IBM Security Verify Identity
7.0

RSA Authentication Manager 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 RSA Authentication Manager Adapter enables communication between the Identity server and the RSA Authentication Manager 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.

- Adding, modifying, suspending, restoring, or deleting user accounts in the identity sources and the security domains of a specific realm.
- Restoring locked user accounts.
- Adding users to and removing them from groups.
- Assigning or unassigning roles to users.
- Enabling and disabling the tokens assigned to users
- Clearing pins for the tokens assigned to the users.
- Creating user accounts in the specified security domain and its associated identity source.
- Reconciling user account information from the managed resource to IBM® Security Verify Identity.
- Reconciling support data for the realm, such as identity sources, security domains, groups, admin roles, and tokens of the specified realm.
- Reconciling support data such as identity sources, security domains, groups, admin roles and tokens of the specified security domain.

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.

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

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

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

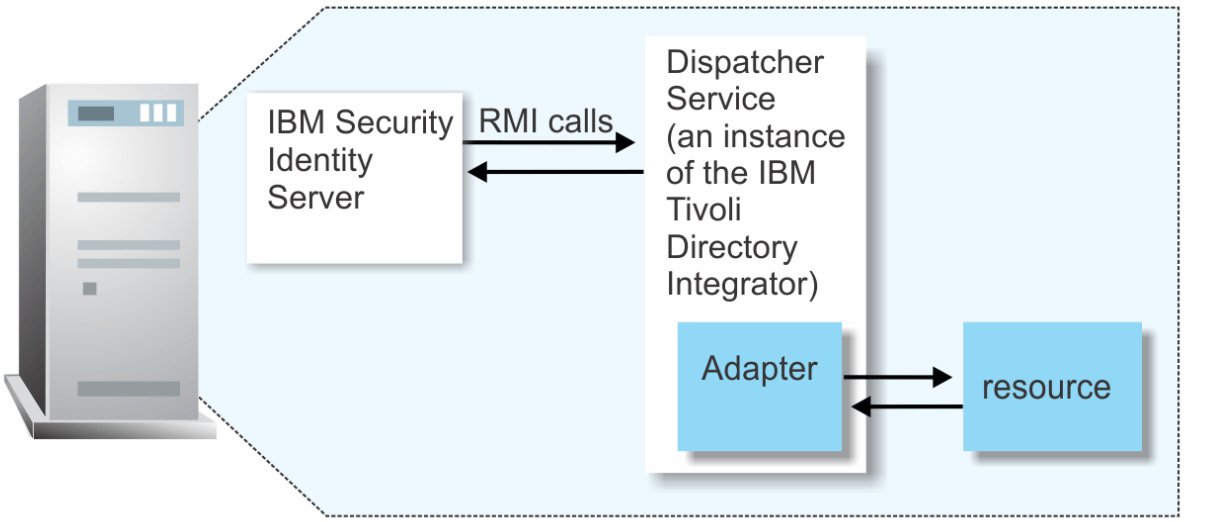

Figure 1. The architecture of the RSA Authentication Manager Adapter

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 Identity server
- The Tivoli® 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

Install the Identity server, the Security Directory Integrator server, and the RSA Authentication Manager Adapter on one server.

This configuration establishes communication with the RSA Authentication Manager server. The RSA Authentication Manager server is installed on a different server as described in Figure 2 on page 3.

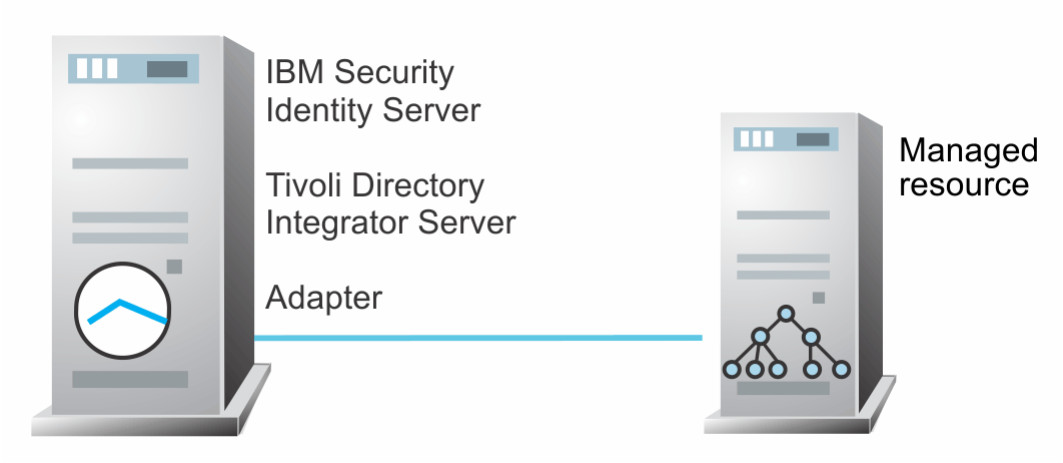

Figure 2. Example of a single server configuration

Multiple server configuration

Install the Identity server, the Security Directory Integrator server, the RSA Authentication Manager Adapter, and the RSA Authentication Manager on different servers.

Install the Security Directory Integrator server and the RSA Authentication Manager Adapter on the same server as described 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

Prerequisites

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

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

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

Table 1. Prerequisites to install the adapter	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
RSA Authentication Manager	Version 7.1 SP4 Version 8.0 Version 8.1
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.

Note:

If you are using an Identity server prior to version 6.0.0.13 or 7.0.1.3:

- The assigned or unassigned state of the RSA Authentication Manager tokens are not updated when you create, modify, or delete an RSA Authentication Manager account.
- You must perform a reconciliation on the RSA Authentication Manager service to synchronize the state of the tokens in IBM Security Verify Identity. See *Reconciling accounts immediately on a service* in the IBM Security Verify Identity Knowledge Center.

If you are using an Identity server version 6.0.0.13, 7.0.1.3 or later:

- The assigned or unassigned state of the RSA Authentication Manager tokens are updated when you successfully create, modify, or delete RSA Authentication Manager accounts.

- The state of tokens are not updated when the operation to create, modify, or delete an account fails or goes into `wait` or `pending` state. To work around this limitation, you can do a reconciliation on the RSA Authentication Manager service to synchronize the state of the tokens in IBM Security Verify Identity. See *Reconciling accounts immediately on a service* in the IBM Security Verify Identity Knowledge Center.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1: Administrator Guide*.

Prerequisites for running the RsaAuthMgr connector

You can use the following lists of requirements to run the **`RsaAuthMgr`** connector.

