IBM Security Identity Manager
Version 6.0

Salesforce.com Adapter Installation and Configuration Guide

SC27-4413-01

IBM Security Identity Manager
Version 6.0

Salesforce.com Adapter Installation and Configuration Guide

SC27-4413-01

Contents

Figures

Tables

Preface

About this book

This installation guide provides the basic information that you need to install and configure the IBM IBM® Security Identity Manager Salesforce.com Adapter.

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

The adapter enables connectivity between the IBM Security Identity Manager server and the managed resource.

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" on page x.

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation see the IBM Security Identity Manager Information Center.

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 Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm site displays the information center welcome page for this product.

IBM Security Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Security Systems Documentation Central and Welcome page
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product documentation and links to the product information center for specific versions of each product.

Welcome to IBM Security Systems Information Centers provides and introduction to, links to, and general information about IBM Security Systems information centers.

IBM Publications Center
The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site 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 45 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

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.

The Salesforce.com Adapter enables communication between the IBM Security Identity Manager server and the Salesforce.com server.

Features of the adapter

The adapter automates the following user account management tasks:

- Creating user accounts in Salesforce.com.

  Use the adapter to add, modify, or delete the user accounts.
- Assigning roles to users

  Use the adapter to assign or unassign roles to the users.
- Assigning profiles to users

  Use the adapter to assign or unassign profiles to the users.
- Reconciling user account information

  Use the adapter to reconcile information from the managed resource to IBM Security Identity Manager for synchronization.
- Reconciling support data

  Use the adapter to reconcile support data.
- Suspending and restoring users.

  Use the adapter to suspend users or restore users.

Architecture of the adapter

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

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

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

Figure 1 on page 2 describes the components that work together to complete the user account management tasks in a Tivoli Directory Integrator environment.

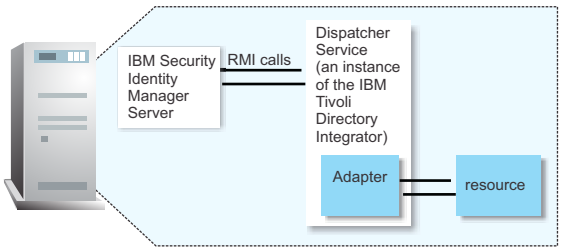

Figure 1. The architecture of the Salesforce.com Adapter

For more information about Tivoli Directory Integrator, see the *Quick Start Guide* at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm.

Supported configurations

The fundamental components in each environment are:

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

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

Single server configuration

In a single server configuration, install the IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the Salesforce.com Adapter on one server to establish communication with Salesforce.com. The Salesforce.com server is on the Internet as described in Figure 2.

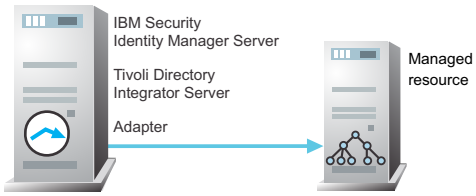

Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the IBM Security Identity Manager server, the Tivoli Directory Integrator server, and the Salesforce.com Adapter, are installed on different servers. Install the Tivoli Directory Integrator server and the Salesforce.com Adapter on the same server as described Figure 3 on page 3.

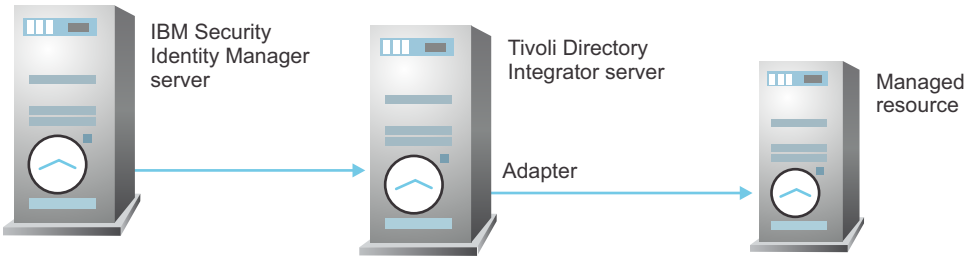

Figure 3. Example of multiple server configuration

Chapter 2. Planning to install the adapter

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

Preinstallation road map

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

Perform the tasks that are listed in Table 1.

Table 1. Preinstallation road map

Task	For more information
Obtain the installation software.	Download the software from Passport Advantage® website. See "Downloading the software" on page 6.
Verify that your environment meets the software and hardware requirements for the adapter.	See "Prerequisites" on page 4 and "Prerequisites for running the connector" on page 5.
Obtain the necessary information for the installation and configuration.	See "Installation worksheet for the adapter" on page 5.
Export and import the Salesforce.com SSL certificate.	See "Exporting and importing the Salesforce.com SSL certificate" on page 7.

Installation road map

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

Table 2. Installation roadmap

Task	For more information
Verify the Dispatcher installation.	See "Verifying the Dispatcher installation" on page 7.
Install the adapter.	See "Installing the adapter" on page 8.
Verify the adapter installation.	See "Verifying the installation" on page 9.

Table 2. Installation roadmap (continued)

Task	For more information
Import the adapter profile.	See "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.
Verify the profile installation.	See "Verifying the adapter profile installation" on page 11.
Create an adapter user account.	See "Creating an adapter user account" on page 11.
Create a service.	See "Creating a service" on page 12.
Configure the adapter.	See "Configuring the adapter" on page 17.

Prerequisites

Verify that your environment meets all the prerequisites before installing 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
IBM Tivoli Directory Integrator	Version 7.1 fix pack 5 or later Version 7.1.1
IBM IBM Security Identity Manager server	Version 6.0
Salesforce.com API	Version 23.0
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. For more information, see the *Dispatcher Installation and Configuration Guide*.
A Salesforce.com API user.	A Salesforce.com user with API permission for your organization. The user must have a valid user name, password, and security token. For more information about security tokens, see "Resetting Your Security Token" in the Salesforce online help.

