IBM Security Verify Governance Identity Manager

SAP HR feed adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The SAP HR feed adapter uses the Security Directory Integrator functionality to enable communication between the Identity server and the SAP Netweaver Application Server ABAP.

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

The adapter is designed to reconcile personal and organizational information from the target system.

It checks the connection between the SAP Netweaver Application Server ABAP and Identity server.

You can install the XSL stylesheet with the adapter to customize and configure the adapter extension to meet the business requirements.

Related concepts

Architecture
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.

Architecture

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:

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

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

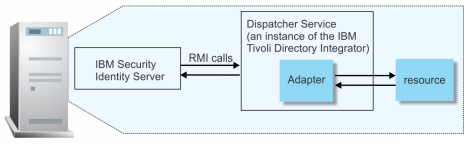

Figure 1. The architecture of the SAP HR feed adapter

Related concepts

Features of the adapter
The adapter is designed to reconcile personal and organizational information from the target system.

Supported configurations

The adapter supports both single and multiple server configurations.

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

Single server configuration

In a single server configuration, the following components are installed in one server to establish communication with the SAP Application Server:

- Identity server
- Security Directory Integrator server
- SAP HR feed adapter

The SAP Netweaver Application Server ABAP is installed on a different server as shown in Figure 2 on page 2.

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the following components are installed on different servers.

- Identity server
- Security Directory Integrator server
- SAP HR feed adapter
- SAP Netweaver Application Server ABAP

TheSecurity Directory Integrator server and the SAP HR feed adapter are installed on the same server as shown in Figure 3 on page 2.

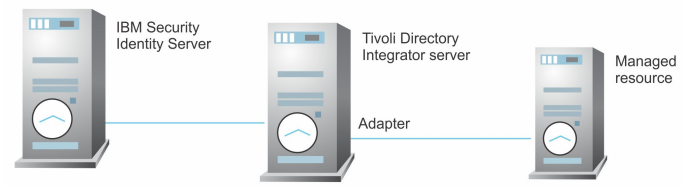

Figure 3. Example of a multiple server configuration

The SAP HR feed adapter is configurable and customizable.

Note: Support can extend only to the configuration of the adapter such as adding the mapping for additional attributes and XSL stylesheets. Support does not cover the additions or modifications of the Security Directory Integrator Assembly Line scripts for example.

Related concepts

Features of the adapter

The adapter is designed to reconcile personal and organizational information from the target system.

Architecture

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

Chapter 2. Planning

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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

b. Configure 2-way authentication.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Prerequisites

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

Table 1 on page 7 identifies the prerequisites for the adapter installation.

Table 1. Prerequisites to install the adapter	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0
SAP Netweaver Application Server ABAP with SAP Basis Component with SAP HR module installed.	Tested with SAP Netweaver 730, Component version SAP ECC 6.0 with SAP HR Fix Pack 22 installed
Security Directory Integrator adapters solution directory	A Security Directory Integrator work directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

Software downloads

Log in to your account on the IBM Passport Advantage® website and download the software.

Go to IBM Passport Advantage. See the *IBM Security Verify Governance Identity Manager Download Document*.

Note: You can also obtain 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.

Note: Ensure that the adapter user is granted access to SNC.

Table 2. Required information to install the adapter		
Required information	**Description**	**Value**
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory, which contains the files for the adapters.	**Windows:** • *drive*\Program Files \IBM\TDI\V7.2 **UNIX:** • /opt/IBM/TDI/V7.2
Adapter Solution Directory	See the *Dispatcher Installation and Configuration Guide*.	**Windows:** • *drive*\Program Files \IBM\TDI\V7.2*timsol* **UNIX:** • /opt/IBM/TDI/V7.2/ *timsol*

Chapter 3. Installing

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

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 stylesheets

The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

About this task

The adapter stylesheets must be copied from the SAP HR feed adapter package to an `xsl` directory.

Procedure

1. If the Dispatcher is installed in the Security Directory Integrator adapters solution directory (for example, `timsol`), navigate to that directory. Otherwise, navigate to the *`ITDI_HOME`* directory.
2. Create a directory with the name `xsl`, if one does not exist.
3. Depending on your Dispatcher installation, copy the files from the `tdi/xsl` directory of the adapter package to the `xsl` directory of the IBM Security Directory Integrator solution directory or *`ITDI_HOME`* directory.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Before you begin

- The Dispatcher must be installed.

