

IBM Security Verify Identity  
7.0

*Remedy AR System Adapter Installation  
and Configuration Guide*





---

# Contents

- Figures..... V**
- Tables..... vii**
- Chapter 1. Overview..... 1**
  - Features of the adapter.....1
  - Architecture of the adapter.....1
  - Supported configurations..... 2
- Chapter 2. Planning..... 5**
  - Roadmap..... 5
  - Prerequisites..... 6
  - Software downloads..... 8
  - Installation worksheet..... 8
  - Copying the Remedy AR System library files..... 9
- Chapter 3. Installing..... 11**
  - Installing the dispatcher.....11
  - Installing the adapter binaries or connector.....11
  - Verifying the adapter installation..... 11
  - Restarting the adapter service..... 12
  - Importing the adapter profile..... 12
  - Attribute mapping..... 13
  - Creating an adapter service/target.....14
  - Service/Target form details..... 15
  - Installing the adapter language package..... 17
  - Verifying that the adapter is working correctly..... 17
- Chapter 4. Upgrading.....19**
  - Upgrading the adapter binaries or connector..... 19
  - Upgrading the adapter profile..... 19
- Chapter 5. Configuring..... 21**
  - Customizing the adapter profile..... 21
  - Editing adapter profiles on the UNIX or LINUX operating system..... 22
  - Password management for account restoration..... 23
  - Verifying that the adapter is working correctly..... 24
- Chapter 6. Troubleshooting..... 25**
  - Techniques for troubleshooting problems..... 25
  - Error messages and problem solving..... 26
- Chapter 7. Uninstalling..... 31**
  - Removing the adapter binaries or connector..... 31
  - Deleting the adapter profile..... 31
- Chapter 8. Reference..... 33**
  - Adapter attributes and object classes..... 33

**Index..... 35**

---

# Figures

- 1. The architecture of the Remedy AR System Adapter..... 2
- 2. Example of a single server configuration..... 3
- 3. Example of multiple server configuration..... 3



---

# Tables

1. Prerequisites to install the adapter.....	7
2. Required information to install the adapter.....	8
3. Warnings, error messages, and corrective action.....	27
4. Account form attributes and their details.....	33





---

# 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 RemedyARSCollector 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.

