IBM Security Verify Governance Identity Manager

Remedy AR System 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 Remedy AR System Adapter enables communication between the Identity server and the Remedy AR System server.

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

Features of the adapter

The adapter automates several administrative and management tasks.

The adapter automates the following tasks:

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Deleting user accounts

Note: The Remedy AR System server does not support the Suspend and Restore tasks, therefore, the adapter does not automate these tasks.

Related concepts

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

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

Architecture of the adapter

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

You must install the following components for the adapter:

- The Dispatcher
- The RemedyARSConnector connector
- IBM® Security Verify Adapter profile

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

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

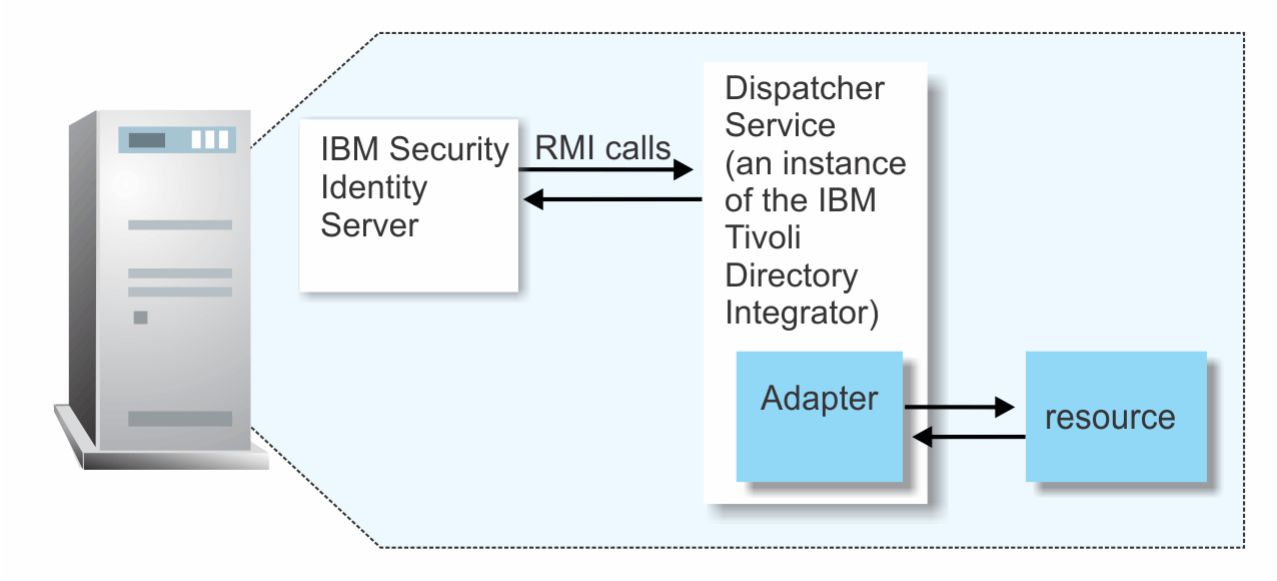

Figure 1. The architecture of the Remedy AR System Adapter

Related concepts

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

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

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

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

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

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator server, and the Remedy AR System Adapter on one server to establish communication with the Remedy AR System server.

The Remedy AR System server is installed on a different server as described in Figure 2 on page 3.

