IBM Security Verify Governance Identity Manager

Salesforce.com Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Salesforce.com Adapter enables communication between the Identity server and the Salesforce.com server.

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

The adapter automates several administrative and 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 Verify Governance 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

Several components are involved in running and using the adapter. Install all these components so that the adapter can function correctly.

- The RMI Dispatcher
- The Security Directory Integrator connector
- IBM Security Verify Adapter profile

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

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

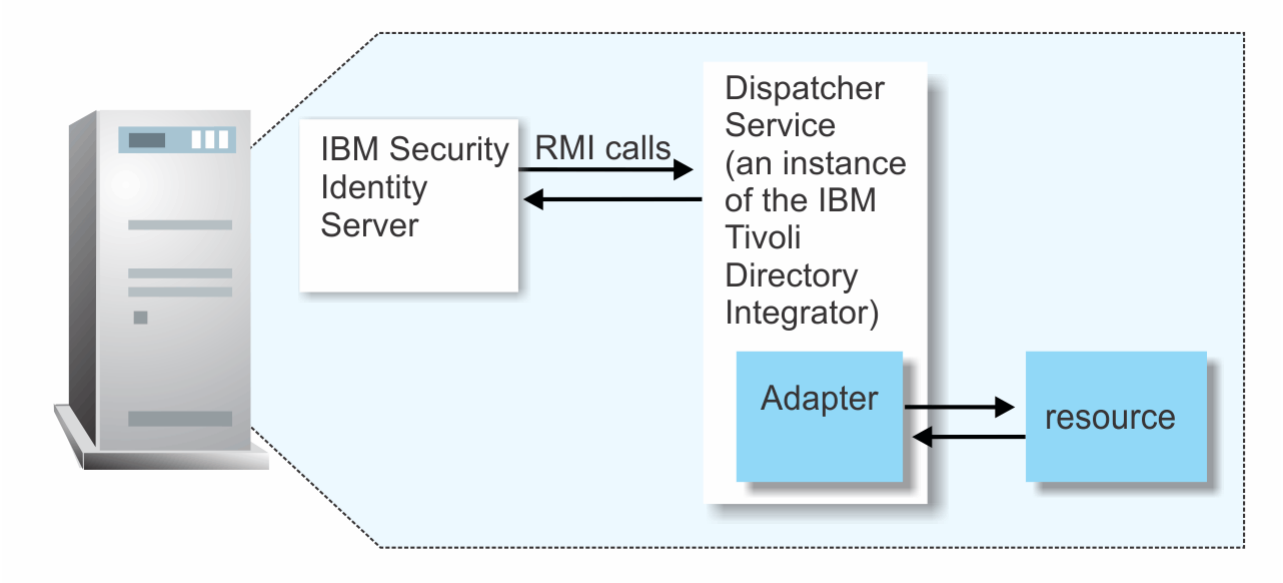

Figure 1. The architecture of the Salesforce.com Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

Supported configurations have the following components:

- The Identity server
- The Tivoli® Directory Integrator server
- The managed resource
- The adapter

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

Single server configuration

In a single server configuration, install the Identity server, the Security 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 on page 3.