Procedure

1. Copy `tdi/connectors/*.jar` from the adapter package to the *ITDI_HOME*`/jars/connectors` directory.
2. Copy `tdi/functions/*.jar` from the adapter package to the *ITDI_HOME*`/jars/functions` directory.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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

Installing the SAP Java Connector (JCo)

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. After you download the JCo package, unpack the contents and then follow these instructions.

Before you begin

- Download the SAP Java Connector (JCo).

  The adapter requires access to the SAP Java Connector (JCo) API at run time. This API must be downloaded from the SAP support portal. Access to this website requires authentication with a valid SAP support ID (S-ID). Contact your SAP marketing representative to obtain one of these IDs.
- Unpackage the content of the file.

Procedure

- **Windows:**
  a) Copy the `sapjco3.jar` file into *ITDI_HOME*`/jars/3rdparty/others`.
  b) Copy the `sapjco3.dll` file into *ITDI_HOME*`/libs`.
  On Windows, JCo 3 requires additional Microsoft Visual C++ 2005 libraries to be installed. Installation details for the package that contains these libraries are specified in Microsoft Knowledge Base article 973544.
  c) Restart the adapter service.
- **UNIX or Linux:**
  a) Create a symbolic link to the `sapjco3.jar` file in *ITDI_HOME*`/jars/3rdparty/others`:

```
ln -s <sapjco_install_dir>/sapjco3.jar
   ITDI_HOME/jars/3rdparty/others/sapjco3.jar
```

  b) Add the SAP JCo installation directory to the dynamic library path:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<sapjco_install_dir>
export LIBPATH=$LIBPATH:<sapjco_install_dir>
```

  c) Restart the Dispatcher.
  For assistance, see “Restarting the adapter service” on page 23.

  Note: These steps ensure that the sapjco3 libraries are included in the executable path and in the loadable library path, when required. The environment variable for dynamic library path and the command for restarting the Dispatcher might vary on different UNIX operation systems.
- **Linux on System z 64-bit architecture (s390x)**
  a) Create a symbolic link to the `sapjco3.jar` file in *ITDI_HOME*`/jars/3rdparty/others`:

```
ln -s <sapjco_install_dir>/sapjco3.jar
   ITDI_HOME/jars/3rdparty/others/sapjco3.jar
```

  b) Add the SAP JCo installation directory to the dynamic library path:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<sapjco_install_dir>
export LIBPATH=$LIBPATH:<sapjco_install_dir>
```

c) SAP JCo is supported on Linux on System z only for 64-bit architecture. The IBM Security Directory Integrator is packaged only with the 31-bit version of Java™. Additionally, it must be configured to run with the 64-bit version of Java.

The following steps change the JVM for the complete IBM Security Directory Integrator instance, not only for the Dispatcher.

a. Stop the Dispatcher:

```
/etc/init.d/ITIMAd stop
```

b. Install the IBM Java 1.5 64-bit release (for example `ibm-java2-s390x-5.0.9.rpm`)

d) Change the IBM Security Directory Integrator JRE to become 64 bit:

```
mv  ITDI_HOME/jvm/jre ITDI_HOME/jvm/jre32
ln -s JAVA_1.5_64BIT_HOME/jre ITDI_HOME/jvm/jre
```

e) Start the Dispatcher:

```
/etc/init.d/ITIMAd 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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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

Enabling the SAP Java Connector (JCo) trace

Activate traces to get more information that can help you analyze errors that are related to connection issues.

Procedure

1. Navigate to the IBM Security Directory Integrator adapters solution directory.
   For example, *ITDI_HOME*\timsol.
2. Open the file in an editor.

   For Windows operating systems
   Open the file ibmdiservice.props

   For UNIX or Linux operating systems
   Open the file ibmdisrv
3. Edit the following property:

   - For Windows operating systems

     ```
     jvmcmdoptions=-Djco.trace_level=10 -Djco.trace_path=E:\jco_trace\ -Djco.rfc=1
     ```

     Where:

     -Djco.trace_level=N
     The trace level can be 0 - 10, where 10 being the most detailed trace.

     -Djco.trace_path=<PATH>
     If a trace path is set, the JCo traces are written to one or multiple files that are named JCO*<date>*_*<time>*.*<no>*.trc in the specified PATH directory. Otherwise, the JCo traces are written to the standard output stream, where, by default is an output to the console.

     Note: The jco_trace directory must be available.

     -Djco.jrfc=1
     If set to 1, JCo trace is enabled for all connections. This configuration should be the last resort.

- For UNIX or Linux operating systems

