IBM Security Verify Identity
7.0

Microsoft SharePoint 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 Microsoft SharePoint Adapter uses the functionality of Security Directory Integrator to enable communication between the Identity server and the Microsoft SharePoint server.

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

Features of the adapter

The adapter automates several administrative and management tasks.

The adapter automates the following tasks

- Creating users
- Modifying SharePoint user attributes
- Deleting user accounts
- Reconciling users and user attributes

Microsoft SharePoint Adapter provides a Web Service interface that is used to manage those tasks. Microsoft SharePoint Adapter adapters are configured to use the existing Web Service, which means that no extra software is required to be deployed on the Microsoft SharePoint Adapter end system.

IBM® Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager communicates with the Microsoft SharePoint Adapter to manage Microsoft SharePoint user accounts. You can perform the following actions on an account:

- Add
- Delete
- Modify
- Search

Note: The management of Microsoft SharePoint Adapter Groups disabled in this release due to lack of Microsoft SharePoint Adapter 2013 and 2016 Client API to properly manage Groups.

Related concepts

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

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

Architecture of the adapter

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

You must install the following components:

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

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

The following figure describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

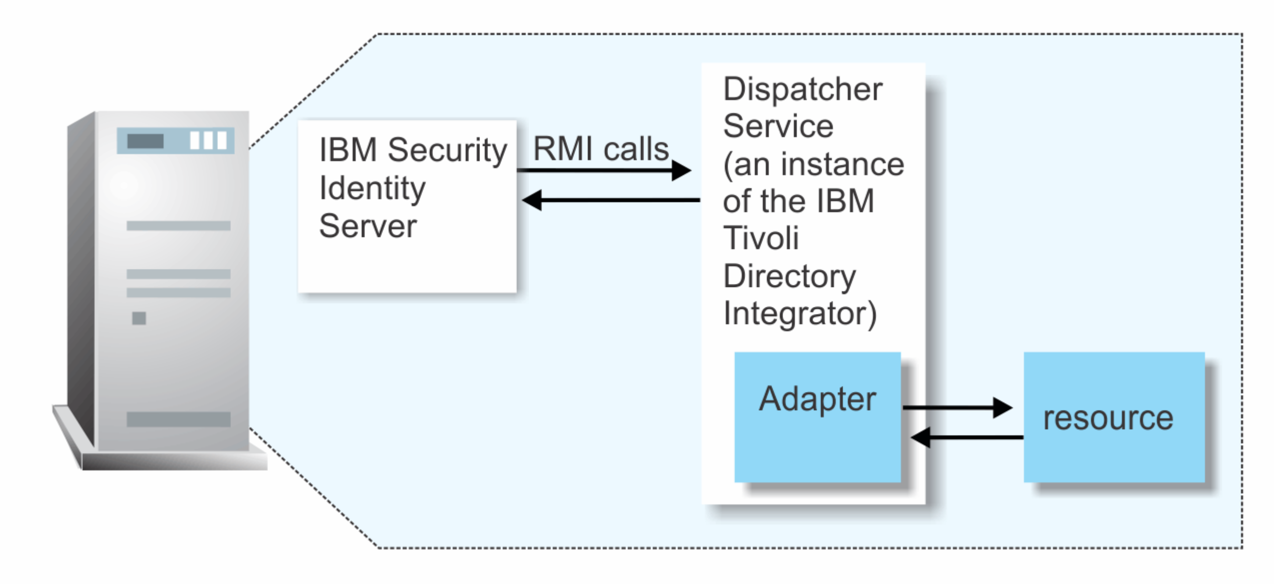
IBM Security Identity Server
RMI calls
Dispatcher Service (an instance of the IBM Tivoli Directory Integrator)
Adapter
resource

Figure 1. The architecture of the Microsoft SharePoint Adapter

The Microsoft SharePoint Adapter consists of Security Directory Integrator AssemblyLines. When an initial request is made by Identity server to the adapter, the AssemblyLines are loaded into the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager. As a result, subsequent service requests do not require those same AssemblyLines to be reloaded.