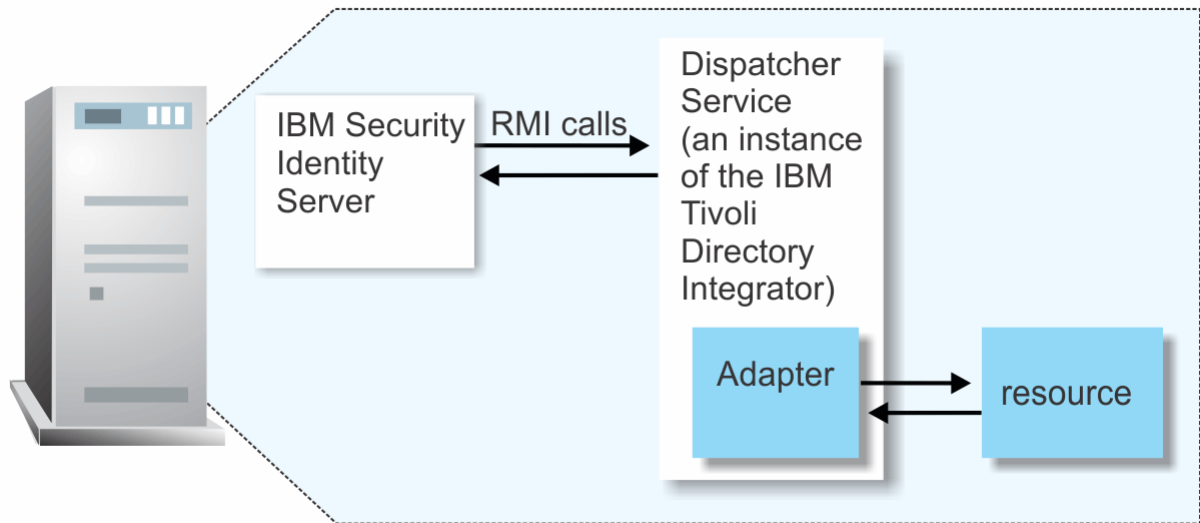


Figure 1. The architecture of the Remedy AR System Adapter

### 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](#).

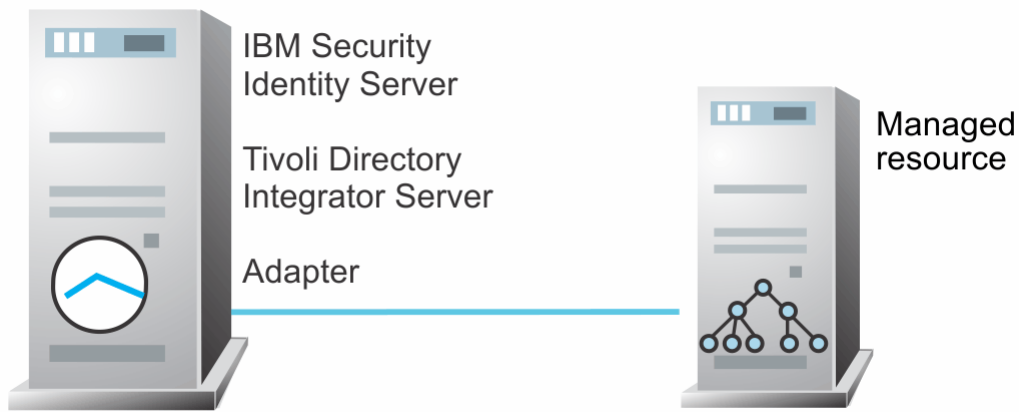


Figure 2. Example of a single server configuration

### 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](#).

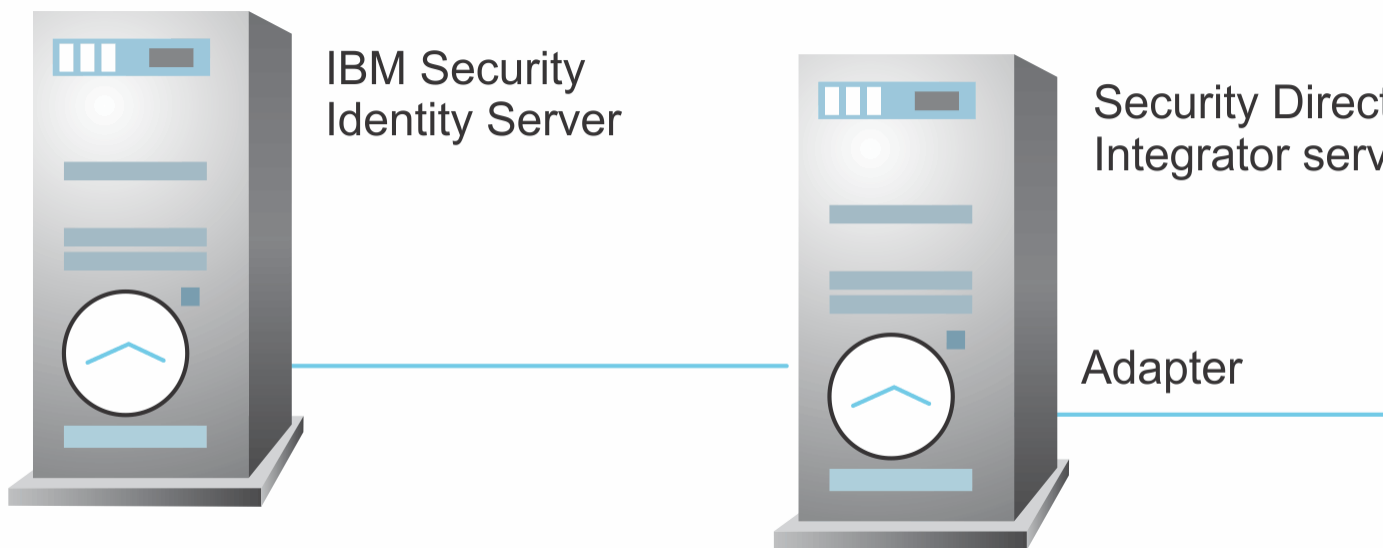


Figure 3. Example of multiple server configuration

### 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 Identity 7.x

---

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

#### 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. Create an adapter service/target.
8. Install the adapter language package.
9. 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	<ul style="list-style-type: none"> <li>IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008</li> <li>IBM Security Directory Integrator Version 7.2</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>
Identity server	<p>The following servers are supported:</p> <ul style="list-style-type: none"> <li>Identity server Version 10.0</li> <li>Identity server Version 10.0</li> <li>IBM Security Privileged Identity Manager Version 2.0</li> <li>Identity server Version 10.0</li> </ul>
Remedy AR System server	<p>Version 7.5</p> <p>Version 7.6.04</p>
System Administrator Authority	<p>To complete the adapter installation procedure, you must have system administrator authority.</p>
Security Directory Integrator adapters solution directory	<p>A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the <i>Dispatcher Installation and Configuration Guide</i>.</p>
Remedy AR System Jar files	<p>See <a href="#">“Copying the Remedy AR System library files” on page 9</a>.</p>

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 Identity 7.x  
 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 Identity 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 Identity 7.x](#)  
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.

Required information	Description	Value
Security Directory Integrator Home Directory	The <i>ITDI_HOME</i> directory contains the <i>jars/connectors</i> subdirectory. This subdirectory contains adapter JAR files.	If Security Directory Integrator is automatically installed with your IBM Security Verify Identity product, the default directory path for Security Directory Integrator is as follows: <b>Windows:</b> <ul style="list-style-type: none"><li>for version 7.1: <code>drive\Program Files\IBM\TDI\V7.1</code></li></ul> <b>UNIX:</b> <ul style="list-style-type: none"><li>for version 7.1: <code>/opt/IBM/TDI/V7.10</code></li></ul>



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 <i>Dispatcher Installation and Configuration Guide</i> .	<p><b>Windows:</b></p> <ul style="list-style-type: none"> <li>for version 7.1:  <code>drive\Program Files\IBM\TDI\V7.1\timsol</code></li> </ul> <p><b>UNIX:</b></p> <ul style="list-style-type: none"> <li>for version 7.1:  <code>/opt/IBM/TDI/V7.1/timsol</code></li> </ul>

### Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x  
 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 Identity 7.x