Table 2. RsaAuthMgr connector prerequisites

Requirement	Description	Task
SSL Certificate	Export the SSL certificate from the managed resource and import it to the certificate authority (CA) certificates of the Security Directory Integrator Java™ Virtual Machine (JVM).	See "Enabling secure communication" on page 21.
License **Note:** This is required only for Version 7.1.	An adapter can have the authority to manage the resource only when it has the `license.bea` file of the WebLogic server on the resource.	Place the `license.bea` file in the adapter solution directory. See the *Dispatcher Installation and Configuration Guide*.
`config.properties`	This file contains the key-value pair information related to the managed resource. This file must be placed in the adapter solution directory and updated appropriately.	See "Authentication Manager config.properties file update" on page 18.
`wlfullclient.jar` on the RSA Authentication Manager server. **Note:** This is required only for Version 7.1.	This JAR file contains information needed for the adapter to communicate with the RSA Authentication Manager server. It must be generated on the server and copied to the *`ITDI_HOME`*`/jars/3rdparty/rsa` directory.	Perform the following steps: 1. From the command prompt on the RSA Authentication Managerserver, change the directory to *`RSA_AM_HOME`*`/appserver/weblogic/server/lib/`. 2. Type: `java -jar ../../modules/com.bea.core.jarbuilder_1.0.0.0.jar -profile wlfullclient`
Authentication Manager JAR files in Security Directory Integrator	The RSA library JAR files provide APIs to perform operations on the managed resource.	Copy the JAR files from the Required JAR files table to the *`ITDI_Home`*`/jars/3rdparty/rsa` directory. See "Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment" on page 13.

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.

Installation worksheet

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

Table 3. Required information to install the adapter

Required information	Description	Value
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter jars.	If Security Directory Integrator version 7.1 is automatically installed, the default directory path depends on the operating system. **Windows** *drive*`\Program Files\IBM\TDI\V7.1` **UNIX** `/opt/IBM/TDI/V7.1`
Adapters solution directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. See the *Dispatcher Installation and Configuration Guide*.	The default solution directory for version 7.1 depends on the operating system. **Windows** *drive*`\Program Files\IBM\TDI\V7.1\`*timsol* **UNIX** `/opt/IBM/TDI/V7.1/`*timsol*

Chapter 3. Installing

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

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

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

Installing the dispatcher

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

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

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

Related concepts

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment

You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Installing the adapter binaries or connector

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

Before you begin

- The Dispatcher must be installed.

About this task

The following connectors are available:

- `connectors/am71/RsaAuthMgrConnector.jar`
- `connectors/am80/RsaAuthMgrConnector.jar`
- `connectors/am81/RsaAuthMgrConnector.jar`
- `connectors/am82/RsaAuthMgrConnector.jar`

Note: You must use the connector jar that corresponds to the RSA Authentication Manager server environment. For example, you cannot use the a*m80* version of the connector jar in anRSA Authentication Manager *7.1* environment

Procedure

1. Create a temporary directory on the workstation where you want to extract the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `connectors/`*`am<version>`*`/RsaAuthMgrConnector.jar` file to the *`ITDI_HOME`*`/jars/connectors` directory.
4. Copy the `resource/rsa_token_types.properties` file to the *`ITDI_HOME`*`/timsol` directory.
5. Copy the `resource/config.properties` file to the *`ITDI_HOME`*`/timsol` directory.
6. Restart the adapter service.

Related concepts
Installing the dispatcher

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment

You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Before you begin

If you are using RSA Authentication Manager 7.1, complete these steps first:

1. On the RSA Authentication Manager server, change to the *RSA_AM_HOME*/appserver/weblogic/server/lib/ directory.
2. Enter the following command on one line:

```
java -jar ../../../modules/com.bea.core.jarbuilder_1.0.0.0.jar
-profile wlfullclient
```

   The `wlfullclient.jar` file is created in the *RSA_AM_HOME*/appserver/weblogic/server/lib directory.

If you are using RSA Authentication Manager 8.0, 8.1, or 8.2 the `wlfullclient.jar` file is already created. Proceed with the following procedure.

Procedure

1. For new installation, create the *ITDI_HOME*/jars/patches/rsa directory.
2. Copy these JAR files to the *ITDI_HOME*/jars/patches/rsa directory.

   Note: Make sure that you delete the previous *ITDI_HOME*/jars/3rdparty/rsa directory before you install the new version of the adapter. This directory exists only if you installed a previous version of the RSA Authentication Manager Adapter.

   RSA Authentication Manager 7.1

Table 4. Required JAR files for RSA Authentication Manager 7.1 and their locations. This table lists the RSA Authentication Manager JAR files that are required by the adapter.

Location in the RSA Authentication Manager server	**JAR file**
RSA_AM_HOME\utils\jars	am-client.jar
	am-server-o.jar
	ims-server-o.jar
	systemfields-o.jar
	ucm-server.jar
RSA_AM_HOME\utils\jars\thirdparty	axis-1.3.jar
	com.bea.core.process_5.3.0.0.jar
	commons-beanutils-1.7.0.jar
	commons-discovery-0.2.jar
	commons-lang-2.2.jar
	commons-logging-1.0.4.jar
	iScreen-ognl-1-1-0rsa-2.jar
	iScreen-1-1-0rsa-2.jar
	jdom-1.0.jar
	jsafe-3.6.jar
	jsafeJCE-3.6.jar
	ogni-2.6.7.jar
	spring-2.0.7.jar

Table 4. Required JAR files for RSA Authentication Manager 7.1 and their locations. This table lists the RSA Authentication Manager JAR files that are required by the adapter. *(continued)*	
Location in the RSA Authentication Manager server	**JAR file**
RSA_AM_HOME\appserver\weblogic\server\lib	EccpressoAsn1.jar
	EccpressoCore.jar
	EccpressoJcae.jar
	wlcipher.jar
	wlfullclient.jar
RSA_AM_HOME\server\servers*Hostname*_server\tmp_WL_user\console-ims\...\war\WEB-INF\lib	ims-client.jar
	ucm-client.jar

RSA Authentication Manager 8.0 and 8.1

The RSA Authentication Manager 8.0 SDK is in the same software package as the RSA Authentication Manager 8.0 appliance. The RSA Authentication Manager 8.1 SDK is on a separate software package from its appliance.

The required JAR files are in the *RSA_SDK_HOME*/lib/java directory where *RSA_SDK_HOME* is the directory where you installed the Authentication Manager SDK. You must copy only these files from the *RSA_SDK_HOME*/lib/java directory into the *ITDI_HOME*/jars/patches/rsa directory.