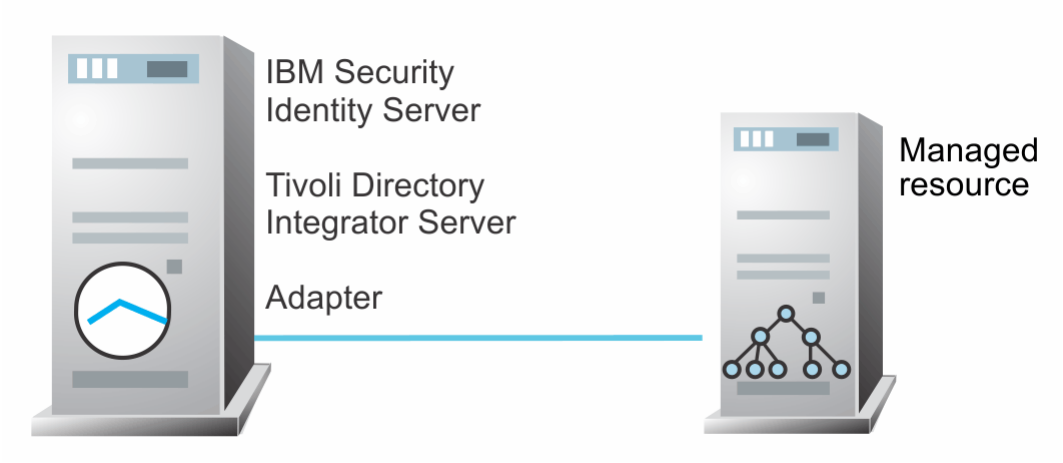

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator, the Remedy AR System Adapter, and the Remedy AR System server are installed on different servers.

Install the Security Directory Integrator server, and the Remedy AR System Adapter on the same server as described in Figure 3 on page 3.

Figure 3. Example of multiple server configuration

Related concepts

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

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

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

Related concepts

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

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

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.

Copying the Remedy AR System library files
If you are managing a Remedy Server, copy the library files from the Remedy Server installation directory and place the files in the IBM Security Directory Integrator setup before installing the adapter. After copying the files, restart the Dispatcher.

Prerequisites

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

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

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

Table 1. Prerequisites to install the adapter	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Remedy AR System server	Version 7.5 Version 7.6.04
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the *Dispatcher Installation and Configuration Guide*.
Remedy AR System Jar files	See "Copying the Remedy AR System library files" on page 9.

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

Related concepts

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.

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

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.

Copying the Remedy AR System library files

If you are managing a Remedy Server, copy the library files from the Remedy Server installation directory and place the files in the IBM Security Directory Integrator setup before installing the adapter. After copying the files, restart the Dispatcher.

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

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.

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

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.

Copying the Remedy AR System library files
If you are managing a Remedy Server, copy the library files from the Remedy Server installation directory and place the files in the IBM Security Directory Integrator setup before installing the adapter. After copying the files, restart the Dispatcher.

Installation worksheet

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

Table 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. This subdirectory contains adapter JAR files.	If Security Directory Integrator is automatically installed with your IBM Security Verify Governance Identity Manager product, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• for version 7.1:
		`drive\Program Files \IBM\TDI\V7.1`
		UNIX:
		• for version 7.1:
		`/opt/IBM/TDI/V7.10`

Table 2. Required information to install the adapter (continued)		
Required information	**Description**	**Value**

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

Related concepts

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.

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

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

Copying the Remedy AR System library files
If you are managing a Remedy Server, copy the library files from the Remedy Server installation directory and place the files in the IBM Security Directory Integrator setup before installing the adapter. After copying the files, restart the Dispatcher.

Copying the Remedy AR System library files

If you are managing a Remedy Server, copy the library files from the Remedy Server installation directory and place the files in the IBM Security Directory Integrator setup before installing the adapter. After copying the files, restart the Dispatcher.

Library file name :`arapiVerNum.jar`

Note: *VerNum* refers to the version number of the file found in the system.

Server installation directory: `C:\ Program Files\BMC Software\ ARSystem\Arserver\api \lib`

IBM Security Directory Integrator location: `ITDI_Home\jars\3rdparty\others`

Note: If you have used the previous versions of the adapter, you have copied library files into `ITDI_Home \jvm\jre\lib\ext`. Remove those files before using the adapter.

Add the `TDI_HOME\libs` folder to the Library path for the UNIX platforms.

For AIX
Set the environment variable *LIBPATH* to `/opt/IBM/TDI/<TDI_VERSION>/libs` path.

For HPUX
Set the environment variable *SHLIB_PATH* to `/opt/IBM/TDI/<TDI_VERSION>/libs` .

For Solaris and Linux
Set the environment *LD_LIBRARY_PATH* to `/opt/IBM/TDI/<TDI_VERSION>/libs` path.