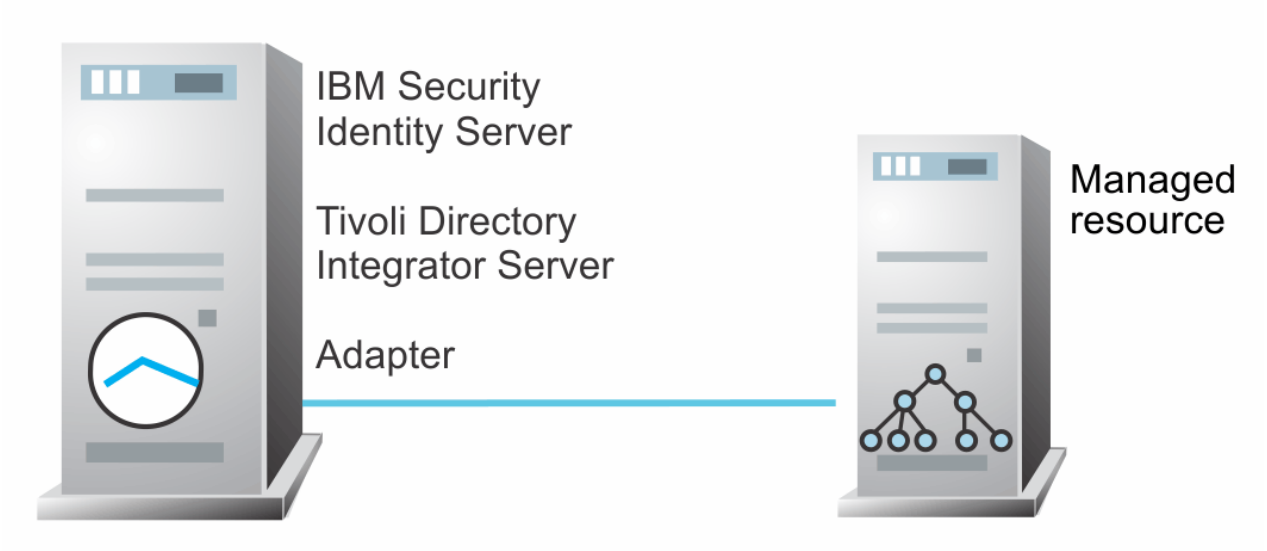

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator server, and the Salesforce.com Adapter, are installed on different servers.

Install the Security Directory Integrator server and the Salesforce.com Adapter on the same server as described in Figure 3 on page 3.

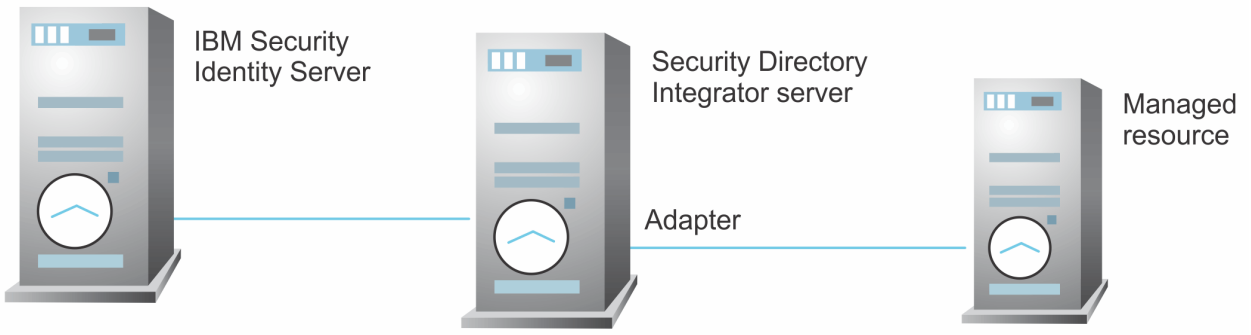

Figure 3. Example of a multiple server configuration

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Note: There is a separate instruction for installing, upgrading or uninstalling adapters from the IBM Security Verify Governance Identity Manager virtual appliance.

Pre-installation

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See *Prerequisites*.
2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

Installation

Complete these tasks.

1. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Load attribute mapping.
8. Set account defaults.
9. Create an adapter service/target.
10. Install the adapter language package.
11. Verify that the adapter is working correctly.

Upgrade

To upgrade the adapter, do a full installation of the adapter. Follow the *Installation roadmap*.

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
    a. Configure 1-way authentication.
    b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
    a. Configure 1-way authentication.

b. Configure 2-way authentication.

3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

Table 1 on page 7 identifies the software and operating system prerequisites for the adapter installation.

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

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Salesforce.com API	Version 31.0
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for 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 Security Directory Integrator, see the *IBM Security Directory Integrator 7.0: Administrator Guide*.

Prerequisites to run the connector

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

Table 2. 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 Security Directory Integrator Java virtual machine (JVM).	See "Exporting and importing the SSL certificate" on page 11.

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 3. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify Governance Identity Manager product, the default directory path for Security 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`

Table 3. Required information to install the adapter (continued)		
Required information	**Description**	**Value**
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 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*

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

All IBM Security 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 the Dispatcher is upgraded. See Verifying the adapter installation.

Depending on your adapter, the Security Directory Integrator connector might already be installed as part of the Security Directory Integrator product and no further action is required. If the connector is not pre-installed, install it after the Dispatcher.

