



Active Roles 8.2.1

Installation Guide

Copyright 2024 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 website (<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/trademark-information.aspx. 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 Installation Guide
Updated - 07 December 2024, 13:35

For the most recent documents and product information, see [Online product documentation](#).

Contents

Introduction	6
Active Roles components	6
Active Roles Setup package	7
System requirements	10
Prerequisites of installing Active Roles	23
Prerequisites of installing the Administration Service	23
Minimum required permissions for the Active Roles service account	25
Service publication in Active Directory	29
Configuring the Administration Service account	31
Access to managed domains	31
Configuring access to Exchange organizations	31
Configuring the permission to read Exchange configuration data	32
Support for remote Exchange Management Shell	33
Access to managed AD LDS instances	34
Access to file servers	34
Access to BitLocker recovery information	35
SQL Server permissions	35
Configuration permissions	36
Operation permissions	37
Replication configuration permissions	39
Replication Agent permissions	40
Installing Active Roles	42
Rolling back to a previous Microsoft OLE DB Driver for SQL Server version	43
Deploying the Administration Service	45
Installing the Administration Service	45
Configuring the Administration Service	46
Backing up the encryption key	47
Configuring an additional Administration Service instance	49
Using a common database for the Administration Service	50
Using the database of an earlier Administration Service installation	51

Using a pre-created blank database	53
Deploying user interfaces	54
Installing the Active Roles Console	54
Restricting access to the Active Roles Console	55
Deploying the Web Interface	56
Installing the Web Interface	56
Performing the initial configuration of the Web Interface	57
Creating or modifying a Web Interface site	59
Configuring the Web Interface for secure communication	61
Deleting a Web Interface site	62
Installing optional tools and components	63
Installing only the Management Shell, ADSI Provider and SDK	63
Installing the Data Collector and Report Pack	64
Installing the Data Collector	64
Deploying the Report Pack	65
Installing the Add-on Manager	66
Installing the Diagnostic Tools	66
Using the System Checker	67
Silent installation of Active Roles components	68
Uninstalling Active Roles	72
Using Active Roles to manage Azure AD objects	73
Configuring Active Roles to manage Azure AD using the Active Roles Configuration Center	73
Configuring a new Azure tenant and consenting Active Roles as an Azure application	73
Importing an Azure tenant and consenting Active Roles as an Azure application	78
Configuring Active Roles to manage hybrid AD objects	82
Active Roles availability on Azure and AWS Marketplace	83
AWS and Azure virtual environment recommendations	83
Supported AWS and Azure environment types	84
Configuring a hybrid on-premises environment for Active Roles	85
Creating Azure or AWS virtual machines for Active Roles	87
Opening communication ports for the Active Roles virtual machine	88
Configuring the Azure or AWS virtual machine	89
Deploying Active Roles on Microsoft Azure VM	90

Configuring Active Roles for AWS Managed Microsoft AD	93
Supported AWS Managed Microsoft AD deployment configuration	93
Deployment requirements for AWS Managed Microsoft AD support	94
Main steps of configuring Active Roles for AWS Managed Microsoft AD	95
Creating the AWS Managed Microsoft AD instance	95
Creating the EC2 instance for Active Roles	96
Joining the EC2 instance to AWS Managed Microsoft AD	96
Creating the RDS instance for the Active Roles SQL Server	97
Verifying connectivity between the EC2 and RDS instances	98
Installing and configuring Active Roles on the EC2 instance	99
About us	102
Contacting us	102
Technical support resources	102

Introduction

This document describes how to install One Identity Active Roles and its components, deploy its services in your organization, or uninstall it.

Active Roles simplifies creating and managing user accounts and groups in Windows Active Directory (AD) environments by automating the following:

- User and group account management in AD and Azure AD.
- Mailbox management in Exchange and Exchange Online.
- Group population, and resource assignment in Windows.

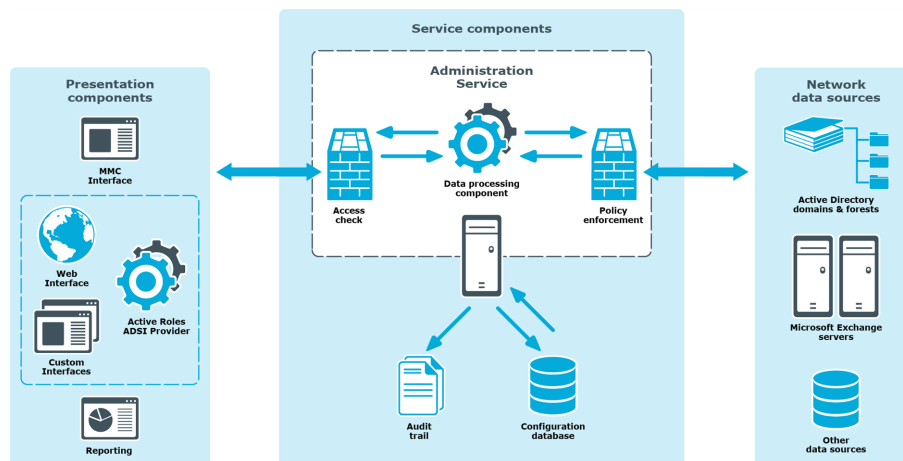
Active Roles enforces security, automates directory management tasks, and provides change approval and a Web Interface.

Active Roles components

Active Roles divides directory administration into 3 functional layers:

- Presentation components
- Service components
- Network data sources.

Figure 1: Active Roles Components



- **Presentation components** are client interfaces for Windows and the Web, allowing users with sufficient rights to perform a defined set of administrative operations. Active Roles can also generate reports on administrative operations.
- **Service components** provide a secure layer between administrators and managed data sources. Service components enforce policies, provide automation capabilities, and integrate business processes for administering Active Directory, Exchange and other corporate data sources.
- **Network data sources** are managed by the Administration Service, a rules-based proxy that is the main component of Active Roles. The Administration Service acts as a bridge between the presentation components and network data sources.

