



One Identity Manager 8.2

Administration Guide for One Identity Active Roles Integration

Copyright 2021 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 highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

One Identity Manager Administration Guide for One Identity Active Roles Integration
Updated - 24 November 2021, 10:15
Version - 8.2

Contents

One Identity Active Roles integration	5
Architecture overview	5
Migrating data between One Identity Manager and One Identity Active Roles	6
Synchronizing Active Directory using One Identity Active Roles	9
Permissions required for synchronizing with One Identity Active Roles	10
Setting up the synchronization server	11
System requirements for the synchronization server	11
Installing One Identity Manager Service with an Active Roles connector	12
Creating a synchronization project for initial synchronization of an Active Directory domain through One Identity Active Roles	15
Information required for setting up a synchronization project	16
Creating an initial synchronization project for Active Directory domains	17
Customizing the synchronization configuration	20
Accelerating provisioning and single object synchronization	21
Running synchronization	22
Starting synchronization	22
Deactivating synchronization	23
Displaying synchronization results	24
Tasks following synchronization	25
Post-processing outstanding objects	25
Adding custom tables to the target system synchronization	27
Managing Active Directory user accounts and Active Directory contacts through account definitions	28
Troubleshooting	29
Ignoring data error in synchronization	29
Interaction with Active Roles workflows	31
Extensions for applying Active Roles workflows	32
Operation ID and status	33
Additional virtual properties in the schema	34
Interaction with Active Roles policies	35

Managing Active Directory objects	36
Adding Active Directory groups automatically to the IT Shop	36
Requesting Active Directory groups through the Web Portal	38
Active Roles specific extensions for Active Directory groups	39
Deprovisioning Active Directory user account and Active Directory groups	40
Deprovisioning not deletion	41
Quick deprovisioning	42
Displaying information about deprovisioning Active Directory user accounts and Active Directory groups	43
Restoring deprovisioned Active Directory user accounts and Active Directory groups in the One Identity Manager	44
Deprovisioning Active Directory user accounts and Active Directory groups	45
Restoring deleted objects	45
Appendix: Configuration parameters for managing an Active Directory environment	47
Appendix: Default project template for One Identity Active Roles	53
Appendix: Active Roles connector settings	54
About us	56
Contacting us	56
Technical support resources	56
Index	57

One Identity 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 primary system 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: The Active Directory Module and the Active Roles Module must be installed as a prerequisite for managing Active Directory in One Identity Manager. For more information about installing, see the *One Identity Manager Installation Guide*.

NOTE: This guide only goes into specific features of using the Active Roles Connector. For more information about managing Active Directory with One Identity Manager, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.

For more information about applying, managing, and configuring an Active Roles server, see your *One Identity Active Roles* documentation.

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.

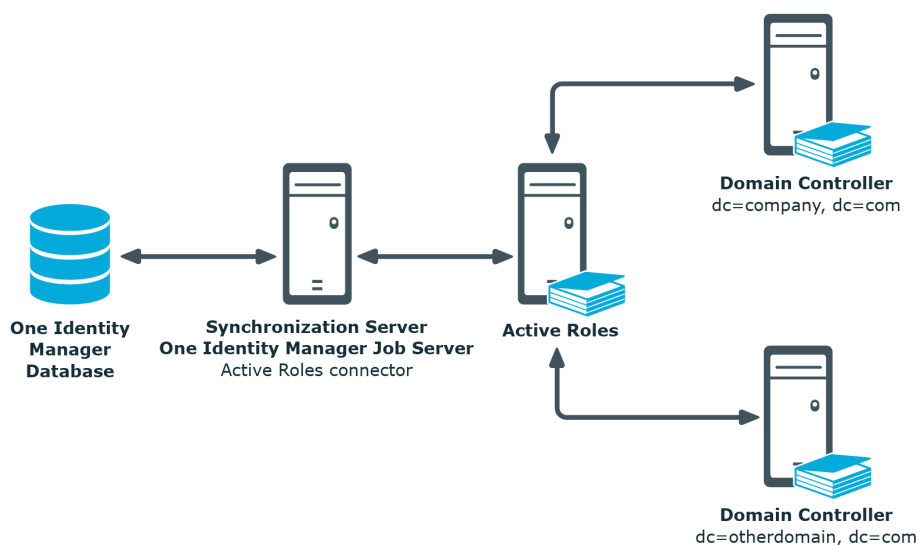
- Synchronization server

Communication of the One Identity Manager Service with Active Roles is run from the synchronization server. 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 One Identity Manager's 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: The synchronization architecture



Migrating data between One Identity Manager and One Identity 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 transferring Active Roles Self-Service Manager functionality to the IT Shop One Identity Manager.

If you are using the **One Identity Manager Edition**, run the following steps before initial synchronization:

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.

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

- [Synchronizing Active Directory using One Identity Active Roles](#) on page 9
- [Adding Active Directory groups automatically to the IT Shop](#) on page 36

Synchronizing Active Directory using One Identity Active Roles

One Identity Manager supports synchronization with Active Roles versions 7.4.1, 7.4.3, 7.4.4. and 7.4.5.

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

1. Prepare a user account with sufficient permissions for synchronization.
2. One Identity Manager components for managing Active Directory environments are available if the **TargetSystem | ADS** configuration parameter is enabled. The components for managing Active Roles are available if the **TargetSystem | ADS | ARS** configuration parameter is set.
 - Check whether the configuration parameters are set in the Designer. Otherwise, set the configuration parameters and compile the database.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.
 - Other configuration parameters are installed when the modules are 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 a Job server in One Identity Manager.
4. In the **One Identity Manager Active Directory Edition** there is direct support for transferring Active Roles Self-Service Manager functionality to the One Identity Manager IT Shop.