The AssemblyLines use the SharePoint User connector and RFC functional component to enable user management-related tasks on the Microsoft SharePoint. It does this enablement remotely by using the login ID and password of a user that has administrator privileges. The AssemblyLines also use server information about the location and site of the SharePoint server to perform this task.

Related concepts

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

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

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- The Identity server
- The Tivoli® Directory Integrator server
- The managed resource
- The adapter

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

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator server, and the Microsoft SharePoint Adapter on one server to establish communication with the Microsoft

SharePoint server. The Microsoft SharePoint server is installed on a different server as described Figure 2 on page 3.

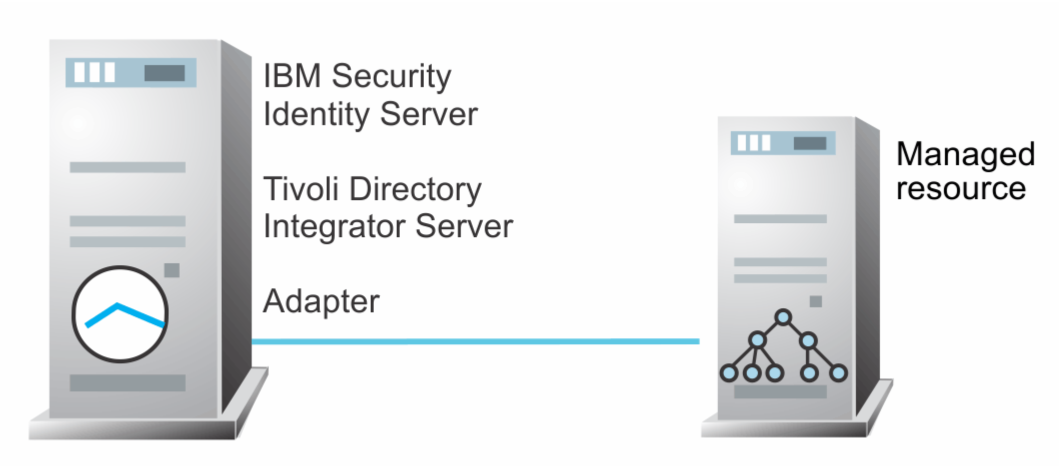

Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the Identity server, the Microsoft SharePoint Adapter, and the Microsoft SharePoint server are installed on different servers. Install the Security Directory Integrator server and the Microsoft SharePoint Adapter on the same server as described Figure 3 on page 3.

