



Active Roles On Demand

Quick Start Guide

**Copyright 2022 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](http://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.

Active Roles On Demand Quick Start Guide  
Updated - 27 May 2022, 13:11

# Contents

<b>Introduction to Active Roles On Demand</b>	<b>4</b>
<b>Active Roles On Demand system requirements</b>	<b>5</b>
Active Roles Management Tools	5
Active Roles Console	7
Active Roles Web Interface Access	8
Optional Active Roles Components	8
Active Roles Synchronization Service	8
Active Roles Synchronization Service Capture Agent	11
Active Roles Reporting	11
Available Active Roles Reports	12
<b>Preparing the offline join of the Active Roles On Demand server</b>	<b>16</b>
<b>Sending required information to One Identity</b>	<b>18</b>
<b>Initial configuration of Active Roles On Demand</b>	<b>21</b>
Installing the One Identity Certificate	22
First-time configuration of Active Roles On Demand	25
Installing the Active Roles Console	28
Installing the Active Roles Management Shell	29
Adding the first domain to the Active Roles Console	30
Validating the Active Roles Web Interfaces	32
Installing the Active Roles Collector and Report Pack	33
Configuring the Active Roles Collector and Report Pack	36
Adding the Reporting Link to the Active Roles Console	43
Installing Active Roles Synchronization Service	44
<b>About us</b>	<b>48</b>
<b>Contacting us</b>	<b>49</b>
<b>Technical support resources</b>	<b>50</b>

# Introduction to Active Roles On Demand

One Identity Active Roles is an access management system designed to assist administrators in the access management of on-premises, hybrid and cloud enterprise infrastructures, such as Microsoft Active Directory (AD), organization mailboxes, Lightweight Directory Services (LDS), and so on. Besides providing tools to provision access to various company resources (user accounts, computers, email addresses, printers, and so on), it also allows you to set up business unit-level or company-level policies and workflows for automating access management tasks to save administration time and operational costs.

One Identity Active Roles On Demand is a complete Active Roles installation, provisioned in the One Identity cloud and connected to your network through a virtual private network (VPN). One Identity operates and monitors the runtime environment for you.

When purchasing and deploying Active Roles On Demand the first time, you must send a set of network and VPN connection information to One Identity via the One Identity Starling portal (<https://www.cloud.oneidentity.com>), and you must upload an offline domain join file. The One Identity Cloud Operations Team then provisions your Active Roles On Demand environment based on the information and offline domain join file you provided.

This provisioning can take up to 24 hours to complete, and some additional VPN configuration may be required to adjust your VPN gateway device to connect to the VPN gateway you hosted.

As One Identity is provisioning Active Roles On Demand in an address that is private to your VPN, One Identity provides the IP address for Active Roles On Demand and the administrator account credentials.

# Active Roles On Demand system requirements

One Identity Active Roles On Demand provides its core features in a SaaS-delivered model. Therefore, you do not need to install the Active Roles Administration Service and the Active Roles Web Interface components on-premises.

However, to access, configure and maintain the Active Roles On Demand solution, you must install certain client-based Active Roles components on-premises with the indicated system requirements.

Before using the 30 May 2022 release of Active Roles On Demand, ensure that you meet the following requirements.

## Active Roles Management Tools

Active Roles Management Tools is a composite component, providing the following client-based tools to configure and manage your Active Roles deployment:

- Active Roles Configuration Center
  - | **NOTE:** Active Roles Configuration Center is available on 64-bit systems only.
- Active Roles Management Shell
- Active Roles SDK
- ADSI Provider

**Table 1: Active Roles Management Tools system requirements**

CPU	Intel x86, Intel 64 (EM64T) or AMD64 processor, 1 GHz or faster.
RAM	1 GB or more.
Disk space	100 MB
Supported OS	<ul style="list-style-type: none"><li>• Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition).</li><li>• Microsoft Windows 8.1 or 10 (Professional or Enterprise edition, 32-bit or 64-bit).</li></ul> <ul style="list-style-type: none"><li>  <b>NOTE:</b> Active Roles is not supported on Windows Server Core installations.</li></ul>
.NET Framework	4.7.2

- |               |   |
|---------------|---|
| Miscellaneous | <ul style="list-style-type: none"><li>• Visual C++ 2017 Redistributable</li><li>• Microsoft Windows Remote Server Administration Tools (RSAT) for AD is required to manage Terminal Services user properties with Active Roles Management Shell or Active Roles Management Tools.</li></ul> |
|---------------|---|
- 

## Configuration Center

Active Roles Configuration Center provides a single solution for configuring the Active Roles Administration Service instances and Active Roles Web Interface sites, allowing administrators to perform the core configuration tasks from a single location. These include the following:

- Creating and configuring the Active Roles Administration Service and the default cloud-based Active Roles Web Interface sites.
- Managing the core Active Roles Administration Service settings, such as the Active Roles administrator account, service account, and database connection.
- Managing the core Active Roles Web Interface settings, such as the site address on the web server and its configuration object in the Active Roles Administration Service.
- Logging options for troubleshooting Active Roles components.

**NOTE:** Currently, when opening the **Logging** settings of the Active Roles Configuration Center, the **Logging** page will be blank. As a workaround, contact the One Identity Cloud Operations Team if you need to change your logging settings.

- The Starling Join feature, enabling Active Roles to connect to the One Identity Starling Cloud Platform and integrate with additional One Identity products for additional functionality.

## Active Roles Management Shell

A set of Management PowerShell cmdlets, providing a means for executing and automating tasks in Active Roles and covering three key areas:

- Active Directory objects
- Active Roles configuration
- Active Roles Synchronization Service

## Active Roles SDK

The Active Roles SDK, providing samples and documentation for developers to help them:

- Customize Active Roles by creating custom client applications and user interfaces.
- Expand the use of Active Roles by integrating it with the existing proprietary applications and network data sources.

## ADSI Provider

The Active Directory Services Interface (ADSI) Provider enables custom user interfaces and applications to access Active Directory services through Active Roles. ADSI Provider translates client requests into DCOM calls and interacts with the Active Roles Administration Service.

The Active Roles ADSI Provider allows custom scripts and applications (such as web-based applications) to communicate with Active Directory, while taking full advantage of the security, workflow integration and reporting benefits of Active Roles.

The data exposed by Active Roles ADSI Provider is organized in a namespace identical to the namespace of the Windows system LDAP provider. The name of the Active Roles ADSI Provider namespace is EDMS://, instead of using the Microsoft LDAP:// namespace).

# Active Roles Console

Active Roles Console (also known as the MMC Interface) is a Microsoft Management Console (MMC) snap-in for a Microsoft Windows-based user interface.

Administrator users can use Active Roles Console to perform most Active Roles configuration actions while standard users can perform daily delegated administration and operations with it.

**Table 2: Active Roles Console system requirements**

CPU	Intel x86, Intel 64 (EM64T) or AMD64 processor, 1 GHz or faster.
RAM	1 GB or more. <b>NOTE:</b> The amount of memory required by Active Roles Console depends on the total number of managed objects.
Disk space	100 MB
Supported OS	<ul style="list-style-type: none"> <li>• Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition).</li> <li>• Microsoft Windows 8.1 or 10 (Professional or Enterprise edition, 32-bit or 64-bit).</li> </ul> <b>NOTE:</b> Active Roles is not supported on Windows Server Core installations.
.NET Framework	4.7.2

Web browser	Microsoft Edge 79 (or newer), based on Chromium
Miscellaneous	Visual C++ 2017 Redistributable

## Active Roles Web Interface Access

The Active Roles Web Interface is a browser-based administration interface for Active Roles users and administrators. Certain Active Roles administration configuration actions (such as Microsoft 365 integration) is only available via the Web Interface.

The Active Roles On Demand solution hosts the Web Interface in a SaaS-delivered model, requiring no on-premises deployment. However, you need to meet the following requirements to access the Web Interface.

**Table 3: Active Roles Web Interface access requirements**

Web browser	<ul style="list-style-type: none"> <li>• Internet Explorer 11</li> <li>• Google Chrome 61 (or newer)</li> <li>• Microsoft Edge 79 (or newer), based on Chromium</li> <li>• Mozilla Firefox 36 (or newer)</li> </ul>
Display resolution	<p>The Active Roles Web Interface is optimized for screen resolutions of 1280x800 or higher.</p> <p>The minimum supported screen resolution is 1024x768.</p>

## Optional Active Roles Components

Active Roles On Demand provides several optional components that you can install on-premises for additional features. These components include:

- Active Roles Synchronization Service
- Active Roles Synchronization Service Capture Agent
- Active Roles Reporting (Data Collector and Report Pack)

## Active Roles Synchronization Service

**NOTE:** If you plan to manage Azure AD or Office 365 operations in your environment, you must install the Active Roles Synchronization Service component.

The Active Roles Synchronization Service lets you:



- Synchronize identity information stored in data systems other than Active Directory (AD) and Active Directory Lightweight Directory Services (AD LDS) supported by the Active Roles Console.
- Automate identity information management among the various supported data systems (for example, by using workflows to create, read, update, delete, or deprovision identity information with Active Roles).

For more information on the Active Roles Synchronization Service, see [Available Active Roles Reports](#).