Table 5. Required JAR files for RSA Authentication Manager 8.0 SDK and 8.1 SDK. This table lists the RSA Authentication Manager JAR files that are required by the adapter.	
Location in the RSA Authentication Manager	**JAR file**
RSA_SDK_HOME/lib/java	am-client.jar
	commons-beanutils.jar
	commons-discovery.jar
	commons-lang.jar
	commons-logging.jar
	iScreen-ognl.jar
	iScreen.jar
	ognl.jar
	spring-aop.jar
	spring-asm.jar
	spring-beans.jar
	spring-context-support.jar
	spring-context.jar
	spring-core.jar
	spring-expression.jar
	wlfullclient.jar

RSA Authentication Manager 8.2

The required JAR files are in the *RSA_SDK_HOME*/lib/java directory where *RSA_SDK_HOME* is the directory where you installed the Authentication Manager SDK. You must copy only these files from the *RSA_SDK_HOME*/lib/java directory into the *ITDI_HOME*/jars/patches/rsa directory.

Table 6. Required JAR files for RSA Authentication Manager 8.2 SDK. This table lists the RSA Authentication Manager JAR files that are required by the adapter.

Location in the RSA Authentication Manager	JAR file
RSA_SDK_HOME/lib/java	am-client.jar
	aopalliance.jar
	clu-common.jar
	commons-beanutils.jar
	commons-lang.jar
	commons-logging.jar
	iScreen-ognl.jar
	iScreen.jar
	log4j.jar
	ognl.jar
	spring-aop.jar
	spring-beans.jar
	spring-context.jar
	spring-core.jar
	spring-expression.jar
	wlfullclient.jar
	xercesImpl.jar

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the license.bea file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The config.properties file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The rsa_token_types.properties file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

Restarting the adapter service

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

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

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

Related tasks

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

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Adapter authority requirement for the license.bea file

For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

An adapter has the authority to manage an RSA Authentication Manager 7.1 server resource only when the `license.bea` file of the server is available. The connector automatically sets the `bea.home` JVM property to the path of the `license.bea` file.

Copy the *RSA_AM_HOME*`/appserver/license.bea` file from the RSA Authentication Manager 7.1 server to the adapters solution directory. An example of the adapters solution directory is *ITDI_HOME*`/`*timsol*.

Related concepts

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

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

Restarting the adapter service

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Authentication Manager `config.properties` file update

The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

When you extracted the adapter files from the package, a `resource` directory was created. Copy the `config.properties` file from the `resource` directory to the adapters solution directory, for example *`ITDI_HOME/timsol`*.

Change the values of the following properties. Assign values that are specific to the RSA Authentication Manager instance.

- `java.naming.provider.url`
- `com.rsa.cmdclient.user`
- `com.rsa.cmdclient.user.password`

Note: Do not modify the other properties.

Note: Even though the adapter does not support SOAP protocol communication or two-way SSL authentication with the RSA Authentication Manager, the properties pertaining to SOAP and two-way SSL must still be present in the `config.properties`.

To find the values for the `com.rsa.cmdclient.user` and `com.rsa.cmdclient.user.password` properties, run the **`rsautil`** command. The **`rsautil`** command lists all the properties with key-value

pairs. From a command prompt on the RSA Authentication Manager server, change the directory to *RSA_AM_HOME*/utils and run the following command:

```
./rsautil manage-secrets --action list
```

When prompted, type your Operations Console username and password.

Copy the values for the com.rsa.cmdclient.user and com.rsa.cmdclient.user.password properties and put them in the config.properties file.

Note: Verify that there are no trailing whitespace on the values that you added.

The config.properties file requires only certain key pairs. The following sample file shows the required keys using sample values for an example server, local1. Modify the sample to fit your environment by changing only the values in italic.

```
# JNDI factory class.
java.naming.factory.initial = weblogic.jndi.WLInitialContextFactory

# Server URL. NOTE: Replace local1 with the hostname of your Authentication
# Manager server
java.naming.provider.url = t3s://local1:7002

# User ID for process-level authentication.  Replace CmdClient with the
# value from your environment.
com.rsa.cmdclient.user = CmdClient

# Password for process-level authentication. Replace password with the value
# from your environment.
com.rsa.cmdclient.user.password = password

# Password for Two-Way SSL client identity keystore
com.rsa.ssl.client.id.store.password = password

# Password for Two-Way SSL client identity private key
com.rsa.ssl.client.id.key.password = password

# Provider URL for Two-Way SSL client authentication
ims.ssl.client.provider.url = t3s://local1:7022

# Identity keystore for Two-Way SSL client authentication
ims.ssl.client.identity.keystore.filename = client-identity.jks

# Identity keystore private key alias for Two-Way SSL client authentication
ims.ssl.client.identity.key.alias = client-identity

# Identity keystore trusted root CA certificate alias
ims.ssl.client.root.ca.alias = root-ca

# SOAPCommandTargetBasicAuth provider URL
ims.soap.client.provider.url = https://local1:7002/ims-ws/services/CommandServer
```

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the license.bea file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Token type description file rsa_token_types.properties update
The rsa_token_types.properties file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

Restarting the adapter service

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Token type description file `rsa_token_types.properties` update

The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

By default the properties file contains the following entries:

- 0=RSA SecurID Standard Card
- 1=RSA SecurID PINPad
- 2=RSA SecurID Key Fob
- 3=RSA Watch Token
- 4=RSA SecurID Software Token
- 5=RSA Smart Card ID Token
- 6=RSA SecurID modem
- 7=RSA Crypto Token
- 8=RSA Proteus Token
- 9=RSA USB Cosmo Token
- 10=RSA Flexible Token

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Enabling secure communication

You must enable secure communication between the adapter and the server that it manages.

About this task

When you install RSA Authentication Manager, the system creates a self-signed server (root) certificate.

For RSA Authentication Manager 7.1
The certificate is stored in *RSA_AM_HOME*/server/security/*server_name*.jks.

For RSA Authentication Manager 8.0 and 8.1
The certificate is stored in *RSA_AM_HOME*/server/security/biztier-identity.jks.

Export this root certificate and store it in a trust store in your Security Directory Integrator environment.

Procedure

1. If you are using RSA Authentication Manager 7.1, use the command prompt to export the root certificate.
   a) From a command prompt on the RSA Authentication Manager server, change to the *RSA_AM_HOME*/appserver directory.
   b) Issue the following command on one line:

```
jdk/jre/bin/keytool –export
–keystore RSA_AM_HOME/server/security/server_name.jks
-file am_root.cer
–alias rsa_am_ca
```

   c) At the prompt for the keystore password, press Enter without typing a password.

      Note: A warning screen is displayed, but the root certificate is exported.