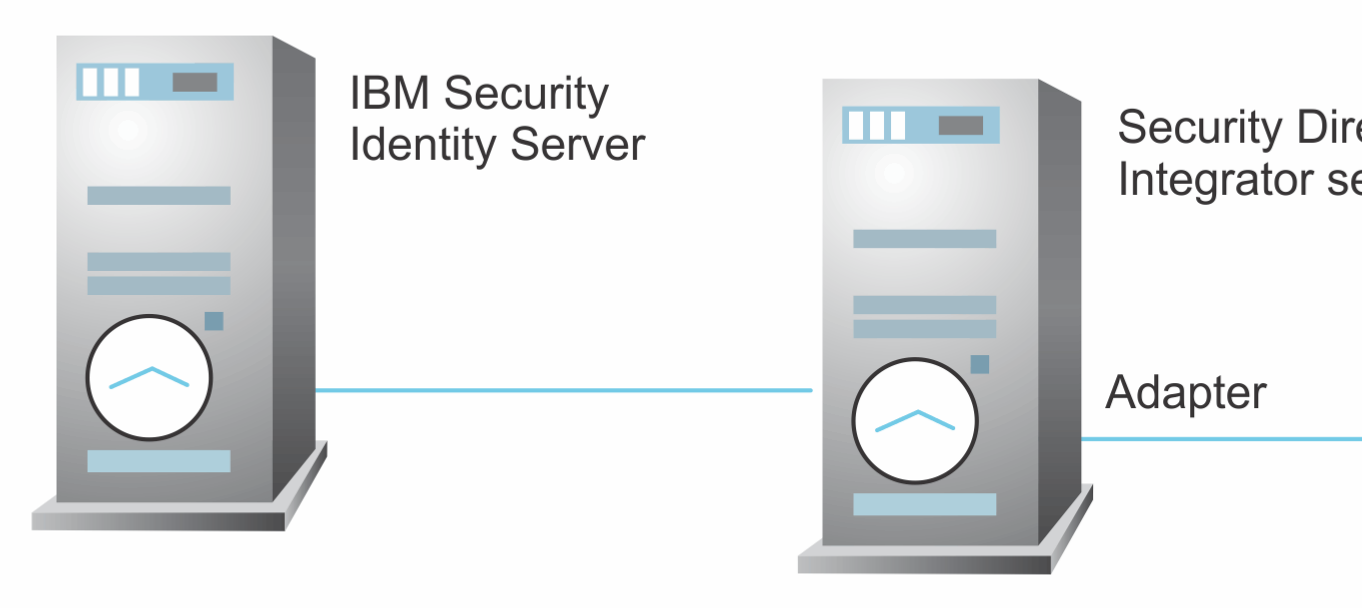

Figure 3. Example of multiple server configuration

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.

Use the Preinstallation roadmap to prepare the environment..

Table 1. Preinstallation roadmap

Task	For more information, see
Verify that your environment meets the software and hardware requirements for the adapter.	"Prerequisites" on page 11
Obtain the installation software.	Software download for the SharePoint adapter.
Obtain the necessary information for the installation and configuration.	"Installation worksheet" on page 13.

Use the Installation and configuration roadmap to complete the actual installation and configuration of the adapter.

Table 2. Installation and configuration roadmap

Task	For more information, see
Install the dispatcher.	"Installing the dispatcher" on page 15.
Install the connector.	"Installing the adapter binaries or connector" on page 16
Configure the authentication providers	"Configuring authentication providers" on page 18
Verify the adapter installation.	"Verifying the adapter installation" on page 21
Import the adapter profile into the Identity server.	Importing the adapter profile
Create an adapter service.	Creating an adapter service
Configure the adapter.	Chapter 5, "Configuring," on page 65

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 6.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 complete re-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

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

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager

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 complete re-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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
   a. Configure 1-way authentication.
   b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
   a. Configure 1-way authentication.
   b. Configure 2-way authentication.
3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Prerequisites

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

Table 3 on page 11 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 3. 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

Table 3. Prerequisites to install the adapter (continued)

Prerequisite	**Description**
Operating System	The Microsoft SharePoint Adapter can be used on any operating system that is supported by Security Directory Integrator.
Network Connectivity	Internet Protocol network
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*.
Microsoft SharePoint Server	Microsoft SharePoint Server 2013 with Service Pack 1 Microsoft SharePoint Server 2016

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

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

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

Table 4. 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. For example, the jars/connectors subdirectory contains the jar for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager product, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• for version 7.1:
		`drive\Program Files \IBM\TDI\V7.1`
		UNIX:
		• for version 7.1:
		`/opt/IBM/TDI/V7.1`

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

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

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

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.
- Enable Basic Authentication in IIS for the Sharepoint site. See the Configure Basic Authentication (IIS 7) topic on the Microsoft TechNet website.
- Check the Sharepoint site configuration for IIS. Set it to **`Integrated Windows - Negotiated (Kerberos)`**.

Procedure

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.

3. Install the adapter JAR files. Copy the `SharePointConnector.jar` file from the adapter package to the *`ITDI_HOME`*`/jars/connectors` directory.
4. Enable Unicode

   See the JVM information in the *Dispatcher Installation and Configuration Guide*.
5. Restart the adapter service.

Related concepts

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

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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

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.

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.

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.

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

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

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

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

Attribute Mapping

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

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

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.

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.

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.

Configuring authentication providers

You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

The following table list the supported Microsoft SharePoint Servers, authentication modes and authentication providers for accounts provisioned from the IBM Security Verify Microsoft SharePoint adapter.

Table 5. Supported Microsoft SharePoint Servers, authentication modes and authentication providers for accounts provisioned

Server version	Authentication mode	Authentication Provider
Microsoft SharePoint 2013 and Microsoft SharePoint 2016	1. Classic Mode 2. Claims Based Authentication(NTLM)	1. Integrated Windows (AD) 2. Forms Based Authentication (FBA)

Information about authentication providers is stored in a configuration file, which is in JSON format. The adapter reads this file and reconciles the list of authentication providers as supporting data.