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

If you already installed the RMI Dispatcher for another adapter, you do not need to reinstall it.

If you have not yet installed the RMI Dispatcher in the Security Directory Integrator environment, download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the *Dispatcher Installation and Configuration Guide*.

Exporting and importing the 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 configured keystore, 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 the *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
com.ibm.di.SSLProtocols=TLSv1.1,TLSv1.2
```

Note:

- If these key properties are not configured, you can set the 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`.
- Salesforce.com no longer supports SSL or TLS 1.0 connections. Salesforce Adapter depends on JVM used by ITDI to handle the connection, and Java 1.6 SR10 is the minimum level that provides TLS 1.1/1.2 support. To configure the adapter to use the higher TLS versions, make sure ITDI is using Java 1.6 SR10 or later.

6. Restart the adapter service.

What to do next

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

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Before you begin

- The Dispatcher must be installed.

About this task

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.
Cannot perform Update Installation. Correct
the path of installed adapter or select Full Installation.
```

Procedure

To install the adapter, take 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 adapter service.

Verifying the adapter installation

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

Table 4. 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 in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Verify Governance 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 in the *`ITDI_Home\adapter solution directory`*`\logs` directory.

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, 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 Security 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

You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Before you begin

- The Identity server is installed and running.
- You have administrator authority on the Identity server.
- The file to be imported must be a Java archive (JAR) file. The `<`*`Adapter`*`>Profile.jar` file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Verify Adapter. The adapter profile must be imported because it defines the types of resources that the Verify Governance Identity Manager server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance Identity Manager server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

What to do next

After the target profile is imported successfully, complete these tasks.

- Import the attribute mapping file. See “Importing attribute mapping file” on page 15.
- Create a connector that uses the target profile. See “Adding a connector” on page 15.

Importing attribute mapping file

After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

About this task

This task involves importing an account attribute mapping definition file, which is included in the adapter package. The imported file must be a DEF file.

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Attribute Mapping**.
   b) Click **Browse** to locate the attribute mapping file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported the file.
7. Click **Close**.

Adding a connector

After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Before you begin

Complete Importing the adapter profile.

Note: If you migrated from Verify Governance Identity Manager V5.2.2 or V5.2.2.1 and want to add or configure a connector, see *Adding and configuring a connector for each target* in the IBM Security Verify Governance Identity Manager product documentation.

About this task

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system.

This task can be completed from the Enterprise Connectors module in the Administration Console.

Procedure

To add a connector, complete these steps.

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.

4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.
   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.
      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.
      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.
      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

The connector is saved and added to the list of connectors in the **Connectors** pane.

If you cannot create a connector with the target profile or open an account on an existing connector, the target profile was not installed correctly during the import. You must import the target profile again.

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see “Enabling connectors” on page 16.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Before you begin

Table 5. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	“Adding a connector” on page 15.
Ensure that you enabled the appropriate channel modes for the connector.	“Reviewing and setting channel modes for each new connector” on page 17.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

A list of connectors is displayed on the **Connectors** tab.

4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

   Enable write-to channel
   Propagates every change in the Access Governance Core repository into the target system.

   For connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

   Enable read-from channel
   Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

   For HR feed connectors, only the check box for enabling the read-from channel is available.

   Enable reconciliation
   Synchronizes the modified data between the Access Governance Core repository and the target system.

Results

The connector is enabled

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

About this task

Note: Legacy Verify Governance Identity Manager Enterprise connectors use `Reconciliation` channel, whereas Identity Brokerage Enterprise connectors use `Read From Channel` and `Change Log Sync`.

For more information about any of tasks in the following steps, see the IBM® Security Identity Governance and Intelligence product documentation.

Procedure

To enable the read-from and write-to channels, and to set the change log synchronization schedule for each new connector, complete these steps in Verify Governance Identity Manager V5.2.3:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel
      Propagates every change in the Access Governance Core repository into the target system.

      Enable read-from channel
      Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

      Enable reconciliation
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.
   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.
      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.
      Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.
       For more information, see "Enabling connectors" on page 16.

       For Identity Brokerage connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

       For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.
12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Verify Governance Identity Manager account attributes.