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.

NOTE: If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the *One Identity Manager Configuration Guide*.

- b. In the Designer, set the **QER | ITShop | GroupAutoPublish | ADSSGroupExcludeList** configuration parameter and specify the Active Directory groups that are not to be added automatically to the IT Shop.

Example:

```
. *Administrator.* | Exchange.* | *. *Admins | *. *Operators | IIS_IUSRS
```

- 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.

TIP: Before you set up synchronization with an Active Directory domain, familiarize yourself with the Synchronization Editor. For more information about this tool, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Migrating data between One Identity Manager and One Identity Active Roles](#) on page 6
- [Permissions required for synchronizing with One Identity Active Roles](#) on page 10
- [Setting up the synchronization server](#) on page 11
- [Creating a synchronization project for initial synchronization of an Active Directory domain through One Identity Active Roles](#) on page 15
- [Running synchronization](#) on page 22
- [Customizing the synchronization configuration](#) on page 20
- [Tasks following synchronization](#) on page 25
- [Troubleshooting](#) on page 29
- [Adding Active Directory groups automatically to the IT Shop](#) on page 36
- [Configuration parameters for managing an Active Directory environment](#) on page 47

Permissions required for synchronizing with One Identity Active Roles

It is recommended to set up a separate user account to use for connecting to Active Directory through for Active Roles. 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. For more information about Active Roles Access Templates, see your *One Identity Active Roles documentation*.

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 any existing Active Roles workflows, you must add the user account to the **Active Roles administrators** group.

Edit the Active Roles admins in the Active Roles Configuration Center. If a user account is entered in the Active Roles Configuration Center as an Active Roles Admin, this is the user account that must be used. For more information about editing the group or the user account for administrative access, see your *One Identity Active Roles documentation*.

Related topics

- [Interaction with Active Roles workflows](#) on page 31

Setting up the synchronization server

All One Identity Manager Service actions are run 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 with the Active Roles connector must be installed on the synchronization server.

Detailed information about this topic

- [System requirements for the synchronization server](#) on page 11
- [Installing One Identity Manager Service with an Active Roles connector](#) on page 12

System requirements for 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 2022
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
 - Microsoft .NET Framework Version 4.7.2 or later
- | **NOTE:** Take the target system manufacturer's recommendations into account.
- One Identity Active Roles Management Shell for Active Directory (x64)
- On 32-bit operating systems, use the Active Roles Management Shell for Active Directory (x86) package.
- For installation instructions, refer to your *One Identity Active Roles documentation*.
- The following packages must be subsequently installed from the Active Roles installation medium:
- On 32-bit systems:
- <source>\Redistributables\vc_redist.x86.exe
 - <source>\Components\ActiveRoles ADSI Provider\ADSI_x86.msi
- On 64-bit systems:
- <source>\Redistributables\vc_redist.x64.exe
 - <source>\Components\ActiveRoles ADSI Provider\ADSI_x64.msi

Furthermore, it is necessary that connections can be established from the Job server to the Active Roles server over the **15172** port. If necessary, a firewall rule must be set up on the Active Roles server.

Installing One Identity Manager Service with an Active Roles connector

| **NOTE:** For existing Active Roles installations:

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

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.

Table 1: Properties of the Job server

Property	Value
Server function	Active Roles connector
Machine role	Server Job server Active Directory

NOTE: If several target system environments of the same type are synchronized under the same synchronization server, it is recommended that you set up a Job server for each target system for performance reasons. This avoids unnecessary swapping of connections to target systems because a Job server only has to process tasks of the same type (re-use of existing connections).

Use the One Identity Manager Service to install the Server Installer. The program runs 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: The program performs a remote installation of the One Identity Manager Service. Local installation of the service is not possible with this program.

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*.

NOTE: To generate processes for the Job server, you need the provider, connection parameters, and the authentication data. By default, 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*.

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

1. Start the Server Installer program on your administrative workstation.
2. On the **Database connection** page, enter the valid connection credentials for the One Identity Manager database.
3. On the **Server properties** page, specify the server on which you want to install the One Identity Manager Service.
 - 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 Job server within the network must have a unique queue identifier. The process steps are requested by the Job queue using this exact 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. 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:
 1. Select **Process collection > sqlprovider**.
 2. Click the **Connection parameter** entry, then click the **Edit** button.
 3. Enter the connection data for the One Identity Manager database.
 - For a connection to the application server:
 1. Select **Process collection**, click the **Insert** button and select **AppServerJobProvider**.
 2. Click the **Connection parameter** entry, then click the **Edit** button.
 3. Enter the connection data for the application server.
 4. Click the **Authentication data** entry and click the **Edit** button.
 5. Select the authentication module. Depending on the authentication module, other data may be required, such as user and password. For detailed information about 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. Change the directory if necessary.
 10. If the database is encrypted, on the **Select private key file** page, select the file with the private key.
 11. On the **Service access** page, enter the service's installation data.
 - **Computer:** Enter the name or IP address of the server that the service is installed and started on.

- **Service account:** Enter the details of the user account that the One Identity Manager Service is running under. Enter the user account, the user account's password and password confirmation.