The configuration file must have a single JSON array only. Each authentication provider is stored as a JSON Object element in the array with the following keys:

- DisplayName
- NameOfOriginalIssuer
- IssuerType
- ClaimsValueType
- ClaimsType
- Prefix

Example of a configuration file with information about the authentication providers.

Note: White spaces added for readability.

```
[
    {
        "DisplayName" : "Windows Authentication (EXAMPLEDOMAIN)",
        "NameOfOriginalIssuer" : "EXAMPLEDOMAIN",
        "IssuerType" : "w",
        "ClaimsValueType" : ".",
        "ClaimsType" : "#",
        "Prefix" : "i:0#.w|EXAMPLEDOMAIN"
    },
    {
        "DisplayName" : "Some Membership Provider",
        "NameOfOriginalIssuer" : "SomeMembershipProvider",
        "IssuerType" : "f",
        "ClaimsValueType" : ".",
        "ClaimsType" : "#",
        "Prefix" : "i:0#.f|SomeMembershipProvider|"
    },
    {
        "DisplayName" : "Example ACS",
        "NameOfOriginalIssuer" : "Example ACS",
        "IssuerType" : "t",
        "ClaimsValueType" : ".",
        "ClaimsType" : "5",
        "Prefix" : "i:05.t|Example ACS|"
    }
]
```

Table 6. Authentication providers listed in the example

JSON Object element in the previous example	**Authentication provider**
Element #1	Windows Authentication provider
Element #2	Forms-Based Authentication provider that is using a String logon name as Claims Value
Element #3	Trusted Identity Provider that is using email as Claims Value

For a full explanation on the valid values for IssuerType, NameOfOriginalIssuer, ClaimsValueType, and ClaimsType, see the *Microsoft SharePoint Products and Technologies Protocol Documentation*. With the four values, it is then trivial to create the Prefix. If the site runs on a Classic Mode authentication web application, the configuration file typically looks like the following example:

```
[
    {
        "DisplayName" : "EXAMPLEDOMAIN",
        "NameOfOriginalIssuer" : "",
        "IssuerType" : "",
        "ClaimsValueType" : "",
        "ClaimsType" : "",
        "Prefix" : "EXAMPLEDOMAIN"
    }
]
```

Generating the configuration file

A Powershell script is provided to assist with generating the configuration file.

Run the script on the SharePoint server with administrator privilege in a command prompt:

```
powershell authprovimport.ps1 -WebApplication http://[sharepointserver]:[port]
    -SaveAs [filename.json]
```

Copy the configuration file to a location on the server that is running the Adapter Dispatcher service. For example, save the file under *TDI_HOME**timsol*\SharePointAdapter folder. Create the SharePointAdapter folder if it does not exist.

SharePoint Site Configuration

If the Microsoft SharePoint site is configured with some other authentication (for exmaple, Form-Based Authentication), we can still manage the site through adapter either by using Basic Authentication or NTLM authentication.

The following steps are recommended to ensure the Adapter works with the Microsoft SharePoint site.

1. Extend the SharePoint Web Application to a new IIS Web Site.
2. Configure the Authentication Provider for the newly extended site.
    a. Select the check box for **Enable Windows Authentication**.
    b. Select the check box for **Integrated Windows authentication(NTLM)/Basic authentication**.

    Note: This configuration option depends on the authentication with which the adapter will be configured on IBM Security Verify Identity or IBM Security Verify Governance Identity Manager.
3. Configure the new IIS Website for SSL.
4. Import the SSL certificate into the Adapter Dispatcher's certificate trust store (view the `IDI_HOME/timsol/solution.properties` file and search for property `javax.net.ssl.trustStore` to determine the location of the trust store file).

For more detailed instructions, refer to the Microsoft SharePoint documentation.

Related concepts

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

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

Verifying the adapter installation

If the adapter is installed correctly, you can verify that the required components exist in the specified directories.

If the adapter is installed correctly, these adapter components exist on the Security Directory Integrator server.