You can use the Administration Service's delegation capabilities to enforce administrative policies that keep data up-to-date and accurate. In large networks, you can deploy multiple instances of Administration Services to improve performance and ensure fault tolerance.

The Administration Service uses the configuration database to store configuration data. Configuration data includes definitions of objects specific to Active Roles, assignments of administrative roles and policies, and procedures used to enforce policies.

The Administration Service provides a complete audit trail by creating records in the Active Roles event log. The log shows all actions performed, including unpermitted actions. The log entries display the success or failure of each action, as well as the attributes that were changed while managing objects in data sources.

Active Roles Setup package

The Active Roles folder contains the following files and folders:

- ActiveRoles.exe
- Components
- Redistributables
- Tools

Content	Description
ActiveRoles.exe	The .exe file allows you to start the setup wizard and install the Active Roles components.
Components	<p>This folder contains separate installer files for the following default components, allowing you to install them individually:</p> <ul style="list-style-type: none"> • Administration Service: The core service of Active Roles, ensuring the reliable enforcement of administrative policies that keep directory data accurate and up-to-date. • ADSI Provider: Enables custom user interfaces and applications to access Active Directory services through Active Roles. • Configuration Center: • Console (also known as the MMC Interface): A comprehensive administrative tool used to manage Active Directory and Microsoft Exchange resources, configure access and administration policies, and set up automation or approval workflows. • Management Shell: Provides Windows PowerShell-based command-line tools (cmdlets), allowing you to run and automate administrative tasks in Active Roles. • Synchronization Service: Automates the process of identity data synchronization among various data systems used in your enterprise environment. • Web Interface: A highly customizable web application, providing administrative coverage for all aspects of Active Directory and Azure AD data management.
Redistributables	<p>This folder contains the following redistributables required by the latest Active Roles version:</p> <ul style="list-style-type: none"> • Microsoft OLE DB Driver 19 for SQL Server • Microsoft .NET Framework 4.8 • Microsoft .NET Framework 4.8 Developer Pack • Microsoft Visual C++ 2015-2022 Redistributable (x64, X86) • Microsoft Edge WebView2 Runtime
Tools	This folder contains the installer files for the following additional

Content

Description

components:

- **Add-in for Outlook:** Allows you to process and submit approvals via Microsoft Outlook. Install this component on a computer running Microsoft Outlook.
- **Add-on Manager:** Allows you to install and manage addons for Active Roles, or even create new addons with its addon editor.
- **Administrative Template:** Allows you to control the behavior and appearance of the Active Roles Console via Group Policy.
- **Data Collector and Report Pack:** Allows you to collect Administration Service data and store them in an on-premises SQL Server or Azure SQL database for reporting purposes.
- **Configuration Transfer Wizard:** Allows you to export your Active Roles configuration resources (such as Access Templates, Managed Units, Policy Objects, Policy Types and so on) to an XML file, then import them to another Active Roles instance.
- **Diagnostic Tools:** Provides you optional tools to check system requirements, logs and changes in your Active Directory domain.
- **Management Pack for SCOM:** Allows you to monitor your Active Roles environment and configure alerts for various error conditions.
- **SPML Provider:** Allows you to exchange user, resource, and service-provisioning information between SPML-enabled enterprise applications and Active Directory.
- **Synchronization Service Capture Agent:** Allows you to synchronize user passwords between Active Directory domains managed by Synchronization Service and other connected data systems.

System requirements

Before installing Active Roles 8.2.1 in an on-premises environment, ensure that your system meets the following minimum hardware and software requirements.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. For more information about environment virtualization, see [One Identity's Product Support Policies](#).

To authenticate and communicate with Azure, the Active Roles Service must have access to the following Microsoft endpoints:

- <https://login.microsoftonline.com/>
- <https://developer.microsoft.com/graph>
- <https://graph.windows.net/>

To manage Azure Active Directory resources, you must install the following prerequisites in the Active Roles Configuration Center.

TIP: To run the PowerShell commands of the following modules, use the 64-bit version of Windows PowerShell.

Requirement	Version	Details
NuGet package provider	Minimum: 2.8.5.201 Maximum: 3.0.0.1	You must install the NuGet package provider on the computer(s) running an Active Roles Administration Service instance or Active Roles Synchronization Service. For more information, see Install-PackageProvider in the <i>Microsoft Package Management documentation</i> .
Exchange Online PowerShell V3 module	Minimum: 3.0.0 Maximum: 3.5.0	You must install the Exchange Online PowerShell module on the computer(s) running an Active Roles Administration Service instance or Active Roles Synchronization Service. For more information, see About the Exchange Online PowerShell module in the <i>Microsoft Exchange PowerShell documentation</i> .

Requirement	Version	Details
Az.Accounts PowerShell module	Minimum: 2.10.3 Maximum: 2.12.1	You must install the Az.Accounts PowerShell module on the computer(s) running an Active Roles Administration Service instance or Active Roles Synchronization Service. For more information, see Az.Accounts in the <i>Microsoft PowerShell Gallery</i> .
Az.Resources PowerShell module	Minimum: 6.4.1 Maximum: 6.6.0	You must install the Az.Resources PowerShell module on the computer(s) running an Active Roles Administration Service instance. For more information, see Az.Resources in the <i>Microsoft PowerShell Gallery</i> .
Microsoft Graph PowerShell module	Maximum: 2.17.0	You must install the Microsoft Graph PowerShell module on the computer(s) running an Active Roles Administration Service instance. For installation instructions, see Microsoft Graph in the <i>Microsoft PowerShell Gallery</i> .
Microsoft Edge WebView2 Runtime	N/A	If no web browser is installed on the machine where you want to install and use Active Roles, download the Microsoft Edge Webview 2 Runtime installer with the following PowerShell command: <pre>Invoke-WebRequest -Uri "https://go.microsoft.com/fwlink/p/?LinkId=2124703" -OutFile "\$([System.IO.Path]::Combine ([System.Environment]::GetFolderPath ('UserProfile'), 'Downloads', 'MicrosoftEdgeWebView2Setup.exe'))"</pre> After the download is finished, locate the installer in your Downloads folder and run it.
(Optional) One Identity certificate	N/A	If your organization enforces the AllSigned policy, you must install the One Identity certificate during the installation of Active Roles.