**Table 4: Active Roles Synchronization Service system requirements**

CPU	Intel x86, Intel 64 (EM64T) or AMD64 processor, 1 GHz or faster.  <b>NOTE:</b> One Identity recommends using a multi-core processor for the best performance.
RAM	2 GB or more.  <b>NOTE:</b> The amount of memory required depends on the number of synchronized objects.
Disk space	250 MB
Supported OS	Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition).  <b>NOTE:</b> Active Roles is not supported on Windows Server Core installations.
Supported databases	<ul style="list-style-type: none"> <li>• Microsoft SQL Server 2019, 2017 or 2016, any edition.</li> <li>• Microsoft SQL Server 2014 or 2012, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Packs.</li> </ul>
.NET Framework	4.7.2
Windows Management Framework	5.1
Miscellaneous	Visual C++ 2017 Redistributable
Supported connector versions	<ul style="list-style-type: none"> <li>• Active Roles versions 7.4.3, 7.4.1, 7.3, 7.2, 7.1, 7.0, and 6.9.</li> <li>• Data sources accessible through an OLE DB provider.</li> <li>• Delimited text files.</li> <li>• Generic LDAP Connector.</li> <li>• IBM AS/400 Connector.</li> <li>• IBM Db2 Connector.</li> <li>• IBM RACF Connector.</li> </ul>

- 
- Micro Focus NetIQ Directory.
  - Microsoft AD Domain Services with the domain or forest functional level of Windows Server 2012 (or higher).
  - Microsoft AD LDS running on any Windows Server operating system supported by Microsoft.
  - Microsoft Exchange Server version 2019, 2016, 2013, or 2010.
  - **NOTE:** Microsoft Exchange 2013 CU11 is not supported. For more information, see [Knowledge Base Article 202695](#) on the *One Identity Support Portal*.
  - Microsoft Lync Server version 2013 (with limited support).
  - Microsoft Skype for Business 2019, 2016 or 2015
  - Microsoft Windows Azure AD (using the Azure AD Graph API version 1.6).
  - Microsoft Office 365 directory.
  - Microsoft Exchange Online service.
  - Microsoft Skype for Business Online service.
  - Microsoft SharePoint Online service.
  - Microsoft SQL Server (any version supported by Microsoft).
  - Microsoft SharePoint 2019, 2016, or 2013.
  - MySQL Connector.
  - One Identity Manager version 7.0 (D1IM 7.0).
  - One Identity Manager version 8.0.
  - Oracle Database.
  - Oracle Database User Accounts.
  - Oracle Unified Directory.
  - OpenLDAP Connector.
  - Salesforce Connector.
  - ServiceNow Connector.

**NOTE:** Data sources accessible through an OLE DB provider, delimited text files, and IBM RACF data systems are supported by Active Roles Synchronization Service without bi-directional support.

---

# Active Roles Synchronization Service Capture Agent

Active Roles Synchronization Service provides a Capture Agent to synchronize user passwords between Active Directory (AD) domains managed by the Synchronization Service and other connected data systems.

**NOTE:** To synchronize passwords from an AD domain to other connected data systems, you must install the Synchronization Service Capture Agent on all domain controllers in the source AD domain.

**Table 5: Active Roles Synchronization Service system requirements**

.NET Framework	4.7.2
Supported OS on domain controllers	Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition).  Both x86 and x64 platforms are supported, with or without any Service Packs.

## Active Roles Reporting

Active Roles offers optional on-premises reporting capabilities with its Data Collector and Report Pack, allowing you to view Active Roles tracking logs for administrative roles, Managed Units (MUs), policy compliance, Policy Objects, and the state of key Active Directory (AD) objects.

Active Roles Data Collector and Report Pack facilitates the collection of environment data (stored in an SQL Server database) and the automated generation of reports on management activities. The Report Pack component is deployed on Microsoft SQL Server Reporting Services (SSRS) to view, save, print, publish, and schedule Active Roles reports. For more information on the available report, see [Available Active Roles Reports](#).

**Table 6: Active Roles Collector and Report Pack system requirements**

.NET Framework	4.7.2
Supported OS on domain controllers	Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition).  <b>NOTE:</b> Active Roles is not supported on Windows Server Core installations.
Supported databases	<ul style="list-style-type: none"><li>• Microsoft SQL Server 2019, 2017 or 2016, any edition.</li><li>• Microsoft SQL Server 2014 or 2012, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Packs.</li></ul>

.NET Framework	4.7.2
Other Active Roles components	The Active Roles Management Tools must be installed and must have the same version as the Active Roles Administration Service, due to using the Active Roles ADSI Provider component.

## Available Active Roles Reports

Active Roles provides reporting services for the following Active Directory and Active Roles objects, components and events.

### Active Directory Assessment

- Domains
  - Domain account SID resolution.
  - Domain Summary.
  - Domain Trusts.
- Group Membership
  - Group Membership by groups.
  - Group Membership by users.
  - Users with domain administration rights.
- Groups
  - Domain group statistics.
  - Empty groups.
  - Group hierarchy.
  - Group list with member statistics.
- Organization Units (OUs)
  - Member statistics by OU.
  - OU hierarchy.
  - OU membership.
- Other Directory Objects.
  - Active Directory object properties.
  - All discontinued computer accounts.
  - Computer accounts.
- Potential Issues
  - Cycled groups.

- Users
  - Account Information
    - Bad password information.
    - Password age information.
    - User account list.
    - User account options.
  - Exchange 2000-2003 (or newer)
    - Email delivery options.
    - Email delivery restrictions.
    - Mailbox information by user.
    - Active Roles tracking log.
  - Miscellaneous Information
    - Objects managed by a user.
    - Personnel hierarchy.
    - User profile information.
    - Users with specified properties.
  - Obsolete Accounts
    - All discontinued user accounts.
    - Deprovisioned user accounts.
    - Disabled user accounts.
    - Expired user accounts.
    - Inactive user accounts.
    - Locked user accounts.
    - User accounts with expired password.

## Active Roles Tracking Log

- Active Directory Management
  - Deprovisioning of user accounts.
  - Directory object management.
  - User attribute management.
- Active Roles Configuration Changes
  - Control delegation.
  - Policy enforcement.
- Active Roles Events

- Active Roles events statistics.
- Active Roles startup failures.
- Active Roles Workflow
  - Approvals and rejections.
  - Workflow monitoring.
- Dashboard
  - User account management.

## **Administrative Roles**

- Access Template permissions.
- Access Template summary.
- Access Templates linked to Managed Units (MUs).
- Access Templates linked to OUs.
- Control delegation by object.
- Control delegation by object (with group hierarchy).
- Control delegation by trustee.
- Control delegation by trustee (with container hierarchy).

## **Managed Units**

- MU members.
- MU membership rules.
- MU summary.
- MUs affected by policies.
- MUs with delegated control.

## **Policy Compliance**

- Objects violating policy rules.
- Violated policy rules.

## **Policy Objects**

- Linked property validation settings.
- Linked property validation settings (with inheritance).
- Linked script settings (with inheritance).
- Policy Object references.
- Policy Object settings.

- Policy Object summary.
- Policy Objects with securable objects.
- Securable objects (with inheritance).

## Preparing the offline join of the Active Roles On Demand server

Before sending the One Identity Active Roles On Demand configuration information required by the One Identity Cloud Operations Team, you must prepare the Active Roles server for an offline domain join by generating a domain join file. You will need upload this file to the One Identity Starling portal (<https://www.cloud.oneidentity.com>) when sending the required configuration information.

### Prerequisites

You must use an account with Active Directory permissions to perform a domain join. By default, Domain Admins have this permission.

### *To prepare the offline join of the Active Roles server*

1. Determine the domain and Organizational Unit (OU) where the Active Roles server will be deployed.

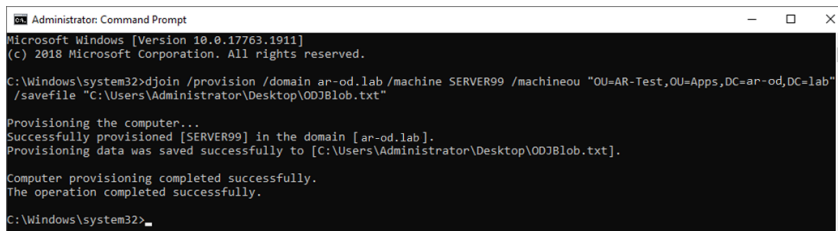
**NOTE:** Consider the following when planning the deployment of the Active Roles server:

- If you have more than one domain and need assistance in determining the proper Active Directory domain to use for this procedure, contact One Identity Support.
- Do not pre-create the Active Roles server name, as this procedure will create the computer object automatically in the specified OU.

2. Generate an offline domain join file for One Identity. To do so, open a Command Prompt with elevated privileges on a Windows server joined to the same domain where the Active Roles server will be deployed, and run the following single-line command:

```
djoin /provision /domain <domain-name> /machine <activeroles-server-netbios-name> /machineou "OU=<OU-name>,DC=<NetBIOS-domain-name>,DC=<domain-suffix>" /savefile <X>:\<folder-name>\ODJBlob.txt
```





```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1911]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>djoin /provision /domain ar-od.lab /machine SERVER99 /machineou "OU=AR-Test,OU=Apps,DC=ar-od,DC=lab"
/savefile "C:\Users\Administrator\Desktop\ODJBlob.txt"

Provisioning the computer...
Successfully provisioned [SERVER99] in the domain [ar-od.lab].
Provisioning data was saved successfully to [C:\Users\Administrator\Desktop\ODJBlob.txt].

Computer provisioning completed successfully.
The operation completed successfully.

C:\Windows\system32>
```

**NOTE:** Do not use a Container (CN) for the target location. Use only an OU instead. If you still prefer to use the default Computers CN, remove the `/machineou` switch and value.