Note: Set the environmental variable CLASSPATH to Java version 1.5 that is required for the adapter installation or upgrade.

For information about the prerequisites and supported operating systems for Tivoli Directory Integrator, see the *IBM Tivoli Directory Integrator 7.0: Administrator Guide*.

Prerequisites for running the connector

The following table lists the requirements to run the Salesforce.com connector.

Table 4. Salesforce.com connector prerequisites

Requirement	Description	Task
Export and Import the SSL Certificate	Export the SSL certificate from the managed resource and import it to the certificate authority (CA) certificates of the Tivoli Directory Integrator Java™ Virtual Machine (JVM).	See "Exporting and importing the Salesforce.com SSL certificate" on page 7.

Installation worksheet for the adapter

The following table identifies the information that you need before installing the adapter.

Table 5. Required information to install the adapter

Required information	Description	Value

Tivoli Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter jars. For example, the jars/connectors subdirectory contains the jar 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 7.0:
		`drive\Program Files\IBM\TDI\V7.0`
		UNIX:
		• for version 7.0:
		`/opt/IBM/TDI/V7.0`

Adapters solution directory	When you install the dispatcher, the adapter prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is located at:
		Windows:
		• for version 7.0:
		`drive\Program Files\IBM\TDI\V7.0\timsol`
		UNIX:
		• for version 7.0:
		`/opt/IBM/TDI/V7.0/timsol`

Downloading the software

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

Go to IBM Passport Advantage.

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

Chapter 3. Installing the adapter

All the Tivoli Directory Integrator-based adapters 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 "Verifying the Dispatcher installation."

After verifying the Dispatcher installation, you might need to 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.

Verifying the Dispatcher installation

If this installation is the first Tivoli Directory Integrator-based adapter installation, you must install the RMI 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*.

Exporting and importing the Salesforce.com SSL certificate

To enable communication between the Salesforce.com Adapter and the Salesforce.com server, keystores must be configured for the RMI Dispatcher.

Procedure

1. Create a keystore that contains the Salesforce.com SSL certificates as trusted certificate entries. Use Internet Explorer to download the Salesforce.com server SSL certificate into the Windows certificate store from `https://login.salesforce.com/`. View the certificate by double-clicking the **SSL lock** icon. If your browser reports that revocation information is not available, double-click **View Certificate**.
2. Click **Certification Path** and select the CA Root certificate. The Java keytool displays a confirmation that the certificate is added to the keystore.
3. Click **View Certificate**.
4. Click the **Details** tab and navigate to **Copy to File using the Base-64 encoded X.509 (.CER) format**.
   - If the RMI Dispatcher has the keystore configured, use the **keytool.exe** program to import the Salesforce.com server certificate.
   - If the keystore is not configured, create a keystore. Issue the following command (as one line) from a command prompt:

     ```
     keytool -import -alias salesforce -file
     c:\salesforce.cer -keystore c:\truststore.jks -storepass passw0rd
     ```
5. Edit `IDI_HOME/timsol/solution.properties` file to specify truststore and keystore information. In the current release, only jks-type is supported:

```
# Keystore file information for the server authentication.
# It is used to verify the server's public key.
# example
javax.net.ssl.trustStore=truststore.jks
javax.net.ssl.trustStorePassword=passw0rd
javax.net.ssl.trustStoreType=jks
```

Note: If these key properties are not configured, you can set truststore to the same value that contains the Salesforce.com server certificate. Otherwise, you must import the Salesforce.com server certificate to the truststore specified in `javax.net.ssl.trustStore`.

6. After modifying the solution.properties file, restart the IBM Security Identity Manager Adapter Service (RMI Dispatcher).

What to do next

For more information about SSL configuration, see the *IBM Security Dispatcher Installation and Configuration Guide*.

Installing the adapter

Take these steps to install the adapter:

Before you begin

Do the following actions:

- Verify that your site meets all the prerequisite requirements. See "Prerequisites" on page 4.
- Obtain a copy of the installation software. See "Downloading the software" on page 6.
- Obtain system administrator authority.
- If you are updating a previous installation, the adapter you want to update must exist. If it does not exist, the software generates the following message:

```
Adapter is not found at specified location.
Can not perform Update Installation. Please correct
the path of installed adapter or select Full Installation.
```

About this task

The adapter uses the Tivoli Directory Integrator Salesforce connector. The connector is not available with the base Tivoli Directory Integrator product. The adapter installation involves the Tivoli Directory Integrator Salesforce.com connector installation. Before you install the adapter, make sure that the Dispatcher is already installed. See "Verifying the Dispatcher installation" on page 7.

Procedure

To install the adapter, perform the following steps:

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `SalesforceConnector.jar` file to the *ITDI_HOME*`/jars/connectors` directory.
4. Copy the `sforce_partner.jar` file to the *ITDI_HOME*`/jars/patches` directory.

5. Restart the IBM Security Identity Manager adapter (Dispatcher) service.

What to do next

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

- Verify that the installation completed successfully. See "Verifying the installation."
- Import the adapter profile. See "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.
- Create a user account for the adapter on IBM Security Identity Manager. See "Creating an adapter user account" on page 11.

Verifying the installation

If the adapter is installed correctly, these components exist in the specified directory:

Table 6. Adapter component

Adapter component	Directory
`SalesforceConnector.jar`	**On the Windows operating system** *drive*`:\Program Files\IBM\TDI\V7.0\jars\connectors\` **On the UNIX operating system** `/opt/IBM/TDI/V7.0/jars/connectors/`
`sforce_partner.jar`	**On the Windows operating system** *drive*`:\Program Files\IBM\TDI\V7.0\jars\patches\` **On the UNIX operating system** `/opt/IBM/TDI/V7.0/jars/patches/`

Review the installer log file, `SalesforceAdapter_Installer.log`, that is located in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Identity Manager. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is located in the *ITDI_Home*`\`*adapter solution directory*`\logs` directory.

