IBM Security Verify Governance Identity Manager

SAP User Management Engine (UME) Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity 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.

The SAP User Management Engine Adapter uses the functionality of Security Directory Integrator to enable communication between the Identity server and the SAP User Management Engine Application Server Java™. This communication happens by using the SPML (DSML V2) protocol.

Features of the adapter

The adapter automates several administrative and management tasks.

- Creating users
- Modifying users' attributes
- Changing user account passwords
- Suspending, restoring, and deleting user accounts
- Reconciling users and user attributes

In some cases, the standard features and functionality of SAP might not satisfy business requirements. The adapter supports configurable extension and customization for you to map the adapter to your desired requirements.

Related concepts

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.

Supported configurations
The adapter supports both single and multiple server configurations.

User types overview
A user can be either a default user or technical user. The user type refers to the security policy applied to a user. An attribute `Security Policy` contains a value that is either of these two user types.

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 adapter requires the following components:

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

You must install the 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.

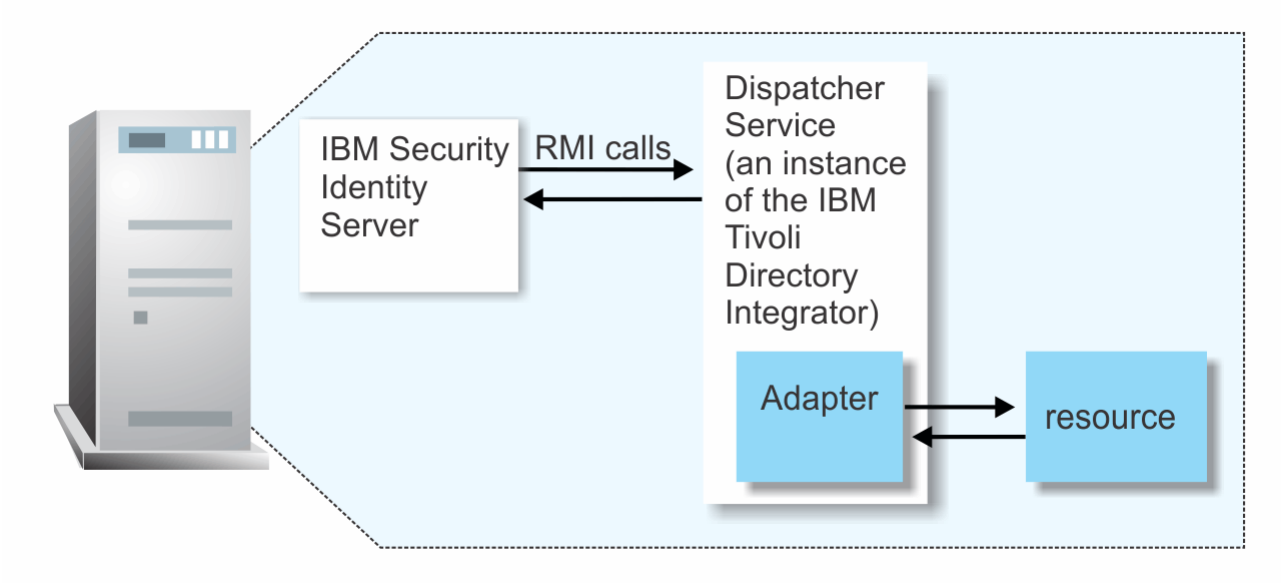

Figure 1. The architecture of the SAP User Management Engine Adapter

Related concepts

Features of the adapter
The adapter automates several administrative and management tasks.

Supported configurations
The adapter supports both single and multiple server configurations.

User types overview
A user can be either a default user or technical user. The user type refers to the security policy applied to a user. An attribute `Security Policy` contains a value that is either of these two user types.

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

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

The adapter must reside directly on the server running the Security Directory Integrator server.

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator server, and the SAP User Management Engine Adapter on one server to establish communication with the SAP User Management Engine Application Server.

The SAP User Management Engine Application Server Java is installed on a different server as described in Figure 2 on page 3.