The service is installed using the user account with which you are logged in to the administrative workstation. If you want to use another user account for installing the service, you can enter it in the advanced options. You can also change the One Identity Manager Service details, such as the installation directory, name, display name, and the One Identity Manager Service description, using the advanced 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 One Identity Active Roles

Use the 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. For more information about setting up synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

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.

Related topics

- [Information required for setting up a synchronization project](#) on page 16
- [Creating an initial synchronization project for Active Directory domains](#) on page 17

Information required for setting up a synchronization project

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

Table 2: Information required for setting up a synchronization project

Data	Explanation
Distinguished name of the domain.	Distinguished LDAP domain name
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. For more information, see Permissions required for synchronizing with One Identity Active Roles on page 10.
DNS name or IP address of the Active Roles server.	DNS name or IP address of the Active Roles server that connects against the synchronization server. Example: <Name of servers>.<Fully qualified domain name>
Synchronization server for Active Directory	All One Identity Manager Service actions are run 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 server. <ul style="list-style-type: none">• Server function: Active Roles connector• Machine role: Server Jobserver Active Directory For more information, see System requirements for the synchronization server on page 11.
One Identity Manager database connection data	<ul style="list-style-type: none">• Database server• Database name• SQL Server login and password• Specifies whether integrated Windows authentication is used Use of the integrated Windows authentication is not recommended. If you decide to use it anyway, ensure that your environment supports Windows authentication.

Data	Explanation
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 the target system to do this. Sometimes direct access from the workstation, on which the Synchronization Editor is installed, is not possible. For example, because of the firewall configuration or 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.</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> <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.</p> <p>For more detailed information about setting up a remote connection, see the <i>One Identity Manager Target System Synchronization Reference Guide</i>.</p>

Creating an initial synchronization project for Active Directory domains

NOTE: The following sequence describes how to configure a synchronization project if the Synchronization Editor is both:

- Run in default mode
- Started from the Launchpad

If you run the project wizard in expert mode or directly from the Synchronization Editor, additional configuration settings can be made. 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 the **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 the Synchronization Editor, do not change any settings.
 - If access is not possible from the workstation on which you started the 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. If possible, servers are determined automatically.
 - In the **Host name/IP address** menu, select a target server.
 - If the server cannot be found automatically, in the **Host name/IP address** field, enter the DNS name or the IP address.
 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, specify how system access should work. You have the following options:

Table 3: Specify target system access

Option	Meaning
	<p>Specifies that 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 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. On the **Synchronization server** page, select the synchronization server to run the 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.

- d. **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.

This sets up, saves and immediately activates the synchronization project.

NOTE:

- If enabled, a consistency check is carried out. If errors occur, a message appears. You can decide 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**.
- 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.
- The connection data for the target system is saved in a variable set and can be modified in the Synchronization Editor in the **Configuration > Variables** category.

Related topics

- [Information required for setting up a synchronization project](#) on page 16
- [Permissions required for synchronizing with One Identity Active Roles](#) on page 10
- [System requirements for the synchronization server](#) on page 11
- [Default project template for One Identity Active Roles](#) on page 53

Customizing the synchronization configuration

For more information about customizing synchronization for an Active Directory environment, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.

Having used the Synchronization Editor to set up a synchronization project for initial synchronization of a Active Directory domain, you can use the synchronization project to load Active Directory objects into the One Identity Manager database. If you manage user accounts and their authorizations with One Identity Manager, changes are provisioned in the Active Directory environment.

You must customize the synchronization configuration to be able to regularly compare the database with the Active Directory environment and to synchronize changes.

- To use One Identity Manager as the primary system during synchronization, create a workflow with synchronization in the direction of the **Target system**.
- You can use variables to create generally applicable synchronization configurations that contain the necessary information about the synchronization objects when

synchronization starts. Variables can be implemented in base objects, schema classes, or processing methods, for example.

- Use variables to set up a synchronization project for synchronizing different domains. Store a connection parameter as a variable for logging in to the domain.
- To specify which Active Directory objects and database objects are included in synchronization, edit the scope of the target system connection and the One Identity Manager database connection. To prevent data inconsistencies, define the same scope in both systems. If no scope is defined, all objects will be synchronized.
- Update the schema in the synchronization project if the One Identity Manager schema or target system schema has changed. Then you can add the changes to the mapping.
- To synchronize additional schema properties, update the schema in the synchronization project. Include the schema extensions in the mapping.

For more information about configuring synchronization, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [Accelerating provisioning and single object synchronization](#) on page 21

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 no longer required, ensure that the synchronization server runs the provisioning processes and single object synchronization.

To configure load balancing

1. Configure the server and declare it as a Job server in One Identity Manager.
 - Job servers that share processing must have the **No process assignment** option enabled.
 - 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.

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*.

Running synchronization

Synchronization is started using scheduled process plans. It is possible to start synchronization manually in the Synchronization Editor. You can simulate synchronization beforehand to estimate synchronization results and discover errors in the synchronization configuration. If synchronization stopped unexpectedly, you must reset the start information to be able to restart synchronization.

If you want to specify the order in which target systems are synchronized, use the start up sequence to run synchronization. In a start up sequence, you can combine start up configurations from different synchronization projects and specify the order in which they are run. For more information about start up sequences, see the *One Identity Manager Target System Synchronization Reference Guide*.