Starting, stopping, and restarting the adapter service

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

About this task

Use the profile to create an adapter service on IBM Security Identity Manager server and establish communication with the adapter.

Before you can add an adapter as a service to the IBM Security Identity Manager server, the server must have an adapter profile to recognize the adapter as a service. The files that are packaged with the adapter include the adapter `SalesforceProfile.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 `SalesforceProfile.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.

To import the adapter profile, perform the following steps:

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform 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 `SalesforceProfile.jar` file in the **Service Definition File** field by performing 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**.

What to do next

- Update the `enRole.properties` file that is located under the server home data directory. Append the attribute **`erSFloginPassword`** to the list of attributes of the **`password.attribute`** property.

```
#########################################################
## Schema information
#########################################################
# specifies which attribute will be encrypted by the dataservices component.

password.attributes=ersynchpassword erServicePassword erServicePwd1
 erServicePwd2 erServicePwd3 erServicePwd4 erADDomainPassword erPersonPassword
 erNotesPasswdAddCert eritamcred erep6umds erposixpassphrase erSFloginPassword
```

- When you import the adapter profile and if you 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 *`ITIM_HOME`*`\data` directory.
- Restart the IBM Security Identity Manager for the change to take effect.

Verifying the adapter profile installation

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 a service" on page 12.

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

Creating an adapter user account

You must create a user account for the adapter on the managed resource. You must provide that account information when you create a service.

For more information about creating a service, see "Creating a service" on page 12.

Ensure that the account has sufficient privileges to administer the Salesforce.com users.

Configuring suspend and restore operations

This version of the adapter supports suspension and restoration of Salesforce.com accounts. You must create a custom profile on Salesforce.com for suspended users.

About this task

A custom profile is assigned to indicate that a Salesforce user is suspended. You can edit the profile in the Salesforce Administrator console to set more rules such as login restriction, or permissions. When a user is marked for suspension, the adapter sets **`ProfileId_Before_Suspended`** to the current profile. It then sets the profile for this user to the *Suspended User* profile. The restore operation resets the user's profile back to the original profile that the user was associated with before suspension. When the user is marked for restoration, the adapter sets the profile of the user that is based on **`ProfileId_Before_Suspended`** and then clears that field on Salesforce.com.

Procedure

1. Add the following custom fields to your organization's user fields in Salesforce.com See the Salesforce.com for information about creating custom fields.

```
Data Type: Text
Label: ProfileId Before Suspended
Length: 18
Field Name: ProfileId_Before_Suspended
```

a. Optional: You can add a descriptive text to identify the field usage.

```
Description and help text: Profile ID that was assigned to this user
                           before suspended by IBM Security Identity Manager
```

b. To ensure that the field is not mistakenly used by other administrators to suspend a user, set the **field visibility** to `invisible` for all users.

2. Create a profile on the Salesforce.com Administrator console that is to be assigned to suspended users.

```
Profile Name: Suspended User
```

See the Salesforce.com documentation for information about creating custom profiles.

a. Note of the License Type of this profile. It might affect the available Salesforce License count for your organization.

b. To prevent logins from suspended users, set the **Login Hours** of this profile to the same time every day.

Login Hours Edit Delete Login Hours Help

Day	Start Time	End Time
Sunday	12:00 AM PDT	12:00 AM PDT
Monday	12:00 AM PDT	12:00 AM PDT
Tuesday	12:00 AM PDT	12:00 AM PDT
Wednesday	12:00 AM PDT	12:00 AM PDT
Thursday	12:00 AM PDT	12:00 AM PDT
Friday	12:00 AM PDT	12:00 AM PDT
Saturday	12:00 AM PDT	12:00 AM PDT

3. Save the profile.

Creating a 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 by using 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 **IDI Salesforce Profile**.
4. Click **Next** to display the adapter service form.

5. Complete the following fields on the service form:

General Information

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
Optional: Specify the URL for the Tivoli Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Tivoli Directory Integrator host and *port* is 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*.

Salesforce.com API URL
Specify the URL to access the Salesforce.com API.

The default URL for logging in to the Salesforce.com API Webservices is `https://login.salesforce.com/services/Soap/u/version_number`. For example, if the API version number is 23.0, specify `https://login.salesforce.com/services/Soap/u/23.0` as the login URL.

For more information about login URLs, see "Implementation Considerations" in the *Salesforce.com API Developer Guide*.

UserName
Specify the user name that is used to log in to the resource and perform user management operations on the organization. Make sure that the user has API access privilege on Salesforce.com.

Password
Specify the password for the user.

If a password generator is used when you create or change user passwords, IBM Security Identity Manager must generate a password with enough complexity to meet Salesforce.com requirements. If necessary, create an IBM Security Identity Manager password policy that meets Salesforce.com requirements. For information about creating a password policy in IBM Security Identity Manager, see "Password Administration" in the *IBM Security Identity Manager Administration Guide*.

You can also use the Salesforce.com Administration User Interface to modify the Salesforce.com password complexity policy. For information about password policies, see "Setting Password Policies" in the Salesforce.com online help.

Security Token
Specify the security token that is associated with this user name.

To use the Webservices API on Salesforce.com, a valid security token must be generated for the Salesforce.com user. A security token is unique to a specific user. To generate a security token for the user to manage the Salesforce.com service in IBM Security Identity Manager, see "Resetting Your Security Token" in the Salesforce.com online help.

Profile for Suspended Users
Specify the name of the profile that is assigned to suspended users on Salesforce.com.

User Fields for Reconciliation
Optional: Specify the fields that are reconciled for users on Salesforce.com. The fields in the list are separated by commas. You must specify `Email`, `Username`, `LastName`, `Alias`, `TimeZoneSidKey`, `LocaleSidKey`, `EmailEncodingKey`, `ProfileId`, `LanguageLocaleKey`, `IsActive`, `Id`. You can specify more fields, however, the reconciliation performance might be affected. If you leave this field blank all fields are reconciled by default.