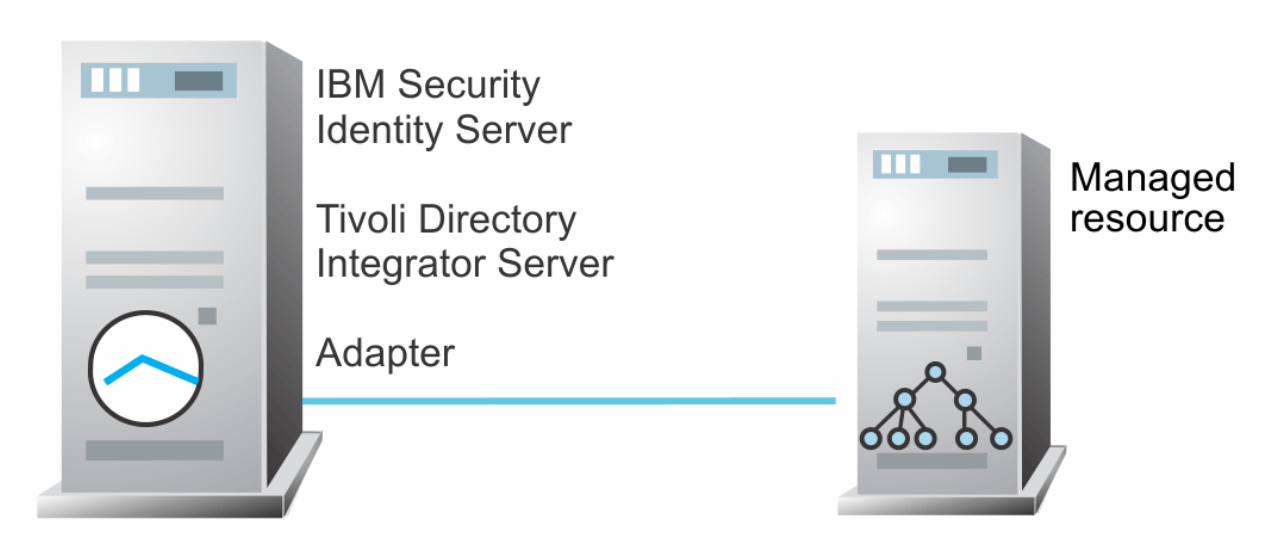

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator server, the SAP User Management Engine Adapter, and the SAP User Management Engine Application Server are installed on different servers.

Install theSecurity Directory Integrator server and the SAP User Management Engine Adapter on the same server as described in Figure 3 on page 3.

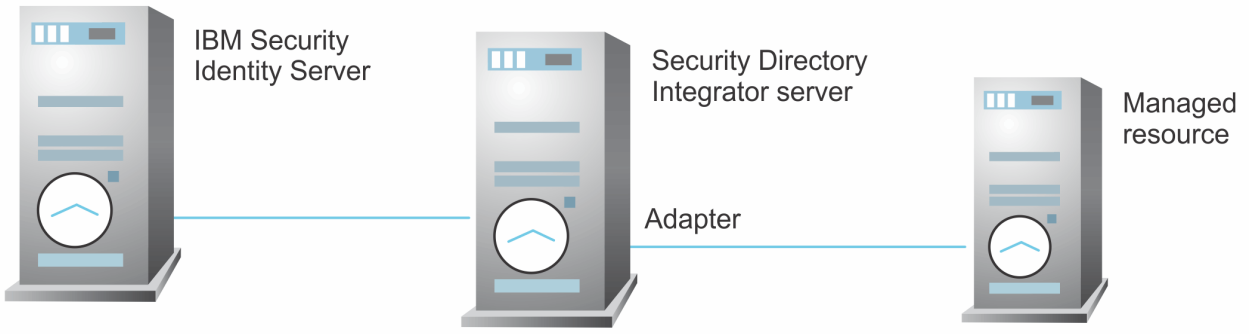

Figure 3. Example of a multiple server configuration

Related concepts

Features of the adapter
The adapter automates several administrative and management tasks.

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.

User types overview
A user can be either a default user or technical user. The user type refers to the security policy applied to a user. An attribute `Security Policy` contains a value that is either of these two user types.

User types overview

A user can be either a default user or technical user. The user type refers to the security policy applied to a user. An attribute `Security Policy` contains a value that is either of these two user types.

For an overview and difference of the user types, see the following table.

Table 1. Difference between a default user and technical user

Default User	**Technical User**
Used for regular generic users.	Used for system-to-system communication.
A profile can be displayed as well as modified.	A profile can be displayed but it cannot be modified directly.
Password must be changed after initial logon else a user password can expire.	Password does not expire for a technical user.
Default users are created by administrators during self-registration, or read from external user management engine (UME) data sources.	Some technical users are created automatically (SAPJSF) and some are created by the user administrator.
UME maps `Dialog users` from the AS ABAP data source to default user type.	UME maps `System users` from the AS ABAP data source to technical user type.
Well-known standard users of default user type are - Administrator and Guest.	Well-known standard users of technical user type are - SAPJSF and ADSuser.

Related concepts

Features of the adapter
The adapter automates several administrative and management tasks.

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.

Supported configurations
The adapter supports both single and multiple server configurations.

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 2 on page 6 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. See the Release Notes bundled with this adapter package for the most current information on supported versions and minimum fix pack versions.

Table 2. Prerequisites to install the adapter

Prerequisite	**Description**
Operating System	The SAP User Management Engine Adapter can be used on any operating system that is supported by Security Directory Integrator.
Network Connectivity	TCP/IP network
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.

Table 2. Prerequisites to install the adapter (continued)	
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
SAP User Management Engine Application Server Java	SAP NetWeaver 730 EP 1 AS Java SAP NetWeaver 740 AS Java

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

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**
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains files for the adapters. For example, the `jars/connectors` subdirectory contains the files for the UNIX adapter.
Solution Directory	See the *Dispatcher Installation and Configuration Guide*.