`/opt/IBM/TDI/<TDI_VERSION>` is the IBM Security Directory Integrator installation directory.

Related concepts

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.

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

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

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.

Chapter 3. Installing

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

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See "Installing the dispatcher" on page 11.

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*.

Installing the adapter binaries or connector

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

About this task

The adapter uses the Security Directory Integrator RemedyARSConnector. This connector is not available with the base Security Directory Integrator product. The adapter installation involves the Security Directory Integrator Remedy ARS System connector installation. After installing the Dispatcher, you must install the connector for the adapter. The connector is included in a separate installer provided with the adapter package. Before you install the adapter, make sure that the Dispatcher is already installed.

Note: If you are running on a 64-bit operating system, you must use the Security Directory Integrator-supplied JVM. The JVM is in *ITDI_HOME*`/jvm/jre/bin/`, where *ITDI_HOME* is the directory where Security Directory Integrator is installed.

Procedure

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

Verifying the adapter installation

Complete the following steps to verify whether the adapter installation was successful or not.

Procedure

- Ensure that `RemedyARSConnector.jar` file is in the *ITDI_HOME*`\jars\connectors` directory.

- If this installation is to upgrade a connector, send a request from the IBM Security Identity Server and verify the connector version in the `ibmdi.log` matches the connector version listed in the Release Notes. The `ibmdi.log` is in the *ITDI_HOME*`\adapter_solution_directory\logs` directory.

Restarting the adapter service

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

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Security Directory Integrator instance.

See the topic about starting, stopping, and restarting the Dispatcher service in the *Dispatcher Installation and Configuration Guide*.

Importing the adapter profile

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

Before you begin

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

About this task

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

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

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

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

Procedure

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

6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
      A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

Results

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

What to do next

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

- Import the attribute mapping file. See “Importing attribute mapping file” on page 13.
- Create a connector that uses the target profile. See “Adding a connector” on page 14.

Importing attribute mapping file

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

About this task

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

Procedure

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

Adding a connector

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

Before you begin

Complete Importing the adapter profile.

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

About this task

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

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

Procedure

To add a connector, complete these steps.

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

Results

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

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

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see “Enabling connectors” on page 15.

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 3. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	“Adding a connector” on page 14.
Ensure that you enabled the appropriate channel modes for the connector.	“Reviewing and setting channel modes for each new connector” on page 16.

Procedure

To enable a connector, complete these steps:

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

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

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

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

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

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

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

Results

The connector is enabled

What to do next

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

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

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

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

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

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

      Enable reconciliation
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.

      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.

      Information about the synchronization is displayed in the **Sync History** tab.

10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.

    For more information, see "Enabling connectors" on page 15.

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

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

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

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

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Service/Target form details

Complete the service/target form fields.

Note: If the following fields on the service form are changed for an existing service, the adapter service on the Security Directory Integrator server must be restarted.

- **AL FileSystem Path**
- **Max Connection Count**

On the General Information tab:

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

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

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

Security Directory Integrator URL

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

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

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

Table 4. Ports

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

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

- 1099
- 2099
- 3099

Host Name
Specify the IP address or the host name of the managed resource.

Note: Enclose the IPv6 address in brackets. An example of a valid IPv6 address format is:

```
http://[fedc:ba98:7654:3210:fedc:ba98:7654:3210]
```

TCP Port
Specify the TCP port number of the managed resource.

User Name
Specify a Login ID of the Remedy AR System server that has administrator permissions.

Password
Specify a password for the Remedy AR System server user that has administrator permissions.

Allow Unqualified Searches
Select Yes for the adapter to perform an Unqualified Search on the Remedy AR System server.

Recon In Batch
Click the check box to reconcile the entries in batches.

On the Dispatcher Attributes tab:

Disable AL Caching
Click the check box to disable the assembly line (test, add, modify, delete) caching in the dispatcher for the service.

