database administrator authority
SEDADM	Security administrator authority

Creating an adapter 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 perform 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 DB2 Adapter Service Profile**.
4. Click **Next** to display the adapter service form.
5. Complete the following fields on the service form:

   On the IBM DB2 Connection tab:

   Service name
   Specify a name that defines the adapter service on the IBM Security Identity Manager server.

   Note: Do not use forward (/) or backward slashes (\) in the service name.

   Description
   Optional: Specify a description that identifies the service for your environment.

   Tivoli Directory Integrator location
   Specify the URL for the IBM Tivoli Directory Integrator instance. The valid syntax for the URL is:

   `rmi://ip-address:port/ITDIDispatcher`

   where:

   ip-address
   The Tivoli Directory Integrator host.

   port The port number for the Dispatcher.

   The default URL is

   `rmi://localhost:1099/ITDIDispatcher`

   For information about changing the port number, see *IBM Security Dispatcher Installation and Configuration Guide*.

   IBM DB2 Server Host
   Specify the host workstation on which the IBM DB2 server is running.

   IBM DB2 Server Port
   Specify the TCP port on which the IBM DB2 server is running. You can specify 50000 to use the default DB2 port.

IBM DB2 Database Name
Specify the database name of the IBM DB2 database that you want to manage, for example SAMPLE.

IBM DB2 Administration User Account
Specify the name of the user who has access to the IBM DB2 resource and who can do administrative operations.

IBM DB2 Administration User Password
Specify the password for the user.

Owner
Optionally, specify a IBM Security Identity Manager user as a service owner.

Service Prerequisite
Specify a IBM Security Identity Manager service that is prerequisite to this service.

On the 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, modify, delete, and test operations are not cached.

AL File System 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:\Files\IBM\TDI\V7.1\profiles`.
Alternatively, you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system: 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` if you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

On the Status and information tab
This 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 is 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. Verify parameters such as the work station name or the IP address of the managed resource and the port.

6. Click **Finish**.

Chapter 4. First steps after installation

After you install the adapter, you must do several other tasks. The tasks include configuring the adapter, setting up SSL, installing the language pack, and verifying that the adapter works correctly.

Adapter configuration

You can use the configuration options for the IBM DB2 Adapter.

- "Customizing the adapter profile"
- "Editing adapter profiles on the UNIX or Linux operating system" on page 14

See the *IBM Security Dispatcher Installation and Configuration Guide* for more configuration options such as:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

Customizing the adapter profile

To customize the adapter profile, you must modify the IBM DB2 Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

About this task

You can also use the Form Designer or the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file for that adapter.

The JAR file is included in the IBM DB2 Adapter compressed file that you downloaded from the IBM website. The JAR file and the files that are contained in the JAR file vary depending on your operating system.

Note: You cannot modify the schema for this adapter. You cannot add or delete attributes from the schema.

The adapter JAR file includes the following files:

- `CustomLabels.properties`
- `erDB2Account.xml`
- `erDB2Service.xml`
- `schema.dsml`
- `service.def`
- `DB2AddUserAL.xml`
- `DB2DeleteUserAL.xml`
- `DB2ModifyUserAL.xml`

- DB2RestoreUserAL.xml
- DB2SearchUserAL.xml
- DB2SuspendUserAL.xml
- DB2TestAL.xml

Procedure

- To edit the JAR file, take these steps:
  1. Log on to the workstation where the IBM DB2 Adapter is installed.
  2. On the **Start** menu, click **Programs → Accessories → Command Prompt**.
  3. Copy the JAR file into a temporary directory.
  4. Extract the contents of the JAR file into the temporary directory by running the following command. The following example applies to the IBM DB2 Adapter profile. Type the name of the JAR file for your operating system.

