One Identity Manager 8.1.2

Administration Guide for Active Roles Integration

One Identity Manager Administration Guide for Active Roles Integration
Updated - January 2020
Version - 8.1.2

Contents

Active Roles integration

One Identity Manager supports the connection of Active Directory systems through an integrated Active Roles connector. Additional Active Directory relevant functionality, for example, Microsoft Exchange, Office Communication Services or Active Directory Lightweight Directory Service (AD LDS), is not supported through this connector.

One Identity Manager is assumed to be the master in the default configuration of processes and synchronization behavior and is allowed to bypass Active Roles workflows. Default behavior requires an administrative account. Active Roles workflows can still be controlled by the integrated Active Roles connector. You may need to define custom processes in One Identity Manager in order to use this functionality.

NOTE: For more detailed information about applying, managing, and configuring an Active Roles server, refer to the *One Identity Active Roles documentation*.

NOTE: This guide only goes into specific features of using the Active Roles Connector. For detailed documentation on managing an Active Directory environment with One Identity Manager, see *One Identity Manager Administration Guide for Connecting to Active Directory*.

Architecture overview

The following servers are used for managing an Active Directory environment with One Identity Manager and Active Roles:

- Active Roles server

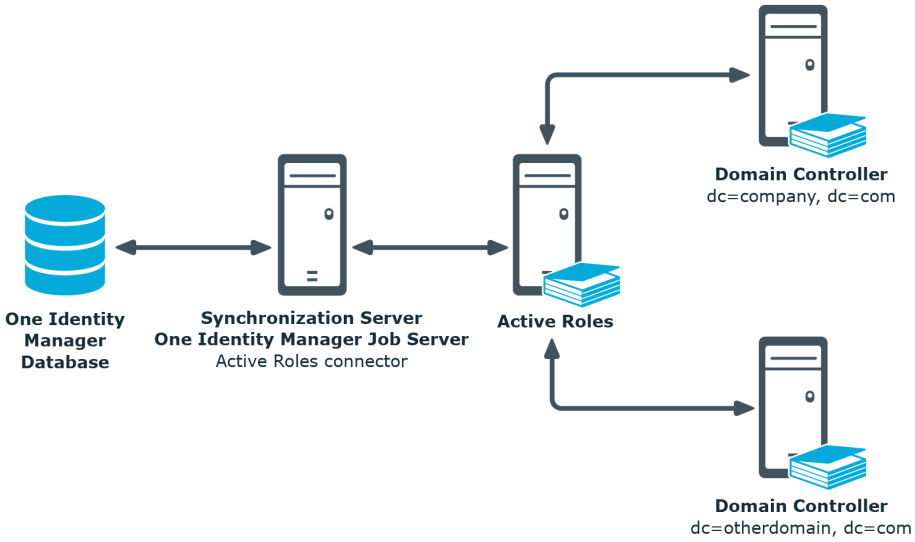
  Active Roles server that establishes the connection to the Active Directory domain controller. The synchronization server connects to this Active Roles server.

- Synchronization server

  The synchronization server executes the communication between the One Identity Manager Service and Active Roles. The One Identity Manager Service with the Active Roles connector is installed on this server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server connects to the Active Roles server.

The Active Roles One Identity Manager connector uses the Active Roles ADSI interface for communicating with an Active Roles instance. The Active Roles connector is used for synchronization and provisioning Active Directory. The Active Roles connector connects to an Active Roles instance, which then connects to the Active Directory domain controller.

Figure 1: The synchronization architecture



Migrating data between One Identity Manager and Active Roles

Scenario

You want to manage an Active Directory domain, currently managed by Active Roles, with One Identity Manager. Active Roles Self-Service Manager is not implemented.

Select one of the following editions modules when you install the One Identity Manager database:

- One Identity Manager Active Directory Edition
- One Identity Manager

Initial synchronization of Active Directory domains with One Identity Manager must be carried out by the Active Roles connector. All other synchronization is also carried out by the Active Roles connector.

- Create a synchronization project with the Synchronization Editor by using the default project template for Active Roles.

Scenario

You want to manage an Active Directory domain, currently managed by Active Roles, with One Identity Manager. Active Roles Self-Service Manager is implemented. The functionality should be transferred to the One Identity Manager‘s IT Shop.

Select one of the following editions modules when you install the One Identity Manager database:

- One Identity Manager Active Directory Edition
- One Identity Manager

In the One Identity Manager Active Directory Edition, there is direct support for transferal of Active Roles Self-Service Manager functionality to the One Identity Manager's IT Shop. If you are using the One Identity Manager Edition, run the following steps before initial synchronization:

1. In the Designer, set the "QER\Policy\GroupAutoPublish" configuration parameter.
2. In the Designer, set the "QER\ITShop\GroupAutoPublish\ADSGroupExcludeList" configuration parameter and specify Active Directory groups which are not to be added automatically to the IT Shop.
3. In the Designer, set the "TargetSystem\ADS\ARS_SSM" configuration parameter.
4. Compile the database.

Active Directory domain synchronization with One Identity Manager must be carried out by the Active Roles connector. All other synchronization is also carried out by the Active Roles connector.

- Create a synchronization project with the Synchronization Editor by using the default project template for Active Roles.