Chapter 3. Installing in the Verify Governance Identity Manager virtual appliance

For Verify Governance Identity Manager target management, you can install an IBM Security Verify Adapters or a custom adapter on the built-in Security Directory Integrator in the virtual appliance instead of installing the adapter externally. As such, there is no need to manage a separate virtual machine or system.

About this task

This procedure is applicable for a selected list of Identity Adapters. See the Identity Adapters product documentation at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

All Identity Governance and Intelligence supported adapters can be installed externally on the virtual appliance. Depending on the adapter, an external Security Directory Integrator may be required.

See the corresponding *Adapter Installation and Configuration Guide* for the specific prerequisites, installation and configuration tasks, and issues and limitations. See the *Adapters Release Notes* for any updates to these references.

Procedure

1. Download the adapter package from the IBM Passport Advantage.
   For example, `Adapter-<Adaptername>.zip`.

   The adapter package includes the following files:

Table 4. Adapter package contents

Files	Descriptions
`bundledefinition.json`	The adapter definition file. It specifies the content of the package, and the adapter installation and configuration properties that are required to install and update the adapter.
Adapter JAR profile	An Security Directory Integrator adapter always include a JAR profile which contains: • `targetProfile.json` – Service provider configuration – Resource type configuration – SCIM schema extensions – List of assembly lines • A set of assembly lines in XML files • A set of forms in XML files • Custom properties that include labels and messages for supported languages. Use the **Target Administration** module to import the target profile.

Table 4. Adapter package contents (continued)	
Files	**Descriptions**
Additional adapter specific files	Examples of adapter specific files: • Connector jar files • Configuration files • Script files • Properties files The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.

2. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.
3. Select the instance of the Security Directory Integrator for which you want to manage the adapters and click **Manage** > **SDI Adapters**

   The **SDI Adapters** window is displayed with a table that list the name, version, and any comments about the installed adapters.
4. On the **SDI Adapters** window, click **Install**.
5. On the **File Upload** window, click **Browse** to locate the adapter package and then click **OK**.
   For example, `Adapter-<Adaptername>.zip`.
6. Provide the missing 3rd party libraries when prompted.
   a) On the **File Upload** for Pre-requisite files window, click **Select Files**.

      A new **File Upload** window is displayed.

   b) Browse and select all the missing libraries. For example, `httpclient-4.0.1.jar`

   c) Click **Open**.

      The selected files are listed in the **File Upload** for Pre-requisite files window.

   d) Click **OK**.

      The missing files are uploaded and the adapter package is updated with the 3rd party libraries.
7. Enable secure communication.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Edit**.

   c) Click the **Enable SSL** check box.

   d) Click **Save Configuration**.
8. Import the SSL certificate to the IBM Security Directory Integrator server.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Manage** > **Certificates**.

   c) Click the **Signer** tab.

   d) Click **Import**.

      The **Import Certificate** window is displayed.

   e) Browse for the certificate file.

   f) Specify a label for the certificate. It can be any name.

   g) Click **Save**.

Chapter 4. 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 Installing the dispatcher.

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*.

Related concepts

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

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.

Procedure

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 `SapUMEConnector.jar` file from the adapter package to the *ITDI_HOME*`/jars/connectors` directory.
4. Copy the `tdi/umeprop/SAPUMEAdapterSSL.properties` file from the adapter package to the *ITDI_HOME*`/timsol/umeprop` directory.

   Note:

   The same keystore must be used for multiple SAP AS JAVA server configurations.

   If the environment is to be configured to access multiple end SAP systems and the user attributes to be supported are different for each SAP system, create separate `.properties` file (with a different name) under *ITDI_HOME*`/timsol/umeprop` directory.

   These files hold the mapping between the attributes of the corresponding SAP system and IBM Security Verify Governance Identity Manager profile
5. Restart the adapter service.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details

Complete the service/target form fields.

Related tasks

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

Verifying the adapter installation

After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

These adapter components must exist on the IBM Security Directory Integrator server.

Table 5. Adapter components

Directory	Adapter component
ITDI_HOME/jars/connectors	SapUMEConnector.jar
ITDI_HOME/timsol/umeprop	• SAPUMEAttributeMap.properties • SAPUMEAdapterSSL.properties

If this installation is to upgrade a connector, send a request from IBM Security Verify Governance Identity Manager and verify that the version number in the ibmdi.log matches the version of the connector.

Related concepts

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.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

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*.

Related concepts

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.

Verifying the adapter installation

After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

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 17.
- Create a connector that uses the target profile. See “Adding a connector” on page 19.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

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**.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

Verifying that the adapter is working correctly

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

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 21.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

Verifying that the adapter is working correctly

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

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 6. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 19.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 22.

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.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

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 21.

       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**.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

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.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details

Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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.

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate

The topic describes the procedure to export and install the SSL certificate.

About this task

Note: Steps to export the certificate are valid for both supported versions of SAP NetWeaver Application Server Java. SAP NetWeaver Application Server Java 7.3 EHP1 SP6 Patch 3, or 7.4 SP1 Patch 3, or later versions.