Owner
Optional: Specify a IBM Security Identity Manager user as a service owner.

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

Dispatcher Attributes:

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 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. For example, 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\V7.0\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIXand Linux operating: `system:/opt/IBM/TDI/V7.0/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can execute simultaneously for the service. For example, enter `10` when you want the dispatcher to execute maximum 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 executed simultaneously for the service.

Status and information

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. For example, verify the work station name or the IP address of the managed resource and the port.

6. Click **Finish**.

Permissions for the /tmp directory

The permissions for the `/tmp` directory on the managed resource must be set to `777` when performing the reconciliation operation by using the sudo user.

Chapter 4. Taking the first steps after installation

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

Configuring the adapter

These sections describe the configuration options for the Salesforce.com Adapter.

- "Adding custom attributes"
- "Edit Salesforce adapter profiles on the UNIX or Linux operating system" on page 21
- "Modifying the maximum length of the account form attributes" on page 22
- "Create a new JAR file and import the profile on the IBM Security Identity Manager" on page 22

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

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

Adding custom attributes

Use these tasks to configure the Salesforce.com Adapter to support customized Salesforce.com attributes.

Salesforce.com supports custom fields for the user object. However, the Salesforce.com Adapter supports only the standard set of attributes. However, you can customize the adapter to support custom attributes. Complete the following tasks to customize the Salesforce.com Adapter to support custom fields in Salesforce.com

Extending the schema and adding the custom attributes

Use the interface and tools provided by Salesforce.com to extend the Salesforce.com User schema and add the custom attributes.

For more information about adding new attributes to the Salesforce.com User schema, see the Salesforce.com documentation.

The Salesforce.com Adapter supports the following types of custom attributes:

- Boolean
- Integer
- Case-sensitive string
- Case-insensitive string
- Coordinated Universal Time (UTC) coded time

Prefix the attribute names with erSF in order to easily identify the attributes that are used with IBM Security Identity Manager.

Note:

- If Tivoli Directory Server is being used as the directory server application, the name of the attribute must be unique within the first 16 characters.
- The Salesforce.com Adapter supports multi-line value for custom attributes with string syntax.
- The custom attributes are supported for User account class only.

Copying the SalesforceProfile.jar file and extracting the files

Use these tasks to customize your environment.

About this task

The profile JAR file, SalesforceProfile.jar, is included in the Salesforce.com Adapter compressed file that you downloaded from the IBM website. The SalesforceProfile.jar file contains a folder named SalesforceProfile with the following files:

- CustomLabels.properties
- erSalesforceAccount.xml
- erSalesforceService.xml
- schema.dsml
- service.def
- sforceAdd.xml
- sforceChangePassword.xml
- sforceDelete.xml
- sforceModify.xml
- sforceRecon.xml
- sforceRestore.xml
- sforceSuspend.xml
- sforceTest.xml

You can modify these files to customize your environment. When you finish updating the profile JAR file, rebuild the jar and install it on the Tivoli Identity Manager server. For more information about the profile installation, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.

To modify the SalesforceProfile.jar file, complete the following steps:

Procedure

1. Log in to the system where the Salesforce.com Adapter is installed.
2. On the **Start** menu, click **Programs** > **Accessories** > **Command Prompt**.
3. Copy the SalesforceProfile.jar file into a temporary directory.
4. Extract the contents of` the SalesforceProfile.jar file into the temporary directory. Run the following commands:

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

   The jar command creates the `c:\temp\SalesforceProfile` directory.

What to do next

Edit the appropriate files by completing the following tasks.

Modifying the assembly lines

Use this task to add new mappings to the assembly lines for custom attributes.

About this task

The Salesforce.com Adapter uses Tivoli Directory Integrator to process requests before submitting it to Salesforce.com. The Salesforce.com Assembly Lines contain mapping instructions from a IBM Security Identity Manager request to Salesforce.com. Modify the assembly lines to add new mappings for custom attributes.

To modify the assembly line, complete the following steps:

Procedure

1. Launch the Tivoli Directory Integrator Configuration Editor.
2. Open the sforceAdd.xml file. Click **File** > **Open Tivoli Directory Integrator Configuration File...,**.
   a. Browse to the SalesforceProfile directory.
   b. Select the sforceAdd.xml file.
3. Optional: If previously edited, assign this configuration file to an existing project. Otherwise, proceed to the next screen to create a project and name it SalesforceProfile.
4. After the file is imported, expand the project to display the AssemblyLines tree in the Navigator pane.
5. Right click **sfAdd assemblyline** and select **Open**. The Add assemblyline configuration is displayed in the main panel.
6. Click **Show Mapping** in the main panel. The mapping table for the assembly line is displayed in the main panel.
7. Locate the **AddUser** section and left click to select it in the table.
8. Click **Map** to display the Add attribute dialog.
9. Enter the name of the custom field exactly as displayed in the API Name on Salesforce.com. For example, `Custom1__c`.
10. After the field is added, locate it in the mapping table and double-click the corresponding row to display an edit dialog.
11. Change the default value of work.[custom field name] to work.[custom attribute name]. For example, change `work.Custom1__c` to `work.erSFCustom1__c`.
12. Save the changes. Click **File** > **Save**.
13. Right click the project in the Navigator pane and select the **Export...** option to export the new assemblyline.
14. In the first screen of the Export dialog, expand the IBM Tivoli Directory Integrator folder and select **Runtime Configuration**.
15. Click **Next**.
16. In the file path field, browse to the SalesforceProfile directory and select the file with the same name from step 2 to overwrite it.
17. Click **Finish**.
18. Repeat the steps 5 through 17 for the Modify assemblyline.

19. Repeat steps 5 through 17 for the Recon assemblyline and perform the following steps instead of steps 10 and 11:
    a. Locate the field in the mapping table and click the Work Attribute cell corresponding to the custom field to rename it.
    b. Enter the attribute name given previously in step 11. For example, `erSFCustom1__c`.