⚠ CAUTION: When importing PowerShell modules with the `$context.0365ImportModules` function, they are imported with the versions specified in the configuration of the Azure-specific prerequisites.

However, after importing the specified versions of the required PowerShell modules, running PowerShell cmdlets without passing them as a string to the `$context.0365ImportModules` function can cause inconsistent behavior in Active Roles. This is because if there are multiple versions of the same PowerShell module installed on the computer running the Active Roles server, PowerShell modules containing the script to run can be imported automatically with different versions.

To avoid inconsistent behavior in Active Roles by importing different PowerShell versions, run PowerShell modules only by passing them as a string to the `$context.0365ImportModules` function.

Hardware requirements

Table 1: Hardware requirements

Requirement	Details
Processor	<p>For Administration Service, Web Interface and Synchronization Service, any of the following:</p> <ul style="list-style-type: none">• Intel 64 (EM64T)• AMD64• Minimum 2 cores• CPU speed: 2.0 GHz or faster <p>NOTE: For Active Roles Synchronization Service, One Identity recommends using a multi-core CPU for the best performance.</p> <p>For Console, SPML Provider and Management Tools, any of the following:</p> <ul style="list-style-type: none">• Intel x86• Intel 64 (EM64T)• AMD64• CPU speed: 1.0 GHz or faster.
Memory	<p>Administration Service: A minimum of 4 GB of RAM.</p> <p>Web Interface, Synchronization Service: A minimum of 2 GB of RAM.</p> <p>Console, SPML Provider and Management Tools: A minimum of 1 GB of RAM.</p>
Hard disk space	<p>Administration Service, Web Interface, Console, SPML Provider and Management Tools: A minimum of 100 MB of free disk space.</p> <p>Synchronization Service: A minimum of 250 MB of free disk space.</p> <p>NOTE: If SQL Server and Synchronization Service are installed on the same computer, the amount required depends on the size of the Synchronization Service database.</p>
Operating system	You can install any of the Active Roles components

Requirement

Details

on a computer running:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016

Active Roles supports the Standard or Datacenter edition of these operating systems.

In addition, you can install the Active Roles Console and Management Tools on a computer running:

- Microsoft Windows 11, Professional or Enterprise edition.
- Microsoft Windows 10, Professional or Enterprise edition, 32-bit (x86) or 64-bit (x64).

Component requirements

CAUTION: To avoid inconsistent behavior in Active Roles when managing Azure Active Directory resources, you must enable Transport Layer Security (TLS) protocol version 1.2. For more information, see [TLS 1.2 enforcement for Azure AD Connect](#) in the *Microsoft Azure documentation*.

All Active Roles components require:

- Microsoft .NET Framework 4.8. For more information, see [Installing .NET Framework for developers](#) in the *Microsoft .NET documentation*.
- Visual C++ 2017 Redistributable.

Table 2: Administration Service requirements

Requirement	Details
SQL Server	<p>You can host the Active Roles database on the following SQL Server versions:</p> <ul style="list-style-type: none">• Microsoft SQL Server 2022, any edition.• Microsoft SQL Server 2019, any edition.• Microsoft SQL Server 2017, any edition.• Microsoft SQL Server 2016, any edition.• Azure SQL hosted databases. <p>To connect Active Roles to a Microsoft SQL Server deployment, install Microsoft OLE DB Driver for SQL Server (MSOLEDBSQL).</p>

IMPORTANT: Starting from version 8.2, Active Roles supports (and its installer is shipped with) Microsoft OLE DB Driver 19.x for SQL Server. However, Active Roles still supports earlier OLE DB Driver versions as well (18.4 or newer).

- If you upgrade to Synchronization Service 8.2.1 from an earlier version and you want to keep using an earlier version of Microsoft OLE DB Driver (version 18.4 or newer), this change has no impacts on your Synchronization Service installation.
- If you upgrade to Synchronization Service 8.2.1 from an earlier version or performed a clean installation, and you want to use Microsoft OLE DB Driver 19.x for SQL Server due to security concerns, make sure that your SQL Server has a certificate trusted by the Synchronization Service server that is assigned to the SQL service network protocols.

To use SSL with your SQL Server, configure a valid certificate. For more information on installing or viewing certificates for SQL Server via SQL Server Configuration Manager, see [Certificate management](#) in the *Microsoft SQL Server documentation*.

For general information about the encryption and certificate requirements of Microsoft OLE DB Driver 19.x, see [Encryption and certificate validation in OLE DB](#) and [Certificate requirements for SQL Server](#) in the *Microsoft SQL Server documentation*.

When configuring the SSL connection, consider the following:

- Microsoft OLE DB Driver 19.x for SQL Server requires a certificate from a Certificate Authority and no longer accepts self-signed certificates. For more information on how to access a Certificate Authority, see [Certification Authority Guidance](#) in the *Microsoft Windows Server documentation*.
- The Service Account running the SQL Server service must have permission to view the private key from the server certificate. For more information, see [Configure SQL Server Database Engine for encrypting connections](#) in the *Microsoft SQL Server documentation*.
- Microsoft OLE DB Driver 19.x for SQL Server requires specifying the Service Principal Names (SPNs). For more information, see the following *Microsoft SQL Server documentation* resources:
 - [Service Principal Name \(SPN\) Support in Client Connections](#)
 - [Service Principal Names \(SPNs\) in Client](#)

Requirement	Details
	<p>Connections (OLE DB)</p> <ul style="list-style-type: none"> • Service Principal Names (SPNs) in Client Connections (OLE DB) in SQL Server Native Client • You might need to change your SQL connection string to match the certificate and the SPN. For more information, see Using Connection String Keywords with OLE DB Driver for SQL Server in the <i>Microsoft SQL Server documentation</i>.
Windows Management Framework	Windows Management Framework 5.1 (available for download) is required on all supported operating systems.
Operating system on domain controllers	<p>The product retains all of its features and functions when managing Active Directory on domain controllers running any of these operating systems, any edition, with or without any Service Packs:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 <p>NOTE: The supported domain functional level is Windows Server 2008 R2 or higher.</p>
Exchange Server	<p>Active Roles is capable of managing Exchange recipients on:</p> <ul style="list-style-type: none"> • Microsoft Exchange Server 2019 • Microsoft Exchange Server 2016