About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Verify Governance Identity Manager account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute> = <target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.

   ```
   [conversion].<target_attribute>.<IGI_attribute> =
   [<target_attribute_value1>=<IGI_attribute_value1>;...;
   <target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

   ```
   [conversion.date].erbirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
   [conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
   [dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
   ```

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.
6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

   For more information, see *Mapping attributes for a connector* in the IBM Security Verify Governance Identity Manager product documentation.

Configuring suspend and restore operations

This version of the adapter supports suspension and restoration of Salesforce.com accounts.

About this task

The Salesforce.com Adapter supports Suspend Account and Restore Account operations, which are not enabled by default. The default setting of **Account Operations Settings** in the service form of the adapter is **Disable Suspend/Restore (Accounts cannot be reactivated)**, which does not enable Suspend Account or Restore Account operations.

To successfully suspend an account or restore an account, you must set the service to enable Suspend Account and Restore Account operations. The setting causes the adapter to deactivate or reactivate the account on Salesforce.com.

Note: Enabling the Suspend Account and Restore Account operations causes deleted accounts to reconcile as orphan accounts in the service.

Procedure

1. In the service form, access the **Connection** tab.
2. In the **Account Operations Settings** menu, select **Enable Suspend/Restore (Deleted accounts reconciled as orphan accounts)**.
3. Enter the Salesforce.com API user password in the **Salesforce API Password** field.
4. Click **OK** to save the changes.

Service/Target form details

Complete the service/target form fields.

Connector Profile

Service Name
Specify a name that defines the adapter service on the Identity server.

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

Description
Optionally, specify a description that identifies the service for your environment.

Security Directory Integrator location

Specify the URL for the IBM Security Directory Integrator instance. The valid syntax for the URL is `rmi://`*`ip-address`*`:`*`port`*`/ITDIDispatcher`, where *ip-address* is the IBM Security Directory Integrator host and *port* is the port number for the RMI Dispatcher.

The default URL for the default SDI1 instance is `rmi://localhost:1099/ITDIDispatcher`.

The following table shows the ports that are open in the firewall for every instance that is created. However, usage of these port numbers do not support high availability.

Table 6. Ports

Instance	Ports
SDI1	1199, 1198, 1197, 1196, 1195, 1194
SDI2	2299, 2298, 2297, 2296, 2295, 2294
SDI3	3399, 3398, 3397, 3396, 3395, 3394
SDI4	4499, 4498, 4497, 4496, 4495, 4494
SDI5	5599, 5598, 5597, 5596, 5595, 5594
SDI6	6699, 6698, 6697, 6696, 6695, 6694
SDI7	7799, 7798, 7797, 7796, 7795, 7794
SDI8	8899, 8898, 8897, 8896, 8895, 8894
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

For a high availability implementation, use any of these port numbers.

- 1099
- 2099
- 3099

Account Operations Settings

Define the behavior of account deletion and enable or disable the Suspend Account and Restore Account operations:

- Enable Suspend/Restore (Deleted accounts are reconciled as orphan accounts.)

  Select this option to enable the Suspend and Restore account operations. Suspended users are marked as “Inactive” on Salesforce. At account deletion, the user is marked “Inactive” on Salesforce; however, the adapter reconciles the user back as an Orphan Account.

- Disable Suspend/Restore (Accounts can be reactivated)

  Select this option to disable Suspend and Restore account operations. An error is returned when an account under the Salesforce.com Service is submitted for restoration or suspension. Deleted accounts are *not* reconciled. If the account was deleted and is later re-created in Identity server, it is restored from Salesforce.com by marking it as “Active” again.

- Disable Suspend/Restore (Accounts cannot be reactivated)

  This default option has behavior that is compatible with previous versions of the adapter. Accounts that are deleted cannot be restored. If the account is re-created later, it fails.

Owner

Optionally, specify a user as a service owner.

Service Prerequisite

Optionally, specify a service that is prerequisite to this service.

Connection

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 do 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, Identity server must generate a password with enough complexity to meet Salesforce.com requirements. If necessary, create a password policy that meets Salesforce.com requirements.

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

A unique security token can be generated for the Salesforce.com account that is configured in the adapter.

To generate a new security token for the user to manage the Salesforce.com service, see “Resetting Your Security Token” in the Salesforce.com online help.

To login without a security token in the adapter, specify `NONE` in the Security Token field on the service form.

Profile for Suspended Users (deprecated)

Specify the name of the profile that is assigned to suspended users on Salesforce.com.

User Fields for Reconciliation
Optionally, 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.

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 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 Identity server. 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 UNIX and Linux® operating: `system:/opt/IBM/TDI/V7.0/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter `10` when you want the dispatcher to run 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 run 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 to which the adapter is connected.

Adapter version
Specifies the version of the adapter that the service uses to provision request to the managed resource.

Profile version
Specifies the version of the profile that is installed in the Identity server.

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

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

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

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

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

Verifying that the adapter is working correctly

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

Procedure

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

Permissions for the `/tmp` directory