Updating the schema.dsml file

The Salesforce.com Adapter schema.dsml file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

About this task

For more information about the attributes in this file, see "The schema.dsml file" on page 35.

To update the schema.dsml file, complete the following steps:

Procedure

1. Locate the schema.dsml file in the `\SalesforceProfile` directory.
2. Edit the schema.dsml file to add an attribute definition for each custom attribute. The Object Identifier (OID) is increased by 1, based on the last entry in the file. For example, if the last attribute in the file uses the OID 1.3.6.1.4.1.6054.3.161.2.85, the first new attribute uses the OID 1.3.6.1.4.1.6054.3.161.2.86. You might want to start a new range of numbers for your custom attributes. For example, start custom attributes with OID 1.3.6.1.4.1.6054.3.161.2.100. This range prevents duplicate OIDs if the adapter is upgraded to support new attributes that are standard for newer versions of Salesforce.com API.
3. Add each of the new attributes to the account class. For example, add the following attribute definition under the erSalesforceAccount section of the schema.dsml file:

   ```
   <attribute ref="erSFCustom1__c" required="false"/>
   ```

4. Save the file when you are finished.

Modifying the CustomLabels.properties file

After you add the custom attributes to the schema.dsml file, the attributes are available for use on the Salesforce.com Adapter form.

About this task

The attributes are displayed in the attribute list for the account form. You can modify the attribute names that are in the attribute list. For more information about the attributes on the adapter form, see "The CustomLabels.properties file" on page 38.

To add the attribute and its corresponding label to the CustomLabels.properties file, complete the following steps:

Procedure

1. Locate the CustomLabels.properties file in the `\SalesforceProfile` directory.
2. Edit the CustomLabels.properties file to add the attribute and its corresponding label. Use the following format:

   ```
   attribute=label
   ```

Note: The attribute name must be in lowercase. For example:

```
#
ADAgent Labels definitions
#
ersfcustom1__c=Custom Field One
ersfcustom2__c=Custom Attribute Field Two
```

3. Save the file when you are finished.

Creating a JAR file and installing the new attributes on the IBM Security Identity Manager server

You must import the modified assembly lines, schema.dsml, CustomLabels.properties, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the IBM Security Identity Manager server.

About this task

To install the new attributes, complete the following steps:

Procedure

1. Create a JAR file by using the files in the `\temp` directory. Run the following commands:

   ```
   cd c:\temp
   jar -cvf SalesforceProfile.jar SalesforceProfile
   ```

2. Import the SalesforceProfile.jar file into the IBM Security Identity Manager Application server. For more information about importing the file, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.
3. Start and stop the IBM Security Identity Manager server.

   Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the IBM Security Identity Manager server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 6, "Upgrading the adapter," on page 29.

Modifying the adapter form (optional)

After the changes are available in the IBM Security Identity Manager server, you can modify the Salesforce.com Adapter forms to use the new custom attributes.

The attributes do not need to be added to the Salesforce.com Adapter form unless you want them to be available. The attributes are returned during reconciliations unless you explicitly exclude them.

For more information about modifying the adapter form, see the IBM Security Identity Manager Information Center.

Edit Salesforce 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.

Modifying the maximum length of the account form attributes

When you want to modify the maximum length of the attributes on the account form, modify the schema.dsml file with their required length.

For example, when you want the First Name attribute's maximum length to 2048, modify the schema.dsml file as:

```
Old profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
 <name>erRsaAmFirstName</name>
 <description>First Name</description>
 <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
 <syntax>1.3.6.1.4.1.1466.115.121.1.15{1024}</syntax>
</attribute-type>

Modified profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
 <name>erRsaAmFirstName</name>
 <description>First Name</description>
 <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
 <syntax>1.3.6.1.4.1.1466.115.121.1.15{2048}</syntax>
</attribute-type>
```

Create a new JAR file and import the profile on the IBM Security Identity Manager

Once you modify the schema.dsml or any other profile files, you must import these files, into IBM Security Identity Manager for the changes to take effect.

About this task

In order to install the new attributes, complete the following steps:

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You need to stop and start the IBM Security Identity Manager server to refresh the cache and the adapter schema. For more information on upgrading an existing adapter, see Chapter 6, "Upgrading the adapter," on page 29.

Procedure

1. Extract the contents of the `SalesforceProfile.jar` file into the temporary directory by running the following command:

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

   The jar command creates the *c*`:\temp\SalesforceProfile` directory.
2. Update the profile files.
3. Create a new JAR file using the files in the `\temp` directory by running the following commands:

   ```
   cd c:\temp
   jar -cvf SalesforceProfile.jar SalesforceProfile
   ```
4. Import the `SalesforceProfile.jar` file into the IBM Security Identity Manager server. For more information about importing the file, see "Importing the adapter profile into the IBM Security Identity Manager server" on page 10.
5. Stop and start the IBM Security Identity Manager server.

Installing the language pack for the Salesforce adapter

The adapters use the same language package as IBM Security Identity Manager.

See the IBM Security Identity Manager information center and search for information about installing language packs.

Verifying the adapter installation

After you install and configure the adapter, perform these tasks:

Procedure

1. Test the connection for the service that you created on IBM Security Identity Manager.
2. Perform a full reconciliation from IBM Security Identity Manager.
3. Perform all supported operations on one user account. Perform these steps when you verify the suspend and restore operations.
   a. Note the current Salesforce.com profile that the user is assigned to.
   b. Suspend the account.
   c. Verify that the user's profile is now set to the *Suspended User* profile.
   d. Restore the account.
   e. Verify that the user's profile is now restored to the same profile that was assigned before the suspend operation.
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 perform an adapter operation.