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 RemedyARSCollector. This collector is not available with the base Security Directory Integrator product. The adapter installation involves the Security Directory Integrator Remedy ARS System collector installation. After installing the Dispatcher, you must install the collector for the adapter. The collector 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 `RemedyARSCollector.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 `RemedyARSCollector.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

---

An adapter profile defines the types of resources that the Identity server can manage. It is packaged with the IBM Security Verify Adapter. Use the adapter profile to create an adapter service on Identity server and establish communication with the adapter.

### Before you begin

- You have root or 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. The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

### About this task

Service definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

### Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System > Manage Service Types**.  
The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.  
The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
  - a) In the **Service Definition File** field, type the directory location of the `<Adapter>Profile.jar` file, or click **Browse** to locate the file.  
For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
  - b) Click **OK** to import the file.

## Results

A message indicates that you successfully submitted a request to import a service type.

## What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is Failed, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the `handler.file.fileDir` property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server `HOME\data` directory. .

## 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 Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

## Creating an adapter service/target

---

After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

### Before you begin

Complete [“Importing the adapter profile”](#) on page 12.

### About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

### Procedure

1. From the navigation tree, click **Manage Services**.  
The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.  
The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.  
The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
  - a) Type information about the business unit in the **Search information** field.
  - b) Select a business type from the **Search by** list, and then click **Search**.  
A list of business units that matches the search criteria is displayed.  
If the table contains multiple pages, you can do the following tasks:
    - Click the arrow to go to the next page.
    - Type the number of the page that you want to view and click **Go**.
  - c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.  
The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.  
If the table contains multiple pages, you can do the following tasks:
  - Click the arrow to go to the next page.
  - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.  
The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.

7. To create a service with NTLM authentication, the administrator login is in the following format:

```
<Domain Name>\<Login Name>
```

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.

9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.