Detailed information about this topic

- [Starting synchronization](#) on page 22
- [Deactivating synchronization](#) on page 23
- [Displaying synchronization results](#) on page 24

Starting synchronization

When you set up the initial synchronization project using the Launchpad, a default schedule for regular synchronization is created and assigned. Activate this schedule to synchronize

on a regular basis.

To synchronize on a regular basis

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
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**.

You can also start synchronization manually if there is no active schedule.

To start initial synchronization manually

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > Start up configurations** category.
3. Select a start up configuration in the document view and click **Run**.
4. Confirm the security prompt with **Yes**.

IMPORTANT: As long as a synchronization process is running, you must not start another synchronization process for the same target system. This especially applies, if the same synchronization objects would be processed.

- If another synchronization process is started with the same start up configuration, the process is stopped and is assigned **Frozen** status. An error message is written to the One Identity Manager Service log file.
 - Ensure that start up configurations that are used in start up sequences are not started individually at the same time. Assign start up sequences and start up configurations different schedules.
- Starting another synchronization process with different start up configuration that addresses same target system may lead to synchronization errors or loss of data. Specify One Identity Manager behavior in this case, in the start up configuration.
 - Use the schedule to ensure that the start up configurations are run in sequence.
 - Group start up configurations with the same start up behavior.

Deactivating synchronization

Regular synchronization cannot be started until the synchronization project and the schedule are active.

To prevent regular synchronization

1. In the Synchronization Editor, open the synchronization project.
2. Select the start up configuration and deactivate the configured schedule.

Now you can only start synchronization manually.

An activated synchronization project can only be edited to a limited extent. The schema in the synchronization project must be updated if schema modifications are required. The synchronization project is deactivated in this case and can be edited again.

Furthermore, the synchronization project must be deactivated if synchronization should not be started by any means (not even manually).

To deactivate the synchronization project

1. In the Synchronization Editor, open the synchronization project.
2. Select the **General** view on the home page.
3. Click **Deactivate project**.

Related topics

- [Creating a synchronization project for initial synchronization of an Active Directory domain through One Identity Active Roles](#) on page 15

Displaying synchronization results

Synchronization results are summarized in the synchronization log. You can specify the extent of the synchronization log for each system connection individually. One Identity Manager provides several reports in which the synchronization results are organized under different criteria.

To display a synchronization log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ► in the navigation view toolbar.
Logs for all completed synchronization runs are displayed in the navigation view.
4. Select a log by double-clicking it.
An analysis of the synchronization is shown as a report. You can save the report.

To display a provisioning log

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Logs** category.
3. Click ⚡ in the navigation view toolbar.

Logs for all completed provisioning processes are displayed in the navigation view.

4. Select a log by double-clicking it.

An analysis of the provisioning is shown as a report. You can save the report.

The log is marked in color in the navigation view. This mark shows you the status of the synchronization/provisioning.

TIP: The logs are also displayed in the Manager under the **<target system> > synchronization log** category.

Synchronization logs are stored for a fixed length of time.

To modify the retention period for synchronization logs

- In the Designer, enable the **DPR | Journal | LifeTime** configuration parameter and enter the maximum retention period.

Tasks following synchronization

After the synchronization of data from the target system into the One Identity Manager database, rework may be necessary. Check the following tasks:

- [Post-processing outstanding objects](#) on page 25
- [Adding custom tables to the target system synchronization](#) on page 27
- [Managing Active Directory user accounts and Active Directory contacts through account definitions](#) on page 28

Post-processing outstanding objects

Objects, which do not exist in the target system, can be marked as outstanding in One Identity Manager by synchronizing. This prevents objects being deleted because of an incorrect data situation or an incorrect synchronization configuration.

Outstanding objects:

- Cannot be edited in One Identity Manager.
- Are ignored by subsequent synchronizations.
- Are ignored by inheritance calculations.

This means, all memberships and assignments remain intact until the outstanding objects have been processed.

Start target system synchronization to do this.

To post-process outstanding objects

1. In the Manager, select the **Active Directory > Target system synchronization: Active Directory** category.

The navigation view lists all the synchronization tables assigned to the **Active Directory** target system type.

2. On the **Target system synchronization** form, in the **Table / object** column, open the node of the table for which you want to post-process outstanding objects.

All objects that are marked as outstanding are shown. The **Last log entry** and **Last method run** columns display the time at which the last entry was made in the synchronization log and which processing method was run. The **No log available** entry can mean the following:



- The synchronization log has already been deleted.
- OR -
- An assignment from a member list has been deleted from the target system.
The base object of the assignment was updated during the synchronization. A corresponding entry appears in the synchronization log. The entry in the assignment table is marked as outstanding, but there is no entry in the synchronization log.
- An object that contains a member list has been deleted from the target system.
During synchronization, the object and all corresponding entries in the assignment tables are marked as outstanding. However, an entry in the synchronization log appears only for the deleted object.


TIP:

To display object properties of an outstanding object

1. Select the object on the target system synchronization form.
 2. Open the context menu and click **Show object**.
3. Select the objects you want to rework. Multi-select is possible.
 4. Click on one of the following icons in the form toolbar to run the respective method.

Table 4: Methods for handling outstanding objects

Icon	Method	Description
	Delete	The object is immediately deleted from the One Identity Manager database. Deferred deletion is not taken into account. The Outstanding label is removed from the object. Indirect memberships cannot be deleted.
	Publish	The object is added to the target system. The Outstanding label is removed from the object.

