



One Identity Manager 8.1.1

Administration Guide for Active Roles Integration

Copyright 2019 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

integration with Active Roles	5
Architecture overview	5
Migrating Data between One Identity Manager and Active Roles	6
Configuring synchronization with Active Directory using One Identity Active Roles	8
One Identity Manager Service access rights required for synchronizing using Active Roles	9
Setting up the synchronization server	10
Creating a synchronization project for initial synchronization of an Active Directory domain through Active Roles	13
Interaction with Active Roles workflows	19
Extensions for the use of Active Roles workflows	20
Operation ID and status	22
Additional virtual properties in the schema	22
Interaction with Active Roles policies	23
Managing Active Directory objects	24
Adding Active Directory groups automatically to the IT Shop	24
Creating new Active Directory groups through the Web Portal	26
Active Roles specific extensions for Active Directory groups	27
Deprovisioning Active Directory user accounts and Active Directory groups	29
Deprovisioning not deletion	29
Quick deprovisioning	30
Displaying information about deprovisioning Active Directory user accounts and Active Directory groups	31
Restoring deprovisioned Active Directory user accounts and Active Directory groups in One Identity Manager	32
Undo deprovisioning	33
Restoring deleted objects	34
Appendix: Default project template for Active Roles	35
About us	37
Contacting us	37

Technical support resources	37
Index	38

integration with Active Roles

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 a One Identity Active Roles server, refer to the *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

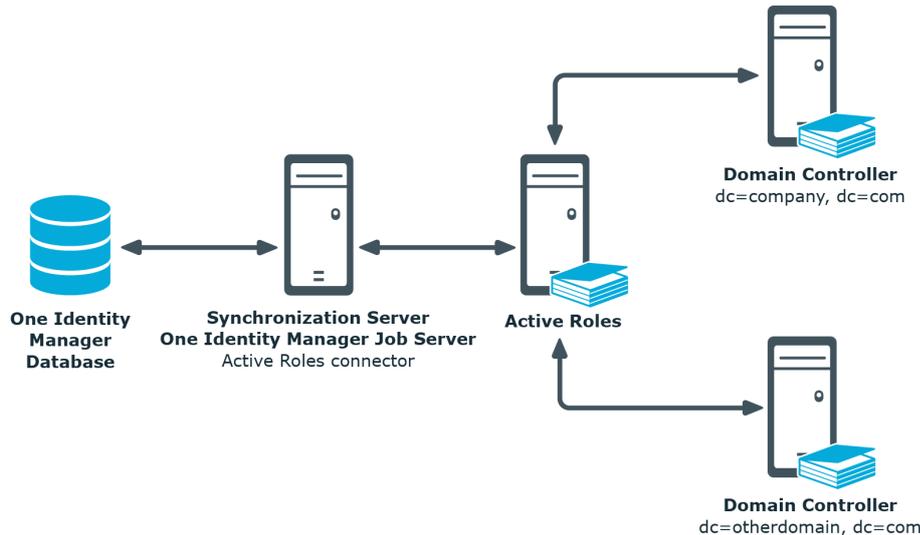
The following servers are used for managing an Active Directory environment with One Identity Manager and Active Roles:

- 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 of the One Identity Manager Service with Active Roles. The One Identity Manager Service is installed on this server with the Active Roles connector. 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 One Identity Manager Active Roles 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: Architecture for synchronization



Migrating Data between One Identity Manager and Active Roles

Scenario

An Active Roles domain managed by Active Directory should be managed 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 done with the Active Roles connector. All other synchronizations are also done with the Active Roles connector.

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

Scenario

An Active Roles domain managed by Active Directory should be managed with One Identity Manager. Active Roles Self-Service Manager is implemented. The functionality should be transferred to the One Identity Manager 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

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

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

Active Directory domain synchronization with One Identity Manager must be done with the Active Roles connector. All other synchronizations are also done with the Active Roles connector.

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

Scenario

An Active Directory domain managed by the Active Roles should be managed with One Identity Manager. Active Directory domain synchronization was done with the Active Directory connector until now.