Scenario

You want to manage an Active Directory domain, currently managed by One Identity Manager, with Active Roles. Currently, Active Directory domain synchronization is carried out by the Active Directory connector.

To manage the Active Directory domains with One Identity Active Roles

1. In the Synchronization Editor, delete the existing synchronization project.
2. Create a synchronization project with the Synchronization Editor by using the default project template for Active Roles.

Detailed information about this topic

- Configuring synchronization with Active Directory using One Identity Active Roles on page 8
- Adding Active Directory groups automatically to the IT Shop on page 25

2

Configuring synchronization with Active Directory using One Identity Active Roles

One Identity Manager supports synchronization with Active Roles versions 6.9, 7.0, 7.2, and 7.3.1.

To load Active Directory objects into the One Identity Manager database for the first time

1. Prepare a user account with sufficient permissions for synchronizing in Active Directory.
2. One Identity Manager components for managing Active Directory environments are available if the **TargetSystem | ADS** configuration parameter is enabled.
    - In the Designer, check if the configuration parameter is set. Otherwise, set the configuration parameter and compile the database.
    - Other configuration parameters are installed when the module is installed. Check the configuration parameters and modify them as necessary to suit your requirements.
3. Install and configure a synchronization server and declare the server as Job server in One Identity Manager.
4. Transfer of One Identity Manager Self-Service Manager functionality into the Active Directory's Active Roles is directly supported in the IT ShopOne Identity Manager Edition. If you are using the One Identity Manager Edition, run the following steps before initial synchronization:
    a. In the Designer, set the **QER | ITShop | GroupAutoPublish** configuration parameter.
    b. In the Designer, set the **QER | ITShop | GroupAutoPublish | ADSGroupExcludeList** configuration parameter and specify the Active Directory groups that are not to be added automatically to the IT Shop.
    c. In the Designer, set the **TargetSystem | ADS | ARS_SSM**

configuration parameter

d. Compile the database.

5. Create a synchronization project with the Synchronization Editor.

Detailed information about this topic

- Migrating data between One Identity Manager and Active Roles on page 6
- One Identity Manager Service access permissions required for synchronizing using Active Roles on page 9
- Setting up the synchronization server on page 10
- Creating a synchronization project for initial synchronization of an Active Directory domain through Active Roles on page 13
- Adding Active Directory groups automatically to the IT Shop on page 25

One Identity Manager Service access permissions required for synchronizing using Active Roles

It is recommended that you set up a special user account for Active Directory, which is used for connecting to Active Roles through the One Identity Manager Service. Use Active Roles Access Templates for the configuration. By using Access Templates, you delegate administration-relevant permissions to an Active Directory user account but without issuing the permissions directly in Active Directory. Refer to your Active Roles documentation for more information about One Identity Active Roles Access Templates.

The following Access Templates are suggested for delegating permissions:

- All Objects - Read All Properties
- All Objects - Full Control

One Identity Manager works without controlling Active Roles workflows. To avoid existing Active Roles workflows, you must add the user account to the Active Roles administrators group. This group is created during Active Roles installation. The name of the group is saved in the registry database under:

- Registration key: HKEY_Local_Machine\Software\Aelita\Enterprise Directory Manager
- Value: DSAdministrators

Related topics

- Interaction with Active Roles workflows on page 20

Setting up the synchronization server

To set up synchronization with an Active Directory environment, a server with the following software installation must be available:

- Windows operating system

  The following versions are supported:

  - Windows Server 2008 R2 (non-Itanium based 64-bit) service pack 1 or later
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019
- Microsoft .NET Framework Version 4.7.2 or later

  NOTE: Take the target system manufacturer's recommendations into account.
- Windows Installer
- One Identity Active Roles Management Shell for Active Directory (x64)

  On 32-bit operating systems, the Active Roles Management Shell for Active Directory (x86) package shall be used.

  For installation instructions, refer to your One Identity Active Roles documentation.
- One Identity Manager Service, Active Roles connector
  - Install One Identity Manager components with the installation wizard.
    1. Select the **Select installation modules with existing database** option.
    2. Select the **Server | Job server | Active Directory** machine role.

  NOTE: For existing Active Roles installations:

  The One Identity Manager Service can be installed on a server using Active Roles.

All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The synchronization server must be declared as a Job server in One Identity Manager.

Use the One Identity Manager Service to install the Server Installer. The program executes the following steps:

- Sets up a Job server.
- Specifies machine roles and server function for the Job server.
- Remotely installs One Identity Manager Service components corresponding to the machine roles.

- Configures the One Identity Manager Service.
- Starts the One Identity Manager Service.

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. In the default case, this information is determined from the database connection data. If the Job server runs through an application server, you must configure extra connection data in the Designer. For detailed information about setting up Job servers, see the *One Identity Manager Configuration Guide*.

NOTE: The program executes remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program. Remote installation is only supported within a domain or a trusted domain.

To remotely install the One Identity Manager Service, you must have an administrative workstation on which the One Identity Manager components are installed. For detailed information about installing a workstation, see the *One Identity Manager Installation Guide*.

To remotely install and configure One Identity Manager Service on a server

1. Start the program Server Installer on your administrative workstation.
2. Enter the valid connection credentials for the One Identity Manager database on the **Database connection** page.
3. Specify the server on which you want to install One Identity Manager Service on the **Server properties** page.
    a. Select a Job server from the **Server** menu.