Table 3: Web Interface requirements

Requirement	Details
Internet Services	<p>Active Roles Web Interface requires the Web Server (IIS) server role with the following role services:</p> <ul style="list-style-type: none"> • Web Server/Common HTTP Features/ <ul style="list-style-type: none"> • Default Document • HTTP Errors • Static Content • HTTP Redirection • Web Server/Security/ <ul style="list-style-type: none"> • Request Filtering • Basic Authentication • Windows Authentication

Requirement	Details
	<ul style="list-style-type: none"> • Web Server/Application Development/ <ul style="list-style-type: none"> • .NET Extensibility • ASP • ASP.NET • ISAPI Extensions • ISAPI Filters • Management Tools/IIS 6 Management Compatibility/ <ul style="list-style-type: none"> • IIS 6 Metabase Compatibility
Feature delegation	<p>Internet Information Services (IIS) must provide Read/Write delegation for the following features:</p> <ul style="list-style-type: none"> • Handler Mappings • Modules <p>To confirm that these features have the Read/Write delegation configured, use the Feature Delegation option of the native Internet Information Services (IIS) Manager tool of the operating system.</p>
.NET Trust Levels	<p>The .NET Trust Level must be set to Full (internal) on every computer where the Web Interface component is installed.</p> <p>To configure this setting:</p> <ol style="list-style-type: none"> 1. In the system-provided Internet Information Services (IIS) Manager tool, under Connections, expand the node of the computer, and navigate to Sites > Default Web Site. 2. On the Default Web Site Home page, double-click .NET Trust Levels. 3. Under Trust level, select Full (internal). <p>NOTE: Setting the .NET Trust Level to any other value will result in a failure when attempting to load any of the configured Active Roles Web Interface sites.</p>
Web browser	<p>You can access Active Roles Web Interface using:</p> <ul style="list-style-type: none"> • Mozilla Firefox 36 (or newer) on Windows. • Google Chrome 61 (or newer) on Windows. • Microsoft Edge 79 (or newer), based on Chromium on Windows 10 and 11. <p>You can use a later version of Firefox and Google Chrome to access Active Roles Web Interface. However, the Active Roles Web Interface was tested only with the browser versions listed above.</p>
Minimum screen	Active Roles Web Interface is optimized for screen resolutions of

Requirement	Details
resolution	1280x800 or higher. The minimum supported screen resolution is 1024x768.

Table 4: Console requirements

Requirement	Details
Web browser	Active Roles Console requires Microsoft Edge 79 (or newer), based on Chromium.

Table 5: Management Tools requirements

Requirement	Details
Windows Management Framework	Windows Management Framework 5.1 (available for download) is required on all supported operating systems.
Remote Server Administration Tools (RSAT)	To manage Terminal Services user properties by using Active Roles Management Shell, Active Roles Management Tools requires Remote Server Administration Tools (RSAT) for Active Directory. For more information on installing the RSAT version applicable to your operating system, see Remote Server Administration Tools (RSAT) for Windows in the <i>Microsoft Windows Server documentation</i> .

Table 6: Synchronization Service requirements

Requirement	Details
Operating system on domain controllers	The product retains all of its features and functions when managing Active Directory on domain controllers running any of these operating systems, any edition, with or without any Service Packs: <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 <p>NOTE: The supported domain functional level is Windows Server 2008 R2 or higher.</p>
SQL Server	You can host the Active Roles Synchronization Service database on: <ul style="list-style-type: none"> • Microsoft SQL Server 2022, any edition. • Microsoft SQL Server 2019, any edition. • Microsoft SQL Server 2017, any edition. • Microsoft SQL Server 2016, any edition. • Azure SQL hosted databases.

Requirement	Details
Windows Management Framework	Windows Management Framework 5.1 (available for download) is required on all supported operating systems.
Supported connections	<p>Active Roles Synchronization Service can connect to the following data systems:</p> <ul style="list-style-type: none"> Data sources accessible via an OLE DB provider. <p>NOTE: To create a connection to an OLE DB-compliant relational database, the OLE DB Connector requires any version of Microsoft OLE DB Driver for SQL Server that is supported by Microsoft to be installed on the machine running Active Roles Synchronization Service.</p> <p>The Active Roles installer is shipped with and automatically installs Microsoft OLE DB Driver 19.x for SQL Server.</p> <ul style="list-style-type: none"> Delimited text files. IBM AS/400, IBM Db2, and IBM RACF systems. LDAP directory service. Micro Focus NetIQ Directory systems. The following Microsoft services and resources: <ul style="list-style-type: none"> Active Directory Domain Services (AD DS) with the domain or forest functional level of Windows Server 2016 or higher. Active Directory Lightweight Directory Services (AD LDS) running on any Windows Server operating system supported by Microsoft. Azure Active Directory (Azure AD) using Microsoft Graph API version 1.0. Exchange Online services. Exchange Server with the following versions: <ul style="list-style-type: none"> Microsoft Exchange Server 2019 Microsoft Exchange Server 2016 Lync Server version 2013 with limited support. SharePoint 2019, 2016, or 2013. SharePoint Online service. Skype for Business 2019, 2016 or 2015. Skype for Business Online service. SQL Server, any version supported by Microsoft. One Identity Active Roles version 7.4.3, 7.4.1, 7.3, 7.2, 7.1, 7.0,

Requirement	Details
	<p>and 6.9.</p> <ul style="list-style-type: none"> • One Identity Manager version 8.0 and 7.0 (D1IM 7.0). • OpenLDAP directory service. • Oracle Database, Oracle Database User Accounts, and Oracle Unified Directory data systems. • MySQL databases. • Salesforce systems. • SCIM-based data systems. • ServiceNow systems.
Legacy Active Roles ADSI Provider	To connect to Active Roles version 6.9, install the Active Roles ADSI Provider. For more information, see <i>Installing additional components</i> in the <i>Active Roles Installation Guide</i> .
One Identity Manager API	To connect to One Identity Manager 7.0, install One Identity Manager Connector on the computer running Active Roles Synchronization Service. This connector works with the RESTful web service and no SDK installation is required.
Internet connection	To connect to cloud directories or online services, the machine running Active Roles Synchronization Service must have a stable Internet connection.