Chapter 5. Troubleshooting the adapter errors

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

These topics provide information and techniques for identifying and resolving problems with the adapter. It also provides 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 starting 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 platform or operating system, or is it common across multiple platforms or 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 have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading 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 need to 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 performed?
- Does a certain sequence of events need to 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. Remember that just because multiple problems might have occurred 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. Consequently, 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?
- Are multiple users or applications encountering 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 45.

Known behaviors

The following behaviors and limitations are known to exist in the operation of the Salesforce.com Adapter.

Changing the email address of a Salesforce user

When IBM Security Identity Manager changes an email address for a Salesforce.com account, it updates the email address in its directory store as soon as the request is successfully sent to Salesforce.com. However, the change is not immediately reflected in Salesforce.com. Salesforce.com requires users to verify the email address change request at the inbox of the new email address. Therefore, a period exists when IBM Security Identity Manager contains the updated email address, while Salesforce.com contains the old email address. During this period one of these behaviors can occur:

The email address is verified by the user
: The email address is synchronized between IBM Security Identity Manager and Salesforce.com. No further action is needed.

The email address is not verified by the user.
: The email address in IBM Security Identity Manager reverts to the old email address at the next reconciliation operation.

The user verifies that the email address after reconciliation occurs.
: IBM Security Identity Manager reverts to the old email address with the reconciliation operation. Salesforce.com updates IBM Security Identity Manager with the new email address at the next reconciliation operation.

Set up a reconciliation policy with sufficient frequency to help keep email addresses consistent between Salesforce.com and IBM Security Identity Manager.

Deleting an account from the IBM Security Identity Manager Salesforce.com Service

Salesforce.com does not delete users. Therefore, the Salesforce.com Adapter marks a user account as `Inactive` when it receives a request to delete the account from IBM Security Identity Manager. If a Salesforce.com administrator reactivates a user from the Salesforce.com user interface, the user is returned as an orphan account at the next reconciliation.

Timeout issues

A network socket timeout might occur if the Salesforce.com connector is unable to complete a network-related operation with the Salesforce.com server within the timeout period specified. The timeout period can be affected by many settings:

- Adapter configuration
- IBM Security Identity Manager server configuration
- Dispatcher configuration
- Java VM configuration
- Operating system configuration
- Network equipment configuration such as switches, or firewalls.

Refer to the corresponding documentation for the default settings of the vendors.

To resolve Salesforce.com Adapter related timeout issues:

- Edit the default socket timeout value for the Salesforce.com connector in the `service.def` file. Change the **`SFSocketTimeout`** value. By default, it is set to `600` seconds or 10 minutes. This setting corresponds to the default Dispatcher **`SearchALUnusedTimeout`** setting. Increase both of these values, if the reconciliation operation takes longer than 10 minutes. See the Dispatcher documentation for instructions about setting the **`SearchALUnusedTimeout`** value.
- The adapter might timeout when it communicates with Salesforce.com because of network issues. To have the connector reestablish a connection to theSalesforce.com server and try the operation again, edit the *`ITDI_HOME`*`\timsol\etc\reconnect.rules` file. Add the line:

  ```
  com.ibm.di.connector.salesforce.SalesforceConnector:
  :com.ibm.di.connector.salesforce.SalesforceConnector
  Exception:reconnect:
  ```

  The line is a generic rule for the connector to reconnect when any exception is encountered.

Session handling

You might receive an `INVALID_SESSION_ID` exception that is logged in your Tivoli Directory Integrator logs. When an `INVALID_SESSION_ID` exception is encountered, the connector automatically tries to establish a new connection to Salesforce.com before it tries the API call again. Otherwise, a failure might occur because of a timeout in the session.

You can ignore `INVALID_SESSION_ID` warnings that are followed immediately by logs that display `RECOVERING FROM INVALID SESSION ID`.

Chapter 6. Upgrading the adapter

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 the connector

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

- If the connector version is higher or same as the previous version, the installer installs the new connector.
- If the connector version is lower than the existing connector version, the installer does not install the connector. A message is displayed indicating that no upgrade is required.

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

Upgrading the profile

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

See “Importing the adapter profile into the IBM Security Identity Manager server” on page 10.

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

Chapter 7. Uninstalling the adapter

To completely uninstall the Salesforce.com Adapter, you need to perform two procedures:

1. Uninstall the adapter from Tivoli Directory Integrator server.
2. Remove the adapter profile from the IBM Security Identity Manager server.

Uninstalling the adapter from the Tivoli Directory Integrator server

The Salesforce.com Adapter installation installs the Tivoli Directory Integrator Salesforce.com connector.

About this task

To uninstall the Dispatcher, see the *Dispatcher Installation and Configuration Guide*.

To remove the Salesforce.com Adapter, complete these steps:

Procedure

1. Stop the Dispatcher service.
2. Remove the SalesforceConnector.jar file from *ITDI_HOME*/jars/connectors directory.
3. Start the Dispatcher service.

Removing the adapter profile from the IBM Security Identity Manager server

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

Examples of objects on theIBM Security Identity Manager server that can reference the adapter profile are:

- 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 Salesforce.com Adapter, do not uninstall the Dispatcher.

For specific information on how to remove the adapter profile, see the online help or the information center for your IBM Security Identity Manager product.

Chapter 8. Reinstalling the adapter

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

For more information, see Chapter 6, “Upgrading the adapter,” on page 29.

Appendix A. Files

You can configure several adapter-specific files. This section includes information about the files that are associated with the Salesforce.com Adapter:

The schema.dsml file

The schema.dsml file contains all of the attributes that are common to all adapters. This common file also contains IBM Security Identity Manager server attributes that can be used by any adapter. The schema.dsml file defines all of the classes used by the adapter. The classes are used to declare accounts, services, and supporting data.

The schema.dsml file defines the attributes and objects that the adapter supports and uses to communicate with the IBM Security Identity Manager server. All attributes must be unique, therefore they are assigned an object identifier (OID).