```
-Djco.trace_level=10 -Djco.trace_path=/opt/jco_trace/ -Djco.rfc=1
```

Where:

-Djco.trace_level=N
The trace level can either be 0 or 10, where 10 being the most detailed trace.

-Djco.trace_path=<PATH>
If a trace path is set, the JCo traces are written to one or multiple files that are named JCO*<date>*_*<time>*.*<no>*.trc in the specified PATH directory. Otherwise, the JCo traces are written to the standard output stream, where, by default is an output to the console.

Note: The `jco_trace` directory must be available.

-Djco.jrfc=1
If set to 1, JCo trace is enabled for all connections. This configuration should be the last resort.

For example:

```
"%TDI_JAVA_PROGRAM%"  -Xdebug -Xnoagent -Djava.compiler=NONE -Djco.trace_level=10
 -Djco.trace_path=/opt/jco_trace/ -Djco.rfc=1
-Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=5555 -classpath
"%TDI_HOME_DIR%\IDILoader.jar" %ENV_VARIABLES% com.ibm.di.loader.ServerLauncher %*
set RC=%ERRORLEVEL%
```

4. Save your changes.
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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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

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

Complete these steps to set up the Dispatcher encoding to UTF-8.

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:

```
"$JRE_PATH/java" -cp "/opt/IBM/TDI/V7.1.1/jars/3rdparty/IBM/
db2jcc_license_c.jar" "-Dlog4j.configuration=file:etc/
log4j.properties" -jar "/opt/IBM/TDI/V7.1.1/IDILoader.jar"
com.ibm.di.server.RS "$@"
```

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

```
"$JRE_PATH/java" -cp "/opt/IBM/TDI/V7.1.1/jars/3rdparty/IBM/
db2jcc_license_c.jar" "-Dfile.encoding=UTF-8" "
-Dlog4j.configuration=file:etc/log4j.properties" -jar
"/opt/IBM/TDI/V7.1.1/IDILoader.jar" com.ibm.di.server.RS "$@"
```

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

On AIX® operating systems

```
/opt/IBM/TDI/V7.1.1/timsol/ITIMAd restartsrc
```

On Linux, Solaris, and HP-UX operating systems

```
/opt/IBM/TDI/V7.1.1/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.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR

file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR

file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

Table 3. Adapter components

Directory	Adapter component
ITDI_HOME/jars/connectors	SapNWUserConnector.jar, SapNWSupport.jar
ITDI_HOME/jars/functions	SapNWRfc.jar
ITDI_HOME/jars/3rdparty/other	sapjco3.jar
ITDI_HOME/libs	sapjco3.dll
ITDI_HOME/solution/xsl	• sapnw_bapi_errors.properties • sapnw_bapi_person_getdetail_precall.xsl • sapnw_bapi_person_address_precall.xsl • sapnw_bapi_person_email_precall.xsl • sapnw_bapi_person_getdetail_postcall.xsl

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

About this task

The **USER_ADD** flow process does not include the **Generate Unique UserID** rule by default. You must manually add the **Generate Unique UserID** rule before you can successfully import HR feed data.

Procedure

1. Log in to the IBM Security Verify Governance Identity Manager Administration Console.
2. Click **Access Governance Core**.
3. Click **Configure** > **Rules** > **Rules**.
4. In the **Rules** tab on the left pane, complete the following fields:
   a) In the **Rule Class** field, select **Live Events**.
   b) In the **Queue** field, select **IN**.
   c) In the **Rule Flow** field, select **USER_ADD**.
5. In the **USER_ADD** flow process, expand and select the **User Add default group** folder for the rule group.
6. In the right pane, expand **Rules Package**.
7. In the **Rules Package** pane, select **Generate Unique UserID**.
8. From the **Actions** menu, click **Add**.
   In the left pane, **Generate Unique UserID** is displayed in the rule group that is named **User Add default group**.
9. In the left pane, move **Generate Unique UserID** so it is located after **Create OrgUnit From User Data** before **Create User**.
10. Restart the Identity server.

a) On the **Appliance Dashboard** of the Verify Governance Identity Manager virtual appliance console, locate the **Server Control** widget.

b) Select .

c) Click **Restart**.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

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 user or OU attributes.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

Related tasks

Installing the adapter stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 26.
- Create a connector that uses the target profile. See “Adding a connector” on page 28.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter’s IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector

The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 30.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter’s IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 4. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 28.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 32.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 30.

       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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets

The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

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 user or OU attributes.

About this task

This task involves either an user or OU attribute mapping definition file, which are both included in the HR adapter package.