Table 7. Adapter component

Adapter component	**Directory**
SharePointConnector.jar	`*TDI_HOME*\jars\connectors`
JSON files containing authentication providers configuration	`*TDI_HOME*\*timsol*\SharePointAdapter`

If this installation is to upgrade a connector, then 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 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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

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

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

repackage the JAR file with the updated files.The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:

   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*`Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.

   b) Click **OK** to import the file.

Results

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

What to do next

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

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

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.

The adapter profile is already imported into the IBM Security Verify Identity virtual appliance. Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Verify Identity.

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the `<Adapter>Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.

   b) Click **OK** to import the file.

Results

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

What to do next

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

`enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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

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

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

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

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

Reviewing and setting channel modes for each new connector

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

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.

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.

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.

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

- The IBM Security Privileged Identity Manager is installed and running.
- You have root or administrator authority on the IBM Security Privileged Identity Manager.
- 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 Privileged 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 IBM Security Privileged Identity Manager by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:

   a) In the **Service Definition File** field, type the directory location of the `<`*`Adapter`*`>Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.

b) Click **OK** to import the file.

Results

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

What to do next

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

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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

Importing attribute mapping file

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

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

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

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

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

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.

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.

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.

Importing the adapter profile

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

Before you begin

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

About this task

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

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

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

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

Procedure

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

   b) Click **Browse** to locate the JAR file that you want to import.

   c) Click **Upload file**.

      A message indicates that you successfully imported a profile.
7. Click **Close**.

   The new profile is displayed in the list of profiles.

Results

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

What to do next

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

- Import the attribute mapping file. See “Importing attribute mapping file” on page 34.
- Create a connector that uses the target profile. See “Adding a connector” on page 35.

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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.

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.

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.

Importing attribute mapping file

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

About this task

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

Procedure

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

   b) Click **Browse** to locate the attribute mapping file that you want to import.

   c) Click **Upload file**.

      A message indicates that you successfully imported the file.
7. Click **Close**.

Related concepts

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

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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.

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.

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.

Adding a connector

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

Before you begin

Complete Importing the adapter profile.

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

About this task

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

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

Procedure

To add a connector, complete these steps.

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

   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.

   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:

   a) Assign a name and description for the connector.

   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.

   c) Select the entity, such as **Account** or **User**.

   Depending on the connector type, this field might be preselected.

   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.

   The available trace levels are DEBUG, INFO, and ERROR.

   e) Optional: Select **History ON** to save and track the connector usage.

   f) Click **Save**.

   The fields for enabling the channels for sending and receiving data are now visible.

   g) Select and set the connector properties in the **Global Config** accordion pane.

   For information about the global configuration properties, see Global Config accordion pane.

   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

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

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

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see "Enabling connectors" on page 38.

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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.

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.

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.

Enabling connectors

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

Before you begin

Table 8. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 35.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 42.

Procedure

To enable a connector, complete these steps:

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

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

   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

   Enable write-to channel

   Propagates every change in the Access Governance Core repository into the target system.

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

   Enable read-from channel

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

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

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

Results

The connector is enabled

What to do next

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

Related concepts

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

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

Importing attribute mapping file

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

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

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

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

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.

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.

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.

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.

3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Verify Governance Identity Manager attribute values.