To manage the Active Directory domains with One Identity Active Roles

1. Delete the existing synchronization project in the Synchronization Editor.
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 24

Configuring synchronization with Active Directory using One Identity Active Roles

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

To load objects from an Active Directory environment 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.
 - Check whether the configuration parameter is set in the Designer. 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 Active Roles Self-Service Manager functionality into One Identity Manager's IT Shop is directly supported in the One Identity ManagerActive Directory Edition. If you are using the One Identity Manager Edition, run the following steps before initial synchronization:
 - a. Enable the **QER | ITShop | GroupAutoPublish** configuration parameter in Designer.
 - b. Enable the **QER | ITShop | GroupAutoPublish | ADSGroupExcludeList** configuration parameter in Designer and specify the Active Directory groups that are not to be added automatically to IT Shop.
 - c. Enable 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 rights 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 24

One Identity Manager Service access rights 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 the Active Roles access template 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 19

Setting up the synchronization server

To set up synchronization with an Active Directory environment, a server must be available on which the following software is installed:

- Windows Operating system

Following versions are supported:

- Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
 - Windows Server 2008 R2 (non-Itanium based 64-bit) Service Pack 1 or later
- 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 **Select installation modules with existing database.**
 2. Select the machine role **Server | Job server | Active Directory.**

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:

- Setting up a Job server.
- Specifying machine roles and server function for the Job server.
- Remote installation of One Identity Manager Service components corresponding to the machine roles.

- Configuration of One Identity Manager Service.
- Starts the One Identity Manager Service.

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.

For remote installation of One Identity Manager Service, you require 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 install and configure One Identity Manager Service remotely 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.

Table 1: Job server properties

Property	Description
Server	Job server name.
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. Example: <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 Designer.

4. Select **Active Directory** on the **Machine roles** page.
5. Select **Active Roles connector** on the **Server functions** page.

6. Check the One Identity Manager Service configuration on the **Service settings** page.

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*.

7. To configure remote installations, click **Next**.

8. Confirm the security prompt with **Yes**.

9. Select the directory with the install files on **Select installation source**.

10. Select the file with the private key on the page **Select private key file**.

NOTE: This page is only displayed when the database is encrypted.

11. Enter the service's installation data on the **Service access** page.

Table 2: Installation data

Data	Description
Computer	Server on which to install and start the service from. To select a server <ul style="list-style-type: none">• Enter a name for the server.- OR -• Select a entry from the list.
Service account	User account data for the One Identity Manager Service. To enter a user account for the One Identity Manager Service <ul style="list-style-type: none">• Enter user account, password and password confirmation.
Installation account	Data for the administrative user account to install the service. To enter an administrative user account for installation <ul style="list-style-type: none">• Enable Advanced.• Enable Current user. This uses the user account of the current user.- OR -• Enter user account, password and password confirmation.

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 Server Installer.

NOTE: The service is entered with the name **One Identity Manager Service** in the server service management.

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. 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 3: 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 rights 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 server with the Active Roles connector. The synchronization server must be declared as a Job server in One Identity Manager. Use the following properties when you set up the Job

Data	Explanation
	server.

Table 4: Additional properties for the Job server

Property	Value
Server function	Active Roles connector
Machine role	Server/Jobserver/Active Directory

For more information, see [Setting up the synchronization server](#) on page 10.

One Identity Manager database connection data	<ul style="list-style-type: none"> • 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.
---	--

Remote connection server	<p>To configure synchronization with a target system, One Identity Manager must load the data from the target system. One Identity Manager communicates directly with 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 to the workstation is not possible, you can set up a remote connection.</p> <p>The remote connection server and the workstation must be in the same Active Directory domain.</p> <p>Remote connection server configuration:</p> <ul style="list-style-type: none"> • One Identity Manager Service is started • RemoteConnectPlugin is installed • Active Roles connector is installed <p>The remote connection server must be declared as a Job server in One Identity Manager. The Job server name is required.</p>
--------------------------	---

TIP: The remote connection server requires the same configuration as the synchronization server (with regard to the installed software 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. Select **Active Roles** connector on the **Choose target system** page.
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. Enter the user account and password on the **Credentials** page for accessing Active Roles.
8. Select the domain you want to synchronize on the **Domain/root entry selection** page 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 5: Specify target system access

Option	Meaning
Read-only access to target system.	<p>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.</p> <p>The synchronization workflow has the following characteristics:</p> <ul style="list-style-type: none">• 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.	<p>Specifies whether a provisioning workflow is to be set up in addition to the synchronization workflow for the initial loading of the target system.</p> <p>The provisioning workflow displays the following characteristics:</p> <ul style="list-style-type: none">• 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. Select the synchronization server to execute synchronization on the **Synchronization server** page.