3. Perform the steps of [Sending required information to One Identity](#) and upload the generated ODJBlob.txt file to the **Technical Information** form of the One Identity Starling portal.

The One Identity Cloud Operations Team will use the attached ODJBlob.txt file to complete the offline domain join and deploy the Active Roles On Demand tenant for your organization.

**NOTE:** Do not proceed to the [Initial configuration of Active Roles On Demand](#) process until One Identity has confirmed that the Active Roles On Demand tenant is ready for configuration.

# Sending required information to One Identity

Before the One Identity Cloud Operations Team can configure and provision your Active Roles On Demand environment, you must send a set of configuration information via the One Identity Starling portal (<https://www.cloud.oneidentity.com>).

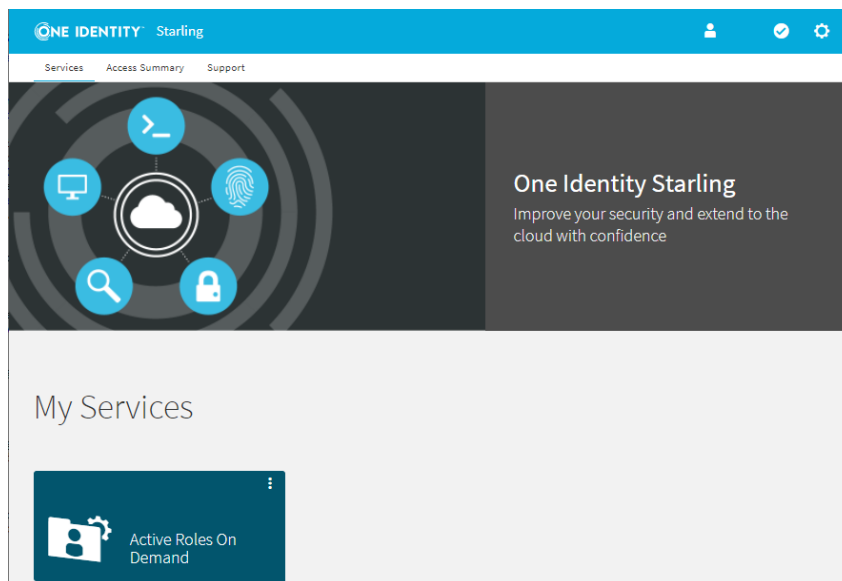
## Prerequisites

Before collecting and sending the required information, make sure that the following conditions are met:

- Your organization is already registered on the [One Identity Starling](#) portal.
- If you configure a product trial, your One Identity representative notified your organization that the product trial has been added to your organization account.
- If you configure a subscribed product, your organization received a subscription confirmation email from One Identity.

## ***To send product configuration information to the One Identity Cloud Operations Team***

1. To open the list of product services available for your organization, in the [One Identity Starling](#) portal, click **Services**.



2. To start configuring the product, open the **Application** page of Active Roles On Demand.

- To configure a product trial, open the **View On Demand services** ribbon at the bottom of the page and click **Active Roles On Demand > Trial**. This will create the trial subscription for you. Continue configuring the trial subscription as described in the next bullet point.
  - To configure a subscribed product (or an active product trial), click **My Services > Active Roles On Demand**.
3. In the **Contact Information** step, specify whether you are the technical contact for the One Identity Cloud Operations Team in your organization.

The screenshot shows the 'Configuration' page in the One Identity Starling web interface. At the top, there are tabs for 'Application' and 'Collaborators'. Below the tabs, the page title is 'Configuration' with a subtitle 'See the status of the On Demand service and provide additional information for the deployment.' A progress bar shows three steps: 1. Contact Information (active), 2. Technical Information, and 3. Setting Up. The 'Contact Information' section has a subtitle 'Contact information for the person who is responsible for the configuration and administration of the On Demand service.' There are two radio buttons: 'I am the technical contact' (selected) and 'Someone else is the technical contact'. Below the radio buttons, a note states 'One Identity Operations will use the information that you provided during Starling registration.' At the bottom right, there is a blue button labeled 'Next: Technical Information'.

- If you are the technical contact (that is you have all the technical information required by One Identity to configure and provision Active Roles On Demand), select **I am the technical contact** and click **Next: Technical information**.
  - If you are not the technical contact, then invite the contact who can provide the required configuration information. This is typically required if the initial On Demand invitation email was sent to you due to organizational policies, even if you are not the technical contact of the On Demand product. To invite the actual technical collaborator:
    - a. Select **Someone else is the technical contact**, then click **Invite Collaborator**.
    - b. In the **Invite Collaborator** dialog, provide the name and email address of the technical contact.
    - c. To send an invitation to the specified contact, click **Invite**.

**TIP:** You can also invite a technical contact by clicking **Collaborators** on the top left corner of the One Identity Starling web interface.

Once you sent the invitation to the technical contact, make sure that they perform the remaining steps.
4. In the **Technical Information** step, provide the required configuration information as instructed on-screen. To upload the offline domain join file created previously as described in [Preparing the offline join of the Active Roles On Demand server](#), click **Active Directory Domain Join File > Upload Join File**.
5. To confirm the information you entered, click **Submit Details**. This opens the **Confirm Details** dialog, where you can either send the information to the One

Identity Cloud Operations Team (**Submit Details**), or return to the **Technical Information** step and make any final changes (**Edit Details**).

**NOTE:** Once you submit the specified information, you cannot make any further changes, unless One Identity rejects the provided configuration information for some reason.

6. Once you sent the configuration information, the **Setting Up** step will indicate the status of provisioning and configuring Active Roles On Demand. One Identity will also send you an email notification each time the status of deployment changes.

The screenshot shows a progress bar at the top with three steps: 1. Contact Information, 2. Technical Information (checked), and 3. Setting Up (active). Below the progress bar, the heading is "Waiting for One Identity" with a subtext: "We are working on setting up your On Demand service. We will send you an update when it is ready." There are three radio button options: "Waiting for an engineer to begin deployment" (unchecked), "Deployment in progress" (checked with a green checkmark), and "On Demand service deployed" (unchecked). Below these options is a blue information box with an 'i' icon, titled "Deployment Information" and containing the text "Deployment will take 4 hours".

The **Setting Up** step will also indicate if configuration fails for any reason (for example, because of incorrect data provided in the **Technical Information** step).

The screenshot shows the same progress bar as the previous image. The heading is "Waiting for One Identity" with the same subtext. The radio button options are: "Waiting for an engineer to begin deployment" (unchecked), "Deployment in progress" (checked with a red 'x'), and "On Demand service deployed" (unchecked). Below these options is a red error box with an 'x' icon, titled "We could not finish the setup" and containing the text "Incorrect IP address provided in Technical Information." At the bottom of the form is a blue button labeled "Update Details".

To open the **Technical Information** step and fix the provided information as requested by the One Identity Cloud Team, click **Update Details**. Once you updated the configuration details, resend them to the One Identity Cloud Operations Team by clicking **Submit Details** again in the **Technical Information** step.

Once Active Roles On Demand is configured for your organization, the **Application** page of Active Roles On Demand will display the connection and configuration data of your On Demand deployment.

# Initial configuration of Active Roles On Demand

When One Identity personnel confirmed to you that the offline join procedure of the Active Roles server has finished, perform the initial configuration of One Identity Active Roles On Demand.

## Prerequisites

Make sure that the following conditions are met before performing initial configuration:

- One Identity confirmed that the Active Roles On Demand tenant is ready for configuration.
  - The Active Roles server deployed by One Identity personnel is joined to the Active Directory of your organization.
  - The Active Roles installation package is downloaded from the [One Identity Support Portal](#).
  - The user account that you use for configuring the Active Roles components is a Local Workstation Administrator, and has all required Active Directory permissions. For more information, see *Required Permissions and Access* in the [Active Roles How-To Guide](#).
  - The workstation where you perform the procedure meets the minimum system requirements (described in [Active Roles On Demand system requirements](#)) and is joined to the same domain as the Active Roles server.
  - The Active Roles Service Account has the proper permissions. For more information, see *Required Permissions and Access* in the [Active Roles How-To Guide](#).
- | **NOTE:** For each added domain, additional service accounts may be required.
- An Active Directory group containing the administrators of Active Roles (and the account used to perform the following procedure) has been created.
  - All required communication ports are open for any firewalls. For more information, see *Appendix C: Communication ports* of the [Active Roles Administration Guide](#).

# Installing the One Identity Certificate

To ensure that the Active Roles Configuration Center installed on-premises can communicate with the Active Roles server deployed by One Identity, you must install the One Identity certificate on the workstation(s) where the Active Roles Configuration Center will be used.

**NOTE:** Perform this procedure only on the workstation(s) of the Active Roles administrator(s) who will run the Active Roles Configuration Center. You do not need to perform this procedure for any other Active Roles users, interfaces or management tools.