The file consists of Verify Governance Identity Manager user or OU attributes and their equivalent attributes in the managed HR target. The file is structured as *<IGI_attribute> = <HR_target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<HR_target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<HR_target_attribute>* of `ersaphraccount`. For example:

```
GIVEN_NAME=ersaphrgivenname
```

Some *<IGI_attribute>* do not have a defined *<HR_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].<HR_target_attribute>.<IGI_attribute> =
   [<HR_target_attribute_value1>=<IGI_attribute_value1>;...;
   <HR_target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

   For example:

   ```
   [conversion].ersaphrgender.GENDER=[M=0;F=1;U=]
   ```

   ```
   [conversion].erptigidisabled.DISABLED=[Y=1;N=0]
   [conversion].erptigigender.GENDER=[M=0;F=1]
   ```

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

   ```
   [conversion.date].ersaphrdob.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.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets

The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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.

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.

The SAP HR feed adapter service form has several tabs, each containing information that you must specify:

- "Adapter Details tab" on page 38
- "SAP Connection Details tab" on page 38
- "Reconciliation Advanced Mapping tab" on page 38
- "Dispatcher Attributes tab" on page 39

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

Verifying that the adapter is working correctly

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

Adapter Details tab

This tab describes service details.

Service name
Specify a name that defines this service on the IBM Security Verify Governance Identity Manager 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, `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.

SAP Connection Details tab

This tab describes the parameters that have to be specified to establish a remote connection to the SAP resource from IBM Security Directory Integrator.

Target Client
The SAP instance client number. This field is mandatory.

Login ID
The SAP User account login ID that adapter uses to connect to the SAP instance. This field is mandatory.

Password
Password for SAP User account. This field is mandatory.

SAP System (DNS hostname or IP)
Host name of the SAP server host computer only if DNS is set up correctly. Otherwise, use the IP address. This field is mandatory.

SAP Systems Number
The SAP server system number. This field is mandatory.

SAP Logon Language
The language ISO identifier to be used by the adapter. This parameter is optional.

Reconciliation Advanced Mapping tab

Settings in this tab apply only during reconciliation and search operation requests.

The following attributes of this tab are all optional service attribute.

- Search Person Basic Iterate Request XSL Stylesheets
- Search Person Basic Iterate Response Stylesheet

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 that are received from IBM Security Verify Governance Identity Manager.

For example:

Windows operating system
`C:\Files\IBM\TDI\V7.2\profiles`

UNIX and Linux operating system
`/opt/IBM/TDI/V7.2/profiles`

Max Connection Count

Specify the maximum number of assembly lines that the Dispatcher can execute simultaneously for the service.

For example, enter 10 if you want the Dispatcher to execute a maximum of 10 assembly lines simultaneously for the service. If you enter 0, the Dispatcher does not limit the number of assembly lines that are executed simultaneously for the service.

Assembly lines occupy the JVM memory. Too many assembly lines can cause an out-of-memory scenario in the IBM Security Directory Integrator server. Each assembly line also creates multiple connections to the end point. The end point might have a limit on the number of remote connections allowed. As such, the adapter requests might fail.

Disable Assembly Line Cache

Select the check box to disable the assembly line caching in the Dispatcher for the service. When disabled, the assembly lines for the Add, Modify, Delete, and Test operations are not cached.

Select the check box if the requirement is to enable caching. When enabled, the entire assembly line object is saved in the cache. The connection to the SAP resource is maintained. The next request that the adapter receives can reuse this connection.

Creating a new connection to the SAP resource can take a lot of time. Caching data can save time and resource utilization.

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 you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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 stylesheets
The SAP HR feed adapter requires a set of stylesheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

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 user or OU attributes.

Chapter 4. Upgrading

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

See the Release Notes® for the supported software versions or for specific instructions.

To upgrade the connector, see “Installing the adapter binaries or connector” on page 11.

Upgrading the Dispatcher

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

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

- If the Dispatcher version that is mentioned in the release notes is later than the existing version on your workstation, install the Dispatcher.
- If the Dispatcher version that is mentioned in the release notes is the same or earlier than the existing version, do not install the Dispatcher.

Note: The Dispatcher installer stops the Dispatcher service before the upgrade and restarts it after the upgrade is complete.

Upgrading the adapter profile

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

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

Chapter 5. Configuring

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

See the *IBM Security Dispatcher Installation and Configuration Guide* for 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

You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

About this task

Use the the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file.

The JAR file is included in the adapter package that you downloaded from the IBM Passport Advantage website. The JAR file and the files in the JAR file vary depending on your operating system.

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

The adapter JAR file includes the following files:

- `CustomLabels.properties`
- `erSapHRAccount.xml`
- `erSapHRService.xml`
- `SapHRSearch.xml`
- `SapHRTest.xml`
- `schema.dsml`
- `service.def`

Procedure

1. Edit the JAR file.
   a) Log on to the workstation where the SAP HR feed adapter is installed.
   b) On the **Start** menu, select **Programs → Accessories → Command Prompt**.
   c) Copy the JAR file into a temporary directory.
   d) Extract the contents of the JAR file into the temporary directory by running the following command. The following example applies to the SAP HR feed adapter profile. Type the name of the JAR file for your operating system.