      The certificate file is *RSA_AM_HOME*/appserver/am_root.cert.
2. If you are using RSA Authentication Manager 8.0 and 8.1, use the Microsoft Internet Explorer to export the root certificate.
   a) Navigate to https://*rsa-authmgr-server-name* :7002. The Error 404 page appears.
   b) Right click anywhere on the Error 404 page and select **Properties** > **Certificates** > **Certification Path**.
   c) Click the top item in the certificate path.
   d) Click **View Certificate** > **Details** .
   e) Click **Copy to File**.
   f) On the **Certificate Export Wizard** page, click **Next**.
   g) On the **Export File Format** page, select **DER encoded binary X.509 (.CER)**, and click **Next**.
   h) On the **File to Export** page, specify the target location for the root certificate.
   i) Set the file name to **am_root.cer** and save the file as **DER Encoded Binary X.509(*.cer)**.
   j) Click **Next**.
   k) On the **Completing the Certificate Export** page, click **Finish**.
   l) Click **OK**.
3. Create a trust store for the root certificate.
   a) Transfer the exported root certificate file to Security Directory Integrator.
   b) Change directory to the adapters solution directory.
      For example, *ITDI_HOME*/*timsol*
   c) Issue the following command on one line:

```
../jvm/jre/bin/keytool -import -keystore rsaTruststore.jks
-storetype JKS -storepass password -alias rsa_am_ca
-file path-to-exported-server-cert
```

      The **keytool** displays a confirmation message that the certificate was added to the trust store, in the *ITDI_HOME*/*timsol* directory.
4. Set the following Java system property:

```
-Dweblogic.security.SSL.trustedCAKeyStore=full-path-to-rsaTruststore.jks
```

The Dispatcher reads this property and makes it available to the RSA run time. For information about setting this property in your Security Directory Integrator environment, see the "Configuring the Dispatcher JVM properties" section of the *Dispatcher Installation and Configuration Guide*.

What to do next

Verify the installation. See "Verifying the adapter installation" on page 24

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

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.

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

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.

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

Verifying the adapter installation

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

Use the following table to verify that you have installed and configured the RSA Authentication Manager Adapter correctly in the Security Directory Integrator environment.

Table 7. Adapter components

Directory	Adapter components	Comments
ITDI_HOME/jars/connectors	RsaAuthMgrConnector.jar	None
ITDI_HOME/jars/patches/rsa	**RSA Authentication Manager 7.1** am-client.jar am-server-o.jar axis-1.3.jar com.bea.core.process_5.3.0.0.jar commons-beanutils-1.7.0.jar commons-discovery-0.2.jar commons-lang-2.2.jar commons-logging-1.0.4.jar EccpressoAsn1.jar EccpressoCore.jar EccpressoJcae.jar ims-client.jar ims-server-o.jar iScreen-1-1-0rsa-2.jar iScreen-ognl-1-1-0rsa-2.jar jdom-1.0.jar jsafe-3.6.jar jsafeJCE-3.6.jar ognl-2.6.7.jar spring-2.0.7.jar systemfields-o.jar ucm-client.jar ucm-server-o.jar wlcipher.jar wlfullclient.jar **RSA Authentication Manager 8.0 and 8.1** am-client.jar commons-beanutils.jar commons-discovery.jar commons-lang.jar commons-logging.jar iScreen-ognl.jar iScreen.jar ognl.jar spring-aop.jar spring-asm.jar spring-beans.jar spring-context-support.jar spring-context.jar spring-core.jar spring-expression.jar wlfullclient.jar	No other JAR files must exist in this directory.

Table 7. Adapter components (continued)

Directory	Adapter components	Comments
ITDI_HOME/*timsol*	`config.properties`	Ensure that this file is configured to your environment. See "Authentication Manager config.properties file update" on page 18.
	`rsaTruststore.jks`	Ensure that this file contains the RSA Authentication Manager self-signed certificate. See "Enabling secure communication" on page 21.
	`license.bea` **Note:** This is applicable for RSA Authentication Manager 7.1 only.	None
Windows operating systems *ITDI_HOME*/*timsol*/`ibmdiservice.props` UNIX and Linux operating systems *ITDI_HOME*/`ibmdisrv`	Dispatcher properties	Ensure that the JVM property `weblogic.security.SSL.trustedCAKeyStore=full-path-to-rsa-truststore` is defined with a **–D** flag. See the section "Configuring the Dispatcher JVM properties" in the *Directory Integrator Dispatcher Installation and Configuration Guide*.

If this installation is to upgrade a connector, send a request from IBM Security Verify Identity. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is at *ITDI_Home**adapter solution directory*\`logs`.

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

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

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

Installing the adapter language package

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Restarting the adapter service

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

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

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

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Importing the adapter profile

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 AD`ProfileJAR` 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. .

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

Installing the adapter language package

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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

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.

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

Attribute mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

5. Import the updated mapping definition file through the Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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.

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

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 27.

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.

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update

The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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

Service/Target form details

Complete the service/target form fields.

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 location

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

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

Security domain name

Specify the name of the security domain that the user can administer and from which principals and support data must be reconciled.

Administrative security domains are specific to an Authentication Manager server but each server is installed with a default top-level security domain (realm). The default realm name is `SystemDomain`.

To specify a security domain that is defined somewhere under a realm, use the full path to the security domain with the > character as a delimiter between security domains in the hierarchy. For example, `SystemDomain>Employees>Division1`.

To specify a top-level security domain (realm), use the realm name. For example, `SystemDomain`.

Administrator Name

Specify the administrator user that is used to log in to the resource and to perform user management operations on the specified security domain.

Administrator Password
Specify the password for administrator user.

Recon Limit
Specify this option to set the limit for the number of user accounts, groups, or roles that are retrieved. The default is `1000`. This value is used only for RSA Authentication Manager v7.1 SP2 and earlier. Later versions of the server ignore this value and return all user accounts, groups, and roles.

Owner
Optional: Specify a user as a service owner.

Service Prerequisite
Optional: Specify a service that is prerequisite to this service.

On the Dispatcher Attributes tab:

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 either of the following file paths to load the assembly lines from the `profiles` directory:

Windows operating systems
`c:\Program Files\IBM\TDI\V7.1\profiles`

UNIX and Linux® operating systems
`/opt/IBM/TDI/V7.1/profiles`

You must extract the assembly line files from the profile JAR file. For example, the command

```
jar xvf RSAProfile.jar
```

extracts the files

RsaAuthMgrrProfile
RsaAuthMgrProfile/AuthMgrAdd.xml
RsaAuthMgrrProfile/AuthMgrDelete.xml
RsaAuthMgrProfile/AuthMgrModify.xml
RsaAuthMgrrProfile/AuthMgrSearch.xml
RsaAuthMgrProfile/AuthMgrTest.xml
RsaAuthMgrProfile/CustomLabels.properties
RsaAuthMgrProfile/erRsaAuthMgrAccount.xml
RsaAuthMgrProfile/erRsaAuthMgrRMIService.xml

RsaAuthMgrProfile/schema.dsml
RsaAuthMgrProfile/service.def

You must copy the assembly line files to the location that you specify for the AL FileSystem Path.

Server Host Name
Specify the managed resource on which you want to control the maximum connections with the dispatcher property Max Connection Count.

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can execute simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines.

Disable AL Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

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.

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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.