10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

Specify the expected access information and any other optional information such as description, search terms, more information, or badges.

11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

The adapter must be running to obtain the information.

12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

**Note:** If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.

13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

## Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

## 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`.

## 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.

## Installing the adapter language package

---

The adapters use a separate language package from IBM Security Verify Identity.

See *Installing the adapter language pack* from the IBM Security Verify Identity product documentation.

## 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.

#### RemedyARSPProfile.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 RemedyARSPProfile.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 RemedyARSPProfile.jar RTCTProfile
```

#### UNIX

```
#jar -cvf RemedyARSPProfile.jar RTCTProfile
```

- b) Import the JAR file into the IBM Security Verify Identity 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 Identity 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 Identity 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 Identity 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.dsm1` 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 Identity 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 3. 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: <ul style="list-style-type: none"> <li>• Login Name</li> <li>• Full Name</li> </ul>
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: <ul style="list-style-type: none"> <li>• Request ID</li> <li>• Create Date</li> <li>• Last Modified By</li> <li>• Last Modified Date</li> </ul> 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. <p>The Remedy AR Systemserver sets the default for this field; however, if you specify a different value, ensure that you:</p> <ul style="list-style-type: none"> <li>• Do not set the value of the field to NULL.</li> <li>• Specify a string value (for example, <i>Demo</i>) or an alphanumeric character (for example, <i>av234</i>.)</li> </ul>
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. <p>Perform the following steps to set the Group List attribute:</p> <ol style="list-style-type: none"> <li>1. Ensure that the group exists on the Remedy AR System server by performing a support data reconciliation operation.</li> <li>2. Select the group from the updated list available for the Group List attribute.</li> </ol>
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. <p>The License Type attribute is replaced by write, full text, or flashboards to indicate the type of fixed license.</p> <p>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.</p>

Table 3. Warnings, error messages, and corrective action (continued)

Warning or error message	Corrective action
ERROR (9860): The application license format is not valid.	<p>This error occurs either when the application license format is not correct or the license information is specified incorrectly.</p> <p>Ensure that the license names end with User Fixed or User Floating and each license for a user is separated by a semicolon (;).</p>
ERROR (8932): You do not have write license.	<p>An attempt was made to add or modify the contents of a field, however, you do not have write access.</p> <p>Ensure that you provide the Resource Administrator name who has read and write permissions on the Remedy AR System server, for example, <i>Demo</i> on the adapter service form on IBM Security Verify Identity.</p>
ERROR (333): You have no access to field; 101.	<p>An attempt was made to add or modify the contents of a field, however, you do not have read or write access.</p> <p>Ensure that you provide the Resource Administrator name who has read and write permissions on the Remedy AR Systemserver, for example, <i>Demo</i> on the adapter service form on IBM Security Verify Identity.</p>
ERROR (302): Entry does not exist in database.	<p>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.</p>
ERROR (90): Message not in catalog; Message number = 90;ONC/RPC program not registered IP Address of Resource.	<p>This error occurs when an attempt to connect to the Remedy AR System server fails. Perform one of the following steps:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Check whether there is successful LAN connection between the Security Directory Integrator and the workstation on which Remedy AR System server is installed.</li> </ul>
ERROR (304): Must have Administrative permissions to perform this operation.	<p>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.</p>