Icon	Method	Description
		<p>This runs a target system specific process that triggers the provisioning process for the object.</p> <p>Prerequisites:</p> <ul style="list-style-type: none"> • The table containing the object can be published. • The target system connector has write access to the target system.
	Reset	The Outstanding label is removed for the object.

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

NOTE: By default, the selected objects are processed in parallel, which speeds up the selected method. If an error occurs during processing, the action is stopped and all changes are discarded.

Bulk processing of objects must be disabled if errors are to be localized, which means the objects are processed sequentially. Failed objects are named in the error message. All changes that were made up until the error occurred are saved.

To disable bulk processing

- Disable the  icon in the form's toolbar.

NOTE: The target system connector must have write access to the target system in order to publish outstanding objects that are being post-processed. That means, the **Connection is read-only** option must not be set for the target system connection.

Adding custom tables to the target system synchronization

You must customize your target system synchronization to synchronize custom tables.

To add custom tables to target system synchronization

1. In the Manager, select the **Active Directory > Basic configuration data > Target system types** category.
2. In the result list, select the **Active Directory** target system type.
3. Select the **Assign synchronization tables** task.
4. In the Add assignments pane, assign **custom** tables to the outstanding objects you want to handle.
5. Save the changes.
6. Select the **Configure tables for publishing** task.

7. Select the custom tables that contain the outstanding objects that can be published in the target system and set the **Publishable** option.
8. Save the changes.

Related topics

- [Post-processing outstanding objects](#) on page 25

Managing Active Directory user accounts and Active Directory contacts through account definitions

In the default installation, after synchronizing, employees are automatically created for user accounts and contacts. If an account definition for the domain is not known at the time of synchronization, user accounts and contacts are linked to employees. However, account definitions are not assigned. The user accounts and contacts are therefore in a **Linked** state.

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

To manage user accounts and contacts through account definitions

1. Create an account definition.
2. Assign an account definition to the domain.
3. Assign a user account in the **Linked** state to the account definition. The account definition's default manage level is applied to the user account.
 - 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.
 - c. In the **Account definition** menu, select the account definition.
 - d. Select the user accounts that contain the account definition.
 - e. Save the changes.

For detailed information about account definitions for Active Directory user accounts and contacts, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.

Troubleshooting

Synchronization Editor helps you to analyze and eliminate synchronization errors.

- **Simulating synchronization**
The simulation allows you to estimate the result of synchronization. This means you can, for example, recognize potential errors in the synchronization configuration.
- **Analyzing synchronization**
You can generate the synchronization analysis report for analyzing problems which occur during synchronization, for example, insufficient performance.
- **Logging messages**
One Identity Manager offers different options for logging errors. These include the synchronization log, the log file for One Identity Manager Service, the logging of messages with NLOG, and similar.
- **Reset start information**
If synchronization stopped unexpectedly, for example, because a server was not available, the start information must be reset manually. Only then can the synchronization be restarted.

For more information about these topics, see the *One Identity Manager Target System Synchronization Reference Guide*.

Related topics

- [Displaying synchronization results](#) on page 24

Ignoring data error in synchronization

By default, objects with incorrect data are not synchronized. These objects can be synchronized once the data has been corrected. In certain situations, however, it might be necessary to synchronize objects like these and ignore the data properties that have errors. This synchronization behavior can be configured in One Identity Manager.

To ignoring data errors during synchronization in One Identity Manager

1. In the Synchronization Editor, open the synchronization project.
2. Select the **Configuration > One Identity Manager connection** category.
3. In the **General** view, click **Edit connection**.
This starts the system connection wizard.
4. On the **Additional options** page, enable **Try to ignore data errors**.

This option is only effective if **Continue on error** is set in the synchronization workflow.

Default columns, such as primary keys, UID columns, or mandatory input columns cannot be ignored.

5. Save the changes.

IMPORTANT: If this option is set, One Identity Manager tries to ignore commit errors that could be related to data errors in a single column. This causes the data changed in the affected column to be discarded and the object is subsequently saved again. This effects performance and leads to loss of data.

Only set this option in the exceptional circumstance of not being able to correct the data before synchronization.

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.

If the Active Roles connector is supposed to trigger workflows, you may have to customize processes so that they wait for the workflows to run and the changes to be made in Active Directory. This is necessary because the One Identity Manager processes defined in the Active Directory are run 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, see your *One Identity Active Roles documentation*.

The following table show the correlation.

Table 5: Correlation to Active Roles workflow control

User Account Member of the Active Roles Administrators?	Option "Run Active Roles workflows" set?	Operation Linked with Active Roles Workflows?	Result
Yes	Yes	No	The operation is run immediately.
Yes	No	No	The operation is run

User Account Member of the Active Roles Administrators?	Option "Run Active Roles workflows" set?	Operation Linked with Active Roles Workflows?	Result
			immediately.
Yes	Yes	Yes	The operation is run immediately without input from workflows.
Yes	No	Yes	The operation is run immediately without input from workflows.
No	Yes	No	The operation is run immediately.
No	No	No	The operation is run immediately.
No	Yes	Yes	The Operation triggers workflows and depends on the final status.
No	No	Yes	The operation quits with an error message.

Related topics

- [Extensions for applying Active Roles workflows](#) on page 32
- [Operation ID and status](#) on page 33
- [Additional virtual properties in the schema](#) on page 34
- [Permissions required for synchronizing with One Identity Active Roles](#) on page 10

Extensions for applying Active Roles workflows

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

To edit main data of an Active Directory domain

1. In the Manager, select the **Active Directory > Domains** category.
2. Select the domain in the result list and run the **Change main data** task.