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

Installing the adapter 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.

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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

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.

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

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.

Upgrading the connector

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

Before you begin

Read the Release Notes to obtain the version level of the new connector.

Procedure

1. Determine the version level of the installed connector
   a) Change to a temporary directory.
   b) Copy the RsaAuthMgrConnector.jar file from the *ITDI_HOME*/jars/connectors directory.
   c) Extract the manifest file by issuing the command:

```
jar xvf RsaAuthMgrConnector.jar META-INF/MANIFEST.MF
```

   d) Change to the META-INF directory and examine the MANIFEST.MF file to determine the version number of the connector.

   This example shows a sample of the manifest file contents.

```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.8.0
Created-By: pxi3260sr9fp1-20110208_03 (SR9 FP1) (IBM Corporation)
Implementation-Vendor: IBM
Implementation-Title: IBM Security Verify Identity IBM RSA Authentica
 tion Manager Adapter Connector
Implementation-Version: 6.0.1.8
```

2. If the required version in the Release Notes is higher than the version installed, copy the new RsaAuthMgrConnector.jar file into the *ITDI_HOME*/jars/connectors directory.
3. Compare the config.properties file with the previous version.
   a) In the temp directory where you extracted the adapter files change to the resources directory. Open the config.properties file.
   b) Compare the content with the content of the config.properties file in the *ITDI_HOME*/*timsol* directory.

   If new entities exist in the newer config.properties, you must update the file. See "Authentication Manager config.properties file update" on page 18.
4. Restart the Security Directory Integrator server.

What to do next

If required, upgrade the adapter profile.

Related concepts

Upgrading the profile

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

Upgrading the profile

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

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 executes the assembly lines from the updated adapter profile.

Related tasks

Upgrading the connector
The new adapter package might require you to upgrade the connector.

Chapter 5. Reinstalling

There are no special considerations for reinstalling the adapter. You do not need to remove the adapter before reinstalling it.

If your RSA Authentication Manager server has changed or you are running an adapter version prior to 6.0.11, uninstall the adapter and install the new version. For more information, see “Installing the adapter binaries or connector” on page 12.

If your RSA Authentication Manager server has not changed and you are replacing an adapter version 6.0.11 or higher:

1. Stop the RMI Dispatcher service. See the *Directory Integrator RMI Dispatcher Installation and Configuration Guide* for instructions.
2. Create a temporary directory on the computer on which you want to extract the new adapter.
3. Extract the contents of the compressed file into the temporary directory.
4. Copy the `connectors/am<version>/RsaAuthMgrConnector.jar` file to the *ITDI_HOME*`/jars/connectors` directory, overwriting the old connector jar file.
5. Restart the RMI Dispatcher service. See the *Directory Integrator RMI Dispatcher Installation and Configuration Guide* for instructions.

Chapter 6. Configuring

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

See the *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

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.

Maximum length modification of account form attributes

When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

For example, when you want the maximum length of the **First Name** attribute to be 2048, modify the `schema.dsml` file as:

```
Old profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
<attribute-type single-value = "true" >
    <name>erRsaAmFirstName</name>
    <description>First Name</description>
    <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15{1024}</syntax>
</attribute-type>

Modified profile:

<!-- ******************************************************** -->
<!-- erRsaAmFirstName -->
<!-- ******************************************************** -->
```

```
<attribute-type single-value = "true" >
    <name>erRsaAmFirstName</name>
    <description>First Name</description>
    <object-identifier>1.3.6.1.4.1.6054.3.150.2.1</object-identifier>
    <syntax>1.3.6.1.4.1.1466.115.121.1.15{2048}</syntax>
</attribute-type>
```

Creating a JAR file and importing the profile

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

About this task

If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You need to stop and start the Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 4, “Upgrading,” on page 41.

Procedure

1. Extract the contents of the `RsaAuthMgrProfile.jar` file into the temporary directory by running the following command:

   ```
   cd c:\temp
   jar -xvf RsaAuthMgrProfile.jar
   ```

   The **`jar`** command creates the *c*`:\temp\RsaAuthMgrProfile` directory.
2. Update the profile files.
3. Create a JAR file by using the files in the `\temp` directory by running the following commands:

   ```
   cd c:\temp
   jar -cvf RsaAuthMgrProfile.jar RsaAuthMgrProfile
   ```
4. Import the `RsaAuthMgrProfile.jar` file into the Identity server.
5. Stop and start the Identity server.

Password management for account restoration

An RSA Authentication Manager account is considered inactive when it is disabled, locked or both. To restore an account from these states, the user’s password is required. If you do not provide the password, the account is enabled but it is not unlocked. Also, when an account is restored from being suspended, you are prompted to supply a new password for the reinstated account. However, in some cases you might not want to supply a new password.

When IBM Security Directory Server is used to restore accounts, you are always prompted to enter the new password. But when Sun Java System Directory Server is used to restore an account, you are not required to enter a new password. For Sun Java System Directory Server, the password requirement to restore an account on the RSA Authentication Manager falls into two categories: allowed and required.

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 RSA Authentication Manager Adapter to require a new password when the account is restored. You can require a new password 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. Adapter profile components also enable remote services to find out whether you discard a password that is entered by the user in a particular

situation. For example, there are multiple accounts on disparate resources that are being restored. In this situation, only some of the accounts that are 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 example, you are ensuring that you are not prompted for a password when an account is restored.

Verifying that the adapter is working correctly

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

Procedure

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

Related concepts

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

Adapter authority requirement for the license.bea file
For RSA Authentication Manager 7.1, the adapter needs the `license.bea` file of the server for authority to manage the resource. This requirement is not relevant to RSA Authentication Manager 8.0 or 8.1.

Authentication Manager config.properties file update
The `config.properties` file contains key-value pairs that are needed to communicate with a particular RSA Authentication Manager server.

Token type description file rsa_token_types.properties update
The `rsa_token_types.properties` file contains the default mapping between token type and token type description. Edit this file if you have a different mapping on your setup.

Verifying the adapter installation
If the adapter is installed correctly, required components exist in the specified directories.

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

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

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

Related tasks

Installing the adapter binaries or connector

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

Copying JAR files from the RSA Authentication Manager server to the Security Directory Integrator environment
You must install certain JAR files in the Security Directory Integrator environment to run the RSA Authentication Manager Adapter.

Enabling secure communication
You must enable secure communication between the adapter and the server that it manages.

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.

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

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.

Chapter 7. 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 message that might be displayed in the user interface when the adapter is installed on your system.