```
cd c:\temp cd /tmp
jar -xvf SapHRProfile.jar
```

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

e) 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.

2. Import the file.

a) Create a JAR file by using the files in the directory.

Run the following commands:

Windows

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

UNIX

```
cd /tmp
jar -cvf SapHRProfile.jar SapHRProfile
```

b) Import the JAR file into the IBM Security Verify Governance Identity Manager application server.

c) Stop and start the Identity server.

d) Restart the adapter service.

Related concepts

XSL stylesheets
The adapter can be configured by modifying the XSL stylesheet advanced mappings.

BAPI method execution with stateful connection
The SAP JCo 3.x connection between SAP R3 and IBM Security Verify Governance Identity Manager, is not stateful by default. The stateful connection is required in case of transactional BAPIs.

Related tasks

Improving the reconciliation operation performance
Use the Java settings to improve the performance of the reconciliation operation.

XSL stylesheets

The adapter can be configured by modifying the XSL stylesheet advanced mappings.

The adapter can function without configuring any advanced mapping XSL transformations. The default values for each advanced mapping are used. Any advanced mappings that are configured by the user, override the listed default XSL transformations.

RECONCILIATION ADVANCED MAPPING TAB

Settings of this tab apply only during reconciliation and search operation requests.

Search Person Basic Iterate Request XSL Stylesheet

This attribute is a multi-valued attribute. The value is a list of XSL transformation file names that are separated by space (" ").

Each transform is run in the defined order and produce an RFC request. Each RFC request is run by the adapter. Each RFC that is run is responsible for returning parts of the user account details.

If more than one transform and resulting RFC is run, the result of each RFC call is appended to an XML result document with a root tag named <bapiResults>. This result list is passed to the **Search Person Basic Iterate Request XSL Stylesheet**. If only one XSL file name is supplied, the resulting RFC is run. The response is passed directly to **Search Person Basic Iterate Request XSL Stylesheet**.

Each XSL transform file must be deployed with the adapter in the xsl directory relative to the Dispatcher solution directory.

If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

```
xsl/sapnw_bapi_person_getdetail_precall.xsl
xsl/sapnw_bapi_person_address_precall.xsl
xsl/sapnw_bapi_person_email_precall.xsl
```

Search Person Basic Iterate Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response or responses from the RFC calls. The calls are run based on the setting of **Search Person Basic Iterate Response Stylesheet**. The result of running this transform is sent to the IBM Security Verify Governance Identity Manager server.

The XSL transform file must be deployed with the adapter in the `xsl` directory relative to the Dispatcher solution directory.

If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
sapnw_bapi_person_getdetail_postcall.xsl
```

Related concepts

BAPI method execution with stateful connection
The SAP JCo 3.x connection between SAP R3 and IBM Security Verify Governance Identity Manager, is not stateful by default. The stateful connection is required in case of transactional BAPIs.

Related tasks

Customizing the adapter profile
You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

Improving the reconciliation operation performance
Use the Java settings to improve the performance of the reconciliation operation.

BAPI method execution with stateful connection

The SAP JCo 3.x connection between SAP R3 and IBM Security Verify Governance Identity Manager, is not stateful by default. The stateful connection is required in case of transactional BAPIs.

To make the connection stateful between Business Application Programming Interfaces (BAPIs) method execution, add the following tags to the XSL files according to your requirement.

To begin a stateful connection, add this tag to your XSL:

```
<CONTEXT_BEGIN> & </CONTEXT_BEGIN> or <CONTEXT_BEGIN/>
```

To end a stateful connection, add this tag to your XSL:

```
<CONTEXT_END> & </CONTEXT_END> or <CONTEXT_END/>
```

It is not necessary to have both <CONTEXT_BEGIN/> and <CONTEXT_END/> tags in the same XSL. Nested <CONTEXT_BEGIN/> and <CONTEXT_END/> tags can also be implemented, if the tags are nested correctly, else unexpected result can occur. Stateful connection started by each <CONTEXT_BEGIN/> tag gets ended by its associated <CONTEXT_END/> tag.