3. On the **Active Roles** tab, enter the following data for utilizing workflows.

Table 6: Extended properties for applying Active Roles workflows

Property	Description
Run Active Roles workflows	<p>Specifies whether to run Active Roles workflows. For more information about Active Roles workflows, see your <i>One Identity Active Roles documentation</i>.</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 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	<p>Specifies whether user accounts are deleted in Active Roles through deprovisioning workflows.</p>
Groups deleted by Active Roles workflows	<p>Specifies whether groups are deleted in Active Roles through deprovisioning workflows.</p>

4. Save the changes.

Related topics

- [Permissions required for synchronizing with One Identity Active Roles](#) on page 10
- [Interaction with Active Roles workflows](#) on page 31
- [Deprovisioning Active Directory user account and Active Directory groups](#) on page 40

Operation ID and status

The ID found by the Active Roles connector is returned in the LastOperationID output parameter of each change operation in Active Directory. 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 run.

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 runs 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 7: Virtual properties for the Active Roles connector

Property	Description
<code>vrtLastOperationID</code>	ID of the last operation in Active Roles.
<code>vrtLastOperationStatus</code>	Status 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.

For more information about Active Roles policies, see your *One Identity Active Roles documentation*.

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 more information about managing Active Directory with One Identity Manager, see 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 36
- [Requesting Active Directory groups through the Web Portal](#) on page 38
- [Active Roles specific extensions for Active Directory groups](#) on page 39
- [Deprovisioning Active Directory user account and Active Directory groups](#) on page 40
- [Restoring deprovisioned Active Directory user accounts and Active Directory groups in the One Identity Manager](#) on page 44

Adding Active Directory groups automatically to the IT Shop

In the **One Identity Manager Active Directory Edition** there is direct support for transferring Active Roles Self-Service Manager functionality to the One Identity Manager IT Shop.

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 | ADSSGroupExcludeList** configuration parameter and specify the Active Directory groups that are not to be added automatically to the IT Shop.

Example:

```
. *Administrator.* | Exchange.* | *. *Admins | *. *Operators | IIS_IUSRS
```

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 Active Directory groups through the Web Portal](#) on page 38
- [Active Roles specific extensions for Active Directory groups](#) on page 39

Requesting Active Directory groups through 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 run 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 **Identity & Access Lifecycle** default shop.

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 36
- [Active Roles specific extensions for Active Directory groups](#) on page 39

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 main 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.
Dynamic group	Specifies whether members in this group are determined dynamically in Active Roles. You are not allowed to make manual changes to a dynamic group.

Property	Description
Additional owners	List of additional owners Active Directory groups or Active Directory user accounts are permitted.
Deprovisioning status	<p>Status of deprovisioning sequence through Active Roles when an object is deleted. The data is loaded from Active Roles on synchronization.</p> <ul style="list-style-type: none"> • No deprovisioning: The Active Directory object is active. • Deprovisioning successful: The Active Directory object was successfully deprovisioned. • Deprovisioning failed: An error occurred while 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 36
- [Requesting Active Directory groups through the Web Portal](#) on page 38
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 43

Deprovisioning Active Directory user account 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. For more information about Active Roles deprovisioning, see 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 41
- [Quick deprovisioning](#) on page 42
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 43
- [Restoring deprovisioned Active Directory user accounts and Active Directory groups in the One Identity Manager](#) on page 44
- [Interaction with Active Roles policies](#) on page 35

Deprovisioning not deletion

To implement this method

- In the Manager, on 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 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**.


NOTE: Active Directory user accounts and Active Directory groups that have the **Protected from accidental deletion** option set cannot be moved or deleted.

To delete a user account

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

To delete an Active Directory group

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

3. Click  in the result list.
4. Confirm the security prompt with **Yes**.

Related topics

- [Extensions for applying Active Roles workflows](#) on page 32
- [Quick deprovisioning](#) on page 42
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 43
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 45
- [Restoring deleted objects](#) on page 45

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**.

NOTE: Active Directory user accounts and Active Directory groups that have the **Protected from accidental deletion** option set cannot be moved or deleted.

To deprovision an Active Directory user account

1. In the Manager, 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. In the Manager, 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 41
- [Displaying information about deprovisioning Active Directory user accounts and Active Directory groups](#) on page 43
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 45

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. <ul style="list-style-type: none">• No deprovisioning: The Active Directory object is active.• Deprovisioning successful: The Active Directory object was successfully deprovisioned.• Deprovisioning failed: An error occurred while 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 main data of deprovisioning an Active Directory user account

1. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Select the **Change main data** task.
4. Select the **Active Roles** tab.

To display main data of deprovisioning an Active Directory group

1. In the Manager, select the **Active Directory > Groups** category.
2. Select the group in the result list.
3. Select the **Change main data** task.
4. Select the **Active Roles** tab.

Related topics

- [Active Roles specific extensions for Active Directory groups](#) on page 39

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 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 the status is changed to **published**.

Detailed information about this topic

- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 45
- [Restoring deleted objects](#)

- [Deprovisioning Active Directory user account and Active Directory groups](#) on page 40

Deprovisioning Active Directory user accounts and Active Directory groups

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. In the Manager, 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. In the Manager, select the **Active Directory > User accounts > 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](#) on page 45
- [Deprovisioning Active Directory user account and Active Directory groups](#) on page 40

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. In the Manager, select the **Active Directory > User accounts** category.
2. Select the user account in the result list.
3. Click  in the result list.