Table 8. Error messages

Error message	Possible cause	Corrective action
`CommandException while making RSA AuthMgr connection: com.rsa.authn. AuthenticationCommandException: Access Denied`	The maximum number of administrative connections that are allowed by the RSA Authentication Manager is too small.	Increase the number of administrative connections that are allowed by the RSA Authentication Manager server.
`Error: Initialize Error: weblogic.socket. MaxMessageSizeExceededException: Incoming message of size: '10000080' bytes exceed the configured maximum of: '10000000' bytes for protocol: 't3s'`	The data (in bytes) sent from the RSA Authentication Manager during a user reconciliation exceeds the maximum message size that is configured for the t3s protocol. This error occurs when large numbers of users are reconciled from RSA Authentication Manager Adapter.	**MaxMessageSize** is one of the JAVA_OPTIONS parameters. Set this parameter to a value that is sufficient to handle the maximum number of user and token records that the adapter processes during reconciliation. Add the following argument in the Security Directory Integrator Java command options to increase the maximum message size that is configured for protocol: 't3s'. `-Dweblogic.MaxMessageSize= MAX_MESSAGE_SIZE` The tested maximum value of **Dweblogic.MaxMessageSize** is 2000000000.

Table 8. Error messages (continued)

Error message	Possible cause	Corrective action

		To change the Security Directory Integrator Java command options.
		Windows operating systems
		1. Change directories to the *Drive:*\ProgramFiles\IBM\TDI\V7.1*timsol*\
		2. Locate the ibmdiservice.props file and update the **jvmcmdoptions** property.
		For example:
		`Jvmcmdoptions = -Dweblogic.MaxMessageSize= 2000000000`
		UNIX and Linux operating systems
		1. Change directories to the /opt/IBM/TDI/V7.1/
		2. Locate the ibmdisrv file and edit the following line:
		`"$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -cp "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J" com.ibm.di.loader.IDILoader com.ibm.di.server.RS "$@"`
		For example:
		`"$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -cp "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J" -Dweblogic.MaxMessageSize = 2000000000 com.ibm.di.loader.IDILoader com.ibm.di.server.RS "$@"`

Table 8. Error messages (continued)

Error message	Possible cause	Corrective action

		After setting the **MaxMessageSize** value as 2000000000 if reconciliation operation fails with the error `java.lang.OutOfMemoryError` then increase the Security Directory Integrator Java heap size as follows:
		
		Add/Update the following argument in the Security Directory Integrator Java command options.
		
		`Xms`*`initial heap size`*
		`-Xmx`*`maximum heap size`*
		
		Defaults are:
		
		`-Xms32m -Xmx128m`
		
		Windows operating systems
		
		1. Change directories to the *`Drive:`*`\ProgramFiles\IBM\TDI\V7.1\`*`timsol`*`\`
		2. Locate the `ibmdiservice.props` file and update the **`jvmcmdoptions`** property.
		
		For example:
		
		`Jvmcmdoptions = -Xms64m`
		`–Xmx256m`
		`-Dweblogic.MaxMessageSize`
		`=2000000000.`
		
		UNIX and Linux operating systems
		
		1. Change directories to the `/opt/IBM/TDI/V7.1/`
		2. Locate the `ibmdisrv` file and edit the following line:
		
		`"$TDI_JAVA_PROGRAM"`
		`$TDI_MIXEDMODE_FLAG -cp`
		`"$TDI_HOME_DIR/IDILoader.jar"`
		`"$LOG_4J"`
		`-Dweblogic.MaxMessageSize =`
		`2000000000`
		`com.ibm.di.loader.IDILoader`
		`com.ibm.di.server.RS "$@"`
		
		For example:
		
		`"$TDI_JAVA_PROGRAM"`
		`$TDI_MIXEDMODE_FLAG -cp`
		`"$TDI_HOME_DIR/IDILoader.jar"`
		`"$LOG_4J" -Xms64m –Xmx256m`
		`-Dweblogic.MaxMessageSize`
		`= 2000000000`
		`com.ibm.di.loader.IDILoader`
		`com.ibm.di.server.RS "$@".`

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 8. Uninstalling

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

Removing the adapter binaries or connector

Use this task to remove the connector file for the RSA Authentication Manager Adapter.

About this task

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

To remove the RSA Authentication Manager Adapter, complete these steps.

Note: Delete the `license.bea` and `config.properties` file only if you are uninstalling the RSA Authentication Manager Adapter 7.1 adapter.

Procedure

1. Stop the RMI Dispatcher service.
   See the *Dispatcher Installation and Configuration Guide*.
2. Delete the *ITDI_HOME*`/jars/connectors/RSAAuthMgrConnector.jar` file.
3. Delete the *ITDI_HOME*`/jars/patches/rsa` directory.
4. Delete the *ITDI_HOME*`/timsol/license.bea` file, if it exists.
5. Delete the *ITDI_HOME*`/timsol/config.properties` file.
6. Delete the *ITDI_HOME*`/timsol/rsaTruststore.jks` file.
7. Delete the **`weblogic.security.SSL.trustedCAKeyStore`** RMI Dispatcher property from the Security Directory Integrator environment.
   See the "Configuring the Dispatcher JVM properties" topic in the *Dispatcher Installation and Configuration Guide*.
8. Start the RMI Dispatcher service.
   See the *Dispatcher Installation and Configuration Guide*.

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 RSA Authentication Manager Adapter.

Chapter 9. Reference

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

Adapter attributes and object classes

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.This topic is not applicable for this adapter.

As part of the adapter implementation, a dedicated account for IBM Security Verify Identity to access the RSA Authentication Manager is created on the RSA Authentication Manager. The adapter consists of files and directories that are owned by the IBM Security Verify Identity account. These files establish communication with the Identity server.

The Identity server communicates with the RSA Authentication Manager Adapter by using attributes that 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 RSA Authentication Manager Adapter.

The following tables list the attributes that are used by the RSA Authentication Manager Adapter. The tables give a brief description and corresponding values of the attribute.

Use this key for the permissions column.

```
R = The value is read-only.  You cannot set or change it through
    IBM Security Verify Identity.
AR = The value is specified during the account create operation through
    IBM Security Verify Identity.  After creation the value is read-only.
RW = The value is specified during the account create operation through
    IBM Security Verify Identity.  You can modify the value through the
    IBM Security Verify Identity account modify operation.
W = The value is specified during the account create or modify operation through
IBM Security Verify Identity.  The
      value is not stored
in the IBM Security Verify Identity LDAP,
but is treated as a send-only
      attribute.
```

erRsaAmAccount object class

Table 9. Attributes for the erRsaAmAccount object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
eruid Specifies the Authentication Manager server user login ID	String	Yes	RW	Yes
erRsaAmFirstName Specifies the given name of the user.	String	Yes	RW	No
erRsaAmLastName Specifies the family name of the user.	String	Yes	RW	Yes