Table 7: Synchronization Service Capture Agent requirements

Requirement	Details
Operating system	<p>The DCs on which you install Active Roles Synchronization Service Capture Agent must run one of the following operating systems with or without any Service Pack:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 <p>For more information, see the <i>Active Roles Synchronization Service Administration Guide</i>.</p>

Table 8: Language Pack requirements

Requirement	Details
Active Roles version	The Active Roles 8.2.1 Language Pack requires Active Roles version 8.2.1 of the Administration Service, Configuration Center, Console, Synchronization Service or the Web Interface installed on the target machine.

Requirement	Details
	The Active Roles 8.2.1 Language Pack will not work properly with earlier versions of Active Roles.
Operating system	You can install the Active Roles Language Pack on 64-bit operating systems only.

Table 9: Add-on Manager requirements

Requirement	Details
Processor	Any of the following: <ul style="list-style-type: none"> • Intel 64 (EM64T) • AMD64 • CPU speed: 1.0 GHz or faster
Memory	A minimum of 1 GB of RAM.
Hard Disk Space	A minimum of 100 MB of free disk space.
Operating System	Any of the following Windows Server operating systems: <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 <p>In addition, you can also install Add-on Manager on a computer running:</p> <ul style="list-style-type: none"> • Microsoft Windows 11, Professional or Enterprise edition. • Microsoft Windows 10, Professional or Enterprise edition, 64-bit (x64)
Active Roles Console	Add-on Manager requires Active Roles 8.2.1 Console installed.
Microsoft Windows PowerShell	Windows PowerShell 5.1 or later
Web Browser	Microsoft Edge 79 or newer (based on Chromium)

Table 10: Diagnostic Tools requirements

Requirement	Details
Processor	1.0 GHz or faster 32-bit (x86) or 64-bit (x64) CPU.
Memory	A minimum of 1 GB of RAM.

Requirement	Details
	NOTE: The amount of RAM required depends on the size of the log file opened with the Log Viewer tool.
Hard disk space	A minimum of 10 MB of free disk space.
Operating system	Any of the following Windows Server operating systems: <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016

Table 11: Data Collector and Reporting Pack requirements

Requirement	Details
Processor	Any of the following: <ul style="list-style-type: none"> • Intel x86 • Intel 64 (EM64T) • AMD64 • CPU speed: 2.0 GHz or faster.
Memory	A minimum of 2 GB of RAM.
Hard disk space	<ul style="list-style-type: none"> • 12 MB for the Data Collector and Reporting Pack. • 10 GB for the SQL Server Reporting Services.
Operating system	Any of the following Windows Server operating systems: <ul style="list-style-type: none"> • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016
SQL Server and SQL Server Reporting Services	You can host the Active Roles Data Collector and Reporting Pack on the following SQL Server versions: <ul style="list-style-type: none"> • Microsoft SQL Server 2022, any edition. • Microsoft SQL Server 2019, any edition. • Microsoft SQL Server 2017, any edition. • Microsoft SQL Server 2016, any edition. • Azure SQL hosted databases.

Requirement	Details
Active Roles ADSI Provider	<ul style="list-style-type: none"><li data-bbox="587 271 1007 293">• Azure SQL hosted databases. <p data-bbox="539 322 1374 385">To connect Active Roles to a Microsoft SQL Server deployment, install Microsoft OLE DB Driver for SQL Server (MSOLEDBSQL).</p> <p data-bbox="539 409 1278 439">Active Roles 8.2.1 Management Tools must be installed.</p>

Prerequisites of installing Active Roles

The following sections describe the prerequisites of installing Active Roles:

- [Prerequisites of installing the Administration Service](#)
- [Minimum required permissions for the Active Roles service account](#)
- [Configuring the Administration Service account](#)
- [SQL Server permissions](#)

Prerequisites of installing the Administration Service

Active Roles requires [Microsoft .NET Framework 4.8](#).

The Administration Service requires Microsoft SQL Server or Azure SQL database server. You can install SQL Server on the Administration Service computer or on a different network computer. If you do not have Microsoft SQL Server deployed in your environment, download one of the versions officially supported by Active Roles (as listed in [System requirements](#)) from the [Microsoft Download Center](#).

Azure SQL Database variants supported in Active Roles are Azure SQL database, Azure SQL Managed Instance, and Azure SQL Elastic Pool.

Now that you have access to SQL Server, you can install the Administration Service.

Use the following checklist to ensure that you are ready to install the Administration Service.

Table 12: Checklist: Deploying the Administration Service

Item to Check	Description
Administration Service	The Administration Service can be installed on any computer that meets the hardware and software requirements.

Item to Check	Description
computer	It is not mandatory to install the Administration Service on a domain controller. However, the Administration Service computer must have reliable network connections with at least one of the domain controllers for each managed domain.
SQL Server	The Administration Service requires Microsoft SQL Server. One Identity recommends to have SQL Server and the Administration Service on different systems with reliable network connection. Administration Service can now be configured on Azure databases, namely Azure SQL database, Azure SQL Managed Instance and Azure SQL Elastic Pool. One Identity recommends to have proper network topology to allow the Azure database configuration.
Administration Service account	<p>The Administration Service logs in with the account that you specify during installation. The account must have sufficient rights for Active Roles to function properly. For more information on the minimum required permissions, see Minimum required permissions for the Active Roles service account.</p> <p>Active Roles uses the Administration Service account when accessing a managed domain unless an override account is specified when registering the domain with Active Roles. Therefore, the Administration Service account must have the appropriate rights in any domain for which an override account is not specified.</p> <p>Additionally, the Administration Service account must have sufficient permissions to publish the Administration Service in Active Directory. Information about how to configure the Administration Service account and an override account can be found later in this document.</p>
Account used for connection to SQL Server	<p>When installing the Administration Service you may configure it to use; Windows authentication or SQL Server authentication or Azure AD authentication.</p> <p>If you choose Windows authentication, the connection is established using the Administration Service account. In this case, the service account must be, at minimum, a member of the db_owner fixed database role and have the default schema of dbo in the Active Roles database.</p> <p>If you choose SQL Server authentication, the connection is established with the login you are prompted to specify when installing the Administration Service. This login must at minimum be a member of the db_owner fixed database role and have the default schema of dbo in the Active Roles database.</p> <p>For connecting to Azure SQL database variants like SQL database and Elastic Pool database using SQL server authentication, the login must be a member of the dbmanager fixed database role and have the</p>