     ```
     cd c:\temp
     jar -xvf DB2AdapterProfile.jar
     ```

     The **jar** command extracts the files into the directory.
  5. Edit the file that you want to change

     After you edit the file, you must import the file into the IBM Security Identity Manager server for the changes to take effect.
- To import the file, take these steps:
  1. Create a JAR file by using the files in the \temp directory. Run the following commands:

     ```
     cd c:\temp
     jar -cvf DB2AdapterProfile.jar DB2AdapterProfile
     ```
  2. Import the JAR file into the IBM Security Identity Manager application server. See "Importing the adapter profile into the IBM Security Identity Manager server" on page 8.
  3. Stop and start the IBM Security Identity Manager server.
  4. Stop and start the IBM DB2 Adapter service. See "IBM DB2 Adapter service start, stop, and restart" on page 8,

Editing adapter profiles on the UNIX or Linux operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the ^M characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the ^M characters. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter `^M` or `Ctrl-M` by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as command.

Verifying that the adapter is working correctly

After you install and configure the adapter, take steps to verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on IBM Security Identity Manager.
2. Run a full reconciliation from IBM Security Identity Manager.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the IBM Security Identity Manager log file `trace.log` to ensure that no errors are reported when you run an adapter operation.

Chapter 5. Adapter error troubleshooting

Troubleshooting can help you determine why a product does not function properly.

Use this information and techniques to identify and resolve problems with the adapter. They also provide information about troubleshooting errors that might occur during the adapter installation.

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 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?
- Must a certain sequence of events take place 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. Multiple problems might happen around the same time, but 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 D, "Support information," on page 39.

Warning and error messages

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

A warning or error might be displayed in the user interface to provide information that you must know about the adapter or about an error. Table 6 contains warnings or errors that might be displayed in the user interface if the IBM DB2 Adapter is installed on your system.

Table 6. Warning and error messages

Message code	Warning or error message	Remedial action
CTGIMT001E	The following error occurred. Error: Either the IBM DB2 service name is incorrect or the service is not up.	Ensure that the IBM DB2 service name given on IBM Security Identity Manager service form is running.
CTGIMT001E	The following error occurred. Error: Either the IBM DB2 host or port is incorrect.	Verify that the host workstation name or the port for the IBM DB2 service is correctly specified.
CTGIMT002E	The login credential is missing or incorrect.	Verify that you provided correct login credential on service form.
CTGIMT001E	The following error occurred. Error: No suitable JDBC driver found.	Ensure that the correct version of the JDBC driver is copied onto the workstation where the adapter is installed. Ensure that the path for the driver is included in the system CLASSPATH variable.
CTGIMT600E	An error occurred while establishing communication with the IBM Tivoli Directory Integrator server.	IBM Security Identity Manager cannot establish a connection with IBM Tivoli Directory Integrator. To fix this problem, ensure that: • IBM Tivoli Directory Integrator is running. • The URL specified on the service form for the IBM Tivoli Directory Integrator is correct.
CTGIMT004E	The adapter does not have permission to add an account: *Account_Name*.	The administrator user that is provided on the IBM Tivoli Directory Integrator service form does not have the required privileges to add a user account. Ensure that an administrator user with the required privileges is specified on service form. These privileges are the minimum that are required for the administrator user: • DBADM - database administrator authority • SECADM - security administrator authority
CTGIMT003E	The account already exists.	Use a different name for the user to be added.

Table 6. Warning and error messages (continued)

Message code	Warning or error message	Remedial action
CTGIMT015E	An error occurred while deleting the *Account_Name* account because the account does not exist.	The user you trying to delete does not exist. Ensure that you are deleting only an existing account.

Chapter 6. Adapter upgrade

You can upgrade the adapter by installing the new version of the adapter.

Upgrading the adapter might also involve more tasks, such as upgrading the connector, the dispatcher, and the existing adapter profile. To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, "Adapter installation," on page 7.

Dispatcher upgrade

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.

Note: Stop the dispatcher service before the upgrading the dispatcher and start it again after the upgrade is complete.

Upgrade of an existing adapter profile

Read the adapter Release Notes for any specific instructions before you import a new adapter profile into IBM Security Identity Manager.

See "Importing the adapter profile into the IBM Security Identity Manager server" on page 8.

Note: Restart the dispatcher service after you import the profile. Restarting the dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

Chapter 7. Adapter uninstallation

To completely uninstall the IBM DB2 Adapter, you need to remove the adapter profile from the IBM Security Identity Manager server.

Adapter profile removal from the IBM Security Identity Manager server

Before you remove the adapter profile, ensure that no objects exist on your IBM Security Identity Manager server that reference the adapter profile.