To restore a group

1. In the Manager, 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

- [Deprovisioning not deletion](#) on page 41
- [Deprovisioning Active Directory user account and Active Directory groups](#) on page 40
- [Deprovisioning Active Directory user accounts and Active Directory groups](#) on page 45

Configuration parameters for managing an Active Directory environment

The following configuration parameters are available in One Identity Manager after the Active Directory Module and the Active Roles Module have been installed.

Table 10: Configuration parameters

Configuration parameters	Description
QER ITShop GroupAutoPublish	<p>Preprocessor relevant configuration parameter for automatically adding groups to the IT Shop. Specifies whether all Active Directory target systems groups are automatically transferred to the IT Shop. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p>
QER ITShop GroupAutoPublish ADSGroupExcludeList	<p>List of all groups that are not be automatically assigned to the IT Shop. 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	<p>Preprocessor relevant configuration parameter for controlling the database model components for the administration of the Active Directory target system. If the parameter is set, the target system components are available. Changes to this parameter require the database to be recompiled.</p>

Configuration parameters	Description
	If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i> .
TargetSystem ADS Accounts	Allows configuration of user account data.
TargetSystem ADS Accounts InitialRandomPassword	Specifies whether a random password is generated when a new user account is added. The password must contain at least those character sets that are defined in the password policy.
TargetSystem ADS Accounts InitialRandomPassword SendTo	Employee to receive an email with the random generated password (manager cost center/department/location/business role, employee's manager or XUserInserted). If no recipient can be found, the password is sent to the address stored in the configuration parameter TargetSystem ADS DefaultAddress .
TargetSystem ADS Accounts InitialRandomPassword SendTo MailTemplateAccountName	Mail template name that is sent to supply users with the login credentials for the user account. The Employee - new user account created mail template is used.
TargetSystem ADS Accounts InitialRandomPassword SendTo MailTemplatePassword	Mail template name that is sent to supply users with the initial password. The Employee - initial password for new user account mail template is used.
TargetSystem ADS Accounts MailTemplateDefaultValues	Mail template used to send notifications about whether default IT operating data mapping values are used for automatically creating a user account. The Employee - new user account with default properties created mail template is used.
TargetSystem ADS Accounts NotRequirePassword	Specifies whether a password is required when creating new Active Directory user accounts in One Identity Manager. If the configuration parameter is not set, entry of a password that meets the defined password guidelines is requested when a new Active Directory user account is created. If the configuration parameter is set, it is not necessary to specify a password when creating new Active Directory user accounts.
TargetSystem ADS	Allows configuration of privileged Active Directory user account

Configuration parameters	Description
Accounts PrivilegedAccount	settings.
TargetSystem ADS Accounts PrivilegedAccount SAMAccountName_ Postfix	Postfix for formatting the login name of privileged user accounts.
TargetSystem ADS Accounts PrivilegedAccount SAMAccountName_ Prefix	Prefix for formatting a login name of privileged user accounts.
TargetSystem ADS Accounts ProfileFixedString	Fixed string appended to the default profile path of a user profile.
TargetSystem ADS Accounts TransferJPegPhoto	Specifies whether changes to the employee's picture are published in existing user accounts. The picture is not part of default synchronization. It is only published when employee data is changed.
TargetSystem ADS Accounts TransferSIDHistory	Specifies whether the SID history is loaded from the target system.
TargetSystem ADS Accounts TSProfileFixedString	Fixed string appended to the default profile path of a user profile on a terminal server.
TargetSystem ADS Accounts UnlockByCentralPassword	Specifies whether the employee's Active Directory user account is unlocked when the central password is synchronized.
TargetSystem ADS Accounts UserMustChangePassword	Specifies whether the Change password at next login option is enabled when a new user account is created.
TargetSystem ADS ARS	<p>Preprocessor relevant configuration parameter to control the database model components for Active Roles. If the parameter is set, Self-Service Management components are available. Changes to this parameter require the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date,</p>

Configuration parameters	Description
	model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i> .
TargetSystem ADS ARS_SSM	<p>Preprocessor relevant configuration parameter for controlling the database model components for One Identity 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 the database to be recompiled.</p> <p>If you disable the configuration parameter at a later date, model components and scripts that are not longer required, are disabled. SQL procedures and triggers are still carried out. For more information about the behavior of preprocessor relevant configuration parameters and conditional compiling, see the <i>One Identity Manager Configuration Guide</i>.</p>
TargetSystem ADS AuthenticationDomains	<p>Pipe () delimited list of domains to be used by the manual Active Directory authentication module to authenticate users. The list is processed in the given order. This list should only contain domains to be synchronized.</p> <p>Example:</p> <p>MyDomain MyOtherDomain</p> <p>For more information about One Identity Manager authentication modules, see the <i>One Identity Manager Authorization and Authentication Guide</i>.</p>
TargetSystem ADS AutoCreateDepartment	Specifies whether departments are automatically created when user accounts are modified or synchronized.
TargetSystem ADS AutoCreateLocality	Specifies whether locations are automatically created when user accounts are modified or synchronized.
TargetSystem ADS AutoCreateHardwaretype	Specifies whether corresponding device types are created automatically in the database for imported printer objects.
TargetSystem ADS AutoCreateServers	Specifies whether entries for missing home servers and profile servers are created automatically when user accounts are synchronized.
TargetSystem ADS AutoCreateServers PreferredLanguage	Language of automatically created servers.