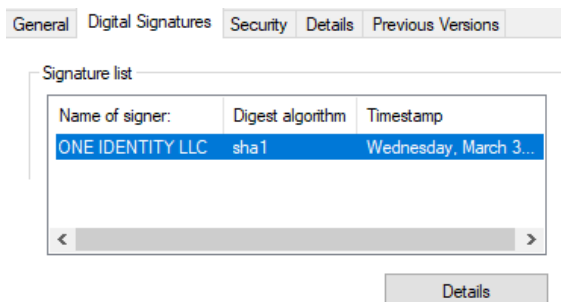
The Active Roles Configuration Center can only connect to the Active Roles server deployed by One Identity if this procedure is performed.

## To install the One Identity Certificate

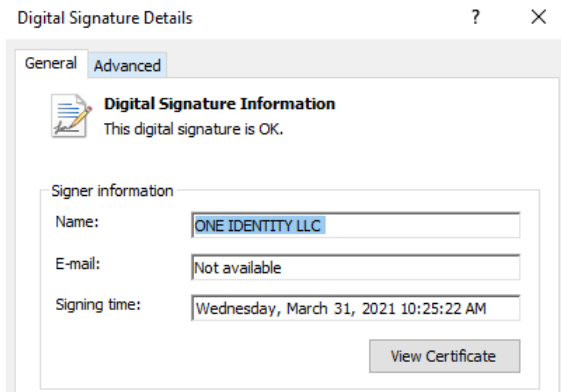
1. On an Active Roles administration workstation, navigate to the following UNC path:

```
\\<active-roles-server-name>\C$\Program Files\One Identity\Active Roles\7.5.3\Shell
```

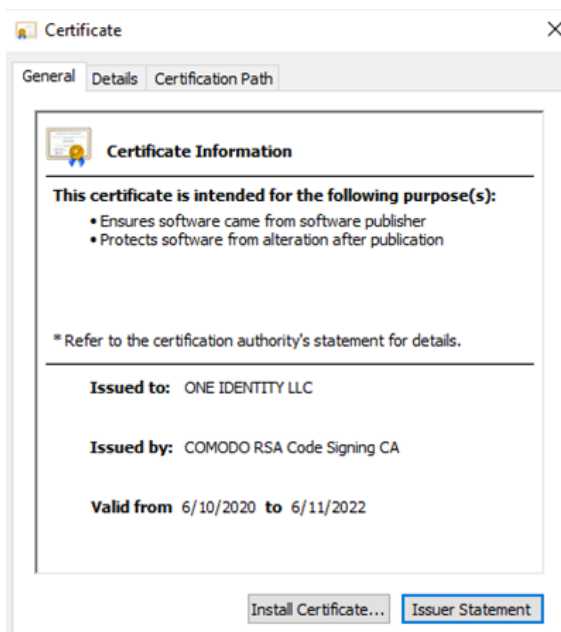
2. To open the list of Active Roles-specific signatures, right-click the ActiveRolesServiceConfiguration.psm1 file and click **Properties > Digital Signatures**.
3. To open the details of the certificate, on the **Digital Signatures** tab, select **ONE IDENTITY LLC** from the **Signature list** and click **Details**.



4. On the **Digital Signature Details > General** tab, click **View Certificate**.



5. To launch the Certificate Import Wizard, on the **Certificate** > **General** tab, click **Install Certificate**.



6. Under **Store Location**, select **Local Machine** and click **Next**.

## Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.


Store Location



☐ Current User

☒ Local Machine

To continue, click Next.

7. In the **Certificate Store** step, select **Place all certificates in the following store** and click **Browse**.



  Certificate Import Wizard

**Certificate Store**  
Certificate stores are system areas where certificates are kept.

---

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

**Browse...**

8. In the browse window that appears, select the **Trusted Publishers** directory and click **OK**.
9. To apply your changes, close all remaining steps of the Certificate Import Wizard by clicking **Next**, **Finish** and **OK**, respectively.



## First-time configuration of Active Roles On Demand

When the One Identity Certificate is installed on the workstation(s) that will run the Active Roles Configuration Center, perform the first-time configuration of One Identity Active Roles On Demand.

### *To perform the first-time configuration of Active Roles On Demand*

1. Copy the downloaded Active Roles .zip or .iso file to the local workstation of an Active Roles administrator. Depending on the file format of the installer, extract the .zip or mount the .iso.
2. To start the installation of the Active Roles Configuration Center, double-click the Configuration Center installation package in the local extracted location or the mounted ISO drive:

```
Components\ActiveRoles Configuration Center\ConfigCenter.msi
```

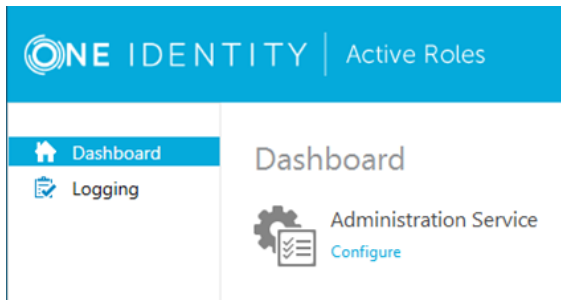
**NOTE:** The installation will progress without interaction, and will complete without a completion prompt.

After the installation is complete, the **Active Roles Configuration Center** will appear in the Windows Start Menu.

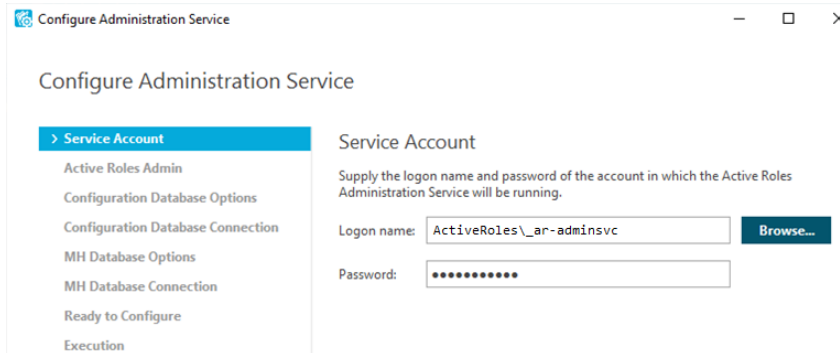
3. Open the **Active Roles Configuration Center** in the Windows Start menu.
4. In the **Select Server** window, select **Another server**, enter the name of the Active Roles server in the **Server** field, and the connection credentials to the **User name** and **Password** fields.

To proceed, click **Connect**. The Active Roles Configuration Center window will then appear.

5. To open the server settings of Active Roles, click **Configure** under **Dashboard > Administration Service**.



The **Configure Administration Service** window then opens.



6. In the **Service Account** tab, enter the Active Roles service account credentials in the **Logon name** and **Password** fields.
7. In the **Active Roles Admin** tab, enter the domain group of the Active Roles administrators.
8. In the **Configuration Database Options** tab, select the **New Active Roles database > Use a pre-created blank database** option.
9. In the **Configuration Database Connection** tab, configure the following options:
  - **Database Type:** Select **Azure SQL Database**.
  - **Database Server Name:** Enter the server name provided by One Identity personnel.
  - **Database Name:** Enter the name of the Configuration database provided by One Identity (**ActiveRoles\_CFG**).
  - **Connect using:** Select **SQL Server authentication** and enter the Azure SQL login credentials provided by One Identity to the **Login** and **Password** fields.
10. In the **Management History Database Options** tab, select **New Active Roles database > Use a pre-created blank database**.
11. In the **Connection to Management History Database** tab, configure the following settings:
  - **Database Type:** Select **Azure SQL Database**.
  - **Database Server Name:** Enter the server name provided by One Identity personnel.

- **Database Name:** Enter the name of the Management History database provided by One Identity (**ActiveRoles\_MH**).
  - **Connect using:** Select **SQL Server authentication** and enter the Azure SQL login credentials provided by One Identity to the **Login** and **Password** fields.
12. (Optional) On the **Encryption Key Backup** tab, set up a password-protected backup of the configuration. To specify the location of the backup file, click **Browse**. To configure password-protection for the backup, select **Protect the backup file with a password** and enter the password for the backup.

**NOTE:** Keep a copy of this file and password in a secure location for future use.

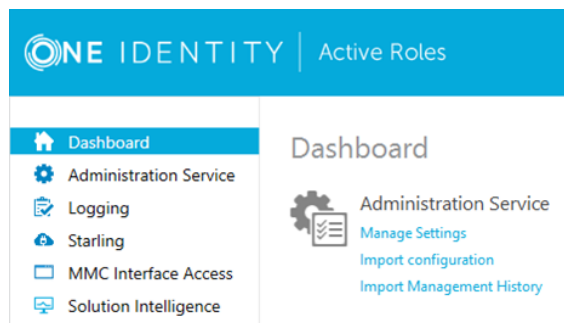
13. On the **Ready to Configure** tab, review your settings. When you are ready to apply the changes, click **Configure**.

The **Configure Administration Service** window will display the configuration progress in the **Execution (Progress)** tab.

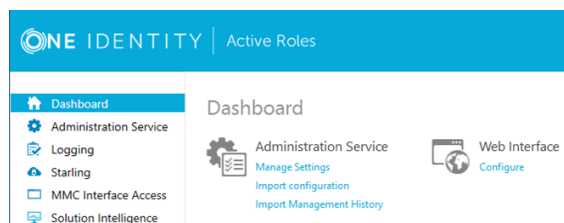
14. When the configuration finished:
- To close the **Configure Administration Service** window, click **Finish**.
  - To open the configuration log, click the **View log** link.