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: *`drive`*`:\Program Files\IBM\TDI\V7.0\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating:`/opt/IBM/TDI/V7.0/profiles`

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

On the Status and information tab
This page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

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

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

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

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

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

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

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

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

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

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

Verifying that the adapter is working correctly

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

Procedure

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

Chapter 4. Upgrading

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

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

Upgrading the adapter binaries or connector

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

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

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

Upgrading the adapter profile

Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Verify Identity.

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

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

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

Customizing the adapter profile

To customize the adapter profile, you must modify the Remedy AR System Adapter JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or `CustomLabels.properties`. Each adapter has a `CustomLabels.properties` file for that adapter.

About this task

Each adapter has a `CustomLabels.properties` file for that adapter.

The JAR file is included in the Remedy AR System Adapter compressed file that you downloaded from the IBM website.

Note: You cannot modify the schema for this adapter. Attributes cannot be added to or deleted from the schema.

RemedyARSProfile.jar

The following files are included in the JAR file:

- CustomLabels.properties
- schema.dsml
- service.def
- erRmdArsAccount.xml
- erRmdArsRMIService.xml
- RmdArsSearch.xml
- RmdArsAdd.xml
- RmdArsModify.xml
- RmdArsTest.xml
- RmdArsAdapter.xml
- RmdArsDelete.xml

To edit the JAR file, log on to the workstation where the Remedy AR System Adapter is installed:

Procedure

1. On the **Start** menu, click **Programs** > **Accessories** > **Command Prompt**.
2. Copy the JAR file into a temporary directory.
3. Extract the contents of the JAR file into the temporary directory by running the following command.

The following example applies to the Remedy AR System Adapter profile. Type the name of the JAR file for your operating system.

```
cd c:\temp
#jar -xvf RemedyARSProfile.jar
```

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

4. Edit the file that you want to change.

   After you edit the file, you must import the file into the Identity server for the changes to take effect.

5. 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 RemedyARSProfile.jar RTCProfile
   ```

   UNIX

   ```
   #jar -cvf RemedyARSProfile.jar RTCProfile
   ```

   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

Password management for account restoration

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement.

Related tasks

Editing adapter profiles on the UNIX or LINUX operating system

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

Verifying that the adapter is working correctly

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

Editing adapter profiles on the UNIX or LINUX operating system

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

About this task

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

Example

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

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

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

Related concepts

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the Remedy AR System Adapter JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or `CustomLabels.properties`. Each adapter has a `CustomLabels.properties` file for that adapter.

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

Password management for account restoration

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement.

You can set the Remedy AR System Adapter to require a new password when the account is restored, if your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password.

In the `service.def` file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the `schema.dsml` file. Adapter profile components also enable remote services to find out if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this situation, only some of the accounts being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Edit the `service.def` file to add the new protocol options, for example:

```
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_REQUIRED_ON_RESTORE"<value>true</value>
</property>
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_ALLOWED_ON_RESTORE"<value>false</value>
</property>
```

By adding the two options in the preceding example, you ensure that you are not prompted for a password when an account is restored.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the Remedy AR System Adapter JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or `CustomLabels.properties`. Each adapter has a `CustomLabels.properties` file for that adapter.

Editing adapter profiles on the UNIX or LINUX operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Verifying that the adapter is working correctly

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

Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on 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

Password management for account restoration
How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the Remedy AR System Adapter JAR file. You might customize the adapter profile to change the account form or the service form. You can also change the labels on the forms by using the Form Designer or `CustomLabels.properties`. Each adapter has a `CustomLabels.properties` file for that adapter.

Editing adapter profiles on the UNIX or LINUX operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Chapter 6. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

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.

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 that might be displayed on the user interface if the adapter is installed on your workstation.

Table 5. Warnings, error messages, and corrective action

Warning or error message	Corrective action
ERROR (307): Required field (without a default) not specified; 101. ERROR (307): Required field (without a default) not specified; 8.	Specify the following required attributes on the account form: • Login Name • Full Name
ERROR (382): The values for this entry violate a unique index that is defined for this form.	Provide a unique login name for the Login Name attribute on the account form when you perform a user add operation.
(52) The field is a core system field and cannot be changed.	An attempt was made to modify the contents of one of the following core system fields: • Request ID • Create Date • Last Modified By • Last Modified Date Do not modify these fields because the Remedy AR System server sets values for these fields.
ERROR (326): Required field cannot be reset to a NULL value; 2.	An attempt was made to delete the value specified in the Creator field. The Remedy AR Systemserver sets the default for this field; however, if you specify a different value, ensure that you: • Do not set the value of the field to NULL. • Specify a string value (for example, *Demo*) or an alphanumeric character (for example, *av234*.)
ERROR (417): Cannot translate a group name in either the Group List or Assignee Group field; 104.	This error occurs when an incorrect value is specified for the Group List attribute during the user add operation. Perform the following steps to set the Group List attribute: 1. Ensure that the group exists on the Remedy AR System server by performing a support data reconciliation operation. 2. Select the group from the updated list available for the Group List attribute.
ERROR (30): You are already at the limit of the number of fixed user licenses of the following type; `Full Text` : (0).	An attempt was made to create a user and assign a fixed license to the user. You reached the limit of the number of fixed user licenses. Add the user with a read, none, or floating license, however, not a fixed license. The License Type attribute is replaced by write, full text, or flashboards to indicate the type of fixed license. If you do not have anymore fixed licenses, ensure that the sample users are deleted. Contact the Remedy AR System server distributor for information about obtaining additional licenses.

Table 5. Warnings, error messages, and corrective action (continued)

Warning or error message	Corrective action
ERROR (9860): The application license format is not valid.	This error occurs either when the application license format is not correct or the license information is specified incorrectly. Ensure that the license names end with User Fixed or User Floating and each license for a user is separated by a semicolon (;).
ERROR (8932): You do not have write license.	An attempt was made to add or modify the contents of a field, however, you do not have write access. Ensure that you provide the Resource Administrator name who has read and write permissions on the Remedy AR System server, for example, *Demo* on the adapter service form on IBM Security Verify Governance Identity Manager.
ERROR (333): You have no access to field; 101.	An attempt was made to add or modify the contents of a field, however, you do not have read or write access. Ensure that you provide the Resource Administrator name who has read and write permissions on the Remedy AR Systemserver, for example, *Demo* on the adapter service form on IBM Security Verify Governance Identity Manager.
ERROR (302): Entry does not exist in database.	An attempt was made to modify a user that does not exist in the Remedy AR System database. Ensure that the user exists in the database by performing a reconciliation operation and then perform the modify operation.
ERROR (90): Message not in catalog; Message number = 90;ONC/RPC program not registered `IP Address of Resource`.	This error occurs when an attempt to connect to the Remedy AR System server fails. Perform one of the following steps: • Check whether you can ping the workstation on which the Remedy AR System server is installed. If you cannot ping the workstation, ensure that the Remedy Action Request System server service is running on the workstation on which the Remedy AR System server is installed. If the service is not running, restart it. • Check whether there is successful LAN connection between the Security Directory Integrator and the workstation on which Remedy AR System server is installed.