       - OR -

       To create a new Job server, click **Add**.

    b. Enter the following data for the Job server.
        - **Server**: Name of the Job server.
        - **Queue**: Name of the queue to handle the process steps. Each One Identity Manager Service within the network must have a unique queue identifier. The process steps are requested by the Job queue using exactly this queue name. The queue identifier is entered in the One Identity Manager Service configuration file.
        - **Full server name**: Full server name in accordance with DNS syntax.

          Syntax:

          `<Name of servers>.<Fully qualified domain name>`

    NOTE: You can use the **Extended** option to make changes to other properties for the Job server. You can also edit the properties later with the Designer.
4. On the **Machine roles** page, select **Active Directory**.
5. On the **Server functions** page, select **Active Roles connector**.
6. On the **Service Settings** page, enter the connection data and check the One Identity Manager Service configuration.

NOTE: The initial service configuration is predefined already. If further changes need to be made to the configuration, you can do this later with the Designer. For detailed information about configuring the service, see the *One Identity Manager Configuration Guide*.

- For a direct connection to the database:
  a. Select **Process collection | sqlprovider**.
  b. Click the **Connection parameter** entry, then click the **Edit** button.
  c. Enter the connection data for the One Identity Manager database.
- For a connection to the application server:
  a. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
  b. Click the **Connection parameter** entry, then click the **Edit** button.
  c. Enter the connection data for the application server.
  d. Click the **Authentication data** entry and click the **Edit** button.
  e. Select the authentication module. Depending on the authentication module, other data may be required, for example, user and password. For detailed information about the One Identity Manager authentication modules, see the *One Identity Manager Authorization and Authentication Guide*.

7. To configure remote installations, click **Next**.
8. Confirm the security prompt with **Yes**.
9. On the **Select installation source** page, select the directory with the install files.
10. On the **Select private key file** page, select the file with the private key.

    NOTE: This page is only displayed when the database is encrypted.
11. On the **Service access** page, enter the service's installation data.
    - **Computer**: Name or IP address of the server that the service is installed and started on.
    - **Service account**: User account data for the One Identity Manager Service.
      - To start the service under another account, disable the **Local system account** option and enter the user account, password and password confirmation.
    - **Installation account**: Data for the administrative user account to install the service.
      - To use the current user's account, set the **Current user** option.
      - To user another user account, disable the **Current user** option and enter the user account, password and password confirmation.
    - To change the install directory, names, display names or description of the One Identity Manager Service, use the other options.
12. Click **Next** to start installing the service.

Installation of the service occurs automatically and may take some time.

13. Click **Finish** on the last page of the Server Installer.

    NOTE: In a default installation, the service is entered in the server's service management with the name **One Identity Manager Service**.

Creating a synchronization project for initial synchronization of an Active Directory domain through Active Roles

Use Synchronization Editor to configure synchronization between the One Identity Manager database and Active Directory environment. The following describes the steps for initial configuration of a synchronization project.

After the initial configuration, you can customize and configure workflows within the synchronization project. Use the workflow wizard in the Synchronization Editor for this. The Synchronization Editor also provides different configuration options for a synchronization project.

Have the following information available for setting up a synchronization project.

Table 1: Information required for setting up a synchronization project

Data	Explanation
Distinguished name of the domain.	Distinguished LDAP domain name Example: `DC=Doku,DC=Testlab,DC=dd`
User account and password for logging into Active Roles.	User account and password for logging into Active Roles. Make a user account available with sufficient permissions. One Identity Manager Service access permissions required for synchronizing using Active Roles on page 9
DNS name of the Active Roles server	Full name of the Active Roles server connecting again the synchronization server. Example: `Server.Doku.Testlab.dd`
Synchronization server for Active Directory	All One Identity Manager Service actions are executed against the target system environment on the synchronization server. Data entries required for synchronization and administration with the One Identity Manager database are processed by the synchronization server. The One Identity Manager Service must be installed on the synchronization sehe connectorActive Directory connectorActive Roles.

<table>
<tr><th>Data</th><th>Explanation</th></tr>
<tr><td></td><td>The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job server.

Table 2: Additional properties for the Job server
<table><tr><th>Property</th><th>Value</th></tr><tr><td>Server function</td><td>Active Roles connector</td></tr><tr><td>Machine role</td><td>Server/Jobserver/Active Directory</td></tr></table>
For more information, see Setting up the synchronization server on page 10.</td></tr>
<tr><td>One Identity Manager database connection data</td><td>Database server
Database
SQL Server login and password
Specifies whether integrated Windows authentication is used. This type of authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.</td></tr>
<tr><td>Remote connection server</td><td>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with the target system to do this. Sometimes direct access from the workstation on which the Synchronization Editor is installed is not possible, because of the firewall configuration, for example, or because the workstation does not fulfill the necessary hardware and software requirements. If direct access is not possible from the workstation, you can set up a remote connection.

The remote connection server and the workstation must be in the same Active Directory domain.

Remote connection server configuration:
One Identity Manager Service is started
RemoteConnectPlugin is installed
Active Roles connector is installed
The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.

TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software</td></tr>
</table>

Data	Explanation
	and entitlements). Use the synchronization as remote connection server at the same time, by simply installing the `RemoteConnectPlugin` as well. For more detailed information about setting up a remote connection, see the *One Identity Manager Target System Synchronization Reference Guide*.

NOTE: The following sequence describes how to set up a synchronization project if Synchronization Editor is executed in default mode.

If you run the Synchronization Editor in export mode, you can make additional configuration settings. Follow the project wizard instructions through these steps.

To set up an initial synchronization project for an Active Directory domain using Active Roles.

1. Start the Synchronization Editor and log into the One Identity Manager database.
2. Select the start page. Click **Start a new synchronization project**.

   This starts the project wizard.
3. Click **Next** on the welcome page.
4. On the **Choose target system** page, select **Active Roles** connector.
5. On the **System access** page, specify how One Identity Manager can access the target system.
   - If access is possible from the workstation on which you started Synchronization Editor, you do not need to make any settings.
   - If access is not possible from the workstation on which you started Synchronization Editor, you can set up a remote connection.

     Enable the **Connect using remote connection server** option and select the server to be used for the connection under **Job server**.
6. On the **Target server** page, enter the Active Roles server to which you want to connect.
7. On the **Credentials** page, enter the user account and password for accessing Active Roles.
8. On the **Domain/root entry selection** page, select the domain you want to synchronize or enter the root entry's distinguished name.
9. On the **One Identity Manager Connection** tab, test the data for connecting to the One Identity Manager database. The data is loaded from the connected database. Reenter the password.

   NOTE: If you use an unencrypted One Identity Manager database and have not yet saved any synchronization projects to the database, you need to enter all

connection data again. This page is not shown if a synchronization project already exists.

10. The wizard loads the target system schema. This may take a few minutes depending on the type of target system access and the size of the target system.

11. On the **Restrict target system access** page, you specify how system access should work. You have the following options:

Table 3: Specify target system access

Option	Meaning
Read-only access to target system.	Specifies whether a synchronization workflow is only to be set up for the initial loading of the target system into the One Identity Manager database. The synchronization workflow has the following characteristics: • Synchronization is in the direction of **One Identity Manager**. • Processing methods in the synchronization steps are only defined for synchronization in the direction of **One Identity Manager**.
Read/write access to target system. Provisioning available.	Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system. The provisioning workflow displays the following characteristics: • Synchronization is in the direction of the **Target system**. • Processing methods are only defined in the synchronization steps for synchronization in the direction of the **Target system**. • Synchronization steps are only created for such schema classes whose schema types have write access.

12. On the **Synchronization server** page, select the synchronization server to execute synchronization.

    If the synchronization server is not declared as a Job server in the One Identity Manager database yet, you can add a new Job server.

    a. Click to add a new Job server.

    b. Enter a name for the Job server and the full server name conforming to DNS syntax.

    c. Click **OK**.

The synchronization server is declared as Job server for the target system in the One Identity Manager database.

NOTE: After you save the synchronization project, ensure that this server is set up as a synchronization server.

13. To close the project wizard, click **Finish**.

    This creates and allocates a default schedule for regular synchronization. Enable the schedule for regular synchronization.

    The synchronization project is created, saved, and enabled immediately.

    NOTE: If enabled, a consistency check is carried out. If errors occur, a message appears. You can decided whether the synchronization project can remain activated or not.

    Check the errors before you use the synchronization project. To do this, in the **General** view on the Synchronization Editor's start page, click **Verify project**.

    NOTE: If you do not want the synchronization project to be activated immediately, disable the **Activate and save the new synchronization project automatically** option. In this case, save the synchronization project manually before closing the Synchronization Editor.

    NOTE: The connection data for the target system is saved in a variable set and can be modified in the **Configuration | Variables** category in Synchronization Editor.

NOTE:

Following a synchronization, employees are automatically created for the user accounts in the default installation. If an account definition for the domain is not yet known at the time of synchronization, user accounts are linked with employees. However, account definitions are not assigned. The user accounts are therefore in a **Linked** state.

To manage the user accounts using account definitions, assign an account definition and a manage level to these user accounts.

To select user accounts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign the account definition and manage level to user accounts in **linked** status.
    a. In the Manager, select the **Active Directory | User accounts | Linked but not configured | <Domain>** category.

       - OR -

       In the Manager, select the **Active Directory | Contacts | Linked but not configured | <Domain>** category.

    b. Select the **Assign account definition to linked accounts** task.

Related topics

- Setting up the synchronization server on page 10
- One Identity Manager Service access permissions required for synchronizing using Active Roles on page 9
- Default project template for Active Roles on page 36

Accelerating provisioning and single object synchronization

To smooth out spikes in data traffic, handling of processes for provisioning and single object synchronization can be distributed over several Job servers. This will also accelerate these processes.

NOTE: You should not implement load balancing for provisioning or single object synchronization on a permanent basis. Parallel processing of objects might result in dependencies not being resolved because referenced objects from another Job server have not been completely processed.

Once load balancing is not longer required, ensure that the synchronization server executes the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as Job server in One Identity Manager.
   - Assign the **Active Roles connector** server function to the Job server.

   All Job servers must access the same Active Directory domain as the synchronization server for the respective base object.
2. In the Synchronization Editor, assign a custom server function to the base object.

   This server function is used to identify all the Job servers being used for load balancing.