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

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

   ```

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

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

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Related concepts

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

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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.

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.

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.

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

1. Log in to the Verify Governance Identity Manager Administration Console.

2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

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

   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

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

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

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

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:

   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

   b) Select a connector, and click **Actions** > **Sync Now**.

      The synchronization process begins.

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

      Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:

    a) Select **Manage** > **Connectors**.

    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.

    c) Click **Save**.

       For more information, see "Enabling connectors" on page 38.

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

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

Related concepts

Installing the dispatcher

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

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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.

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.

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.

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 24.

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.

Configuring authentication providers

You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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 29.

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 **Services** table, 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**.
6. On the **Service Information** page, specify the appropriate values for the service instance.

   The content of the **Service Information** page depends on the type of service that you are creating.
7. Click **Test Connection** to validate that the data in the fields is correct.

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

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

Enabling connectors

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

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

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

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.

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.

Service/Target form details

Complete the service/target form fields.

On the Adapter Details 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.

TDI URI

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

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

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

Table 9. Ports

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

Table 9. Ports (continued)

Instance	Ports
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

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

- 1099
- 2099
- 3099

Owner
Optional: Specify a user as a service owner.

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

On the SharePoint Domain Details tab

Sharepoint hostname/ Site URL

For On-premises Microsoft SharePoint, specify the host name or IP address of the SharePoint site.

For Microsoft SharePointOnline, specify the Microsoft SharePoint Online Site URL. For example, `https://<domain>.sharepoint.com/sites/<site name>`.

Admin Login/ Client ID

For On-premises Microsoft SharePoint, specify the password for administrator user.

Note: For NTLM authentication, Administrator login must be in this format: `<Domain Name>\<Login Name>`.

For Microsoft SharePoint Online, specify the *Site Client Secret*.

Admin Password/ Client Secret

For On-premises Microsoft SharePoint specify the password for administrator user.

For Microsoft SharePoint Online specify the *Site Client Secret*.

Microsoft SharePoint On-premises and Microsoft SharePoint Online

For On-premises Microsoft SharePoint select the authentication mode with which the adapter connects to the SharePoint site.

Note: For NTLM Authentication, select *OnPrem Claims-Based Authentication*.

For Microsoft SharePoint Online select the option: *SharePoint Online*

SharePoint site (On-premises only)
Optional: Specify the trailing URL to the SharePoint site. For the Sharepoint site `subsite` with the location `http://sharepointhost/subsite`, the field entry is `subsite`. If you leave this field blank, the default value is the top-level Sharepoint site.

SharePoint port (On-premises only)
Specify the Microsoft SharePoint server port number. The default is port 80.

Enable SSL
Specifies whether you want to enable secure communications. The default response is not to enable SSL.

Authentication Provider Configuration File (On-premises only)
The file name that includes the full path to the authentication provider file.

It lists the authentication providers configured on the Microsoft SharePoint site. While provisioning account, you can select one of the authentication providers listed in this file.

For more information, see “Configuring authentication providers” on page 18. If the file is stored in the same location as Dispatcher home, for example, *TDI_HOME/timsol*, you can omit the path and provide only the file name.

SharePoint Site Domain Name (Online only)
Specify the Microsoft SharePoint Online Domain Name.

On the SharePoint Generic Configuration tab
These properties are internal properties. They are listed for informational purposes only. Do not change theMicrosoft SharePointm from the default configuration.

Adapter Task
This property allows for plug-able tasks to be called. The format is `<Label>:<classname>,<Label>:<Classname>.` The label must have a matching Adapter Authenticator

Adapter Authenticator
This property is the plug-able authenticator for the task. The format is `<Label>:<classname>,<Label>:<Classname>.`. The label must have a matching Task Authenticator.

Create Order
This property specifies the order in which the tasks are called during a create operation. The format is `<Label>|<Label>.`

Delete Order
This property specifies the order in which the tasks are called during a delete operation. The format is `<Label>|<Label>.`

Update Order
This property specifies the order in which the tasks are called during an update operation. The format is `<Label>|<Label>.`

Read Order
This property specifies the order in which the tasks are called during a read operation. The format is `<Label>|<Label>.`