Procedure

1. Start the SSL configuration tool in the SAP NetWeaver administrator. Go to **Configuration Management** > **Security** > **SSL**.
2. Select the added SSL access point or port in the SSL `Access Points` section. Port details are displayed.
3. From the `Server Identity` tab, select the private key entry, and choose `Export Entry` to export the server certificate directly from its private key entry.
4. In the `Export Entry to File` dialog box, select export format **`PKCS#8 Key Pair`**.
   Two files are created: a `PKCS#8 key pair` file and an `X.509 certificate` file.
   For example, `ssl-credentials-cert1.crt`.
5. Download the certificate file and store it in the same directory as the client keystore. For example, the `cacerts` file of the Java Virtual Machine of Security Directory Integrator. The keystore or the `cacerts` file location depends upon the location of Java virtual machine of IBM Security Directory Integrator. The default location is *`ITDI_HOME`*`\jvm\jre\lib\security\cacerts`.

6. Import the downloaded certificate to IBM Security Directory Integrator keystore by using the keytool utility. By default, the keytool utility is located in *ITDI_HOME*\jvm\jre\bin\ directory.
   a) In a command prompt, navigate to the directory *ITDI_HOME*\jvm\jre\lib\security.
   b) Run the following command.

```
keytool -import -alias <local_alias or certificate_name> -file <certificate_file> -
keystore <keystore_name>
```

   Where,

   <local_alias or certificate_name> is the unique name to identify the certificate entry in the Java Virtual Machine keystore.
   <certificate_file> is the name of the SSL certificate from SAP NetWeaver Application Server Java.
   <keystore_name> is the name of the keystore file that is used by SAP UME adapter. The default value is cacerts.

   For example, **keytool -import -alias my_ssl_cert -file ssl-credentials-cert1.crt -keystore cacerts**
7. Enter the keystore password. The initial password of the cacerts keystore is changeit.
8. Type y and press Enter at the prompt that confirms whether you trust the certificated to be imported.

Results

SSL certificate is added to the client keystore cacerts.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

Enabling connectors

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

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.

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

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

Verifying the SPML provisioning interface web link

You must verify the SPML provisioning interface web link.

About this task

SAP provides out-of-the-box SPML provisioning link with SAP Application Server Java.

Procedure

1. Verify `http(s)://<SAP host name or IP>:<port number>/spml/provisioning`

   where:

   <SAP host name or IP>
   Host name of SAP User Management Engine Application Server Java or end resource.

   <port number>
   The HTTP(S) port number for SPML Provisioner of SAP User Management Engine Application Server Java. The port number is calculated as follows:

   50000 + 100*<instance number>

   where:

   <instance number>
   SAP instance of SAP Application Server Java

   For example: If the instance is number 7, then the provisioner is `https(s)://sap_host_name:50107/spml/provisioning`
2. Open the provisioning link in a web brwoser.
3. Provide the SPML provisioning user ID and password.

Results

SPML Provider is successfully installed and configured (full access).

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

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

Service/Target form details

Complete the service/target form fields.

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

An administrator account on the managed resource that has administrative rights and SPML provisioning rights. For example, you want to manage `Resource1` and the SAP User Management Engine Adapter is installed on `Resource1`, then `Admin1` account must have a **Role** containing the following **SAP authorization objects**:

- spmlRole
- Spml_Write_Action
- Spml_Read_Action
- $SAP_J2EE_Engine_Upload

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Related tasks

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.

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

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

SERVICE INFORMATION TAB

This tab describes service details.

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

Note: Slash (/) and backslash (\) characters are not allowed in the service name.

Description
Optional: Specify a description for this service.

IBM Security Directory Integrator location
Optional: Specify the URL for the IBM Security Directory Integrator instance. Valid syntax is `rmi://`*`ip-address`*`:`*`port`*`/ITDIDispatcher`, where *ip-address* is the IBM Security Directory Integrator host and *port* is the port number for the Dispatcher. For example, you might specify the URL as

`rmi://localhost:1099/ITDIDispatcher`. For information about changing the port number, see the *Dispatcher Installation and Configuration Guide*.

Service prerequisite
Prerequisite services names.

Owner
Service owner.

PROVISIONER DETAILS TAB

This tab describes connection details.

SPML Provisioning URL
The full qualified domain name of SAP SPML provisioning interface link. This field is mandatory.

SPML Provisioning User ID
The SAP User account login ID that adapter uses to connect to the SAP instance and performs SPML provisioning. This field is mandatory.

Password
The SAP user password that the adapter uses to connect to SAP instance and performs SPML provisioning. This is field is mandatory.

PROP FILE DETAILS TAB

This tab describes the file path for custom properties file.

Path for Attribute map properties file

This attribute is optional. Specify the file path from where the adapter loads the properties file for a service. If the adapter is configured to use more than one end SAP systems, then each end resource need to have its corresponding properties files. The properties files must have different file names. All these files must reside under *ITDI_HOME*`/timsol/umeprop/directory`.

The default properties file name is `SAPUMEAttributeMap.properties`.