Objects on the IBM Security Identity Manager server can reference the adapter profile:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

Note: The Dispatcher component must be installed on your system for adapters to function correctly in a Tivoli Directory Integrator environment. When you delete the adapter profile for the IBM DB2 Adapter, do not uninstall the Dispatcher.

For specific information about how to remove the adapter profile, see the online help or the IBM Security Identity Manager product documentation.

Chapter 8. Adapter reinstallation

There are no special considerations for reinstalling the adapter. You are not required to remove the adapter before reinstalling.

For more information, see Chapter 6, “Adapter upgrade,” on page 21.

Appendix A. Adapter attributes

As part of the adapter implementation, a dedicated account that allows IBM Security Identity Manager to access the IBM DB2 is created on the IBM DB2.

The adapter consists of files and directories that are owned by the IBM Security Identity Manager account. These files establish communication with the IBM Security Identity Manager server.

Attribute descriptions

The IBM Security Identity Manager server communicates with the adapter by using attributes in transmission packets that are sent over a network.

The combination of attributes depends on the type of action that the IBM Security Identity Manager server requests from the adapter.

Table 7 lists the account form attributes that the adapter uses.

Table 7. Attributes, descriptions, and corresponding data types

Attribute	Directory server attribute	Description	Data format
Administration User Account	erRmiUDBAdminName	Specify the user ID that is used to connect to the IBM DB2. The value of this key must be the administrator user of the cataloged database. Administration User Account is the required field.	String
Administration User Password	erServicePwd1	Specify the password for the user ID that is used to connect to the IBM DB2. The value of this key must be the password of the administrator user of the cataloged database. Administration User Password is the required field.	String
IndexName	erRmiUDBIndexName	Specifies the name of the index.	String
PrivAlterinSchema	erRmiUDBPrivAlterinSchema	Specifies all schemas on which the privilege to alter objects in the schema is granted to the user. It is multivalued.	String

Table 7. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivAlterinSchemaWGr	erRmiUDBPrivWGrAlterinSchema	Specifies all schemas on which the privilege to alter objects in the schema with grant option is granted to the user. It is multivalued.	String
PrivAlterTab	erRmiUDBPrivAlterTab	Specifies all tables on which the alter privilege is granted to the user. It is multivalued.	String
PrivControlIndex	erRmiUDBPrivIndexControl	Specifies all indexes on which the control privilege is granted to the user. It is multivalued.	String
PrivControlView	erRmiUDBPrivViewControl	Specifies all views on which the control privilege is granted to the user. It is multivalued	String
PrivCreateinSchema	erRmiUDBPrivCreateinSchema	Specifies all schemas on which the privilege to create objects in the schema is granted to the user. It is multivalued.	String
PrivCreateinSchemaWGr	erRmiUDBPrivWGrCreateinSchema	Specifies all schemas on which the privilege to create objects in the schema with grant option is granted to the user. It is multivalued.	String
PrivDatabase	erRmiUDBPrivDatabase	Specifies the database authorities and privileges that are granted to the user. It is multivalued.	String
PrivDeleteTab	erRmiUDBPrivDeleteTab	Specifies all tables on which the delete privilege is granted to the user. It is multivalued.	String
PrivDeleteTabWGr	erRmiUDBPrivWGrDeleteTab	Specifies all tables on which the delete privilege with grant option is granted to the user. It is multivalued.	String
PrivDeleteView	erRmiUDBPrivDeleteView	Specifies all views on which the delete privilege is granted to the user. It is multivalued.	String