Note: Stateful connection that is started by each <CONTEXT_BEGIN/> tag gets ended by its associated <CONTEXT_END/> tag. If the <CONTEXT_BEGIN/> tag does not have its associated <CONTEXT_END/> tag, the stateful connection gets terminated at the end of JCo connection.

For example, the <CONTEXT_BEGIN/> and <CONTEXT_END/> tags are added to the following files:

- `sapnw_bapi_charact_create.xsl` file

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
   version="1.0"
   xmlns:xalan="http://xml.apache.org/xslt">
…..
…..
<BAPI_CHARACT_CREATE>
```

```
<CONTEXT_BEGIN/>
…..
…..
</BAPI_CHARACT_CREATE>
…..
…..
</xsl:stylesheet>
```

- `sapnw_bapi_transaction_commit.xsl` file

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
   version="1.0"
   xmlns:xalan="http://xml.apache.org/xslt">
…..
…..
<BAPI_TRANSACTION_COMMIT>
…..
…..
<CONTEXT_BEGIN/>
</BAPI_TRANSACTION_COMMIT>
…..
…..
</xsl:stylesheet>
```

Related concepts

XSL stylesheets

The adapter can be configured by modifying the XSL stylesheet advanced mappings.

Related tasks

Customizing the adapter profile

You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

Improving the reconciliation operation performance

Use the Java settings to improve the performance of the reconciliation operation.

Improving the reconciliation operation performance

Use the Java settings to improve the performance of the reconciliation operation.

Procedure

1. Navigate to the *JAVA_Home*`/lib` directory.
2. Rename `jaxp.properties.sample` to `jaxp.properties`.
3. In the `jaxp.properties` file, remove the comment tags for the following properties:

```
javax.xml.transform.TransformerFactory=
  com.ibm.xtq.xslt.jaxp.compiler.TransformerFactoryImpl
javax.xml.xpath.XPathFactory=
  org.apache.xpath.jaxp.XPathFactoryImpl
javax.xml.parsers.SAXParserFactory=
  org.apache.xerces.jaxp.SAXParserFactoryImpl
javax.xml.parsers.DocumentBuilderFactory=
  org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
```

4. Check the performance of the reconciliation operation. If it fails, continue to step 5.
5. Set the following system property:

```
export IBM_JAVA_OPTIONS=-Djavax.xml.transform.TransformerFactory=
  org.apache.xalan.processor.TransformerFactoryImpl
```

6. Check the performance of the reconciliation operation again.

Related concepts

XSL stylesheets

The adapter can be configured by modifying the XSL stylesheet advanced mappings.

BAPI method execution with stateful connection

The SAP JCo 3.x connection between SAP R3 and IBM Security Verify Governance Identity Manager, is not stateful by default. The stateful connection is required in case of transactional BAPIs.

Related tasks

Customizing the adapter profile

You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

For more information about the settings, see the following resources:

Chapter 6. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

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

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

```
<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 can 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.

When you click the **Test** button on the SAP HR feed adapter service form, the service, environment, and configuration values are sent to the IBM Security Directory Integrator log during the test. These collected information can help diagnose 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.

The following table contains warnings or errors, which might be displayed when the SAP HR feed adapter is installed on your system.

Table 5. Specific warning and error messages and actions

Message	Action
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGIMT401E An error occurred while starting the AssemblyLines/SapHRTest_SAP - TV2_test-no-requestid_9dbf1884-29b1-11b2-689a-00000a020011 agent. Error: java.lang.ExceptionInInitializerError: Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: sapjco3 (Not found in java.library.path) operation on the IBM Security Directory Integrator server. Error: {1}	The Microsoft Visual C++ 2005 libraries are not installed, or the permissions for the .dll file are not correct. Verify the installation steps and permissions.
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 SapHRTest_SAP_R/3_NW_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, “/”.

Table 5. Specific warning and error messages and actions (continued)	
Message	**Action**
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS809E handleException - cannot handle exception , script java.lang.NoClassDefFoundError: com.sap.conn.jco.ext.DestinationDataProvider	SAP JCo is not installed, or permissions for the .jar file are not correct. Verify the installation steps and permissions.
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** Caused by: java.io.FileNotFoundException: app/itdi611/ solution/xsl/ sapnw_bapi_errors.properties (No such file or directory)	The property and .xsl files were copied to the wrong directory during the adapter installation, or file permissions are not correct. Verify the installation steps and permissions.
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS809E handleException - cannot handle exception , script java.lang.ExceptionInInitializerError: Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: sapjco3 (Not found in java.library.path)	The path for the SAP JCo dynamic library is not correct. Correct it and restart the IBM Security Verify Governance Identity Manager adapter service.
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 and Configuration Guide, and Release Notes. Restart the IBM Security Verify Governance Identity Manager adapter service.

Table 5. Specific warning and error messages and actions (continued)

Message	Action
Reconciliation doesn't 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. Complete the following steps on the WebSphere® host machine: **Note:** Do not increase the JVM memory to a value higher than the system memory. 1. Log in to the WebSphere Administrative Console. 2. From the left menu, select **Servers** and then **Application Servers**. A table displays the names of known application servers on your system. 3. 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, the attempt to reconcile a large number of accounts using the IBM Security Verify Access adapter will result in log file errors. The reconciliation process will not complete successfully. The adapter log files will contain entries that state **ErmPduAddEntry** failed. The `WebSphere_install_dir/logs/itim.log` file will contain **java.lang.OutOfMemoryError** exceptions.

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.

Procedure

1. Stop the IBM Security Verify Governance Identity Manager Dispatcher Service.
2. Remove the SAP HR feed adapter JAR files.
   a. Delete SapHRProfile.jar and SAPNWConnector.jar, SAPNWUserConnector.jar from the *ITDI_HOME*/jars/connectors directory.
   b. Delete SapNWRfc.jar from the *ITDI_HOME*/jars/functions directory.

      Note: If you are using this IBM Security Directory Integrator to provision to a SAP NetWeaver target then do not delete theSAPNWConnector.jar, SAPNWUserConnector.jar and SapNWRfc.jar.
3. Remove the adapter stylesheets from the *ITDI_HOME*/*solution*/xsl directory.
4. Delete the adapter profile from the Identity server.

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

Chapter 8. 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.

The SAP HR feed adapter supports a standard set of attributes.

Table 6. Supported attributes

Attribute Name	Description	Required	Managed Resource Attribute
erUid	Employee number	YES	PERNR
ersaphrgivenname	First name of person	NO	FIRSTNAME
ersaphrlastname	Last name of person	NO	LASTNAME
ersaphrgender	Gender	NO	GENDER
ersaphrdob	Date of birth	NO	DATEOFBIRTH
ersaphrbirthplace	Place of birth	NO	BIRTHPLACE
ersaphrbirthcountry	Country of birth	NO	COUNTRYOFBIRTH
ersaphrzipcode	Zip Code	NO	POSTALCODECITY
ersaphrcountry	Country	NO	NAMEOFCOUNTRY
ersaphrphoneno	Phone number	NO	TELEPHONENUMBER