The OID is defined using the `<object-identifier>...</object-identifier>`

The schema.dsml file has the following format:

```
SCHEMA.DSML File
<?xml version="1.0" encoding="UTF-8"?>
<dsml>
<!-- ********************************************************* -->
<!-- Schema supported by the Salesforce.com adapter. -->
<!-- ********************************************************* -->
<directory-schema> ...
<!-- ********************************************************* -->
<!-- eraSFString1-->
<!-- ********************************************************* -->
<attribute-type single-value="true">
<name>erSFString1</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.162.2.100</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
<!-- ********************************************************* -->
<!-- erSFInteger-->
<!-- ********************************************************* -->
<attribute-type single-value="true">
<name>erSFInteger</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.162.2.101</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.27</syntax>
</attribute-type>
<!-- ********************************************************* -->
<!-- erSFDate-->
<!-- ********************************************************* -->
<attribute-type single-value="true">
<name>erSFDate</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.162.2.102</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.24</syntax>
</attribute-type>
<!-- ********************************************************* -->
<!-- erSFBoolean-->
```

```
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erSFBoolean</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.162.2.103</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.7</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erSFMultiValueString-->
<!-- ******************************************************** -->
<attribute-type>
<name>erSFMultiValueString</name>
<description>List of string values</description>
<object-identifier>1.3.6.1.4.1.6054.3.162.2.104</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type> ...
<!-- ******************************************************** -->
<!-- erSalesforceAccount Class -->
<!-- ******************************************************** -->
<class superior="top">
<name>erSalesforceAccount</name>
<description>Class representing a Salesforce account.</description>
<object-identifier>1.3.6.1.4.1.6054.3.162.1.1</object-identifier> ...
<attribute ref="erSFBoolean" required="false"/>
<attribute ref="erSFDate" required="false"/>
<attribute ref="erSFInteger" required="false"/>
<attribute ref="erSFMultiValueString" required="false"/>
<attribute ref="erSFString1" required="false"/>
</class> ...
</directory-schema>
</dsml>
```

Object identifier

The IBM Security Identity Manager server uses LDAP directory services to add, delete, modify, and search IBM Security Identity Manager data. Each data item in an LDAP directory server must have a unique object identifier (OID). Therefore, each attribute and class that is defined in the schema.dsml file in IBM Security Identity Manager has an OID.

OIDs have the following syntax:

enterprise ID.product ID.adapter ID.object ID.instance ID

- The *enterprise ID* is always 1.3.6.1.4.1.6054 for IBM.
- The *product ID* is always 3 because these schema.dsml files are used with adapters.
- The *adapter ID* is 161 for the Salesforce.com Adapter.
- The *object ID* is 2. An attribute uses 2 as the object ID.
- The *instance ID* is a sequential number of the object.

Attribute definition

Before defining unique attributes for the adapter, ensure that the attribute does not exist in the common schema.dsml file.

The following example defines an attribute:

```
<!-- ******************************************** -->
<!-- erSampleHome -->
<!-- ******************************************** -->
<attribute-type single-value = "true" >
<name>erSampleHome</name>
```

```
<description>User home directory</description>
<object-identifier>1.3.6.1.4.1.6054.3.125.2.100</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
```

Comment lines are denoted by the `<!-- ... -->` markers

The attribute type is defined as single-value or multi-value. A single-value attribute is denoted by the line:`<attribute-type single-value ="true">`. To denote a multi-valued attribute, change the `true` value to `false`.

The name of the attribute that is used by the IBM Security Identity Manager server is defined in the schema. To simplify the tracking of new Salesforce.com Adapter attributes, use *erSF* as the preface for all new attributes.

The description of the attribute is denoted by the line:`<description>...</description>` tag.

The OID is defined by the `<object-identifier>...</object-identifier>` tag. Because OIDs are already assigned to the existing, standard attributes, the OID can be copied from the last attribute in the list. However, the last number must be incremented by one for each new attribute that you add to the schema.dsml file.

The data type is defined using the `<syntax>...</syntax>` tag. The following table lists various data types and the value you specify in the syntax tags.

Table 7. Syntax tag data types and values

Data type	Value
Bit string	1.3.6.1.4.1.1466.115.121.1.6
Boolean	1.3.6.1.4.1.1466.115.121.1.7
Directory string	1.3.6.1.4.1.1466.115.121.1.15
UTC coded time	1.3.6.1.4.1.1466.115.121.1.24
Integer	1.3.6.1.4.1.1466.115.121.1.27

Classes

At least one account class and one service class must be defined in the schema.dsml file.

Each class requires at least one attribute to identify the class: a name attribute. Additional attributes might be required depending on the class defined.

The following syntax defines a class:

```
<class superior="top">
<name> ... </name>
<description> ... </description>
<object-identifier> ... </object-identifier>
<attribute ref = "..." required = "true" />
<attribute ref = "..." required = "true" />
</class>
```

In order to make an attribute optional for a class, change `required = "true"` to `required = "false"` in the<attribute ref> tag.

An account class defines the attributes that are used to describe an account. An account class must be defined in the schema.dsml file.

The following example defines an account class:

```
<class superior="top" >
<name>erSampleAccount</name>
<description>Sample Account</description>
<object-identifier>1.3.6.1.4.1.6054.3.125.1.101</object-identifier>
<attribute ref = "eruid" required = "true" />
<attribute ref = "erAccountStatus" required = "false" />
<attribute ref = "erSampleGroups" required = "false" />
<attribute ref = "erSampleHome" required = "false" />
<attribute ref = "erSampleDesc" required = "false" />
<attribute ref = "erPassword" required = "false" />
</class>
```

In the preceding example, the class name is erSampleAccount and the only required attribute is eruid. However, note that erAccountStatus is a required attribute to suspend or restore accounts.

The CustomLabels.properties file

The CustomLabels.properties file is a text file that defines the labels on the form for the adapter.