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 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 under **Configuration | Variables** in Synchronization Editor.

To configure the content of the synchronization log

1. Open the synchronization project in the Synchronization Editor.
2. To configure the synchronization log for target system connection, select the category **Configuration | Target system**.
3. To configure the synchronization log for the database connection, select **Configuration | One Identity Manager connection**.
4. Select the **General** view and click **Configure**.
5. Select the **Synchronization log** view and set **Create synchronization log**.
6. Enable the data to be logged.

 **NOTE:** Some content generates a particularly large volume of log data. The synchronization log should only contain data required for troubleshooting and other analyses.

7. Click **OK**.

To synchronize on a regular basis

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Start up configurations**.
3. Select a start up configuration in the document view and click **Edit schedule**.
4. Edit the schedule properties.

5. To enable the schedule, click **Activate**.
6. Click **OK**.

To start initial synchronization manually

1. Open the synchronization project in the Synchronization Editor.
2. Select the category **Configuration | Start up configurations**.
3. Select a start up configuration in the document view and click **Execute**.
4. Confirm the security prompt with **Yes**.

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 Manager, select **Active Directory | User accounts | Linked but not configured | <Domain>**.
- OR -
In Manager, select **Active Directory | Contacts | Linked but not configured | <Domain>**.
 - b. Select **Assign account definition to linked accounts**.

Related topics

- [Setting up the synchronization server on page 10](#)
- [One Identity Manager Service access rights required for synchronizing using Active Roles on page 9](#)
- [Appendix: Default project template for Active Roles on page 35](#)

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 Active Roles connector integrated in One Identity Manager 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 6: 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

User Account Member of the Active Roles Administrators?	Option <Execute Active Roles workflows> Set?	Operation Linked with Active Roles Workflows?	Result
			executed immediately.
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 the use of Active Roles workflows](#) on page 20
- [Operation ID and status](#) on page 22
- [Additional virtual properties in the schema](#) on page 22
- [One Identity Manager Service access rights required for synchronizing using Active Roles](#) on page 9

Extensions for the use of Active Roles workflows

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

To edit master data for an Active Directory domain

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

Table 7: Extended properties for applying Active Roles workflows

Property	Description
Execute Active Roles workflows	<p>Specifies whether Active Roles workflows should be executed. For more information about Active Roles workflows, refer to your One Identity Active Roles documentation.</p> <p>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 in order to use this functionality.</p> <p>If this option is not set, One Identity Manager works without input from Active Roles workflows (default configuration). Default behavior requires an administrative account.</p> <p>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.</p>
User accounts deleted by Active Roles workflows	Specifies whether user accounts above deprovisioning workflows are deleted in Active Roles.
Groups deleted by Active Roles workflowsGroups	Specifies whether groups are deleted in Active Roles through deprovisioning workflows.

4. Save the changes.

Related topics

- [One Identity Manager Service access rights required for synchronizing using Active Roles](#) on page 9
- [Interaction with Active Roles workflows](#) on page 19
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 29

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 8: 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.

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. See the documentation for managing Active Directory with One Identity Manager in the One Identity Manager Administration Guide for Connecting to Active Directory.

Detailed information about this topic

- [Adding Active Directory groups automatically to the IT Shop](#) on page 24
- [Creating new Active Directory groups through the Web Portal](#) on page 26
- [Active Roles specific extensions for Active Directory groups](#) on page 27
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 29
- [Restoring deprovisioned Active Directory user accounts and Active Directory groups in One Identity Manager](#) on page 32

Adding Active Directory groups automatically to the IT Shop

Table 9: 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 ADSSGroupExcludeList	<p>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.</p> <p>Example:</p> <pre>.*Administrator.* Exchange.* .*Admins .*Operators IIS_IUSRS</pre>
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 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 IT Shop

1. Enable the **QER | ITShop | GroupAutoPublish** configuration parameter in Designer.
2. Enable the **QER | ITShop | GroupAutoPublish | ADSSGroupExcludeList** configuration parameter in Designer and specify the Active Directory groups that are not to be added automatically to IT Shop.
3. Enable the **TargetSystem | ADS | ARS_SSM** configuration parameter in Designer
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 step 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 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 owner, 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 owner, 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