   If there is no custom server function for the base object, create a new one.

   For more information about editing base objects, see the *One Identity Manager Target System Synchronization Reference Guide*.
3. In the Manager, assign this server function to all the Job servers that will be processing provisioning and single object synchronization for the base object.

   Only select those Job servers that have the same configuration as the base object's synchronization server.

   For more detailed information about editing server, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.

Once all the processes have been handled, the synchronization server takes over provisioning and single object synchronization again.

To use the synchronization server without load balancing.

- In the Synchronization Editor, remove the server function from the base object.

For detailed information about load balancing, see the *One Identity Manager Target System Synchronization Reference Guide*.

3

Interaction with Active Roles workflows

In the default configuration of processes and synchronization behavior, the integrated Active Roles connector works without input from Active Roles workflows. Changes are published immediately in Active Directory. An administrative user account. which is member in the Active Roles group is required for default behavior.

The One Identity Manager connector integrated in Active Roles does, however, allow Active Roles workflows to be controlled. That means, every operation in the Active Roles that is linked to a workflow starts that workflow.

You may have to customize processes so that they wait for the execution of workflows and therefore also the execution of changes in Active Roles if the Active Directory connector is supposed to trigger workflows. This is necessary because the One Identity Manager processes defined in the Active Directory are executed synchronously. The Active Roles connector is provided with additional functions to support you when querying the status of workflows.

The domain configuration and One Identity Manager Service user account permissions determine whether workflows are triggered.

NOTE: If the One Identity Manager Service's user account is a member in the Active Roles administrators group, workflows are always bypassed irrespective of the option setting.

For more information about Active Roles workflows, refer to your One Identity Active Roles documentation.

The following table show the correlation.

Table 4: Correlation to Active Roles workflow control

User Account Member of the Active Roles Administrators?	Option <Execute Active Roles workflows> Set?	Operation Linked with Active Roles Workflows?	Result
Yes	Yes	No	The operation is executed immediately.

User Account Member of the Active Roles Administrators?	Option <Execute Active Roles workflows> Set?	Operation Linked with Active Roles Workflows?	Result
Yes	No	No	The operation is executed immediately.
Yes	Yes	Yes	The operation is executed immediately without input from workflows.
Yes	No	Yes	The operation is executed immediately without input from workflows.
No	Yes	No	The operation is executed immediately.
No	No	No	The operation is executed immediately.
No	Yes	Yes	The Operation triggers workflows and depends on the final status.
No	No	Yes	The operation is aborted with an error message.

Related topics

- Extensions for applying Active Roles workflows on page 21
- Operation ID and status on page 23
- Additional virtual properties in the schema on page 23
- One Identity Manager Service access permissions required for synchronizing using Active Roles on page 9

Extensions for applying Active Roles workflows

NOTE: The One Identity Manager sets up the domains in the Synchronization Editor database.

To edit master data for an Active Directory domain

1. Select the **Active Directory | Domains** category.
2. Select the domain in the result list and run the **Change master data** task.
3. Enter the following data for utilizing workflows on the **Active Roles** tab.

Table 5: Extended properties for applying Active Roles workflows

Property	Description
Execute Active Roles workflows	Specifies whether Active Roles workflows should be executed. For more information about Active Roles workflows, refer to your One Identity Active Roles documentation. If this option is set, Active Roles workflows can be controlled by the integrated Active Roles connector. You may need to define custom processes in One Identity Manager to use this functionality. If this option is not set, One Identity Manager works without input from Active Roles workflows (default configuration). Default behavior requires an administrative account. NOTE: If the One Identity Manager Service user account is a member in the Active Roles administrators group, Active Roles workflows are always bypassed independent of the option.
User accounts deleted by Active Roles workflows	Specifies whether user accounts above deprovisioning workflows are deleted in Active Roles.
Groups deleted by Active Roles workflows	Specifies whether groups are deleted in Active Roles through deprovisioning workflows.

4. Save the changes.

Related topics

- One Identity Manager Service access permissions required for synchronizing using Active Roles on page 9
- Interaction with Active Roles workflows on page 20
- Deprovisioning Active Directory user accounts and Active Directory groups on page 30

Operation ID and status

The ID found by the Active Directory connector is returned in the "LastOperationID" output parameter of each change operation in Active Roles. The operation status passed from Active Roles is returned in the "LastOperationStatus" parameter. If no workflow is triggered and the operation is successful, the status "Completed" is returned. If a workflow is triggered, then the status "Pending" is returned. You can use these task parameters in follow-up processes to wait for the workflows to be executed.

Additional virtual properties in the schema

The Active Roles schema is provided with additional virtual properties for querying the current status of workflows.

NOTE: Virtual properties do not require any extension to the Active Directory schema. Active Roles behaves as though these properties really exist.

These virtual properties are defined as "read-only" and exist for all objects but are not mapped in the default project template. To use this functionality, you must adapt the custom mapping.

When the properties are read, the Active Roles connector executes an "OperationSearchRequest" call to Active Roles. To limit the impact on performance, the result of the queries is held for 30 seconds in cache.

Table 6: Virtual properties for the Active Roles connector

Property	Description
vrtLastOperationID	ID of the last operation in Active Roles.
vrtLastOperationStatus	ID of the last operation in Active Roles. Possible statuses are "Unknown", "Pending", "Completed", "Rejected", "Failed", and "Canceled".