The syntax for the information in the file is:

attribute=text

where:

- *attribute* is the same attribute defined in the schema.dsml file.
- *text* is the label that is on the form in the IBM Security Identity Manager user interface for the account.

The *attribute* must be in lowercase. This requirement is from the IBM Security Identity Manager server.

Appendix B. Adapter attributes

An adapter provides an interface between a managed resource and the IBM Security Identity Manager server.

As part of the adapter implementation, a dedicated account for IBM Security Identity Manager to access the Salesforce.com is created on the Salesforce.com. 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 Salesforce.com Adapter using attributes that are included in transmission packets that are sent over a network.

The combination of attributes, included in the packets, depends on the type of action that the IBM Security Identity Manager server requests from the Salesforce.com Adapter.

Table 8 is a listing of the attributes that are used by the Salesforce.com Adapter. The table gives a brief description and corresponding values of the attribute.

Use this key for the permissions column.

```
R = Read only
RW = Add, read, modify, write
AR = Add, Read
```

Table 8. Attributes for the erSFAccount object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erSFaboutMe	String	Yes	RW	No
erSFaccountId	String	Yes	R	No
erSFalias	String	Yes	RW	Yes
erSFcallCenterId	String	Yes	RW	No
erSFcity	String	Yes	RW	No
erSFcommunityNickname	String	Yes	RW	No
erSFcompanyName	String	Yes	RW	No
erSFcontactId	String	Yes	RW	No
erSFcountry	String	Yes	RW	No
erSFcreatedById	String	Yes	R	No
erSFcreatedDate	Datetime	Yes	R	No
erSFcurrentStatus	String	Yes	RW	No
erSFdelegatedApproverId	String	Yes	RW	No
erSFdepartment	String	Yes	RW	No
erSFdigestFrequency	String	Yes	RW	No

Table 8. Attributes for the erSFAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erSFdivision	String	Yes	RW	No
erSFemail	String	Yes	RW	Yes
erSFemailEncodingKey	String	Yes	RW	Yes
erSFemployeeNumber	String	Yes	RW	No
erSFextension	String	Yes	RW	No
erSFfax	String	Yes	RW	No
erSFfederationIdentifier	String	Yes	RW	No
erSFfirstName	String	Yes	RW	No
erSFforecastEnabled	Boolean	Yes	RW	No
erSFfullPhotoUrl	String	Yes	R	No
erSFisActive	Boolean	Yes	RW	No
erSFlanguageLocaleKey	String	Yes	RW	Yes
erSFlastLoginDate	Datetime	Yes	R	No
erSFlastModifiedById	String	Yes	R	No
erSFlastModifiedDate	Datetime	Yes	R	No
erSFlastName	String	Yes	RW	Yes
erSFlastPasswordChangeDate	Datetime	Yes	R	No
erSFlocaleSidKey	String	Yes	RW	Yes
erSFmanagerId	String	Yes	RW	No
erSFmobilePhone	String	Yes	RW	No
erSFname	String	Yes	R	No
erSFofflinePdaTrialExpirationDate	Datetime	Yes	R	No
erSFofflineTrialExpirationDate	Datetime	Yes	R	No
erSFphone	String	Yes	RW	No
erSFpostalCode	String	Yes	RW	No
erSFprofileId	String	Yes	RW	Yes
erSFreceivesAdminInfoEmails	Boolean	Yes	RW	No
erSFreceivesInfoEmails	Boolean	Yes	RW	No
erSFsmallPhotoUrl	String	Yes	R	No
erSFstate	String	Yes	RW	No
erSFstreet	String	Yes	RW	No
erSFsystemModstamp	Datetime	Yes	R	No
erSFtimeZoneSidKey	String	Yes	RW	Yes
erSFtitle	String	Yes	RW	No
erSFuserPermissionsCallCenterAutoLogin	Boolean	Yes	RW	No
erSFuserPermissionsInteractionUser	Boolean	Yes	RW	No
erSFuserPermissionsKnowledgeUser	Boolean	Yes	RW	No
erSFuserPermissionsMarketingUser	Boolean	Yes	RW	No
erSFuserPermissionsMobileUser	Boolean	Yes	RW	No

Table 8. Attributes for the erSFAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erSFuserPermissionsOfflineUser	Boolean	Yes	RW	No
erSFuserPermissionsSFContentUser	Boolean	Yes	RW	No
erSFuserPermissionsSupportUser	Boolean	Yes	RW	No
erSFuserPreferencesActivityRemindersPopup	Boolean	Yes	RW	No
erSFuserPreferencesApexPagesDeveloperMode	Boolean	Yes	RW	No
erSFuserPreferencesDisableAutoSubForFeeds	Boolean	Yes	RW	No
erSFuserPreferencesEventRemindersCheckboxDefault	Boolean	Yes	RW	No
erSFuserPreferencesReminderSoundOff	Boolean	Yes	RW	No
erSFuserPreferencesTaskRemindersCheckboxDefault	Boolean	Yes	RW	No
erSFuserRoleId	String	Yes	RW	No
erSFuserType	String	Yes	R	No
eruid	String	Yes	R	Yes
erPassword	String	Yes	RW	Yes

Appendix C. Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

`Monospace`

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide uses the Windows convention for specifying environment variables and for directory notation.

When using the Unix command line, replace %variable% with $variable for environment variables and replace each backslash (\) with a forward slash (/) in directory paths. The names of environment variables are not always the same in Windows and UNIX. For example, %TEMP% in the Windows operating system is equivalent to $tmp in a UNIX operating system.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

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 information center for IBM Security Identity Manager. However, sometimes you need to look beyond the information center 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.

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*".

About this task

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 Information Center, 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 contained 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 might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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 to enable: (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
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might 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 might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might 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 the future direction or intent of IBM 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 that conform 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. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2012. All rights reserved.

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

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: http://www.ibm.com/legal/copytrade.shtml

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

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

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

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

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Index

T

U

V

Printed in USA

SC27-4413-01