- [Creating new Active Directory groups through the Web Portal](#) on page 26
- [Active Roles specific extensions for Active Directory groups](#) on page 27
- One Identity Manager IT Shop Administration Guide

Creating new Active Directory groups through the Web Portal

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

To request a new Active Directory group

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

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

- An entry is created in the Active Directory for the One Identity Manager group.
- The Active Directory group is labeled with the option **Group is published to Self-Service Manager**.
- 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.

i **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 24
- [Active Roles specific extensions for Active Directory groups](#) on page 27
- 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 Manager, select **Active Directory | Groups**.
2. Select the group in the result list.

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

The following properties are displayed:

Table 10: 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.								
	<table border="1"> <thead> <tr> <th>Status</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>	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.
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 24](#)
- [Creating new Active Directory groups through the Web Portal on page 26](#)
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups on page 31](#)

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.

- ① **NOTE:** The deprovisioning policy configuration in Active Roles may conflict with the default One Identity Manager configuration. In this case, make the appropriated customizations, for example, to templates or processes.

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 29
- [Quick deprovisioning](#) on page 30
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 31
- [Restoring deprovisioned Active Directory user accounts and Active Directory groups in One Identity Manager](#) on page 32
- [Interaction with Active Roles policies](#) on page 23

Deprovisioning not deletion

To implement this method

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

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

Related topics

- [Extensions for the use of Active Roles workflows](#) on page 20
- [Quick deprovisioning](#)
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 31
- [Undo deprovisioning](#) on page 33
- [Restoring deleted objects](#) on page 34

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

To deprovision an Active Directory group

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

Related topics

- [Deprovisioning not deletion](#) on page 29
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 31
- [Undo deprovisioning](#) on page 33

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 11: 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.

Property	Description	
	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.	

To display master data for deprovisioning an Active Directory user account

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

To display master data for deprovisioning an Active Directory group

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

Related topics

- [Active Roles specific extensions for Active Directory groups](#) on page 27

Restoring deprovisioned Active Directory user accounts and Active Directory groups in 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:

- Undoing 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 Active Directory container and in the One Identity Manager 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

- [Undo deprovisioning](#) on page 33
- [Restoring deleted objects](#)
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 29

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

To undo Active Directory group deprovisioning

1. Select **Active Directory | Groups | Deprovisioned groups**.
2. Select the group in the result list.
3. Select **Undo deprovisioning**.
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 29

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

Related topics

- [Undo deprovisioning](#) on page 33
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 29

Appendix: 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 12: 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
organization	ADSContainer
organizationalUnit	ADSContainer
printQueue	ADSPrinter

Schema type in Active Roles	Table in the One Identity Manager Schema
------------------------------------	---

rpcContainer	ADSContainer
--------------	--------------

user	ADSAccount
------	------------

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 or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

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

A

Active Directory domain

- deprovision group 29
- deprovision user account 29
- workflow 20

Active Directory group

- add to IT Shop (automatically) 24
- approval by owner 27
- create 26
- delete 29-30
- deprovision 29-30
- deprovisioning date 31
- deprovisioning status 27, 31
- master dataActive Directory group
 - deprovisioning date 27
- owner 27
- published 27
- request 26
- restore 32-34
- undo deprovisioning 32-34

Active Directory user account

- delete 29-30
- deprovision 29-30
- deprovisioning date 31
- deprovisioning status 31
- restore 32-34
- undo deprovisioning 32-34

Active Roles

- architecture 5
- connector 5
- deprovision 29

- deprovisioning date 31
- deprovisioning status 31
- policies 23
- schema 22
- synchronization server 10
- virtual properties 22
- workflow 19-20, 22

D

direction of synchronization

- to Manager 13
- to target system 13

P

- product owner 24
- project template 35

S

start synchronization 13

synchronization 8

- configure 13
- connection parameters 13
- rights 9
- synchronization project
 - create 13
- user account 9
- workflow 13

synchronization project

- create 13

- project template 35
- synchronization server
 - configuring 10
 - installing 10
 - Job server 10
- synchronization workflow
 - create 13