Item to Check	Description
Active Roles Admin	<p>default schema of dbo in the Active Roles database.</p> <p>If you choose Azure Active Directory authentication, the connection is established with the login you are prompted to specify when installing the Administration Service.</p> <p>For more information on what permissions must be granted to the account for connection to SQL Server, see SQL Server permissions.</p> <p>Active Roles Admin is a group for which Active Roles does not perform permission checking. If the Administration Service itself has sufficient rights to perform a certain task, then Active Roles Admin can also perform that task using Active Roles.</p> <p>In addition, Active Roles Admin is authorized to perform any task related to the Active Roles configuration, such as adding managed domains and managing replication settings. Therefore, the membership in the Active Roles Admin group should be restricted to highly trusted individuals.</p> <p>By default, Active Roles Admin is the Administrators local group on the computer running the Administration Service. You can change this setting when installing the Administration Service.</p>

Minimum required permissions for the Active Roles service account

To properly perform operations on objects on behalf of delegated users, the Active Roles service account requires a number of permissions. One Identity recommends that you give the Active Roles proxy account the Domain Admin membership to ensure that Active Roles has all the required access.

You can separate the tasks managed by the Active Roles service account by using domain management to specify different accounts for the Active Roles service and for managing the domain.

The service account credential has five main roles:

- Accessing local resources on the Active RolesAdministration Service host. This requires the Active Roles service account to be a member of the **Administrators** group on the computer running the Administration Service.
- Creating the Service Connection Point in Active Directory.

After configured, the Administration Service attempts to publish itself in Active Directory, so that Active Roles clients can automatically discover the Administration Service instance.

NOTE: While this functionality is not critical, if the service publication permissions are not provided, Active Roles clients will not be able to automatically discover the Active Roles Administration Service instance. However, they can still connect to the Administration Service if they specify in Active Roles Console either the service name or the IP address of the computer running the instance.

For more information, see [Service publication in Active Directory](#).

- Running all script modules under the security context of the Active Roles service account. The permissions that custom scripts require will vary according to the needs of the scripts, so review them on a case-by-case basis as a best practice security model.
- (Optional) Connecting to the Microsoft SQL database. This step might also require specifying an SQL authentication credential.

In some configurations, assigning these permissions to the service account is optional, as it requires specifying an SQL authentication credential and assigning the necessary permissions to that SQL authentication credential.

For more information on the necessary SQL Server permissions, see [SQL Server permissions](#).

- (Optional) Synchronizing native permissions to Active Directory. Perform this step only if Active Roles is configured to do so.

The Active Roles service account must have the **Read Permissions** and **Modify Permissions** rights on the Active Directory objects and containers where it is needed to use the Active Roles security synchronization feature.

NOTE: If you use the service account for domain management, you must also give the service account the permissions for domain management accounts.

NOTE: Due to a known issue (275523), in the Active Roles Console, in **Active Directory > <domain-name> - Deleted Objects**, opening the **Advanced Properties** of a deleted object and selecting the **Show all possible attributes** check box results in an error message and stops the Active Roles Service.

As a workaround, One Identity recommends adding your service account as a member of the **Domain Admins** group.

Table 13: Permissions required by the Active Roles service account and the group Managed Service (gMSA) account used as service account

	Permissions	Requirement reason	Affected features
SQL Server	db_owner	Required to use the Configuration and Management History databases.	All Active Roles features that rely on the database (for example, virtual attributes, workflows, policies, Management History, and so on).
	db_creator	Required by the Active Roles	Creating the database

Permissions	Requirement reason	Affected features	
	Service to create the Configuration and Management History databases. You can omit this permission if you pre-create the database.	with the Active Roles Installer during initial configuration.	
db_datareader	Required by the source database when importing databases.	Database import	
Active Roles Server Local Computer (lusrmgr.msc)	Member of Administrators group on local computer	Required by the Administration Service account to access local resources on the computer.	Active Roles requires this permission to function properly.

Table 14: Permissions required by the domain management account (service or override account)

Permissions	Requirement reason	Affected features	
ADSI Edit (adsiedit.msc)	<p>In the System/Aelita sub-container:</p> <ul style="list-style-type: none"> • Create Container objects • Create serviceConnection Point objects <p>In the System container:</p> <ul style="list-style-type: none"> • Delete the serviceConnection Point objects <p>Replicating directory changes on the following AD partitions:</p> <ul style="list-style-type: none"> • Domain (Default Naming Context) • Configuration • Schema <p>For the Microsoft Exchange container:</p>	<p>Required by the Active Roles Service to publish itself to Active Directory. These permissions are not mandatory, but they help clients automatically discover the Active Roles Service.</p> <p>Active Roles Service monitors the AD partitions with directory synchronization (DirSync), and requires this permission to enable domain management capabilities.</p> <p>You can set this permission in the</p>	<p>Service publication</p> <p>Domain management capabilities</p> <p>Exchange management tasks</p>