Table 3. Warnings, error messages, and corrective action (continued)

Warning or error message	Corrective action
<p>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</p>	<p>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.</p>
<p>ERROR [com.remedy.arsys.api.NativeLibraryLoader] - Could not load native library java.lang.UnsatisfiedLinkError: arjni70 (Not found in java.library.path)</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Copy the C API files for AIX operating system to the <i>ITDI_HOME/jvm/jre/bin/classic</i> directory. See “Copying the Remedy AR System library files” on page 9.</li> <li>2. Navigate to the <i>ITDI_HOME/jvm/jre/bin/classic</i> directory.</li> <li>3. Run the following commands: <pre data-bbox="803 808 1453 892">ln -s libicui18nbmc32.0.a libicui18nbmc32.a ln -s libicudatabmc32.0.a libicudatabmc32.a ln -s libicuucbmc32.0.a libicuucbmc32.a</pre> </li> <li>4. Restart the Dispatcher service.</li> </ol>
<p>ERROR [com.remedy.arsys.api.NativeLibraryLoader] - Could not load native library java.lang.UnsatisfiedLinkError: arjni70 (Not found in java.library.path)</p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Copy the C API files for HP-UX operating system to the <i>ITDI_HOME/jvm/jre/lib/PA_RISC2.0/server</i> directory. See Remedy AR System.</li> <li>2. Navigate to the <i>ITDI_HOME/jvm/jre/lib/PA_RISC2.0/server</i> directory.</li> <li>3. Run the following commands: <pre data-bbox="803 1260 1453 1344">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</pre> </li> <li>4. Restart the Dispatcher service.</li> </ol>

### 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/RemedyARSCconnector.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 Identity 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.

<b>Attribute name on the Remedy AR System 7.0 Adapter account form</b>	<b>Attribute name on the Tivoli Directory server</b>	<b>Data type</b>	<b>Single valued</b>	<b>Read or write</b>	<b>Required</b>
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

## A

- account
  - password requirements [23](#)
  - restoration [23](#)
- adapter
  - attributes
    - account form [33](#)
    - combination by action type [33](#)
    - description [33](#)
  - features [1](#)
  - installation
    - errors [25](#)
    - steps [11](#)
    - troubleshooting [25](#)
    - verifying [11](#), [17](#), [24](#)
    - warnings [25](#)
    - worksheet [8](#)
  - overview [1](#)
  - post-installation tasks
    - configuration [21](#)
    - language pack [21](#)
    - SSL setup [21](#)
    - verification [21](#)
  - profile
    - customizing [21](#)
    - dispatcher restart required [19](#)
    - upgrade [19](#)
  - supported configurations
    - multiple servers [2](#)
    - single server [2](#)
  - task automation [1](#)
  - uninstallation [31](#)
  - upgrading [19](#)
- adapter installation [11](#)
- adapters
  - removing profiles [31](#)
- attributes, description [33](#)

## C

- connector
  - files, removing [31](#)
  - upgrading [19](#)
- customizing, adapter profiles [21](#)

## D

- dispatcher
  - installation [11](#)
- download, software [8](#)

## E

- error messages [26](#)

## I

- installation
  - adapter
    - errors [25](#)
    - steps [11](#)
    - troubleshooting [25](#)
    - verifying [11](#)
    - warnings [25](#)
  - language pack [17](#)
  - planning roadmaps [5](#)
  - verification
    - adapter [17](#), [24](#)
  - worksheet [8](#)

## L

- language pack
  - installation [17](#)
  - same for adapters and server [17](#)

## M

- messages
  - error [26](#)
  - warning [26](#)
- MS-DOS ASCII characters [22](#)

## O

- overview, adapter [1](#)

## P

- password
  - account
    - requirements [23](#)
    - restoration [23](#)
  - requirements [23](#)
- profile
  - editing on UNIX or Linux [22](#)

## R

- removing
  - adapter profiles [31](#)
  - removing connector files [31](#)
- roadmaps
  - planning [5](#)

## S

- service
  - restart [12](#)
  - start [12](#)
  - stop [12](#)

- software
  - [download 8](#)
  - [prerequisites 6](#)
  - [requirements 6](#)
  - [website 8](#)
- supported configurations
  - [adapter 2](#)
  - [multiple servers 2](#)
  - [overview 2](#)
  - [single server 2](#)

## T

- troubleshooting
  - [error messages 26](#)
  - [identifying problems 25](#)
  - [techniques for 25](#)
  - [warning messages 26](#)
- troubleshooting and support
  - [troubleshooting techniques 25](#)

## U

- uninstalling
  - [adapter 31](#)
  - [from the directory integrator 31](#)
- upgrade
  - [adapter 19](#)
  - [connector 19](#)

## V

- verification
  - [dispatcher installation 11](#)
  - [installation 17, 24](#)
  - operating system
    - [prerequisites 6](#)
    - [requirements 6](#)
  - software
    - [prerequisites 6](#)
    - [requirements 6](#)
- vi command [22](#)

## W

- [warning messages 26](#)