For example: If two SAP servers, *Server1* and *Server2* are configured to use the same Security Directory Integrator, IBM Security Verify Governance Identity Manager service, *service1* is configured for user attributes of *Server1* and *service2*, is configured for user attributes of *Server2*. If the number of attributes for *service1* and *service2* are configured to provision different attributes, two properties files must be created, `propFile1.properties` for *Server1* and `propFile2.properties` for *Server2*. In this case, this attribute must have a value assigned as `umeprop/propFile1.properties` for *service1* and `umeprop/propFile2.properties` for *Server2*.

DISPATCHER ATTRIBUTES TAB

This tab describes Dispatcher attributes.

Assembly Line File System Path
Specify the file path from where the Dispatcher loads the assembly lines. If you do not specify a file path, the Dispatcher loads the assembly lines received from IBM Security Verify Governance Identity Manager. For example, you can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: `C:\Files\IBM\TDI\V7.1\profiles` or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux® operating system: `/opt/IBM/TDI/V7.1/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the Dispatcher can execute simultaneously for the service. For example, enter 10 when you want the Dispatcher to execute maximum ten assembly lines simultaneously for the service. If you enter 0 in the **Max Connection Count** field, the Dispatcher does not limit the number of assembly lines that are executed simultaneously for the service.

Disable Assembly Line Cache
Select the checkbox to disable the assembly line caching in the Dispatcher for the service. The assembly lines for the Add, Modify, Delete, and Test operations are not cached.

STATUS AND INFORMATION TAB

This page contains read-only information about the adapter and managed resource.

These files are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields

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

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

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

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

Profile version
Specifies the version of the adapter 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 ehre 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 workstation name of 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.

Related concepts

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.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

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.

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

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.

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

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.

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

Exporting and installing the Secure Sockets Layer (SSL) certificate
The topic describes the procedure to export and install the SSL certificate.

Verifying the SPML provisioning interface web link
You must verify the SPML provisioning interface web link.

Chapter 5. 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.

For installation steps, see “Installing the adapter binaries or connector” on page 12.

Chapter 6. Configuring

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

- “Customizing the adapter profile” on page 37
- “Adapter attributes and object classes” on page 49
- Special attributes
- “Adapter configuration properties” on page 38

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

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

Customizing the adapter profile

To customize the adapter profile, you must modify the SAP User Management Engine Adapter JAR file. You might customize the adapter profile to change the account form or the service form. Use the Form Designer or `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file for that adapter.

About this task

The JAR file is included in the SAP User Management Engine Adapter compressed file that you downloaded from the IBM website.

The following files are included in the SAP User Management Engine JAR file:

- CustomLabels.properties
- ersapumeaccount.xml
- ersapumeservice.xml
- SapUMEAdd.xml
- SapUMEDel.xml
- SapUMEModify.xml
- SapUMERecon.xml
- SapUMETestAL.xml
- schema.dsml
- service.def

Procedure

1. To edit the JAR file, log on to the workstation where the SAP User Management Engine Adapter is installed.
2. Copy the JAR file into a temporary directory.
3. Extract the contents of the JAR file into the temporary directory.

The following example applies to the SAP User Management Engine Adapter profile. Type the name of the JAR file for your operating system. Run the following command.

```
#cd /tmp
#jar -xvf SapUMEProfile.jar
```

The **jar** command extracts the files into the SAPUMEProfile directory.

4. Edit the file that you want to change.

   After you edit the file, you must import the file into the Identity server for the changes to take effect.
5. To import the file, create a JAR file by using the files in the /tmp directory

   Run the following commands:

```
#cd /tmp
#jar -cvf SapUMEProfile.jar SAPUMEProfile
```

6. Import the JAR file into the IBM Security Verify Governance Identity Manager application server.
7. Stop and start the Identity server
8. Restart the adapter service.

Adapter configuration properties

For guidance on setting IBM Security Directory Integrator configuration properties for the operation of the SAP User Management Engine Adapter, see the *Dispatcher Installation and Configuration Guide*.

Enabling Unicode

To support multibyte character encoding, you must configure the Dispatcher JVM properties.

About this task

The Dispatcher process is a running instance of the IBM Security Directory Integrator server.

The IBM Security Directory Integrator is a Java application that is running its own JVM. You can supply standard JVM properties to the Dispatcher such as:

- Encoding
- Memory allocation initial size
- Memory allocation maximum size

As an example, to set up the dispatcher encoding to UTF-8, perform the following steps:

Procedure

- **On Windows operating systems**
  a) Stop the IBM Security Directory Integrator (Security Adapters) service.
  b) Navigate to the adapter *timsol* directory.
  c) Open the ibmdiservice.props file with a text editor.
  d) Set the value of the jvmcmdoptions property to the Java property value that you want to change to.

     For example, if you want the Dispatcher JVM to run with UTF-8 encoding, then set jvmcmdoptions=- Dfile.encoding=UTF-8.