ERROR (304): Must have Administrative permissions to perform this operation.	An attempt was made to add, modify, or delete a user without the Administrator permissions and Fixed License of the Remedy AR System server. Ensure that you have Administrator permissions and a Fixed License of the Remedy AR System server to perform the operation.

Table 5. Warnings, error messages, and corrective action (continued)

Warning or error message	Corrective action
WARNING (77): No free floating full text license tokens are available. Currently accessing the system without full text search capability. License will upgrade when one is available; `Hostname` of Remedy AR System server	You are assigned a floating, Full Text Search Option license, however, there are no floating, Full Text Search Option tokens available at this time. You can access the database without access to the full text search (FTS) engine. The system tries to upgrade your license type when a token is available. The system uses the default database search capability on all fields, including the fields that are FTS indexed.

ERROR [com.remedy.arsys.api.NativeLibraryLoader] - Could not load native library java.lang.UnsatisfiedLinkError: arjni70 (Not found in java.library.path)	Perform the following steps:
	1. Copy the C API files for AIX operating system to the *ITDI_HOME*`/jvm/jre/bin/classic` directory. See "Copying the Remedy AR System library files" on page 9.
	2. Navigate to the *ITDI_HOME*`/jvm/jre/bin/classic` directory.
	3. Run the following commands:
	`ln -s libicui18nbmc32.0.a libicui18nbmc32.a`
	`ln -s libicudatabmc32.0.a libicudatabmc32.a`
	`ln -s libicuucbmc32.0.a libicuucbmc32.a`
	4. Restart the Dispatcher service.

ERROR [com.remedy.arsys.api.NativeLibraryLoader] - Could not load native library java.lang.UnsatisfiedLinkError: arjni70 (Not found in java.library.path)	Perform the following steps:
	1. Copy the C API files for HP-UX operating system to the *ITDI_HOME*`/jvm/jre/lib/PA_RISC2.0/server` directory. See Remedy AR System.
	2. Navigate to the *ITDI_HOME*`/jvm/jre/lib/PA_RISC2.0/server` directory.
	3. Run the following commands:
	`ln -s libicui18nbmc.sl.32.0 libicui18nbmc.sl.32`
	`ln -s libicudatabmc.sl.32.0 libicudatabmc.sl.32`
	`ln -s libicuucbmc.sl.32.0 libicuucbmc.sl.32`
	4. Restart the Dispatcher service.

Related concepts

Techniques for troubleshooting problems

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

Chapter 7. Uninstalling

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

If you take the server offline, completed adapter requests might not be recovered when the server is back online.

Removing the adapter binaries or connector

Use this task to remove the connector file for the Remedy AR System Adapter.

About this task

Note: The Dispatcher is required for all Security Directory Integrator adapters. If you uninstall the Dispatcher, none of the other installed adapters work. To uninstall the Dispatcher, see the *Dispatcher Installation and Configuration Guide*

To remove the Security Directory Integrator connector, complete these steps:

Procedure

1. Stop the adapter service.

   For information about stopping the service, see Start, stop, and restart of the adapter service.
2. Delete the *ITDI_HOME*`/jars/connectors/RemedyARSConnector.jar` file.
3. Start the adapter service.

Related concepts

Deleting the adapter profile

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

Deleting the adapter profile

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

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

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

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

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

Related tasks

Removing the adapter binaries or connector

Use this task to remove the connector file for the Remedy AR System Adapter.

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

Adapter attributes and object classes are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter. The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

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

The following table lists the account form attributes that the adapter uses.

Table 6. Account form attributes and their details

Attribute name on the Remedy AR System 7.0 Adapter account form	Attribute name on the Tivoli Directory server	Data type	Single valued	Read or write	Required
Login Name	eruid	String	True	RW	True
Full Name	erRmdArsFullName	String	True	RW	True
License Type	erRmdArsLcnsType	Integer	True	RW	True
Full Text License Type	erRmdArsFullTxtLcnsType	Integer	True	RW	True
Creator	erRmdArsCreator	String	True	RW	True
Request ID	erRmdArsReqID	String	True	R	False
Password	erPassword	String	True	RW	False
Group List	erRmdArsGrpList	String	False	RW	False
Computed Group List	erRmdArsCmptGrpList	String	False	R	False
Application License	erRmdArsAppLcns	String	True	RW	False
Default Notify Mechanism	erRmdArsDefaultNotifyMech	Integer	True	RW	False
Email Address	erRmdArsEmailAddr	String	True	RW	False
Unique Identifier	erRmdArsUID	String	True	RW	False
Create Date	erRmdArsCreateDate	Date	True	R	False
Last Modified By	erRmdArsLastModBy	String	True	R	False
Modified Date	erRmdArsModDate	Date	True	R	False

Note:

- The maximum character limit for the Login Name (eruid) attribute is 243 characters because of the Remedy AR System API limitation.
- The adapter does not support the Application License attribute. It is hidden attribute, however, you can customize the attribute on the adapter account form by using Form Customization.

Index

T

U

V

W