Attributes Passed Down
These attributes are the ones that are required during an authentication phase and are passed down to the Task Authenticator during initialization. The format is `<Attribute Name>|<Attribute Name>.`

Attribute Mapping
This attribute allows for attributes to be overloaded. In some cases attributes must be converted from and to different names in the adapter task. The format is `<ISIM Attribute Name>|<Task Attribute Name>,<ISIM Attribute Name>|<Task Attribute Name>.`

On the Status and information tab
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, such as 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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

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 serverIdentity server.
2. Run a full reconciliation from the Identity serverIdentity 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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

Importing the adapter profile

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

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

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

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

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

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

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.

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.

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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

Chapter 4. Upgrading

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

To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, “Installing,” on page 15.

Upgrading the connector

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

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

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

Related concepts

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

Upgrading the adapter profile

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

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

Related concepts

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

Chapter 5. 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.

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 IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager for the changes to take effect.

About this task

In order to install the new attributes, complete the following steps:

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must 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 63.

Procedure

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

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

The **jar** command creates the c:\temp\SharePointProfile directory.

2. Update the profile files.
3. Create a JAR file using the files in the \temp directory by running the following commands:

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

4. Import the SharePointProfile.jar file into the Identity server.
5. Stop and start the Identity server.

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 serverIdentity server.
2. Run a full reconciliation from the Identity serverIdentity 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.

Configuring authentication providers
You must configure the adapter with one of the authentication providers that is supported by the Microsoft SharePoint Web Application. Authentication providers can be AD Domains or a claims provider.

Verifying the adapter installation
If the adapter is installed correctly, you can verify that the 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.

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.

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.

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.

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

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

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

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

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

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

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.

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.

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.

Chapter 6. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

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

Error messages and problem solving

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

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

Table 10. Warning and error messages and actions

Message	Action

Related concepts

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

Chapter 7. Uninstalling

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

Removing the adapter binaries or connector

The Microsoft SharePoint Adapter installation process also installs the Security Directory Integrator SharePoint connector.

About this task

To remove the Microsoft SharePoint Adapter, complete these steps:

Procedure

1. Stop the adapter service.
2. Remove the SharePointConnector.jar file from the *ITDI_HOME*/jars/connectors directory.
3. Start the service.

Related concepts

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

Deleting the adapter profile

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

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

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

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

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

Related tasks

Removing the adapter binaries or connector
The Microsoft SharePoint Adapter installation process also installs the Security Directory Integrator SharePoint connector.

Chapter 8. Reference

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

Adapter attributes and object classes

The Identity server communicates with the Microsoft SharePoint Adapter using attributes that are included in transmission packets that are sent over a network.

After you install the adapter profile, the Microsoft SharePoint Adapter supports a standard set of attributes. The following tables list the standard attributes and object classes supported by the adapter.

The combination of attributes depends on the type of action that the Identity server requests from the Microsoft SharePoint Adapter.

Standard attributes

The following table lists the attributes that are used by the Microsoft SharePoint Adapter. The table gives a brief description and corresponding values of the attribute.

Table 11. Supported attributes

IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	Attribute Name	Description	Data type
SharePoint Hostname	ersphostname	The host name of the Sharepoint server	String
`URL of TDI`	eritdiurl	The `URL of the TDI` dispatcher	String
Description	description	Description field for the adapter	String
SharePoint port	erspport	The port that Sharepoint is listening to	String
Administrator Account	erspadminaccount	The administration account used to update Sharepoint	String