For more information see your One Identity Active Roles documentation.

4

Interaction with Active Roles policies

When you are defining templates in One Identity Manager, you need to take the policies defined in Active Roles into account. Values generated in One Identity Manager are passed to the Active Roles connector without checking adherence to the Active Roles policies. If the values that are passed violate the Active Roles policies, the entire process fails. To prevent this, you need to customize the One Identity Manager templates for Active Roles.

Refer to your Active Roles documentation for more information about One Identity Active Roles policies.

Managing Active Directory objects

You can set up organizational units in a hierarchical container structure in One Identity Manager. Organizational units (divisions or departments) are used to logically organize Active Directory objects like user accounts and groups, thus simplifying administration.

NOTE: In the following, you are provided with details about the special features of managing Active Directory objects using Active Roles. For detailed documentation on managing an Active Directory environment with One Identity Manager, see One Identity Manager Administration Guide for Connecting to Active Directory.

Detailed information about this topic

Adding Active Directory groups automatically to the IT Shop

Table 7: Configuration parameter for automatically add groups in the IT Shop

Configuration parameter	Description
QER | ITShop | GroupAutoPublish	Preprocessor-relevant configuration parameter for automatically adding groups to the IT Shop. This configuration parameter specifies whether all Active Directory and SharePoint target system groups are automatically added to the IT Shop. Changes

Configuration parameter	Description
	to this parameter require the database to be recompiled.
QER | ITShop | GroupAutoPublish | ADSGroupExcludeList	This configuration parameter contains a list of all Active Directory groups for which automatic IT Shop assignment should not take place. Names are listed in a pipe (|) delimited list that is handled as a regular search pattern. Example: `.*Administrator.*|Exchange.*|.*Admins|.*Operators|IIS_IUSRS`
TargetSystem | ADS | ARS_SSM	Preprocessor-relevant configuration parameter for controlling the database model components for Active Roles Self-Service Management in the One Identity Manager IT Shop. If the parameter is set, Self-Service Management components are available. Changes to this parameter require recompilation of the database.

Transfer of One Identity Manager Self-Service Manager functionality into the Active Directory's Active Roles is directly supported in the IT Shop One Identity Manager Edition. If you are using the One Identity Manager Edition, run the following steps before initial synchronization:

To add groups automatically to the IT Shop

1. In the Designer, set the **QER \| ITShop \| GroupAutoPublish** configuration parameter.
2. In the Designer, set the **QER \| ITShop \| GroupAutoPublish \| ADSGroupExcludeList** configuration parameter and specify the Active Directory groups that are not to be added automatically to the IT Shop.
3. In the Designer, set the **TargetSystem \| ADS \| ARS_SSM** configuration parameter
4. Compile the database.

The groups are added automatically to the IT Shop from now on.

- Synchronization ensures that the groups are added to the IT Shop. If necessary, you can manually start synchronization with the Synchronization Editor.
- New groups created in One Identity Manager are added to the IT Shop.

The following steps are run to add a group to the IT Shop.

1. A service item is determined for the group.

   The service item is tested and modified for each group as required. The service item name corresponds to the name of the group. The service item is assigned to one of the default service categories.

- The service item is modified for groups with service items.
- Groups without service items are allocated new service items.
- The service item is enabled or disabled depending on whether the group is published in Active Roles Self-Service Manager.

2. An application role for product owners is determined and the service item is assigned. Product owners can approve requests for membership in these groups. By default, the group's account manager is established as product owner.

   NOTE: The application role for the product owner must be added under the **Request & Fulfillment | IT Shop | Product owner** application role.

   - If the account manager of the group is already a member of an application role for product owners, this application role is assigned to the service item. Therefore, all members of this application role become product owners of the group.
   - If the account manager of the group is not yet a member of an application role for product owners, a new application role is created. The name of the application corresponds to the name of the account manager.
     - If the account manager is a user account or a contact, the user account's employee or the contact's employee is added to the application role.
     - If it is a group of account managers, the employees of all this group's user accounts are added to the application role.
   - If the group does not have an account manager, the **Request & Fulfillment | IT Shop | Product owner | Without owner in AD** default application role is used.

3. The group is labeled with the **IT Shop** option and assigned to the **Active Directory Groups** IT Shop shelf in the **Identity & Access Lifecycle** shop.

Then the shop customers can request group memberships through the Web Portal.

NOTE: When a One Identity Manager group is irrevocably deleted from the database, the associated service item is also deleted.

Related topics

- Requesting new Active Directory groups using the Web Portal on page 27
- Active Roles specific extensions for Active Directory groups on page 28
- One Identity Manager IT Shop Administration Guide

Requesting new Active Directory groups using the Web Portal

NOTE: If you request group membership, "Approval of Active Directory group membership requests" in the default installation.

To request a new Active Directory group

- In the Web Portal, in the **Service catalog | Requests** menu, select the service category "Active Directory groups".
- Request the Active Directory group using the "New Active Directory distribution list" or the "New Active Directory security group" product.

The following steps are automatically executed when you request a new Active Directory groups:

- An entry is created for the Active Directory group in One Identity Manager.
- The Active Directory group is labeled with the **Group is published to Self-Service Manager** option.
- The Active Directory group is labeled with the **IT Shop** option.
- The associated service item is created. A new application role is set up with the requester as member. The application role is entered as product owner in the service item.