Table 9. Attributes for the erRsaAmAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmUserGroup Specifies the groups that the user belongs to.	String	No	RW	No
erRsaAmSecurityDomain Specifies the security domain to which the user belongs.	String	Yes	RW	No
erRsaAmIdentitySource Specifies the identity source that defines the user account.	String	Yes	AR	No
erRsaAmGUID Specifies the unique identifier for the user in the RSA Authentication Manager server.	String	Yes	R	No
erRsaAmCertdn Specifies the Distinguished Name of the certificate.	String	Yes	RW	No
erPassword Specifies the password for the account.	String	Yes	RW	Yes
erAccountStatus Specifies the status of the account during a suspend or restore operation.	Boolean	Yes	RW	No
erRsaAmIsAdmin Specifies whether the user is an administrator.	Boolean	Yes	R	No
erRsaAmForcePwdChange Specifies whether to force the user to change the user password at the next login.	Boolean	Yes	RW	No
erRsaAmNotes Specifies the user description.	String	Yes	RW	No
erRsaAmMiddleName Specifies the middle name of the user.	String	Yes	RW	No
erRsaAmEmail Specifies the email address of the user	String	Yes	RW	No
erRsaAmExpireDate Specifies the date that the user account expires.	Date	Yes	RW	No
erRsaAmAdminRole Specifies the roles that are assigned to the administrator.	String	No	RW	No
erRsaAmStartDate Specifies the date that the account begins.	Date	Yes	RW	No

Table 9. Attributes for the erRsaAmAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmLastAuthenticationDate Specifies the last login date.	Date	Yes	R	No
erRsaAmLastMdfDate Specifies the date that the account was last modified.	Date	Yes	R	No
erRsaAmLastModifiedBy Specifies the ID of the person that last modified the account.	String	Yes	R	No
erRsaAmAccLockByLockoutPolicy Specifies whether the account is locked by a lockout policy.	Boolean	Yes	R	No
erRsaAmAcctLockOutOfEmergencyAuth Specifies whether the account is locked by an emergency authentication policy.	Boolean	Yes	R	No
erRsaAmT1TokenNotes Specifies the description for token number 1.	String	Yes	RW	No
erRsaAmT1Assign The identifier of the token assigned to the user. **Note:** The schema defines this attribute as multi-valued, but it must only have one value.	String	No	RW	No
erRsaAmT1StartDate Specifies the date when the token number 1 is active.	Date	Yes	R	No
erRsaAmT1ImportDate Specifies the date that token number 1 was imported.	Date	Yes	R	No
erRsaAmT1ImportedBy Specifies the user that imported token number 1.	String	Yes	R	No
erRsaAmT1AssignDate Specifies the date that token number 1 was assigned to the user.	Date	Yes	R	No
erRsaAmT1AssignedBy Specifies who assigned token number 1 to the user	String	Yes	R	No
erRsaAmT1EnableDate Specifies the last date that token number 1 was enabled or disabled.	Date	Yes	R	No
erRsaAmT1ExpireDate Specifies the date on which token number 1 expires.	Date	Yes	R	No

Table 9. Attributes for the erRsaAmAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmT1LastLogonDate Specifies the last date that token number 1 was used to authenticate a user.	Date	Yes	R	No
erRsaAmT1Enable On add or modify, specifies whether to enable token number 1. After recon, it specifies whether token number 1 is enabled.	Boolean	Yes	RW	No
erRsaAmT1ReqAuthPasscode Specifies whether a passcode is needed when using token number 1 for authentication.	Boolean	Yes	RW	No
erRsaAmT1ForcePINChange Specifies whether to require a personal identification number (PIN) change at the next user login that uses token 1.	Boolean	Yes	RW	No
erRsaAmT1SetSecurIDPIN Specifies whether the SecureID PIN is set for token number 1.	String	Yes	R	No
erRsaAmT1ClearSecurIDPIN On add or modify, specifies whether to clear the PIN for token number 1. **Note:** This attribute is ignored if its value is false.	Boolean	Yes	RW	No
erServicePwd1 On add or modify, specifies the PIN for token number 1.	String	Yes	W	No
erRsaAmT1ReplacementToken Specifies the name of the token to replace token number 1.	String	Yes	RW	No
erRsaAmT1RplNextToken On add or modify, specifies whether to replace token number 1 with the next available token. **Note:** This attribute is ignored if its value is false.	Boolean	Yes	W	No
erRsaAmT1SecurityDomain Specifies the security domain for token number 1.	String	Yes	RW	Yes
erRsaAmT2TokenNotes Specifies the description for token number 2.	String	Yes	RW	No
erRsaAmT2Assign The identifier of the token assigned to the user. **Note:** The schema defines this attribute as multi-valued, but it must only have one value.	String	Yes	RW	No

Table 9. Attributes for the erRsaAmAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmT2StartDate Specifies the date when the token number 2 is active.	Date	Yes	R	No
erRsaAmT2ImportDate Specifies the date that token number 2 was imported.	Date	Yes	R	No
erRsaAmT2ImportedBy Specifies the user that imported token number 2.	String	Yes	R	No
erRsaAmT2AssignDate Specifies the date that token number 2 was assigned to the user.	Date	Yes	R	No
erRsaAmT2AssignedBy Specifies who assigned token number 2 to the user	String	Yes	R	No
erRsaAmT2EnableDate Specifies the last date that token number 2 was enabled or disabled.	Date	Yes	R	No
erRsaAmT2ExpireDate Specifies the date on which token number 2 expires.	Date	Yes	R	No
erRsaAmT2LastLogonDate Specifies the last date that token number 2 was used to authenticate a user.	Date	Yes	R	No
erRsaAmT2Enable On add or modify, specifies whether to enable token number 2. After recon, it specifies whether token number 2 is enabled.	Boolean	Yes	RW	No
erRsaAmT2ReqAuthPasscode Specifies whether a passcode is needed when using token number 2 for authentication.	Boolean	Yes	RW	No
erRsaAmT2ForcePINChange Specifies whether to require a personal identification number (PIN) change at the next user login that uses token number 2.	Boolean	Yes	RW	No
erRsaAmT2SetSecurIDPIN Specifies whether the SecureID PIN state is set for token number 2.	String	Yes	R	No
erRsaAmT2ClearSecurIDPIN On add or modify, specifies whether to clear the PIN for token number 2. **Note:** This attribute is ignored if its value is false.	Boolean	Yes	RW	No