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

Chapter 4. Upgrading

Upgrading an IBM Security Directory Integrator-based adapter involves tasks such as upgrading the dispatcher, the connector, and the adapter profile. Depending on the adapter, some of these tasks might not be applicable. Other tasks might also be required to complete the upgrade.

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

Upgrading the adapter binaries or 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 adapter profile

Read the adapter Release Notes® for any specific instructions before you import a new adapter profile.

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

Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

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

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

Customized 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.

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.

Salesforce.com custom user attributes, such as multi-select picklists can be configured to store multiple values in a single field. The adapter supports multi-value custom attributes. To configure the adapter to support fields with multiple values, perform the following steps:

1. Add the custom attribute as per the Installation and Configuration Guide. After installation, click **Adapter configuration** > **Customized attributes**.
2. When updating the `schema.dsml` file, ensure that attribute-type single-value="false".
3. In the `service.def` file, locate the section `<operation cn="sfModify">`. Add a child element to the operation with the following format `<replaceMultiValue name="custom_mutlivalue_attribute_name" />` and replace the text `custom_multivalue_attribute_name` inside the quotes with the name of the custom attribute specified in `schema.dsml`.
4. To add the field into the Service's Account Form, edit the form in the Form Designer. Typically, the attribute type to handle a multi-select picklist in the Form Designer would be a ListBox. However, you may choose any controls that support multiple values. For more information about modifying the adapter form, see the IBM Security Verify Identity product documentation.

Note: It is recommended to populate the values of the control in the Form Designer to correspond to those specified in the custom field on Salesforce.com.

Related concepts

Modification of 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.

Related tasks

Editing 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.

Creating a JAR file and importing the profile

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

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Schema extensions and custom attributes

Use the interface and tools that are 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
- Not case-sensitive string
- Coordinated Universal Time (UTC) coded time

Prefix the attribute names with `erSF` to easily identify the attributes that are used with IBM Security Verify Governance Identity Manager.

Note:

- If Security 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 a multi-line value for custom attributes with string syntax.
- The custom attributes are supported for User account class only.

Related concepts

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Salesforce.com Adapter forms to use the new custom attributes.

Related tasks

Copying the SalesforceProfile.jar file and extracting the files
Use these tasks to customize your environment.

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

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.

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.

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

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 file and install it on the Identity server. For more information about the profile installation, see *Importing the adapter profile*.

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.

Related concepts

Schema extensions and custom attributes

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

Adapter form modification (optional)

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

Related tasks

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

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.

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.

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

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 Security Directory Integrator to process requests before you submit them to Salesforce.com.

The Salesforce.com assembly lines contain mapping instructions from a IBM Security Verify Governance Identity Manager request to Salesforce.com. Modify the assembly lines to add new mappings for custom attributes.

Procedure

1. Start the Security Directory Integrator Configuration Editor.
2. Open the `sforceAdd.xml` file. Click **File** > **Open Security 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 assembly line.
14. In the first screen of the **Export** dialog, expand the IBM Security 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 assembly line.
19. Repeat steps 5 through 17 for the Recon assembly line and do 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 that is specified previously in step 11.
    For example, `erSFCustom1__c`.

Related concepts

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

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Salesforce.com Adapter forms to use the new custom attributes.

Related tasks

Copying the SalesforceProfile.jar file and extracting the files
Use these tasks to customize your environment.

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.

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.

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

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 45.

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 1.3.6.1.4.1.6054.3.162.2.85, the first new attribute uses the OID 1.3.6.1.4.1.6054.3.162.2.86.

You might want to start a new range of numbers for your custom attributes. For example, start custom attributes with OID 1.3.6.1.4.1.6054.3.162.2.1000. 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.

Related concepts

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

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Salesforce.com Adapter forms to use the new custom attributes.

Related tasks

Copying the SalesforceProfile.jar file and extracting the files
Use these tasks to customize your environment.

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

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.

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

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. See “CustomLabels.properties file” on page 47.

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:

   ```
   #
   Adapter Labels definitions
   #
   ```