  Through this procedure, the Active Directory group requester has approval permissions for requesting memberships in this Active Directory group.
- The Active Directory group is assigned to the shelf "Active Directory groups" in the default shop "Identity & Access Lifecycle".

Active Directory group membership can then be requested by customers of this shop through the Web Portal.

NOTE: If an Active Directory group is permanently deleted from the One Identity Manager database, the associated service item is also deleted.

Related topics

- Adding Active Directory groups automatically to the IT Shop on page 25
- Active Roles specific extensions for Active Directory groups on page 28
- One Identity Manager Web Portal User Guide
- One Identity Manager IT Shop Administration Guide

Active Roles specific extensions for Active Directory groups

To display Active Roles group data ascertained from Active Directory

1. In the Manager, select the **Active Directory | Groups** category.
2. Select the group in the result list.

3. Select the **Change master data** task.
4. Select the **Active Roles** tab.

The following properties are displayed:

Table 8: Active Roles specific properties of an Active Directory group

Property	Description
Group is published to Self-Service Manager	If an Active Directory group is published, the Active Directory group can be requested in the Web Portal immediately after successful synchronization. The data is loaded from Active Roles on synchronization. This information is published when an Active Directory group is added through the Web Portal in order to start other workflows in Active Roles if necessary.
Approval by the group owner	Specifies whether the Active Directory group owner (account manager) must approve group membership. The information affects the approval workflow in the IT Shop.
Approval by a additional owner of the group	Specifies whether the additional Active Directory group owner must approve group membership. The information affects the approval workflow in the IT Shop.
Additional owners	List of additional owners Active Directory groups or Active Directory user accounts are permitted.
Deprovisioning status	Status of deprovisioning sequence through Active Roles when an object is deleted. The data is loaded from Active Roles on synchronization.

Status	Description
No deprovisioning	The Active Directory object is enabled.
Deprovisioning successful	The Active Directory object was successfully deprovisioned
Deprovisioning failed	An error occurred deprovisioning the Active Directory object.

Deprovisioning date	Status of deprovisioning sequence through an Active Roles when a object is deleted. The information is loaded from the Active Roles during synchronization.

Related topics

- Adding Active Directory groups automatically to the IT Shop on page 25
- Requesting new Active Directory groups using the Web Portal on page 27
- Displaying information about deprovisioning Active Directory user accounts and Active Directory groups on page 32

Deprovisioning Active Directory user accounts and Active Directory groups

One Identity Manager supports deprovisioning through Active Roles. Based on deprovisioning policies configured in Active Roles, an Active Directory object is modified such that it is temporarily or permanently disabled and possibly is not deleted until a certain time period has expired. You can find detailed information about Active Roles deprovisioning in your One Identity Active Roles documentation.

NOTE: The deprovisioning policy configuration in Active Roles may conflict with the default One Identity Manager configuration. In this case, make any appropriate adjustments to templates or processes, for example.

The following procedures are implemented for deprovisioning Active Directory user accounts and Active Directory groups with One Identity Manager:

- Deprovisioning not deletion
- Quick deprovisioning

Detailed information about this topic

- Deprovisioning not deletion on page 30
- Quick deprovisioning on page 31
- Displaying information about deprovisioning Active Directory user accounts and Active Directory groups on page 32
- Restoring deprovisioned Active Directory user accounts and Active Directory groups in the One Identity Manager on page 33
- Interaction with Active Roles policies on page 24

Deprovisioning not deletion

To implement this method

- In the Active Directory domain, set the **User accounts deleted by Active Roles workflows** and **Groups deleted by Active Roles workflows** options.

If an Active Directory user account or an Active Directory group is deleted in One Identity Manager, a deprovisioning process is generated in the Active Roles instead of the default deletion process. This process queues the Active Directory object for deprovisioning in Active Roles, sets a deprovisioned status, and checks the deprovisioning sequence. Active Directory objects continue to be processed in One Identity Manager depending this.

- If the Active Directory object was deleted immediately in Active Roles, the Active Directory object is also deleted in One Identity Manager.

- If the Active Directory object in Active Roles was renamed or moved to another Active Directory container, this is done in One Identity Manager as well.

  The Active Directory object remains in the One Identity Manager database with the status "deleted".

To delete a user account

1. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Delete the user account.
4. Confirm the security prompt with **Yes**.

To delete an Active Directory group

1. Select the **Active Directory | Groups** category.
2. Select the group in the result list.
3. Delete the group using .
4. Confirm the security prompt with **Yes**.

Related topics

- Extensions for applying Active Roles workflows on page 21
- Quick deprovisioning
- Displaying information about deprovisioning Active Directory user accounts and Active Directory groups on page 32
- Undoing deprovisioning on page 34
- Restoring deleted objects on page 35

Quick deprovisioning

You can apply this method if the Active Directory domain is not marked for deprovisioning. The **Deprovision** task is provided on these objects for the deprovisioning of individual Active Directory user accounts or Active Directory groups.

A deprovisioning process is generated in Active Roles. This process queues the Active Directory object for deprovisioning in Active Roles, sets a deprovisioned status, and checks the deprovisioning sequence. Active Directory objects continue to be processed in One Identity Manager depending this.