Administrator Password	erservicepwd1	The password for the administration account	Password
Authentication Mode	erSPSiteAuthType	The authentication mode for the corresponding SharePoint server version	String
Authentication Provider Configuration File	erSPSiteAuthProvFilePath	The file path to the authentication provider configuration file	String
Site URL	erspsiteurl	A specific site on the Sharepoint host that is not the root site	String

Table 11. Supported attributes (continued)

IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	Attribute Name	Description	Data type
Enable SSL	erspenablessl	If this attribute is enabled, then HTTPS is used instead of HTTP	String
Adapter Name	erspadapter	This attribute is used to load the Sharepoint adapter.	String
Adapter Authentication	erspadapterauthn	This attribute is used to load the Sharepoint adapter authentication module.	String
Create Order	erspadaptercreateorder	Describes the order in which adapters are called	String
Delete Order	erspadapterdeleteorder	Describes the order in which adapters are called	String
Update Order	erspadapterupdateorder	Describes the order in which adapters are called	String
Read Order	erspadapterreadorder	Describes the order in which adapters are called	String
Attribute Mapping	erspadapterattributemap	This attribute is used to map common IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager attributes to adapter-specific attributes.	String
Configuration Attributes	erspconfigurationattributes	This list the adapter-specific configuration attributes that are passed by the service.def	String
User ID	eruid	The Sharepoint user ID. Typically, the login name or claims value	String
`User Name`	erspusername	The user display name for the Sharepoint user	String
`User Email`	erspemail	The email address for the Sharepoint user	String

Table 11. Supported attributes (continued)			
IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	**Attribute Name**	**Description**	**Data type**
User Notes	erspusernotes	Notes about the Sharepoint user. **Note:** This field is deprecated. It is kept in the schema for backwards-compatibility purpose only.	String
Authentication Provider	erspdomain	Authentication provider used by the account.	String
Group List	erspgrouplist	The list of groups that this user is part of in Microsoft SharePoint	String
Authentication Provider Name	erSPAuthProvName	The display name for the authentication provider	String
Authentication Provider Prefix	erSPAuthProvPrefix	The prefix for the authentication provider. If it is for the Classic Mode Authentication site, then this is the domain name. If it is for the Claims-Based Authentication site, then this is the claims prefix	String
Claims Type	erSPAuthClaimsType	The claim type encoding	String
Claims Value Type	erSPAuthClaimsValueType	The claims value type, normally a period (.) to indicate string	String
Authentication Issuer Type	erSPAuthIssuerType	The issuer type of the claims provider	String
Original Issuer Name	erSPAuthOriginalIssuer	The original issuer name of the claims provider	String

Supported object classes

The following table lists the object classes that are used by the Microsoft SharePoint Adapter. The table gives a brief description and corresponding values of the object class.

Table 12. Supported object classes

Description	Object class name in schema	Superior
Account class	erspaccount	top
Group class	erspgroupaccount	top
Authentication Provider class	erspauthenticationprovider	top

Adapter configuration properties

For information about setting Security Directory Integrator configuration properties for the operation of the Microsoft SharePoint Adapter, see the *Dispatcher Installation and Configuration Guide*.

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.

Adapter usage screens

Each screen has different fields. The following topics describe the fields and some of their limitations.

Group creation

The following table lists the required fields that are used to create a group.

Table 13. Required group creation fields

Title	Description
`Group Name`	The name of the group.
`Group Description`	A description for the group.
`Group Owner Type`	User or Group. The `Group Owner ID` must be either a user or group based on this selection.
`Group Owner ID`	If the user is selected in the `Group Owner Type` field, the full domain qualified user ID or Claims ID must be specified. If the group is selected, it must be a group that exists in Sharepoint. **Note:** To obtain the full Claims ID, append the Claims Prefix, which is stored as erspdomain in the account object, with the Claims Value, which is stored as eruid in the account object. If it is a Windows Authentication claim, add a backslash (\) after the domain name.
`Group Default User`	A full domain qualified user ID. The user must exist in the backing store. If no user is specified then the administration user that is used in the configuration of the profile is set in this field.

Group reconciliation

No specific screens exist for a reconciliation. The reconciliation operation does not return the `Group Default User`.

Group modification

During a modify operation, the parameters are changed if you specify the `Group Default User`.

If you do not specify the `Group Default User`, no changes are made.

Group deletion

No specific screens exist for deleting a group.

If a group is deleted, any users mapped to the group are removed from the mapping. The users are not removed from Microsoft SharePoint.

User creation

When you create a user in Microsoft SharePoint through IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager, you must specify certain attributes.

These attributes must be specified when you create a user.

Table 14. Required attributes for creating a user

Attribute	Description
User ID	This attribute is the SharePoint user backing store account name without the domain or claims prefix. For Example: Administrator. This user must be exist on the backing store.
User Name	The user display name for SharePoint.
User Email	An email address for SharePoint to send notifications and alerts to this user.
Domain	The domain or claims provider that this user ID belongs to.
Groups	Selection of the groups.

Note: The User Notes attribute is deprecated. It is removed from the account form. However, the attribute is maintained in the schema for backwards-compatibility reason.

User reconciliation

No specific screens exist for a user reconciliation.

The same user ID in different domains or claims providers is not supported for a reconciliation. For example, the “Administrator” ID is returned from one location only.

User modification

During a modify operation, the screen contains the same attributes that are listed when you create a user.

Modifying a field changes the SharePoint user. Do not change the `UserID` or the `Domain` field. Changing either of these attributes causes the modification to fail.

User deletion

No specific screens exist for deleting a user.

The user is removed from any groups to which the user belongs. If the user is the last member of the group, the group is not deleted. You must use the **`remove group`** command to delete a group.

Index