     Note: When you set multiple properties, separate two properties with a space.
  e) Save and close the ibmdiservice.props file.
  f) Start the IBM Security Directory Integrator (Security Adapters) service.
- **On UNIX or Linux operating systems**

a) Navigate to the *ITDI_HOME* installation directory.

b) Run the following command:

```
vi ibmdisrv
```

c) Modify the string value in the following format:

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

For example, if you want the JVM to use UTF-8 encoding, then modify the command as:

```
"$JRE_PATH/java" -cp "/opt/IBM/TDI/V7.1/jars/3rdparty/IBM/
db2jcc_license_c.jar" "-Dfile.encoding=UTF-8" "
-Dlog4j.configuration=file:etc/log4j.properties" -jar
"/opt/IBM/TDI/V7.1/IDILoader.jar" com.ibm.di.server.RS "$@"
```

d) Restart the dispatcher service. Run one of the following commands to restart the process:

– On AIX® operating systems:

```
/opt/IBM/TDI/V7.1/timsol/ITIMAd restartsrc
```

– On Linux, Solaris, and HP-UX operating systems:

```
/opt/IBM/TDI/V7.1/timsol/ITIMAd restart
```

- **Enabling UTF-8 encoding for the Dispatcher and adapter log file is suggested.**

  Logging capabilities are provided by IBM Security Directory Integrator. Encoding settings can be enabled as follows:

  a) Open the file `ITDI_HOME/`*`solution`*`/etc/log4j.properties` in a text editor.

  b) After the line `log4j.appender.Default.file=logs/ibmdi.log`, add the following setting:

```
log4j.appender.Default.file.encoding=UTF-8
```

  c) The resulting entry looks like the following example:

```
log4j.appender.Default=org.apache.log4j.FileAppender
log4j.appender.Default.file=logs/ibmdi.log
log4j.appender.Default.file.encoding=UTF8
log4j.appender.Default.layout=org.apache.log4j.PatternLayout
log4j.appender.Default.layout.ConversionPattern=%d{ISO8601} %-5p [%c] - %m%n
log4j.appender.Default.append=false
```

  d) Restart the IBM Security Directory Integrator Adapter (Dispatcher) service.

Configuring the Secure Sockets Layer (SSL)

To enable a secure communication between SAP UME adapter and the server, you must configure the SSL.

Before you begin

- You must have the required administrative permissions to perform the keystore maintenance on the AS Java.
- Install the SAP Cryptographic Library. For more information, see Installing the SAP Cryptographic Library for SSL.
- Install the SSL on the SAP NetWeaver Application Server Java. For more information, see Configure the Use of SSL on the AS Java.

To configure SSL, complete the following steps.

Procedure

1. Export the SSL server (SAP NetWeaver AS Java) certificate from the SAP NetWeaver Administrator. See “Exporting and installing the Secure Sockets Layer (SSL) certificate” on page 26.
2. Import the exported certificate to the keystore that is used by the SAP UME adapter on IBM Security Directory Integrator.

   Modifying the client server's keystore, enables the SAP UME adapter trust the server and thus enables the secure communication.
3. Update the SAPUMEAdapterSSL.properties file. See “Updating the SAPUMEAdapterSSL.properties file” on page 51.

Adding a new attribute to the Account form of SAP User Management Engine Adapter

The SAP User Management Engine Adapter can be customized to suit your needs.

Procedure

1. Find the name of the attribute that corresponds to the SPML provisioning for SAP User Management Engine Adapter server.
2. Decide the name of attribute for IBM Security Verify Governance Identity Manager to be mapped.
3. Add the IBM Security Verify Governance Identity Manager attribute name to SAPUMEProfile.jar. See “Customizing the adapter profile” on page 37.
4. Open the *ITDI_HOME*/timsol/umeprop/SAPUMEAttributeMap.properties file.
5. Map the attribute name of the SAP User Management Engine Adapter SPML provisioning and attribute name of the IBM Security Verify Governance Identity Manager profile as follows and save the file:

   ```
   <Attribute_Name_From_SAP_UME>=<Attribute_Name_from_ISIM_profile>
   ```

   where:

   Attribute_Name_From_SAP_UME
   Name of attribute in SAP User Management Engine Adapter SPML provisioning or in a SAP User Management Engine server.

   Attribute_Name_From_ISIM_profile
   Corresponding name of the attriubute in ISIMprofile.jar.

   For example, logonname = eruid

Customizing the SAP User Management Engine Adapter

You can customize the adapter to suit your needs.

About this task

You can increase the range of years on IBM Security Verify Governance Identity Manager for the "Valid From" and "Valid To" calendar widget.