**TIP:** Use the provided support links of this tab to access the video tutorials, knowledge base articles and other support resources of Active Roles.

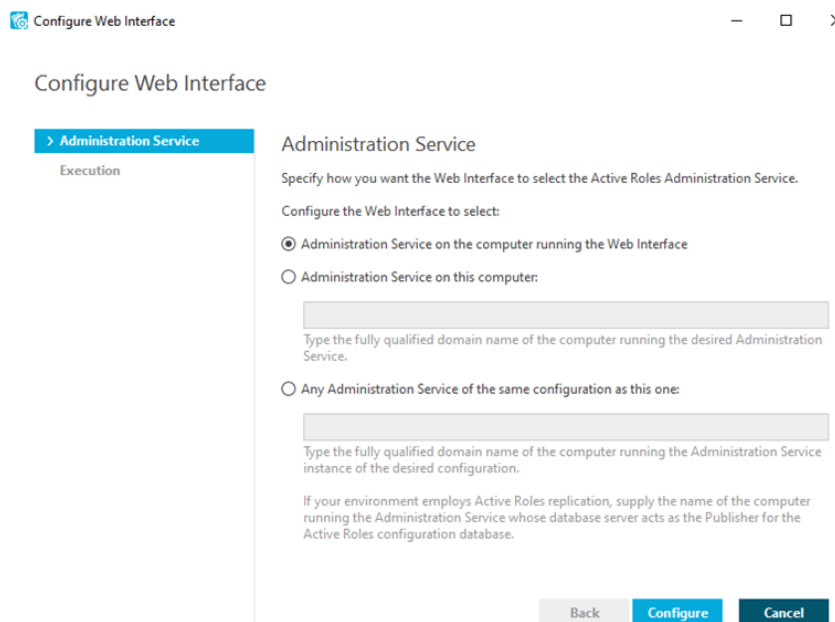
15. On the **Active Roles Configuration Center**, click **Manage Settings** under **Dashboard > Administration Service**.



16. Wait for the Administration Service to change from **Getting ready** to **Ready for use** status. When this happens, open the **Configure Web Interface** window by navigating to **Dashboard > Web Interface > Configure**.



17. In the **Administration Service** tab, select **Administration Service on the computer running the Web Interface** and click **Configure**.



The **Configure Web Interface** window will show the configuration progress in the **Execution (Progress)** tab.

With the SSL certificates also installed, the first-time configuration of Active Roles On Demand is finished, and it is ready to add and manage any Active Directory domains. Close the **Active Roles Configuration Center**.

## Installing the Active Roles Console

The Active Roles Console (also known as the MMC Interface) is a comprehensive administrative tool for managing Active Directory and Microsoft Exchange objects. Using the Console, Active Roles administrators can specify administrative roles and delegate control, define administrative policies and automation scripts, easily find directory objects, and perform various administrative tasks.

**NOTE:** The Active Roles Console can be installed and used by any Active Roles On Demand user.

### To install the Active Roles Console

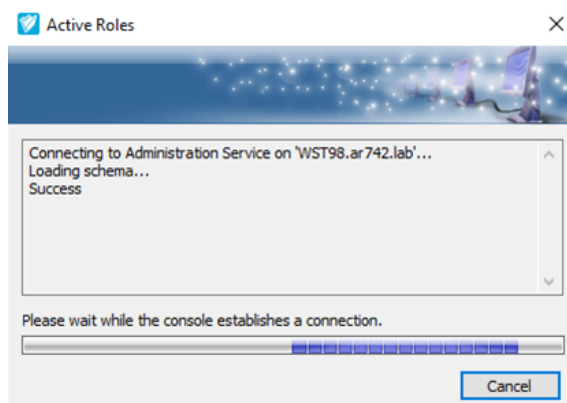
1. Launch the installer package of the Console from the Active Roles source files. The files are available at the following locations of the extracted Active Roles installer (when using the .zip file) or the mounted .iso image:
  - If you use a 32-bit operating system, run \Components\ActiveRoles Console\x86\Console\_x86.msi

- If you use a 64-bit operating system, run `\Components\ActiveRoles Console\x64\Console_x64.msi`

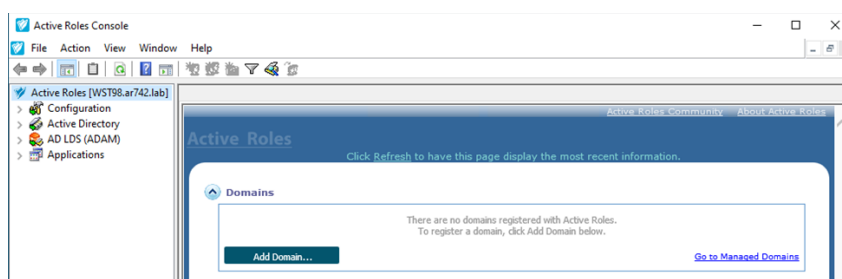
**NOTE:** The installation will progress without interaction, and will complete without a completion prompt.

Upon completion, the Active Roles Console will be visible in the Windows Start Menu as **Active Roles 7.5.3 Console**.

2. Start the Active Roles Console by clicking **Active Roles 7.5.3 Console** in the Windows Start Menu, and wait until the Active Roles Console establishes a connection to the Active Roles server and opens.



3. When Active Roles Console first opens, its **Domains** section will be blank. To configure the first domain, see [Adding the first domain to the Active Roles Console](#).



After adding the first domain, it will appear for all other users when they open the Active Roles Console on any workstation or server.

## Installing the Active Roles Management Shell

The Active Roles Management Shell component allows you to manage and configure Active Directory and Active Roles objects, Active Roles Administration Service instances, or Web Interface sites via PowerShell scripting.

**NOTE:** The Active Roles Management Shell can be installed and used by any Active Roles On Demand user.

### **To install the Active Roles Management Shell**

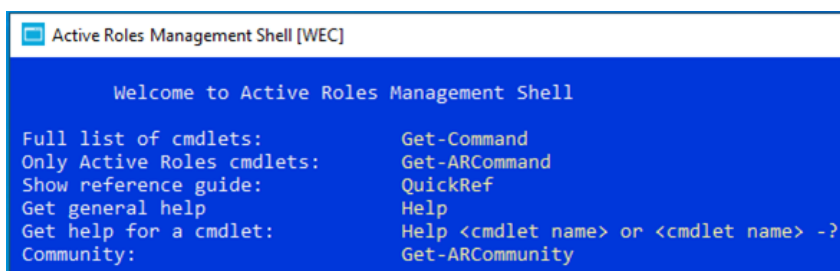
1. Launch the installer package of the Management Shell from the Active Roles source files. The files are available at the following locations of the extracted Active Roles installer (when using the .zip file) or the mounted .iso image:
  - If you use a 32-bit operating system, run `\Components\ActiveRoles Management Shell\x86\Shell_x86.msi`
  - If you use a 64-bit operating system, run `\Components\ActiveRoles Management Shell\x64\Shell_x64.msi`

**NOTE:** The installation will progress without interaction, and will complete without a completion prompt.

Upon completion, the Active Roles Management Shell will appear in the Windows Start Menu as **Active Roles 7.5.3 Management Shell**.

2. To verify that the Management Shell has been installed properly, launch it by clicking **Active Roles 7.5.3 Management Shell** in the Windows Start Menu.

The Management Shell interface will appear.



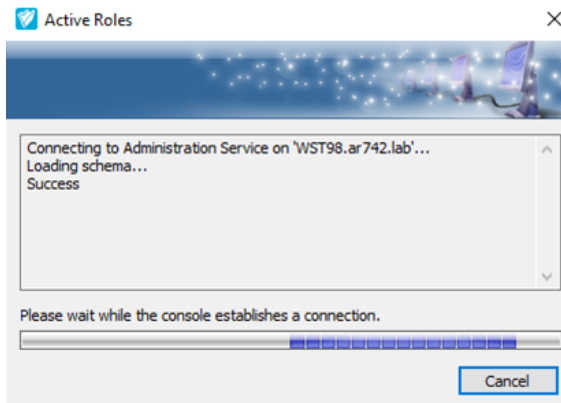
## **Adding the first domain to the Active Roles Console**

After installing the Active Roles Console (also known as the MMC Interface) as described in [Installing the Active Roles Console](#), you must add a new domain to Active Roles On Demand with it.

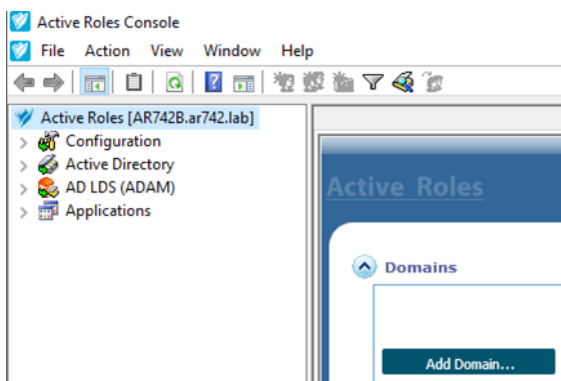
### **To add a Domain to Active Roles On Demand**

1. On a workstation where the Active Roles Console is installed, launch the Console from the Windows Start Menu by navigating to **One Identity Active Roles 7.5.3 > Active Roles 7.5.3 Console**.