```
ersfcustom1__c=Custom Field One
ersfcustom2__c=Custom Attribute Field Two
```

3. Save the file when you are finished.

Related concepts

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

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the Salesforce.com Adapter forms to use the new custom attributes.

Related tasks

Copying the SalesforceProfile.jar file and extracting the files
Use these tasks to customize your environment.

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

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.

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

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

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 Identity server.

   For more information about importing the file, see Importing the adapter profile.

3. Start and stop the Identity 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 Identity server to refresh the cache and the adapter schema. See Chapter 4, “Upgrading,” on page 25.

Related concepts

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

Adapter form modification (optional)

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

Related tasks

Copying the SalesforceProfile.jar file and extracting the files
Use these tasks to customize your environment.

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

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.

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.

Adapter form modification (optional)

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

You do not have to add the attributes 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 Verify Governance Identity Manager product documentation.

Related concepts

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

Related tasks

Copying the SalesforceProfile.jar file and extracting the files
Use these tasks to customize your environment.

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

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.

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.

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

Editing 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 a command.

Related concepts

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

Modification of 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.

Related tasks

Creating a JAR file and importing the profile
After you modify the `schema.dsml` or any other profile files, you must import these files, into IBM Security Verify Governance Identity Manager for the changes to take effect.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Modification of 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 2048 as the maximum length of the **First Name** attribute, 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>
```

Related concepts

Customized attributes

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

Related tasks

Editing 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.

Creating a JAR file and importing the profile

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

Verifying that the adapter is working correctly

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

Creating a JAR file and importing the profile

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

About this task

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 4, “Upgrading,” on page 25.

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 JAR file with 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 Identity server.
5. Stop and start the Identity server.

Related concepts

Customized attributes

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

Modification of 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.

Related tasks

Editing 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.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on IBM Security Verify Governance Identity Manager.
2. Do a full reconciliation from IBM Security Verify Governance Identity Manager.
3. Perform all supported operations on one user account.

   Do these steps when you verify the suspend and restore operations, if it is configured on the service form.

   a) Suspend the account.

   b) Verify that the account is disabled by checking the user's **IsActive** status on Salesforce.com.

   c) Restore the account.

   d) Verify that the account is enabled by checking the user's **IsActive** status on Salesforce.com.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

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

Modification of 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.

Related tasks

Editing 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.

Creating a JAR file and importing the profile
After you modify the `schema.dsml` or any other profile files, you must import these files, into IBM Security Verify Governance Identity Manager for the changes to take effect.

Chapter 6. Troubleshooting

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. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

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 find the cause of the problem. This step includes asking yourself basic questions:

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

- Does the problem always occur when the same task is being done?
- Is a certain sequence of events required 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 occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

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

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

Related concepts

Known behaviors and limitations

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

Known behaviors and limitations

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

Email address change of a Salesforce user

When IBM Security Verify Governance 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 Verify Governance 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 Verify Governance 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 Verify Governance 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 Verify Governance Identity Manager reverts to the old email address with the reconciliation operation. Salesforce.com updates IBM Security Verify Governance 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 Verify Governance Identity Manager.

Account deletion from the 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 Verify Governance 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
- Identity 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 timeout issues that are related to the Salesforce.com Adapter:

- 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 the Salesforce.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 Security 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.

Login Rate Exceeded error

Salesforce.com has a default limit for the number of login attempts per hour.

To address this limit, the adapter is designed to use *sessionID* to authenticate operations after first login. You must enable **Assembly Line Caching**. Otherwise, if you perform operations that exceed 3600 within an hour, you might see a Login Rate Exceeded error from Salesforce.com.