Permissions	Requirement reason	Affected features
<ul style="list-style-type: none"> List contents Read all properties 	<p>Configuration/Services/Microsoft Exchange container via ADSI Edit. It is required for Exchange management. You do not need to set this permission if the service account is a member of the Domain Admins or the Organization Management group.</p>	
<p>For AD:</p> <ul style="list-style-type: none"> Read permissions Modify permissions 	Required to modify system-provided AD permissions.	Synchronizing system-provided permissions to AD.
Access to managed AD LDS instances	Commands running under the Active Roles service account's context (for example, scheduled tasks or script modules) are limited by the service account's permissions. Set these permissions based on your needs for the tasks that Active Roles must perform.	Managed AD LDS instance
Active Directory Users And Computers (dsa.msc)	Full Control on msFVE-RecoveryInformation objects	BitLocker recovery
	Permissions to managed domain	Managed domain
	Account Operators security group	Account management tasks

	Permissions	Requirement reason	Affected features
Exchange Server	Recipient Management role group	Required for Exchange management. For more information, see Manage role group members in Exchange Server in the <i>Microsoft Exchange Server documentation</i> .	Exchange management tasks
	Enable to use remote Exchange Management Shell	Required for Exchange management. For more information, see Enable Remote Exchange Management Shell for a User in the <i>Microsoft Exchange Server PowerShell documentation</i> . NOTE: This permission does not work with gMSA accounts.	Exchange management tasks
CMD (DsacIs)	View/Write permission for the Deleted objects container	For view permission only, run the following command: <code>dsacIs "CN=Deleted Objects,DC=Domain,DC=com" /g DOMAIN\YourUser:LCRP</code> For write permission, run the following commands: <code>dsacIs "CN=Deleted Objects,DC=Domain,DC=com" /g DOMAIN\YourUser:WPCC</code> <code>dsacIs dc=Domain,dc=com /g "YourUser:ca;Reanimate Tombstones"</code>	Deleted objects container view
File Servers	Server Operators or Administrator group membership on file servers hosting home folders.	Required to manage home folders within Active Roles.	Home folder operations (for example, autoprovisioning or deprovisioning).

Service publication in Active Directory

After configured, the Administration Service attempts to publish itself in Active Directory, so that Active Roles clients can automatically discover the Administration Service instance.

NOTE: While this functionality is not critical, if the service publication permissions are not provided, Active Roles clients will not be able to automatically discover the Active Roles Administration Service instance. However, they can still connect to the Administration Service if they specify in Active Roles Console either the service name or the IP address of the computer running the instance.

Service publication requires that the service account have the following permissions in the domain of the computer running the Administration Service and in every managed domain as well:

- Permissions on the **System** container:
 - **Delete the serviceConnectionPoint objects**
 - **Write permission for the keywords attribute of the serviceConnectionPoint objects**
- Permissions on the **System > Aelita** container:
 - **Create Container Objects**
 - **Create serviceConnectionPoint Objects**

If the service account has **Domain Administrator** rights, it has the required permissions by default. Otherwise, provide these permissions to the account with the system-provided ADSI Edit tool of the Windows Server operating system.

To grant service publication permissions for Administration Service in Active Directory

1. Open the ADSI Edit console and connect to the Domain naming context.
2. In the console tree, expand the **System** container, right-click the **Aelita** subcontainer, then click **Properties**.

If the **Aelita** container does not exist, create it by right-clicking **System**, selecting **New > Object**, then in the **Create Object** wizard, selecting the **Container** class and entering **Aelita** for the cn value.
3. In **Properties > Security**, click **Advanced**.
4. In **Advanced Security Settings > Permissions**, click **Add**.
5. On the **Permission Entry** page, configure the permission entry:
 - a. Click the **Select a principal link**, and select the desired account.
 - b. Verify that the **Type** box indicates **Allow**.
 - c. Verify that the **Applies onto** box indicates **This object and all descendant objects**.
 - d. In the **Permissions** area, select the **Create container objects** and **Create serviceConnectionPoint objects** check boxes.
 - e. Click **OK**.
6. To close the **Advanced Security Settings** dialog, click **OK**.
7. To close the **Properties** dialog, click **OK**.

Configuring the Administration Service account

When installing the Administration Service, you are prompted for the name and password of the Administration Service account—the account the Administration Service logs on to. This account must have sufficient permissions to:

- Gain administrative access to the computer running the Administration Service.
- Publish the Administration Service in Active Directory.
- Access any managed domain for which an override account is not specified.

NOTE: When registering a domain with Active Roles, you can specify an override account. If you specify an override account, the Administration Service uses the override account rather than the service account to access the domain.

Access to managed domains

Active Roles access to a domain is limited by the access rights of the service account, or the override account, if specified. For all managed domains with no override account specified, configure the service account to have permissions you want Active Roles to have in those domains. If you use an override account when registering a domain with Active Roles, ensure that the override account (rather than the service account) has these permissions for the domain. In addition, the service account (or the override account, if any) must have the **Read Permissions** and **Modify Permissions** rights on the Active Directory objects and containers where you are planning to use the Active Roles security synchronization feature.

For more information, see [Minimum required permissions for the Active Roles service account](#).

Configuring access to Exchange organizations

To manage Exchange recipients on Exchange Server 2019 or 2016, the service account or the override account must be configured to have sufficient rights in the Exchange organization. The rights must be delegated to the service account if an override account is not used, otherwise, the rights must be delegated to the override account.

To configure the service account or the override account

1. Add the account to the **Recipient Management** role group.
For instructions for Exchange 2019, see [Add Members to a Role Group](#) in the *Microsoft Exchange Server 2019 documentation*.
2. Add the account to the **Account Operators** domain security group.
3. Enable the account to use remote Exchange Management Shell.
For instructions for Exchange 2019, see [Use the Exchange Management Shell to enable or disable remote access for a user](#) in the *Microsoft Exchange PowerShell documentation*.
4. Ensure that the account can read Exchange configuration data. For more information, see [Configuring the permission to read Exchange configuration data](#).
5. Restart the Administration Service after you have changed the configuration of the account: Start Active Roles Configuration Center, go to the **Administration Service** page in the Configuration Center main window, then click the **Restart** button at the top of the **Administration Service** page.

NOTE:

- For instructions for Exchange 2016, and 2019, see the relevant pages in the *Microsoft Exchange documentation*.
- Active Roles service account must be a part of **Recipient Management group** to run Exchange hybrid commands.