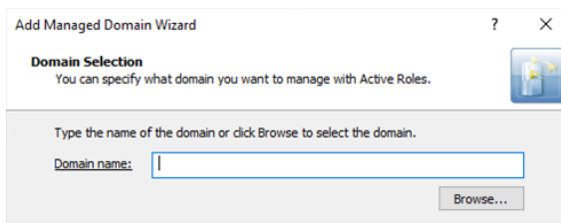
The Console will automatically find the Active Roles server and connect.



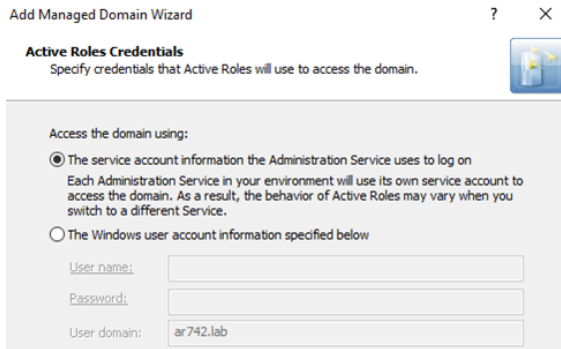
2. To open the **Add Managed Domain Wizard**, click **Add Domain** in the middle pane, then click **Next**.



3. In the **Domain Selection** step, either enter the name of the Active Directory domain you want to manage in Active Roles into the **Domain name** field, or click **Browse** to select it.



4. In the **Active Roles Credentials** step, select the default service account Active Roles was configured with.



- For typical use cases, select **The service account information the Administration Service uses to log on.**
  - If the domain to add is not in the same domain as the Active Roles server, or you must use a different account because of any technical or administrative reason, select **The Windows user account information specified below**, and provide the service account credentials.
5. Review your changes, then to apply the domain configuration, click **Finish**.
  6. The configured domain then appears grayed out on the Active Roles Console while it loads information into Active Roles. To refresh the loading status, click **Click to update the display**.

When this one-time loading operation finished, the **Domain information is being loaded** state will change to **Available for management**, and the Active Directory domain will appear in the Active Roles Console on the left pane under the **Active Roles > Active Directory** node.

## Validating the Active Roles Web Interfaces

When you specified a new domain as described in [Adding the first domain to the Active Roles Console](#), confirm that each Active Roles web interface (that is the Administrator Site, the Help Desk Site and the Self-Service Site) opens and works properly.

### **To validate the Active Roles Web Interfaces**

On any workstation, open each of the following web sites in a supported browser to confirm they are working properly:

- Administrator Site: `http://<activeroles-fqdn-servername>/ARWebAdmin`
- Help Desk Site: `http://<activeroles-fqdn-servername>/ARWebHelpDesk`

**NOTE:** The home page level of the Help Desk Site looks the same as the Administrator Site.

- Self-Service Site: `http://<activeroles-fqdn-servername>/ARWebSelfService`



When prompted for credentials for any of the interfaces, use your Active Directory credentials.

# Installing the Active Roles Collector and Report Pack

Optionally, if you require Active Roles reporting capabilities, install the Active Roles Collector and Report pack. For more information on the available reports, see [Available Active Roles Reports](#).

**NOTE:** Although this component must be installed on-premises, the reporting database itself is hosted in the Active Roles SaaS tenant in Azure SQL. Therefore, no on-premises database sizing is required.

## Prerequisites

Make sure that the following conditions are met before installing the Active Roles Collector and Report Pack:

- The SQL server and SQL Server Reporting Services are installed, configured, and confirmed to be running on premises.

**TIP:** One Identity recommends the Reporting Services web portals use SSL certificates.

- A server is available to:
  - Install the Active Roles Collector and Report Pack component.
  - Host a Windows Scheduled Task that will gather data about Active Roles and Active Directory populating the reports.

This server will act as the on-premises Active Roles Reporting Server, and will be referred to as such in later parts of the configuration procedure.

- The following PowerShell modules are available:

- [Exchange Online PowerShell v2 module x64](#)

**NOTE:** Use version v2.0.3 of the module.

To install the module, enter the following command:

```
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 2.0.3
```

- [Azure AD Module](#)

To install the module, enter the following command:

```
Install-Module -Name AzureAD
```

- [Microsoft Azure Az Module](#)

To install the module, enter the following command:

**Install-Module -Name Az**

- [Microsoft Teams cmdlets module](#)

To install the module, enter the following command:

**Install-Module MicrosoftTeams**

- (Optional) [SharePoint Online Management Shell](#) (x64 version)

To install the module, enter the following command:

**Install-Module -Name Microsoft.Online.SharePoint.PowerShell**

- A dedicated Active Roles Reporting domain service account is available.

**NOTE:** When using a dedicated Active Roles Reporting domain service account, you must explicitly grant **Log on as a batch job** user rights assignment on the Active Roles Reporting Server, as indirect membership will not work.

***To grant Log on as a batch job user rights assignment for the Active Roles domain service account***

1. On the Active Roles Reporting Server, right-click the Windows Start menu and click **Run**.
  2. Type `gpedit.msc` and click **OK**.
  3. Navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
  4. Double-click **Log on as a batch job** and add the Active Roles Reporting domain service account.
  5. To refresh the policy change and have it take effect immediately, open a Command Prompt and type `gpupdate /force`.
- The Active Roles Reporting domain service account must be a member of:
    - The Active Roles Administrators group, so that it can read all Active Roles configuration data. For more information on configuring the Active Roles Administrators group, see [First-time configuration of Active Roles On Demand](#)
    - (Optional) The local **Event Log Readers** group of the Active Roles Reporting Server to read all event logs from the **Active Roles Admin Service** event log. However, leveraging a Log Management or SIEM solution may be preferred instead.

***To install the Active Roles Collector and Report pack***

1. On the Active Directory Reporting Server, in the root folder of the extracted Active Roles installer (when using the .zip file) or the mounted .iso image, right-click `ActiveRoles.exe` and run it as an administrator.
2. On the **Introduction** screen, select the **Due to the new features...** check box, and review the linked license requirements. When you are ready, click **Next**.
3. In the **License Terms** step, select **I accept the terms in the license agreement** and click **Next**.

4. In the **Component Selection** step, select only **Management Tools** from the list, and specify the installation folder path.

## Active Roles



### Component Selection

Select the Active Roles components to install on this computer.

1 of 5 components selected

25 MB required

<input type="checkbox"/>	Administration Service	▼
<input type="checkbox"/>	Web Interface	▼
<input type="checkbox"/>	Console (MMC Interface)	▼
<input checked="" type="checkbox"/>	Management Tools	▼
<input type="checkbox"/>	Synchronization Service	▼

Path to installation folder:

C:\Program Files\One Identity\Active Roles\

Browse...

5. In the **Ready to Install** step, verify that only the Management Tools are selected and click **Install**.

**NOTE:** The **Install** button may be grayed out if any prerequisite software is missing at this point. All missing software are listed and linked in this step.

## Active Roles



### Ready to Install

Review the installation settings you have specified.

Before you install Active Roles, download and install the following prerequisite software

[SharePoint Online Management Shell - x64 Version \(Optional\)](#)

[Azure AD Module.](#)

[Azure Az Module.](#)

[Microsoft Teams.](#)

Active Roles components to install

Management Tools

Click Install to perform Active Roles installation.

Installation folder: C:\Program Files\One Identity\Active Roles\

[Back](#)[Install](#)[Cancel](#)

To finish the installation of the Active Roles Management Tools, install all listed prerequisite software, click **Back**, then **Next**, and finally **Install**, when it is enabled.

6. The installation will begin. Monitor the progress on the **Setup Progress** page. When installation is ready, on the **Completion** page, click **Finish**

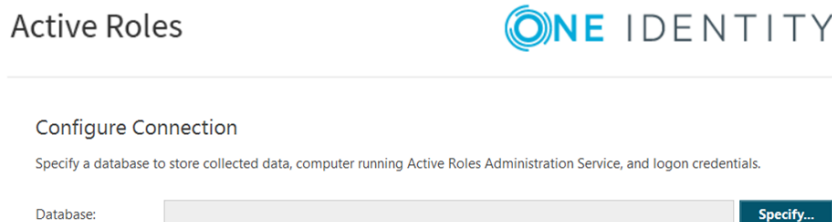
7. From the Active Roles source files of the extracted Active Roles installer (when using the .zip file) or the mounted .iso image, run the \Solutions\Collector and Report Pack\ActiveRolesCollectorAndReports\_7.5.3.msi package.
8. On the introduction screen, click **Next**.
9. In the **License Terms** step, accept the license terms and click **Next**.
10. In the **Installation Folder** step, enter the path where you want to install Active Roles Collector and Report Pack.
11. In the **Ready to Install** step, click **Install**, then click **Finish** when installation completed.

## Configuring the Active Roles Collector and Report Pack

If you have optionally installed the Active Roles Collector and Report Pack as described in [Installing the Active Roles Collector and Report Pack](#), you must configure it to use its data collection and reporting features.

### *To configure the Active Roles Collector and Report Pack*

1. From the Windows Start Menu, launch **One Identity Active Roles 7.5.3 > Active Roles 7.5.3 Collector and Report Pack**.
2. In the **Select Task** step, select **Collect data from the network** and click **Next**.
3. In the **Configure Connection** step, to specify a new data collection database, click **Specify** next to the **Database** field.