To enable Assembly Line Caching:

- Select **Enable AL Caching** on the service form.
- Verify that the AL Caching is enabled in the dispatcher setting.
- Verify the itim_listener.properties in the *TDI* folder and ensure that the **ALCacheSize** value is set to greater than 0. For example, 100.
- Restart the dispatcher service to apply the changes.

Related concepts

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Chapter 7. Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Security Directory Integrator based adapter mainly involves removing the connector file, and the adapter profile from the Identity server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

Removing the adapter binaries or connector

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

About this task

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

Procedure

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

Deleting the adapter profile

Remove the adapter service/target type from the Identity server. Before you delete the adapter profile, ensure that no objects exist on the Identity server that reference the adapter profile.

Objects on the Identity server that can reference the adapter profile:

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

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

For specific information about how to delete the adapter profile, see the IBM Security Verify Governance Identity Manager product documentation.

Chapter 8. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Files

You can configure several adapter-specific files that are associated with the Salesforce.com adapter.

- "The schema.dsml file" on page 45
- "CustomLabels.properties file" on page 47

The `schema.dsml` file

The `schema.dsml` file contains all of the attributes that are common to all adapters. This common file also contains Identity server attributes that can be used by any adapter. The `schema.dsml` file defines all of the classes that are 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 Identity server. All attributes must be unique. Therefore, they are assigned an object identifier (OID).

The OID is defined with 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 Identity server uses LDAP directory services to add, delete, modify, and search IBM Security Verify Governance 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 Verify Governance 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 you define 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 Identity 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 with 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. More attributes might be required depending on the class that is 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>
```

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, erAccountStatus is a required attribute to suspend or restore accounts.

CustomLabels.properties file

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

Use this syntax for the information in the file:

```
attribute=text
```

where:

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

The value of *attribute* must be in lowercase. This requirement is from the Identity server.

Adapter attributes

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

As part of the adapter implementation, a dedicated account for IBM Security Verify Governance 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 Verify Governance Identity Manager account. These files establish communication with the Identity server.

Attribute descriptions

The Identity server communicates with the Salesforce.com Adapter with 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 Identity server requests from the Salesforce.com Adapter.

Table 8 on page 48 lists the attributes that are used by the Salesforce.com Adapter. The table provides a description and the 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	Description
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	
erSFcountryCode	Picklist	Yes	RW	No	
erSFcreatedById	String	Yes	R	No	
erSFcreatedDate	Datetime	Yes	R	No	Displays current time if Salesforce returns null for the attribute
erSFcurrentStatus	String	Yes	RW	No	

Table 8. Attributes for the erSFAccount object class (continued)					
erSFdefaultCurrencyIsoCode	Picklist	Yes	RW	No	
erSFdefaultDivision	Picklist	Yes	RW	No	
erSFdelegatedApproverId	String	Yes	RW	No	
erSFdepartment	String	Yes	RW	No	
erSFdigestFrequency	Picklist	Yes	RW	No	
erSFdivision	String	Yes	RW	No	
erSFemail	String	Yes	RW	Yes	
erSFemailEncodingKey	String	Yes	RW	Yes	
erSFEmailPreferencesAutoBcc	Boolean	Yes	RW	No	
erSFEmailPreferencesAutoBccStayInTouch	Boolean	Yes	RW	No	
erSFEmailPreferencesStayInTouchReminder	Boolean	Yes	RW	No	
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	
erSFisPortalEnabled	Boolean	Yes	RW	No	
erSFisPrmSuperUser	Boolean	Yes	RW	No	
erSFJigsawImportLimitOverride	Int	Yes	RW	No	
erSFlanguageLocaleKey	String	Yes	RW	Yes	
erSFlastLoginDate	Datetime	Yes	R	No	Displays current time if Salesforce returns null for the attribute.
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	
erSFmanager	Picklist	Yes	RW	No	
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	
erSFSenderEmail	Email	Yes	RW	No	

Table 8. Attributes for the erSFAccount object class (continued)					
erSFSenderName	String	Yes	RW	No	
erSFSignature	String	Yes	RW	No	
erSFStayInTouchNote	String	Yes	RW	No	
erSFStayInTouchSignature	String	Yes	RW	No	
erSFStayInTouchSubject	String	Yes	RW	No	
erSFsmallPhotoUrl	String	Yes	R	No	
erSFstate	String	Yes	RW	No	
erSFstateCode	Picklist	Yes	RW	No	
erSFstreet	String	Yes	RW	No	
erSFsystemModstamp	Datetime	Yes	R	No	
erSFtimeZoneSidKey	String	Yes	RW	Yes	
erSFtitle	String	Yes	RW	No	
erSFpermissionSetID	String	No	RW	No	
erSFuserPermissionsCallCenterAutoLogin	Boolean	Yes	RW	No	
erSFUserPermissionsChatterAnswersUser	Boolean	Yes	RW	No	
erSFuserPermissionsInteractionUser	Boolean	Yes	RW	No	
erSFuserPermissionsJigsawProspectingUser	Boolean	Yes	RW	No	
erSFuserPermissionsKnowledgeUser	Boolean	Yes	RW	No	
erSFuserPermissionsMarketingUser	Boolean	Yes	RW	No	
erSFuserPermissionsMobileUser	Boolean	Yes	RW	No	
erSFuserPermissionsOfflineUser	Boolean	Yes	RW	No	
erSFuserPermissionsSFContentUser	Boolean	Yes	RW	No	
erSFuserPermissionsSiteforceContributorUser	Boolean	Yes	RW	No	
erSFuserPermissionsSiteforcePublisherUser	Boolean	Yes	RW	No	
erSFuserPermissionsSupportUser	Boolean	Yes	RW	No	
erSFUserPermissionsWorkDotComUserFeature	Boolean	Yes	RW	No	
erSFuserPreferencesActivityRemindersPopup	Boolean	Yes	RW	No	
erSFuserPreferencesApexPagesDeveloperMode	Boolean	Yes	RW	No	
erSFuserPreferencesContentNoEmail	Boolean	Yes	RW	No	
erSFuserPreferencesContentEmailAsAndWhen	Boolean	Yes	RW	No	
erSFUserPreferencesDisableAllFeedsEmail	Boolean	Yes	RW	No	
erSFuserPreferencesDisableAutoSubForFeeds	Boolean	Yes	RW	No	
erSFUserPreferencesDisableBookmarkEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableChangeCommentEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableEndorsementEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableFileShareNotificationsForApi	Boolean	Yes	RW	No	
erSFUserPreferencesDisableFollowersEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableLaterCommentEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableLikeEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableMentionsPostEmail	Boolean	Yes	RW	No	
erSFuserPreferencesDisableMessageEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableProfilePostEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisableSharePostEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisCommentAfterLikeEmail	Boolean	Yes	RW	No	

Table 8. Attributes for the erSFAccount object class (continued)					
erSFUserPreferencesDisMentionsCommentEmail	Boolean	Yes	RW	No	
erSFUserPreferencesDisProfPostCommentEmail	Boolean	Yes	RW	No	
erSFUserPreferencesEnableAutoSubForFeeds	Boolean	Yes	RW	No	
erSFuserPreferencesEventRemindersCheckboxDefault	Boolean	Yes	RW	No	
erSFuserPreferencesHideCSNDesktopTask	Boolean	Yes	RW	No	
erSFuserPreferencesHideCSNGetChatterMobileTask	Boolean	Yes	RW	No	
erSFUserPreferencesHideS1BrowserUI	Boolean	Yes	RW	No	
erSFUserPreferencesJigsawListUser	Boolean	Yes	RW	No	
erSFuserPreferencesOptOutOfTouch	Boolean	Yes	RW	No	
erSFuserPreferencesReminderSoundOff	Boolean	Yes	RW	No	
erSFUserPreferencesShowCityToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowCityToGuestUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowCountryToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowCountryToGuestUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowEmailToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowFaxToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowManagerToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowMobilePhoneToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowPostalCodeToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowPostalCodeToGuestUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowProfilePicToGuestUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowStateToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowStateToGuestUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowStreetAddressToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowTitleToExternalUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowTitleToGuestUsers	Boolean	Yes	RW	No	
erSFUserPreferencesShowWorkPhoneToExternalUsers	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	
erSFuserGroupId	String	No	RW	No	

Index

S

T

U

V