- If the Active Directory object was deleted immediately in Active Roles, the Active Directory object is also deleted in One Identity Manager.
- If the Active Directory object in Active Roles was renamed or moved to another Active Directory container, this is done in One Identity Manager as well.

The Active Directory object remains in the One Identity Manager database with the status "changed". All the Active Directory object properties are loaded in the One Identity Manager database by the next synchronization and set to "published".

To deprovision an Active Directory user account

1. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Deprovision** task.
4. Confirm the security prompt with **Yes**.
5. Confirm with **OK**.

To deprovision an Active Directory group

1. Select the **Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Deprovision** task.
4. Confirm the security prompt with **Yes**.
5. Confirm with **OK**.

Related topics

- Deprovisioning not deletion on page 30
- Displaying information about deprovisioning Active Directory user accounts and Active Directory groups on page 32
- Undoing deprovisioning on page 34

Displaying information about deprovisioning Active Directory user accounts and Active Directory groups

The following properties are displayed for deprovisioning Active Directory user accounts and Active Directory groups:

Table 9: Deprovisioning data

Property	Description
Deprovisioning status	Status of deprovisioning sequence through Active Roles when an object is deleted. The data is loaded from Active Roles on synchronization.

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>No deprovisioning</td><td>The Active Directory object is enabled.</td></tr>
<tr><td>Deprovisioning successful</td><td>The Active Directory object was successfully deprovisioned</td></tr>
<tr><td>Deprovisioning failed</td><td>An error occurred deprovisioning the Active Directory object.</td></tr>
</table>
</td></tr>
<tr><td>Deprovisioning date</td><td>Status of deprovisioning sequence through an Active Roles when a object is deleted. The information is loaded from the Active Roles during synchronization.</td></tr>
</table>

To display master data for deprovisioning an Active Directory user account

1. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Select the **Change master data** task.
4. Select the **Active Roles** tab.

To display master data for deprovisioning an Active Directory group

1. Select the **Active Directory | Groups** category.
2. Select the group in the result list.
3. Select the **Change master data** task.
4. Select the **Active Roles** tab.

Related topics

- Active Roles specific extensions for Active Directory groups on page 28

Restoring deprovisioned Active Directory user accounts and Active Directory groups in the One Identity Manager

You can restore deprovisioned Active Directory user account and Active Directory groups using One Identity Manager if required. The following methods are used to do this:

- Undo deprovisioning
- Restoring deleted objects

Both methods initiate a process for deprovisioning Active Directory objects in Active Roles. The process finds the deprovisioning status, updates some of the Active Directory object properties, like the name and the One Identity Manager container and in the Active Directory database, and sets the Active Directory object status to "changed". All the Active Directory object properties are loaded in the One Identity Manager database by the next synchronization and changed to "published".

Detailed information about this topic

- Undoing deprovisioning on page 34
- Restoring deleted objects
- Deprovisioning Active Directory user accounts and Active Directory groups on page 30

Undoing deprovisioning

Use this method to undo Active Directory user account and Active Directory group deprovisioning. You can use this method independent of the deprovisioning method implemented.

To undo Active Directory user account deprovisioning

1. Select the **Active Directory | User accounts | Deprovisioned accounts** category.
2. Select the user account in the result list.
3. Select the **Undo deprovisioning** task.
4. Confirm the security prompt with **Yes**.
5. Confirm with **OK**.

To undo Active Directory group deprovisioning

1. Select the **Active Directory | Groups | Deprovisioned groups** category.
2. Select the group in the result list.
3. Select the **Undo deprovisioning** task.
4. Confirm the security prompt with **Yes**.
5. Confirm with **OK**.

Related topics

- Restoring deleted objects
- Deprovisioning Active Directory user accounts and Active Directory groups on page 30

Restoring deleted objects

You can use this method as an alternative for Active Directory user accounts and Active Directory groups you have deprovisioned using the method "Deprovision not delete". You find the deprovisioned Active Directory object, in this case, in the One Identity Manager database with status "Deleted".

To restore a user account

1. Select the **Active Directory | User accounts** category.
2. Select the user account in the result list.
3. Click **Undo delete** in the result list toolbar.

To restore a group

1. Select the **Active Directory | Groups** category.
2. Select the group in the result list.
3. Click **Undo delete** in the result list toolbar.

Related topics

- Undoing deprovisioning on page 34
- Deprovisioning Active Directory user accounts and Active Directory groups on page 30

Appendix A

Default project template for Active Roles

A default project template ensures that all required information is added in One Identity Manager. This includes mappings, workflows, and the synchronization base object. If you do not use a default project template you must declare the synchronization base object in One Identity Manager yourself.

Use a default project template for initially setting up the synchronization project. For custom implementations, you can extend the synchronization project with the Synchronization Editor.

The template uses mappings for the following schema types.

Table 10: Mapping Active Roles schema types to tables in the One Identity Manager schema.

Schema type in Active Roles	Table in the One Identity Manager Schema
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
msExchSystemObjectsContainer	ADSContainer
oganization	ADSContainer
organizationalUnit	ADSContainer
printQueue	ADSPrinter

Schema type in Active Roles	Table in the One Identity Manager Schema
rpcContainer	ADSContainer
user	ADSAccount

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index