Table 7. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivDeleteViewWGr	erRmiUDBPrivWGrVwDeleteView	Specifies all views on which the delete privilege with grant option is granted to the user. It is multivalued.	String
PrivDropinSchema	erRmiUDBPrivDropinSchema	Specifies all schemas on which the privilege to drop objects in the schema is granted to the user. It is multivalued.	String
PrivDropinSchemaWGr	erRmiUDBPrivWGrDropinSchema	Specifies all schemas on which the privilege to drop objects in the schema with grant option is granted to the user. It is multivalued.	String
PrivIndexTab	erRmiUDBPrivIndexTab	Specifies all tables on which the index privilege is granted to the user. It is multivalued.	String
PrivIndexTabWGr	erRmiUDBPrivWGrIndexTab	Specifies all tables on which the index privilege with grant option is granted to the user. It is multivalued.	String
PrivInsertTab	erRmiUDBPrivInsertTab	Specifies all tables on which the insert privilege is granted to the user. It is multivalued.	String
PrivInsertTabWGr	erRmiUDBPrivWGrInsertTab	Specifies all tables on which the insert privilege with grant option is granted to the user. It is multivalued.	String
PrivInsertView	erRmiUDBPrivInsertView	Specifies all views on which the insert privilege is granted to the user. It is multivalued	String
PrivInsertViewWGr	erRmiUDBPrivWGrVwInsertView	Specifies all views on which the insert privilege with grant option is granted to the user. It is multivalued.	String
PrivRefTab	erRmiUDBPrivRefTab	Specifies all tables on which the reference privilege is granted to the user. It is multivalued.	String

Table 7. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivRefTabWGr	erRmiUDBPrivWGrRefTab	Specifies all tables on which the reference privilege with grant option is granted to the user. It is multivalued.	String
PrivSelectTab	erRmiUDBPrivSelectTab	Specifies all tables on which the select privilege is granted to the user. It is multivalued.	String
PrivSelectTabWGr	erRmiUDBPrivWGrSelectTab	Specifies all tables on which the select privilege with grant option is granted to the user. It is multivalued.	String
PrivSelectView	erRmiUDBPrivSelectView	Specifies all views on which the select privilege is granted to the user. It is multivalued.	String
PrivSelectViewWGr	erRmiUDBPrivWGrVwSelectView	Specifies all views on which the select privilege with grant option is granted to the user. It is multivalued.	String
PrivUpdateTab	erRmiUDBPrivUpdateTab	Specifies all tables on which the update privilege is granted to the user. It is multivalued.	String
PrivUpdateTabWGr	erRmiUDBPrivWGrUpdateTab	Specifies all tables on which the update privilege with grant option is granted to the user. It is multivalued.	String
PrivUpdateView	erRmiUDBPrivUpdateView	Specifies all views on which the update privilege is granted to the user. It is multivalued.	String
PrivUpdateViewWGr	erRmiUDBPrivWGrVwUpdateView	Specifies all views on which the update privilege with grant option is granted to the user. It is multivalued.	String
PrivUseTabSpace	erRmiUDBPrivUseTabSpace	Specifies all table spaces on which the use privilege is granted to the user. It is multivalued.	String

Table 7. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
PrivUseTabSpaceWGr	erRmiUDBPrivWGrUseTabSpace	Specifies all table spaces on which the use privilege with grant option is granted to the user. It is multivalued.	String
SchemaName	erRmiUDBSchemaName	Specifies the name of the schema.	String
TableName	erRmiUDBTableName	Specifies the name of the table.	String
TabSpaceName	erRmiUDBTabSpaceName	Specifies the name of the table space.	String
UserName	erUid	Specifies the name of the user to be managed.	String
UserStatus	erAccountStatus	Specifies whether a user account is suspended.	String
ViewName	erRmiUDBViewName	Specifies the name of the view.	String
Roles	erRmiUDBPrivRole	Specifies the Role that is assigned to the user.	String

IBM DB2 adapter attributes by action

The following lists describe typical adapter actions that are organized by their functional transaction group. The lists include more information about required and optional attributes that are sent to the adapter to complete that action.

Database login add

A database login add is a request to create a user account with the specified attributes.