ersaphraddress	Address	NO	STREETANDHOUSENO
ersaphrcity	City	NO	DISTRICT
ersaphremailid	Email ID	NO	EMAIL
ersaphrpersonou	Organizational unit	NO	ORGANIZATION NAME

USER_ERC attribute mapping

The following table lists which adapter attributes are mapped to the attributes stored in the IBM Security Verify Governance Identity Manager USER_ERC table.

Table 7. USER_ERC attribute mapping

USER_ERC attributes	Description	Required	SAP HR feed adapter attribute name
ID	Table unique identifier. The sequence `user_erc_seq` might be called to generate this unique number.	YES	
PM_CODE	USER ID or User Code. It is not required. USER ID can be generated using a rule.	NO	
OU	Organizational unit code. Used to store the user in the OU available in the system. This attribute might or might not be in the database. Create the new OU in the `root`.	YES	**ersaphrpersonou**
USER_TYPE	User type name. This attribute might or might not be in the database. It can be created dynamically using a custom rule.	NO	
PROCESSED	Deprecated	NO	
LAST_MOD_USER	Contains the name of the last user or process that modified the USER_ERC table.	NO	
LAST_MOD_TIME	Contains the date and time when the last change occurred. Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed.	NO	
POST_EVENT	Deprecated	NO	
SKIP	Deprecated	NO	
ACTION_TYPE	SAP HR property information.	NO	
ACTION_CAUSE	SAP HR property information.	NO	
ACTION_TYPE_LAST	SAP HR property information.	NO	

Table 7. USER_ERC attribute mapping (continued)

USER_ERC attributes	Description	Required	SAP HR feed adapter attribute name
ACTION_CAUSE_LAST	SAP HR property information.	NO	
GIVEN_NAME	User name	YES	**ersaphrgivenname**
SURNAME	User surname	YES	**ersaphrlastname**
GENDER	• 0 = male • 1 = female	NO	**ersaphrgender**
BIRTHDAY	Birthday	NO	**ersaphrdob**
BIRTH_PLACE	Birth place	NO	**ersaphrbirthplace**
BIRTH_COUNTRY	Birth country	NO	**ersaphrbirthcountry**
ACCOUNT_EXPIRY_DATE	The Verify Governance Identity Manager account can be created with an expiration date. Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed.	NO	
IDENTIFICATION_NUMBER	User ID present into HR system	NO	**eruid**
CURRENTOU	Deprecated	NO	
NATION	Nation	NO	
ZIPCODE	Zip code	NO	**ersaphrzipcode**
COUNTRY	Country	NO	**ersaphrcountry**
PHONE_NUMBER	Phone number	NO	**ersaphrphoneno**
DISABLED	Indicates that the user is disabled and it disables all user accounts	NO	
DELETED	Use this attribute to implement a particular logic when a user is deleted from HR system. For example, a user can keep all his account for 3 weeks and then the user is deleted	NO	
ATTR1	Spare attribute	NO	
ATTR2	Spare attribute	NO	
ATTR3	Spare attribute	NO	
ATTR4	Spare attribute	NO	
ATTR5	Spare attribute	NO	

Table 7. USER_ERC attribute mapping (continued)			
USER_ERC attributes	**Description**	**Required**	**SAP HR feed adapter attribute name**
ATTR6	Spare attribute	NO	
ATTR7	Spare attribute	NO	
ATTR8	Spare attribute	NO	
ATTR9	Spare attribute	NO	
ATTR10	Spare attribute	NO	
ATTR11	Spare attribute	NO	
ATTR12	Spare attribute	NO	
ATTR13	Spare attribute	NO	
ATTR14	Spare attribute	NO	
ATTR15	Spare attribute	NO	
SCHEDULE	Deprecated	NO	
ADDRESS	User address	NO	**ersaphraddress**
CITY	User city	NO	**ersaphrcity**
EMAIL	User email	NO	**ersaphremailid**

OrganizationalUnit_ERC attribute mapping

The following table lists which adapter attributes are mapped to the attributes stored in the IBM Security Verify Governance Identity Manager OrganizationalUnit_ERC table.

Table 8. OrganizationalUnit_ERC attribute mapping			
OrganizationalUnit_ERC attributes	**Description**	**Required**	**SAP HR feed adapter attribute name**
ID	Table unique identifier. The sequence `organizational_unit_erc_seq` might be called to generate this unique number.	YES	
PARENT	Organizational unit parent code This attribute might or might not be in the database. Create the new OU in the `root`.	NO	
OU	Organizational unit code (unique identifier)	YES	**ersaphrorgid**
DESCRIPTION	Description	NO	**ersaphrorgdesc**
NAME	Organizational unit name	YES	**ersaphrorgname**

Table 8. OrganizationalUnit_ERC attribute mapping (continued)			
OrganizationalUnit_ERC attributes	**Description**	**Required**	**SAP HR feed adapter attribute name**
LAST_MOD_USER	Contains the name of the last user or process that modified the USER_ERC table.	NO	
LAST_MOD_TIME	Contains the date and time when the last change occurred. Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed.	NO	
TIPO	Organizational unit type name. This attribute might or might not be in the database. It can be created dynamically using a custom rule.	NO	
SCHEDULE	Deprecated	NO	
ATTR1	Spare attribute	NO	
ATTR2	Spare attribute	NO	
ATTR3	Spare attribute	NO	
ATTR4	Spare attribute	NO	
ATTR5	Spare attribute	NO	
ATTR6	Spare attribute	NO	
ATTR7	Spare attribute	NO	
ATTR8	Spare attribute	NO	
ATTR9	Spare attribute	NO	
ATTR10	Spare attribute	NO	
ATTR11	Spare attribute	NO	
ATTR12	Spare attribute	NO	
ATTR13	Spare attribute	NO	
ATTR14	Spare attribute	NO	
ATTR15	Spare attribute	NO	

Adapter configuration properties

To set the IBM Security Directory Integrator configuration properties for the operation of the SAP HR feed adapter, see the *Dispatcher Installation and Configuration Guide*.

Index

V

X