Active Roles

ONE IDENTITY

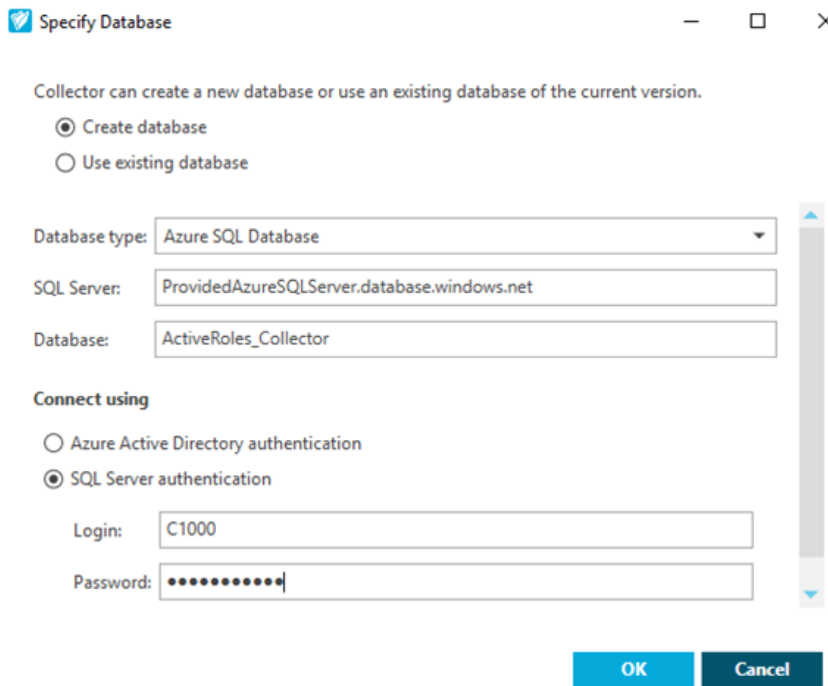
---

Configure Connection

Specify a database to store collected data, computer running Active Roles Administration Service, and logon credentials.

Database:  **Specify...**

4. In the **Specify Database** step, select **Create Database** and configure the following settings.



**Specify Database**

Collector can create a new database or use an existing database of the current version.

☒ Create database  
☐ Use existing database

Database type: Azure SQL Database

SQL Server: ProvidedAzureSQLServer.database.windows.net

Database: ActiveRoles\_Collector

**Connect using**

☐ Azure Active Directory authentication  
☒ SQL Server authentication

Login: C1000

Password: ••••••••

OK Cancel

- **Database Type:** Select **Azure SQL Database**.
- **SQL Server:** Enter the name of the Azure SQL server provided by One Identity.
- **Database:** Enter **ActiveRoles\_Collector**.
- **Connect using:** Select **SQL Server authentication** and enter the Azure SQL login credentials provided by One Identity to the **Login** and **Password** fields.

To continue configuration, click **OK**. The database will be created in the Azure SQL instance of your Active Roles SaaS tenant. When the database is created, the **Database** field of the **Configure Connection** step will be automatically populated.

5. In the **Configure Connection** step, specify the Active Roles Service server name in the **Active Roles Service** field, then select **Log on as > Specified user** and provide the login details of the Active Roles Reporting domain service account credentials created as a prerequisite for [Installing the Active Roles Collector and Report Pack](#).

## Configure Connection

Specify a database to store collected data, computer running Active Roles Administration Service, and logon credentials.

Database:  [Specify...](#)

Active Roles Service:

Log on as

☐ Current user

☒ Specified user

User name:

Password:

- In the **Data Collection Tasks** step, select **Active Directory** and **Policy Compliance Information** as the type of data that the Active Roles Collector and Report Pack will collect.

## Active Roles

## Data Collection Tasks

Select the data collection tasks you want to perform.

- ☒ **Active Directory**  
Collect information about users, groups, computers, organizational units, and domains from Active Directory.
- ☒ **Policy Compliance Information**  
Collect data to determine whether directory objects comply with the policies defined by Active Roles. Note that this option requires the Active Directory option to be selected.
- ☐ **Active Roles event log**  
Collect events from the Active Roles event log on the computers running Active Roles Administration Service.

**TIP:** You can also select **Active Roles event log** to collect application event logs with the Active Roles Collector and Report Pack. However, One Identity recommends to use a dedicated Log Management or SIEM solution to gather and archive event logs.

- In the **Data to Collect** step, select all categories except **Access Templates**, and click **Next**.

**NOTE:** Selecting all check boxes (including **Access Templates**) in this step will result in a data collection error as described in [Knowledge Base Article 230239](#) in the *One Identity Support Portal*.

This error occurs when configuring either an immediate or a scheduled data collection operation (configured with the **Now** and **On a schedule** settings of the **Select Operation Mode** step, respectively). When running an immediate data collection operation, this error is visible on the user interface. When performing a scheduled run, the error is logged only in the collector log file at the following location:

```
C:\ProgramData\One Identity\Active Roles\Logs\Collector\Collector-Active Roles Collector (<task-name>)-<timestamp>.log
```

8. In the **Select Domains or OUs** step, to specify a new domain with the **Browse for Container** dialog, click **Add**.
9. In the **Browse for Container** dialog, select the domain to use and click **OK**.

**NOTE:** If the domain to select is missing in this dialog, check the following:

- Make sure that **Use subtree search** is selected.
- Make sure that a domain has already been added to Active Roles as described in [Adding the first domain to the Active Roles Console](#). If no domain has been previously added, this dialog will be empty.

The selected domain will appear in the **Select Domains or OUs** step.

10. In the **Select Operation Mode** step, under **Run Active Roles Collector**, select **On a schedule** and name the mode (for example: **Daily Collection**).

Active Roles



#### Select Operation Mode

Select whether to perform the task immediately or to schedule it for a convenient time, and specify whether to disable SID resolving.

##### Run Active Roles Collector

☐ Now

☒ On a schedule

Name:

Description:

11. In the **Schedule** step, to specify a new data collection schedule, click **Add**.
12. In the **Configure Schedule** dialog, configure the schedule with the available settings and click **OK**.

**TIP:** One Identity recommends configuring a daily schedule that runs data collection in off-peak hours to minimize potential performance issues.

13. When the schedule is configured, it must appear in the **Schedule** step.

## Schedule

Click Change to set the time and day you want the task to start. Click Account to specify the user account under which the task will run.

Type	Start Time	Start Date	Details
Run on a daily basis	1:00 AM	4/30/2021	Recur every 1 days

Add...

Edit...

Remove

User account under which the task will run

User name: ActiveRoles\_ar-reporting

Password: .....

Back

Next

Cancel

Under **User account under which the task will run**, specify the Active Roles Reporting domain service account credentials.

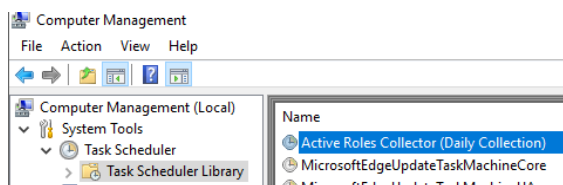
- To close the Active Roles Collector and Report Pack setup, click **Finish**.

**NOTE:** The log file of the configured logging operation is stored at the following location by default:

```
C:\ProgramData\One Identity\Active Roles\Logs\Collector\Collector-<date>-<time>.log
```

The ProgramData folder of the operating system is hidden by default.

- Confirm that the configured collection task is listed in the Windows Task Scheduler. Right-click the Windows Start Menu, and navigate to **Computer Management > System Tools > Task Scheduler > Task Scheduler Library**. In this example, the task is named Active Roles Collector (Daily Collection).



- To perform the first data collection run, right-click the **Active Roles Collector (Daily Collection)** task and select **Run**.
- When the task completed successfully, configure Active Roles Collector and Report Pack so that it deploys reports to a report server. Open **Active Roles Collector and Report Pack** again, and in the **Select Task** step, select **Deploy reports to Report Server**.



## Select Task

Select the task you want to perform.

- ☐ **Collect data from the network**  
Collect data and events from computers running Active Roles Administration Service, and store the collected information in a SQL Server database to make the information available for reporting.
- ☐ **Process gathered events**  
Export collected events to another SQL Server database, or delete obsolete events from the database.
- ☐ **Import events from an earlier database version**  
As Report Pack is only compatible with the current database version, you need to import events from the database of an earlier version to the database of the current version if you want to use those events for reporting.
- ☒ **Deploy reports to Report Server**  
Publish the reports from Active Roles Report Pack to your SQL Server Reporting Services (SSRS) Report Server.

Back

Next

Cancel

18. In the **Report Server** step, specify the **Report Server Web Service URL**.

## Report Server

Supply the address of the Report Server to which you want to publish the Active Roles reports.

Report Server Web Service URL:

If secure communication protocol (SSL) is enabled on Report Server, use https:// in Report Server Web Service URL.

Back

Next

Cancel

**TIP:** By default, Active Roles Collector and Report Pack may populate the **Report Server Web Service URL** field with an https:// scheme. Using this scheme if you do not have a valid certificate and SSL enabled for SQL Server Reporting Services will result in a **Verification Failed** error when Active Roles Collector and Report Pack attempts accessing the Report Web Server service.

To avoid this error, change https:// to http:// in the URL in such cases.