Table 8. Add request attributes

Required attribute	Optional attribute	
erUid	erRmiUDBPrivWGrVwUpdateView	erRmiUDBPrivWGrVwSelectView
	erRmiUDBPrivCreateinSchema	erRmiUDBPrivInsertView
	erRmiUDBPrivWGrCreateinSchema	erRmiUDBPrivWGrVwInsertView
	erRmiUDBPrivAlterinSchema	erRmiUDBPrivUpdateView
	erRmiUDBPrivWGrAlterinSchema	erRmiUDBPrivInsertTab
	erRmiUDBPrivDropinSchema	erRmiUDBPrivWGrInsertTab
	erRmiUDBPrivWGrDropinSchema	erRmiUDBPrivDatabase
	erRmiUDBPrivSelectTab	erRmiUDBPrivDeleteView
	erRmiUDBPrivWGrSelectTab	erRmiUDBPrivWGrVwDeleteView
	erRmiUDBPrivDeleteTab	erRmiUDBPrivViewControl
	erRmiUDBPrivRole	erRmiUDBPrivUseTabSpace
	erRmiUDBPrivWGrIndexTab	erRmiUDBPrivWGrUseTabSpace
	erRmiUDBPrivRefTab	erRmiUDBPrivIndexTab
	erRmiUDBPrivWGrRefTab	erRmiUDBPrivAlterTab
	erRmiUDBPrivIndexControl	erRmiUDBPrivUpdateTab
	erRmiUDBPrivSelectView	erRmiUDBPrivWGrUpdateTab
		erRmiUDBPrivWGrDeleteTab

Database login change

A database login change is a request to change one or more attributes for the specified users.

Table 9. Change request attributes

Required attribute	Optional attribute	
erUid	erRmiUDBPrivDatabase	erRmiUDBPrivWGrInsertTab
	erRmiUDBPrivCreateinSchema	erRmiUDBPrivWGrUseTabSpace
	erRmiUDBPrivWGrCreateinSchema	erRmiUDBPrivInsertView
	erRmiUDBPrivAlterinSchema	erRmiUDBPrivWGrVwInsertView
	erRmiUDBPrivWGrAlterinSchema	erRmiUDBPrivUpdateTab
	erRmiUDBPrivDropinSchema	erRmiUDBPrivWGrUpdateTab
	erRmiUDBPrivWGrDropinSchema	erRmiUDBPrivDeleteTab
	erRmiUDBPrivSelectTab	erRmiUDBPrivWGrDeleteTab
	erRmiUDBPrivWGrSelectTab	erRmiUDBPrivAlterTab
	erRmiUDBPrivWGrVwUpdateView	erRmiUDBPrivIndexTab
	erRmiUDBPrivRole	erRmiUDBPrivWGrIndexTab
	erRmiUDBPrivSelectView	erRmiUDBPrivRefTab
	erRmiUDBPrivWGrVwSelectView	erRmiUDBPrivWGrRefTab
	erRmiUDBPrivDeleteView	erRmiUDBPrivIndexControl
	erRmiUDBPrivWGrVwDeleteView	erRmiUDBPrivUpdateView
	erRmiUDBPrivViewControl	
	erRmiUDBPrivUseTabSpace	
	erRmiUDBPrivInsertTab	

Database login delete

A database login delete is a request to remove the specified user from the directory.

Table 10. Delete request attributes

Required attribute	Optional attribute
erUid	None

Database login suspend

A database login suspend is a request to disable a user account.

The user is not removed. User attributes are not modified.

Table 11. Suspend request attributes

Required attribute	Optional attribute
erUid erAccountStatus	None

Database login restore

A database login restore is a request to activate a user account that was previously suspended.

After an account is restored, the user can access the system by using the same attributes as the ones before the Suspend function was called.

Table 12. Restore attributes

Required attribute	Optional attribute
erUid erAccountStatus	None

Ping

Use Ping to verify connection between the adapter and the IBM Security Identity Manager server. Ping does not require any variables.

Table 13. Ping attributes

Required attribute	Optional attribute
None	None

Reconciliation

The reconciliation function synchronizes user account information between IBM Security Identity Manager and the adapter.

Table 14. Reconciliation attributes

Attribute
All supported attributes

Appendix B. Adapter installation on a zOS operating system

To install the adapters on the zOS UNIX file system, you must install the Dispatcher. The adapter uses the Tivoli Directory Integrator JDBC connector that is available with the base Tivoli Directory Integrator product.

For information about installing the Dispatcher, see the *Tivoli Directory Integrator Dispatcher Installation and Configuration Guide*.

After the installation of the adapter is complete, verify the startup and shutdown of the adapter. For more detailed instructions, see"IBM DB2 Adapter service start, stop, and restart" on page 8.

Appendix C. 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 D. 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 E. 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

U

V

W

Printed in USA

SC27-5601-01