Procedure

1. Use your preferred LDAP browser to locate the following entry:
   erformname=erITIMService,ou=formTemplates,ou=itim,<tenant>,<rootsuffix>
2. Find the **erXML** attribute in the entry.
3. Update the **erXML** attribute to have the following **formElement**:

Set the MIN_YEAR and MAX_YEAR to the year range you want the calendar to display (e.g. from 1900 to 2099). Use the **spanYearRange** option to show the year values between *MIN_YEAR* and *MAX_YEAR*.

```
<formElement direction="inherit" label="$ersapumevalidfrom"
name="data.ersapumevalidfrom">
<dateInput mixYear="MIN_YEAR" maxYear="MAX_YEAR"
spanYearRange="Yes" hoursAndMinutes="false"/>
</formElement>

<formElement direction="inherit" label="$ersapumevalidto"
name="data.ersapumevalidto">
<dateInput mixYear="MIN_YEAR" maxYear="MAX_YEAR"
spanYearRange="Yes" hoursAndMinutes="false"/>
</formElement>
```

For instance, the following example will have the calendar widget contains all the values from 1900 to 2099.

```
<formElement direction="inherit" label="$ersapumevalidfrom"
name="data.ersapumevalidfrom">
<dateInput mixYear="1900" maxYear="2099" spanYearRange="Yes"
hoursAndMinutes="false"/>
</formElement>
```

Note:

- Do **not** combine **spanYearRange** and a **maxYear** of 9999. Because this significantly increases the amount of data that must be sent to the browser for the page to be displayed, and which consequently hurts the performance.
- If you want to include years earlier than 1990, then use the **minYear** attribute. For example, `<dateInput minYear="1974"/>`.
- Any customization done through the IBM Security Verify Governance Identity Manager UI (Form Editor Applet) MUST be done prior to adding any manual date attribute modifications. The Form Editor UI is not equipped to handle these additional date attribute customizations. When edited, the Form Editor UI writes out standard Date attributes regardless of any manual modification previously added. Thus, the manual updates must be redone, or their functionality will be not be effective.

4. Save the updated **erXML** attribute to the LDAP.

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

You can remove the SAP User Management Engine Adapter with a sequence of steps.

Procedure

1. Stop the Dispatcher Service.
2. Delete `SapUMEConnector.jar` from the *`ITDI_HOME`*`/jars/connectors` directory.
3. Remove the adapter `SAPUMEAdapterProps.properties` and `SAPUMEAdapterSSL.properties` file from the `ITDI_HOME/`*`timsol`*`/umeprop` directory.
4. Delete the adapter profile from the Identity server.

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

Chapter 8. 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?

Logs

Logs added to the log file for the adapter or the Dispatcher have a specific format.

```
<Log Level> [<Assembly Line_ProfileName>_<Request Id>]_
[<Connector Name>] - <message>
```

Log Level
Specifies the logging level that you configured for the adapter. The options are DEBUG, ERROR, INFO, and WARN. For information about using the `log4j.properties` file to configure logging, see the *Dispatcher Installation and Configuration Guide*.

Assembly Line
Specifies the name of the assembly line that is logging the information.

ProfileName
Specifies the name of the profile. Profile names may vary based on the adapter that is running or the operating system.

Request ID
Specifies the number of the request. The Request ID is used to uniquely identify a specific request.

Connector Name
Specifies the adapter connector.

Message
Specifies the informational message .

Click the **Test** button on the SAP User Management Engine Adapter service form to send the service, environment, and configuration values to the IBM Security Directory Integrator log during testing. The information collected during the test might assist in diagnosing issues.

Error messages and problem solving

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

This table describes the error messages displayed during run time and corresponding problem descriptions.

Table 7. Error messages and problem descriptions

Error messages	Problem descriptions
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS067E Unable to find configuration for AssemblyLine SapUMETest_SAP_R/3_UME_test-no-requestid_c41b1d60-28f8-11b2-e832-00001ff87342.]	The service name might contain special characters that IBM Security Directory Integrator can not handle, for example "/".
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** Exception Class:org.xml.sax. SAXParseExceptionorg.xml.sax. SAXParseException: Invalid byte 1 of 1-byte UTF-8 sequence.	Java property "–`Dfile.encoding=UTF-8`" needs to be added. Add the property as described in the Installation Guide and Release Notes®, and restart the adapter service.
ibmdi.log Server returned HTTP response code: 401 for URL:	Either user ID or password of the provisioning user is wrong or the user does not have the requires authorization role assigned. Verify the user ID and password by using a web browser.

Table 7. Error messages and problem descriptions (continued)	
Error messages	**Problem descriptions**
Reconciliation does not return all SAP accounts. Reconciliation is successful but some accounts are missing.	For the adapter to reconcile a large number of accounts successfully, you might need to increase Websphere's JVM memory. To do so, complete the following steps on the WebSphere® host machine: **Note:** The JVM memory must not be increased to a value higher than the System memory. 1. Login to the WebSphere Administrative Console. 2. From the left menu, select **Servers** and then click **Application Servers**. 3. A table displays the names of known application servers on your system. Click the link for your primary application server. 4. On the **Configuration** tab, select **Process Definition**. 5. Select the **Java Virtual Machine** property. 6. Enter a new value for **Maximum Heap Size**. The default value is 256 MB. If the allocated JVM memory is not large enough, an attempt to reconcile a large number of accounts by using the adapter result in log file errors, and the reconciliation process might not complete successfully. The Adapter log files contain entries stating why ErmPduAddEntry failed. The `WebSphere_install_dir/logs/itim.log` file will contain **java.lang.OutOfMemoryError** exceptions.