19. In the **Data Source** step, click **Configure Data Source**.
20. In the **Configure Data Source** dialog, configure the following settings:

Database type:

SQL Server:

Database:

## Connect using

- ☐ Azure Active Directory authentication
- ☒ SQL Server authentication

Login:

Password:

OK

Cancel

- **Database Type:** Select **Azure SQL Database**.
- **SQL Server:** Enter the name of the Azure SQL server provided by One Identity.
- **Database:** Enter **ActiveRoles\_Collector**.
- **Connect using:** Select **SQL Server authentication** and enter the Azure SQL login credentials provided by One Identity to the **Login** and **Password** fields.

When ready, click **OK** to return to the **Data Source** step. The **Database** field will display the configured data source.

21. Active Roles Collector and Report Pack will then start publishing the report definitions. Use the progress bar to check the publish status. When the process is completed:
  - To close the Active Roles Collector and Report Pack, click **Finish**.
  - To check the log of the procedure, click **View log**.


**NOTE:** The log file of the configured logging operation is stored at the following location by default:

```
C:\ProgramData\One Identity\Active Roles\Logs\Collector\Collector-<date>-<time>.log
```

The ProgramData folder of the operating system is hidden by default.

22. To validate whether Active Roles is present in the domain and that reporting works as configured, open the SQL Reporting Services web portal with the */Reports* path of your Active Roles server (<http://<FQDN-of-server>/Reports>). Navigate to **Active Roles > 7.5.3 > Active Directory Assessment > Domains > Domain Summary**, and verify that the page is populated with data reports.

**NOTE:** Starting from Active Roles 7.4.4, Internet Explorer is no longer supported by the Active Roles Web Interface. Therefore, One Identity recommends using one of the following supported browsers when using any web-based Active Roles 7.5.3 interfaces:

- Mozilla Firefox 36 (or newer)
  - Google Chrome 61 (or newer)
  - Microsoft Edge 79 (or newer), based on Chromium
23. To open the settings of the SQL Reporting Services web portal, click  > **Site Settings** at the top right corner of the page.
  24. To assign administrator privileges to the Active Roles administrators (configured in [First-time configuration of Active Roles On Demand](#)) for the configured Active Roles report, navigate to **Security > Add group or user**.
  25. In the **Group or user** field, enter the name of the Active Roles Administrators AD group (for example, ARAdmins). Under **Role**, select the **System Administrator** role. To close the dialog, click **OK**.

26. In the SQL Reporting Services web portal, confirm that the configured administrator group is now listed as **System Administrator**.

**TIP:** Even if the **Configure Data Source > Database type** option of the Active Roles Collector and Report Pack is set to **Azure SQL Database**, the SQL Reporting Services portal will identify it as **Microsoft SQL Server**.

This has no impact on the data collection operation, but you can still change the server type designation with the following steps:

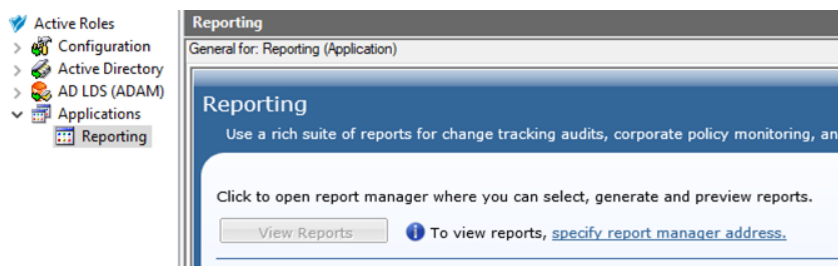
1. On the SQL Reporting Services web interface, navigate to **Active Roles > Shared Data Sources > Manage Active Roles 7.5.3 Report Data > Properties**.
2. Under **Connection**, change the **Type** from **Microsoft SQL Server** to **Microsoft Azure SQL Database**.

## Adding the Reporting Link to the Active Roles Console

When the Active Roles Collector and Report Pack is [installed](#) and [configured](#), add the reporting link to the Active Roles Console (also known as the MMC Interface).

### ***To add the reporting link to the Active Roles Console***

1. On a workstation where the Active Roles Console is installed, launch the Console from the Windows Start Menu by navigating to **One Identity Active Roles 7.5.3 > Active Roles 7.5.3 Console**.
2. In the left pane of the Active Roles Console, navigate to **Applications > Reporting**, and click **To view reports, specify report manager address**.



3. In the **Report Manager Address** dialog, enter the URL of the Active Roles Reports resource:

**http://<activeroles-server-name>.<domain-name>.com/Reports/browse/Active%20Roles/7.5.3**

4. To apply your changes, click **OK**.

The **Applications > Reporting > View Reports** button becomes enabled, allowing you to access the Active Roles reports from the Active Roles Console.

## Installing Active Roles Synchronization Service

Optionally, you can install the Active Roles Synchronization Service component to automate identity data synchronization between the data systems used in your organization.

**NOTE:** If you plan to manage Azure AD or Office 365 operations in your environment, you must install the Active Roles Synchronization Service component.

### Prerequisites

Before installing Active Roles Synchronization Service, make sure that the following hardware and software resources are available:

- An installed, configured and functional on-premises SQL server.
- An on-premises server to host Active Roles Synchronization Service. This can be the same server that hosts the on-premises Active Roles Reporting components (described in [Installing the Active Roles Collector and Report Pack](#)).
- The following PowerShell modules are available:
  - [Exchange Online PowerShell v2 module x64](#)

**NOTE:** Use version v2.0.3 of the module.

To install the module, enter the following command:

```
Install-Module -Name ExchangeOnlineManagement -RequiredVersion 2.0.3
```

- [Azure AD Module](#)

To install the module, enter the following command:

```
Install-Module -Name AzureAD
```

- [Microsoft Azure Az Module](#)

To install the module, enter the following command:

```
Install-Module -Name Az
```

- [Microsoft Teams cmdlets module](#)

To install the module, enter the following command:

```
Install-Module MicrosoftTeams
```

- (Optional) [SharePoint Online Management Shell](#) (x64 version)

To install the module, enter the following command:

```
Install-Module -Name Microsoft.Online.SharePoint.PowerShell
```

- .NET Framework 4.7.2 or newer.

- A domain service account with the required permissions. For more information, see [Active Roles KB Article 71413](#) on the One Identity Support Portal.

## To install Active Roles Synchronization Service

1. On the on-premises server that will host the Active Roles Synchronization Service component, navigate to and launch the Synchronization Service installer package. The file is available at the following location of the extracted Active Roles installer (when using the .zip file) or the mounted .iso image:

```
\Components\ActiveRoles Synchronization Service\SyncService.msi
```

**NOTE:** The installation will progress without interaction, and will complete without a completion prompt.

2. To launch the Synchronization Service Configuration Wizard, in the Windows Start Menu, click **Active Roles 7.5.3 Synchronization Service**.
3. In the **Service Account and Mode** step of the **Configuration Wizard**, configure the following settings:

### Configuration Wizard

#### Service Account and Mode

Enter the account under which you want Synchronization Service to run and specify whether you want to use this Synchronization Service in the local or remote mode.

#### Synchronization Service account

User name:

Password:

#### Synchronization Service mode:

- ☒ Local  
☐ Remote

Select the remote mode if you want to manage this Synchronization Service instance and connectors remotely.

- **Synchronization Service account:** Enter the domain service account credentials to use the Synchronization Service component (for example, ActiveRoles\ar-syncservice).
  - **Synchronization Service mode:** Select **Local**.
4. In the **Instance Configuration** step, select **Create a new configuration** and click **Next**.
  5. In the **Database Connection** step, configure the following settings:

#### Configuration Wizard

##### Database Connection

Specify SQL Server and databases where you want Synchronization Service to store its data.

SQL Server:

Database:

☒ Store sync data in a separate database

Synchronization database:

☐ Use Windows authentication

☒ Use SQL Server authentication

Login:

Password:

- **SQL Server:** Enter the name of the on-premises Azure SQL server.
- **Database:** Enter **ActiveRoles\_SyncSvcCfg** as the database name.

**NOTE:** Make sure that you enter the database name exactly as specified above.

6. Select **Store sync data in separate database**, and under **Synchronization database**, enter **ActiveRoles\_SyncSvcCfg**.
- NOTE:** Make sure that you enter the database name exactly as specified above.
7. Select the authentication method (**Use Windows authentication** or **Use SQL Server authentication**) preferred to access the on-premises Azure SQL server.
8. (Optional) In the **Configuration File** step, set up a password-protected backup of the configuration.

#### Configuration Wizard

##### Configuration File

Specify a file to save the Synchronization Service configuration profile you created in this wizard.

Configuration file:

☒ Protect the file with the following password:

Make sure you keep this file in a safe place. You will need to provide this file if you want another Synchronization Service instance to use the same configuration settings.

To specify the location of the configuration file, click **Browse**. To configure password-protection for the backup, check **Protect the file with the following**

**password** and enter the password for the file. To complete the configuration, click **Finish**.

| **NOTE:** Keep a copy of this file and password in a secure location for future use.

Active Roles then starts the configuration of Synchronization Service. Upon successful completion, the Synchronization Service component will open and will be ready to use.

| **TIP:** For more information about configuring Active Roles Synchronization Service for specific connectors, such as Azure AD or Microsoft 365, see the [Active Roles Synchronization Service Administration Guide](#).

# About us

---

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



# Contacting us

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

# Technical support resources

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

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

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