Table 9. Attributes for the erRsaAmAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmT2ReplacementToken Specifies the name of the token to replace token number 2.	String	Yes	RW	No
erRsaAmT2RplNextToken On add or modify, specifies whether to replace token number 2 with the next available token. **Note:** This attribute is ignored if its value is false.	Boolean	Yes	RW	No
erRsaAmT2SecurityDomain Specifies the security domain for token number 2.	String	Yes	RW	Yes
erServicePwd2 On add or modify, specifies the PIN for token number 2.	String	Yes	W	No
erRsaAmT3TokenNotes Specifies the description for token number 3.	String	Yes	RW	No
erRsaAmT3Assign The identifier of the token assigned to the user. **Note:** The schema defines this attribute as multi-valued, but it must only have one value.	String	Yes	RW	No
erRsaAmT3StartDate Specifies the date when the token number 3 is active.	Date	Yes	R	No
erRsaAmT3ImportDate Specifies the date that token number 3 was imported.	Date	Yes	R	No
erRsaAmT3ImportedBy Specifies the user that imported token number 3.	String	Yes	R	No
erRsaAmT3AssignDate Specifies the date that token number 3 was assigned to the user.	Date	Yes	R	No
erRsaAmT3AssignedBy Specifies who assigned token number 3 to the user	String	Yes	R	No
erRsaAmT3EnableDate Specifies the last date that token number 3 was enabled or disabled.	Date	Yes	R	No
erRsaAmT3ExpireDate Specifies the date on which token number 3 expires.	Date	Yes	R	No

Table 9. Attributes for the erRsaAmAccount object class (continued)

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmT3LastLogonDate Specifies the last date that token number 3 was used to authenticate a user.	Date	Yes	R	No
erRsaAmT3Enable On add or modify, specifies whether to enable token number 3. After recon, it specifies whether token number 3 is enabled.	Boolean	Yes	RW	No
erRsaAmT3ReqAuthPasscode Specifies whether a passcode is needed when using token number 3 for authentication.	Boolean	Yes	RW	No
erRsaAmT3ForcePINChange Specifies whether to require a personal identification number (PIN) change at the next user login that uses token number 3.	Boolean	Yes	RW	No
erRsaAmT3SetSecurIDPIN Specifies whether the SecureID PIN state is set for token number 3.	String	Yes	R	No
erRsaAmT3ClearSecurIDPIN On add or modify, specifies whether to clear the PIN for token number 3. **Note:** This attribute is ignored if its value is false.	Boolean	Yes	RW	No
erRsaAmT3ReplacementToken Specifies the name of the token to replace token number 3.	String	Yes	RW	No
erRsaAmT3RplNextToken On add or modify, specifies whether to replace token number 3 with the next available token. **Note:** This attribute is ignored if its value is false.	Boolean	Yes	RW	No
erRsaAmT3SecurityDomain Specifies the security domain for token number 3.	String	Yes	RW	Yes
erServicePwd3 On add or modify, specifies the PIN for token number 3.	String	Yes	W	No
erRsaAmT1SerialNumber Specifies the serial number of token 1 assigned to the user.	String	Yes	R	No
erRsaAmT2SerialNumber Specifies the serial number of token 2 assigned to the user.	String	Yes	R	No

Table 9. Attributes for the erRsaAmAccount object class (continued)				
Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erRsaAmT3SerialNumber Specifies the serial number of token 3 assigned to the user.	String	Yes	R	No

erRsaAmRMIService object class

Table 10. Attributes for the erRsaAmRMIService object class				
Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erServiceName Specifies the name of the service.	String	Yes	RW	Yes
description Specifies the service description.	String	Yes	RW	No
erITDIurl Specifies the URL for the dispatcher.	String	Yes	RW	Yes
erRsaAmRealm Specifies the security domain that is being managed.	String	Yes	RW	Yes
erServiceUid Specifies the identifier for the service administrative user.	String	Yes	RW	Yes
erPassword Specifies the password for the service administrative user.	String	Yes	RW	Yes
erRsaAmSetLimit Specifies the maximum number of principals, groups, or roles that can be reconciled. This attribute is used only for RSA Authentication Manager v7.1 SP2 or earlier versions.	String	Yes	RW	No
erRsaAmDisableALCache Specifies whether to disable assembly line caching on the Security Directory Integrator server.	Boolean	Yes	RW	No
erRsaAmALFileSystemPath Specifies a fully qualified file system path where the service assembly lines are found.	String	Yes	RW	No
erRsaAmMaxConnectionCnt Specifies the maximum number of connections the Security Directory Integrator server can make for this service.	Integer	Yes	RW	No
erRsaAmServerHostName Specifies the host on which the RSA Authentication Manager server is running.	String	Yes	RW	Yes

Table 10. Attributes for the erRsaAmRMIService object class (continued)				
Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erRsaAmReconBatchSize Specifies the number of principals, groups, and tokens to be returned per-batch when the adapter operates in batch mode. (RSA Authentication Manager v7.1 SP3 and later). The default number is 1000. This attribute is ignored for RSA Authentication Manager v7.1 SP2 and earlier.	String	Yes	RW	No

erRsaAmGroups object class

Table 11. Attributes for the erRsaAmGroups object class				
Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erRsaAmGroupName Specifies the name of the group.	String	Yes	R	Yes
erRsaAmGroupGUID Specifies the unique identifier for the group in the RSA Authentication Manager server.	String	Yes	R	Yes
description Specifies the group description.	String	Yes	R	No

erRsaAmTokens object class

Table 12. Attributes for the erRsaAmTokens object class				
Attribute name and definition	**Data type**	**Single-valued**	**Permissions**	**Required**
erRsaAmTokenNumber Specifies the token serial number.	String	Yes	R	Yes
erRsaAmTokenGUID Specifies the unique identifier for the token in the RSA Authentication Manager server.	String	Yes	R	Yes
erRsaAmTokenAssign Specifies whether the token is assigned to a user.	Boolean	Yes	R	Yes
description Specifies the token description.	String	Yes	R	No
erRsaAmTokenType Specifies the numerical value of the token type.	String	Yes	R	No
erRsaAmTokenTypeDesc Specifies the description of the token type.	String	Yes	R	No

erRsaAmSecurityDomains object class

Table 13. Attributes for the erRsaAmSecurityDomains object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmSDName Specifies the security domain name.	String	Yes	R	Yes
erRsaAmSDGUID Specifies the unique identifier for the security domain in the RSA Authentication Manager server.	String	Yes	R	Yes
description Specifies the security domain description.	String	Yes	R	No

erRsaAmIdentitySources object class

Table 14. Attributes for the erRsaAmIdentitySources object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmISName Specifies the identity source name.	String	Yes	R	Yes
erRsaAmISGUID Specifies the unique identifier for the security domain in the RSA Authentication Manager server.	String	Yes	R	Yes
description Specifies the identity source description.	String	Yes	R	No

erRsaAmAdminRoles object class

Table 15. Attributes for the erRsaAmAdminRoles object class

Attribute name and definition	Data type	Single-valued	Permissions	Required
erRsaAmAdmRoleName Specifies the administrative role name.	String	Yes	R	Yes
erRsaAmAdmRoleGUID Specifies the unique identifier for the administrative role in the RSA Authentication Manager server.	String	Yes	R	Yes
description Specifies the administrative role description.	String	Yes	R	No

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.This topic is not applicable for this adapter.

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Index

S

T

U

V

W