Configuration parameters	Description
TargetSystem ADS DefaultAddress	Default email address of the recipient for notifications about actions in the target system.
TargetSystem ADS HardwareInGroupFrom Org	Specifies whether computers are added to groups based on group assignment to roles.
TargetSystem ADS MaxFullsyncDuration	Maximum runtime of a synchronization in minutes. No recalculation of group memberships by the DBQueue Processor can take place during this time. If the maximum runtime is exceeded, group membership are recalculated.
TargetSystem ADS MembershipAssignCheck	Specifies whether membership validity is verified on saving when group memberships are assigned in the One Identity Manager database. Disable this configuration parameter if several trusted domains with access across memberships are managed in the database.
TargetSystem ADS MemberShipRestriction	General configuration parameter for restricting membership in Active Directory.
TargetSystem ADS MemberShipRestriction Container	Number of Active Directory objects allowed per container before warning email is sent.
TargetSystem ADS MemberShipRestriction Group	Number of Active Directory objects allowed per group before warning email is sent.
TargetSystem ADS MemberShipRestriction MailNotification	Default mail address for sending warning emails.
TargetSystem ADS PersonAutoDefault	Mode for automatic employee assignment for user accounts added to the database outside synchronization.
TargetSystem ADS PersonAutoDisabledAccounts	Specifies whether employees are automatically assigned to disabled user accounts. User accounts are not given an account definition.
TargetSystem ADS PersonAutoFullSync	Mode for automatic employee assignment for user accounts that are added to or updated in the database by synchronization.
TargetSystem ADS PersonExcludeList	Listing of all user account without automatic employee assignment. Names are listed in a pipe () delimited list that is handled as a regular search pattern. Example:

Configuration parameters	Description
	ADMINISTRATOR GUEST KRBTGT TSINTERNETUSER IUSR_.* IWAM_.* SUPPORT_.* . * \$
TargetSystem ADS PersonUpdate	Specifies whether employees are updated if their user accounts are changed. This configuration parameter is set to allow ongoing update of employee objects from associated user accounts.
TargetSystem ADS ReplicateImmediately	Speeds up synchronization of modifications between two domain controllers. When set, the accumulated modifications in Active Directory are immediately replicated between domain controllers.
TargetSystem ADS VerifyUpdates	Specifies whether changed properties are checked when the system is updated. If this parameter is set, the objects in the target system are verified after every update.

Default project template for One Identity 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 project template uses mappings for the following schema types.

Table 11: Schema type mapping

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
rpcContainer	ADSContainer
user	ADSAccount

Active Roles connector settings

The following settings are configured for the system connection with the Active Roles connector.

Table 12: Active Roles connector settings

Setting	Meaning
Domain	Full domain name. Variable: CP_Rootdn
User account	User for logging in to Active Roles Variable: CP_User
Password	The user account's password. Variable: CP_Password
DNS name or IP address of the Active Roles server.	DNS name or IP address of the Active Roles server that connects against the synchronization server. Example: <Name of servers>.<Fully qualified domain name> Variable: CP_Server
Reason for workflows	Reason that is entered when the workflows are running. Variable: DefaultWorkflowReason
Run Active Roles workflows	Specifies whether to run Active Roles workflows. If the value is False , no Active Roles workflows are run. The user account requires permissions as in Permissions required for synchronizing with One Identity Active Roles on page 10. If the value is true , the connector will attempt to run the Active Roles workflows associated with the operation. This works only if the connection account is not a member of the Active Roles administrators group. Default: False

Setting	Meaning
	Variable: RunArsWorkflowsByDefault
ForestName	Name of the domain forest. Variable: ForestName

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

A

Active Directory domain

- deprovision user account 40
- group deprovisioning 40
- workflow 32

Active Directory group

- add to IT Shop (automatic) 36
- approval by owner 39
- create 38
- delete 41-42
- deprovision 40-42
- deprovisioning date 39, 43
- deprovisioning status 39, 43
- main data 39
- owner 39
- publish 39
- request 38
- restore 44-45
- revoke deprovisioning 44-45

Active Directory user account

- delete 41-42
- deprovision 40-42
- deprovisioning date 43
- deprovisioning status 43
- restore 44-45
- revoke deprovisioning 44-45

Active Roles

- architecture 5
- connector 5
- deprovision 40
- deprovisioning date 43

- deprovisioning status 43
- policies 35
- schema 34
- synchronization server 11
- virtual properties 34
- workflow 31-34

C

calculation schedule 22

- deactivate 23

configuration parameter 47

D

direction of synchronization

- direction target system 15
- in the Manager 15

J

Job server

- load balancing 21

L

load balancing 21

O

object

- delete immediately 25
- outstanding 25
- publish 25

outstanding object 25

P

product owners 36

project template 53

provisioning

accelerate 21

S

single object synchronization

accelerate 21

synchronization 9

authorizations 10

calculation schedule 22

configure 15, 20

connection parameter 15, 20

prevent 23

scope 20

start 15, 22

synchronization project

create 15

user account 10

variable 20

workflow 15

synchronization configuration

customize 20

synchronization log 24

synchronization project

create 15

deactivate 23

project template 53

synchronization server

configure 11

install 11

Job server 11

synchronization workflow

create 15

T

target system synchronization 25