Reconciliation of supporting data

All supporting data can be reconciled through the use of the search filter in the reconciliation query.

To reconcile supporting data only, use the following search filter:

```
(!(objectclass=ersapumeaccount))
```

The SAP systems can have tens of thousands of roles, profiles, and other support data entries. To reconcile accounts only, use the following search filter:

```
(objectclass=ersapumeaccount)
```

Chapter 9. Reference

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

Adapter attributes and object classes

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

After you install the adapter profile, the SAP User Management Engine Adapter supports a standard set of attributes.

The following table lists the standard attributes supported by the SAP User Management Engine Adapter.

Table 8. Supported account attributes

IBM Security Verify Governance Identity Manager Name	Attribute Name	Description	Data Type
User ID	eruid	User's login ID	Character or numeric string
First name	ersapumefirstname	First Name	Character or numeric string
Last name	ersapumelastname	Last Name	Character or numeric string
Email address	ersapumeemail	Email address	Character or numeric string
Language	ersapumelang	Language	SAP predefined value
Security Policy	ersapumesecuritypolicy	Security Policy	SAP predefined value. For more information on user types, see “User types overview” on page 3
Valid From	ersapumevalidfrom	Valid From Date	Up to 6 data format versions
Password	erpassword	Password to log into SAP system. Required for all requests.	SAP predefined value
Valid To	ersapumevalidto	Valid To Date	Up to 6 data format versions
Telephone	ersapumetelephone	Telephone Number	Numeric value
Fax	ersapumefax	Fax Number	Numeric value
Mobile	ersapumemobile	Mobile Number	Numeric value

Table 8. Supported account attributes (continued)

IBM Security Verify Governance Identity Manager Name	Attribute Name	Description	Data Type
Street	ersapumestreetaddress	Street Address	Character or numeric string
City	ersapumecity	City Name	String
State	ersapumestate	State Name	String
Zip	ersapumezip	ZIP Code	Numeric value
Country	ersapumecountry	Country Name	SAP predefined value
Time Zone	ersapumetimezone	Time Zone	SAP predefined value
Organizational Unit	ersapumeorgunit	Organizational Unit	Character or numeric string
Position	ersapumejobtitle	Position	Character or numeric string
Department	ersapumedepartment	Department	Character or numeric string
Role List	ersapumerolelist	Role List	String
User Roles	ersapumeassignedroles	User Roles	String
Display Name	ersapumeroledispname	Display Name of Role	String
Description	ersapumeroledescription	Description of Role	String
Last Modify Date	ersapumerolelastmodifydate	Last Modify Date	String (Read Only)
SAP Role ID	ersapumeroleid	SAP Role ID	String
Data Source	ersapumeroledatasource	Data Source of Role	SAP predefined value
Group List	ersapumegrouplist	Group List	String
Display Name	ersapumegrpdispname	Display Name of Group	String
Description	ersapumegrpdescription	Description of Group	String
Last Modify Date	ersapumegrplastmodifydate	Last Modify Date	String (Read Only)
SAP Group ID	ersapumegrpid	SAP Group ID	String
Data Source	ersapumegrpdatasource	Data Source of Group	SAP predefined value

Updating the SAPUMEAdapterSSL.properties file

The SAPUMEAdapterSSL.properties file contains properties that are specific to the SSL configuration. The SAPUMEAdapterSSL.properties file is located in the *ITDI_HOME*\jvm\jre\lib\security directory.

Adapters use the keystore for SSL certificate validation by using the key value pairs. When SPML provisioning interface of SAP NW AS Java server uses HTTPS, set the following key value pairs.

```
#TDI JVM trustStore location
javax.net.ssl.trustStore=<Path_for_Trust_Store>
```

```
#TDI JVM trustStore password
javax.net.ssl.trustStorePassword=<Password_for_Trust_Store>
```

```
#TDI JVM keystore location
javax.net.ssl.keyStore=<Path_for_Key_Store>
```

```
#TDI JVM keystore password
javax.net.ssl.keyStorePassword=<Password_for_Key_Store>
```

```
#TDI JVM trustStore file type
javax.net.ssl.trustStoreType=<File_extension_of_Trust_Store>
```

Example

To configure SSL using cacert keystore that is available in the Java Virtual Machine of IBM Security Directory Integrator, assign the following values.

```
#TDI JVM trustStore location
javax.net.ssl.trustStore=ITDI_HOME/jvm/jre/lib/security/cacerts
```

```
#TDI JVM trustStore password
javax.net.ssl.trustStorePassword=changeit
```

```
#TDI JVM keystore location
javax.net.ssl.keyStore=ITDI_HOME/jvm/jre/lib/security/cacerts
```

```
#TDI JVM keystore password
javax.net.ssl.keyStorePassword=changeit
```

```
#TDI JVM trustStore file type
javax.net.ssl.trustStoreType=JCEKS
```

Where, *ITDI_HOME* is a full qualified path of IBM Security Directory Integrator.

Index

U

V