The Exchange 2016 management tools are not required on the computer running the Administration Service.

Configuring the permission to read Exchange configuration data

To perform Exchange recipient management tasks, Active Roles requires read access to Exchange configuration data in Active Directory. This requirement is met if the service account (or the override account, if specified) has administrator rights (for example, is a member of the **Domain Admins** or **Organization Management** group). Otherwise, give the account the Read permission in the **Microsoft Exchange** container. You can do this by using the ADSI Edit console that ships with all Windows Server versions [officially supported](#) by Active Roles.

To give Read permission to Exchange configuration data

1. Open the ADSI Edit console and connect to the Configuration naming context.
2. In the ADSI Edit console, navigate to the **Configuration > Services** container, right-click **Microsoft Exchange** in that container, and then click **Properties**.
3. On the **Security** tab in the **Properties** dialog that appears, click **Advanced**.

4. On the **Permissions** tab in the **Advanced Security Settings** dialog, click **Add**.
5. On the **Permission Entry** page, configure the permission entry:
 - a. Click the **Select a principal** link, and select the desired account.
 - b. Verify that the **Type** box indicates **Allow**.
 - c. Verify that the **Applies onto** box indicates **This object and all descendant objects**.
 - d. In the **Permissions** area, select the **List contents** and **Read all properties** check boxes.
 - e. Click **OK**.
6. To close the **Advanced Security Settings** dialog, click **OK**. Then, to close the **Properties** dialog, click **OK** again.

Support for remote Exchange Management Shell

When performing Exchange recipient management tasks on Exchange Server, Active Roles uses remote Exchange Management Shell to communicate with Exchange Server, so you do not need to install the Exchange management tools on the computer running the Administration Service.

Prerequisites

To use remote Exchange Management Shell, the Administration Service must be running on a computer that has:

- A Windows Server version supported by Active Roles (see *System requirements* in the *Active Roles Release Notes*).
- [Microsoft .NET Framework 4.8](#).
- [Windows Management Framework 5.1](#).

Remote Shell also requires the following:

- TCP port 80 must be open between the computer running the Administration Service and the remote Exchange server.
- The user account the Administration Service uses to connect to the remote Exchange server (the service account or the override account) must be enabled for remote Shell. To enable a user account for remote Shell, update that user account by using the **Set-User** cmdlet with the **RemotePowerShellEnabled** parameter set to **\$True**.
- Windows PowerShell script initialization must be enabled on the computer running the Administration Service. To enable script initialization for signed scripts, run the **Set-ExecutionPolicy RemoteSigned** command in an elevated Windows PowerShell window.

Access to managed AD LDS instances

Active Roles access to Active Directory Lightweight Directory Services (AD LDS) instances is limited by the access rights of the service account, or the override account, if specified. For all managed AD LDS instances with no override account specified, you should configure the service account to have permissions you want Active Roles to have in those instances. If you use an override account when registering an AD LDS instance with Active Roles, ensure that the override account (rather than the service account) has these permissions for that instance.

To control access to directory data, AD LDS provides four default, role-based groups: **Administrators**, **Instances**, **Readers**, and **Users**. These groups reside in the configuration partition and in each application partition, but not in the schema partition. To register an AD LDS instance with Active Roles, the service account or, if specified, the override account must, at a minimum, be a member of the following groups:

- **Instances** (CN=Instances,CN=Roles) in the configuration partition.
- **Readers** (CN=Readers,CN=Roles) in the configuration partition and in each application partition.

To allow Active Roles full access to the AD LDS instance, add the account to the following group:

- **Administrators** (CN=Administrators,CN=Roles) in the configuration partition.

NOTE: If you add the account to the **Administrators** group, you do not need to add it to the **Instances** or **Readers** group.

Access to file servers

To enable Active Roles to perform the provisioning and deprovisioning tasks related to user home folders and home shares, the service account (or the override account, if specified) must belong to the Server Operators or Administrators group on each file server that hosts the user home folders to be administered by Active Roles.

Active Roles provides the following policy categories to automate the management of user home folders and home shares:

- **Home Folder AutoProvisioning:** Performs the provisioning actions needed to assign home folders and home shares to user accounts, including the creation of home folders for newly created user accounts and renaming home folders upon renaming of user accounts. Specifies the server on which to create home folders and shares, and configures access rights to the newly created home folders and shares.
- **Home Folder Deprovisioning:** Makes the changes needed to prevent deprovisioned users from accessing their home folders, including the removal of the user's permissions on the home folder, changing the ownership of the home folder, and deleting the home folder when the user account is deleted.

The service account or override account must be configured so that it has sufficient rights to perform the operations provided for by those policies: create, modify (including the ability to change permission settings and ownership), and delete folders and shares on the designated file servers.

You can give the required permissions to the service account or override account by adding that account to the appropriate administrative group (Administrators or Server Operators) on each file server where you are planning Active Roles to manage user home folders.

Access to BitLocker recovery information

Viewing BitLocker recovery passwords in Active Roles requires the domain administrator rights for the account being used by the Active Roles Administration Service to access the domain. Ensure that the service account or, if specified, the override account is a member of the Domain Admins group in each managed domain where you want to use Active Roles for viewing BitLocker recovery passwords.

With the domain administrator rights given to the Active Roles Administration Service, Active Roles allows delegated administrators to locate and view BitLocker recovery passwords held in the Active Directory domain. To view BitLocker recovery passwords, the delegated administrator must be granted the appropriate permissions in Active Roles. The **Computer Objects - View BitLocker Recovery Keys** Access Template provides sufficient permissions to view BitLocker recovery passwords.

In addition, viewing BitLocker recovery passwords in a given domain requires the following:

- The domain must be configured to store BitLocker recovery information. For more information, see [Backing Up BitLocker and TPM Recovery Information to AD DS](#) in the *Microsoft BitLocker Drive Encryption documentation*.
- The computers protected by BitLocker must be joined to the domain.
- BitLocker Drive Encryption must be enabled on the computers.

The BitLocker recovery information is displayed on the **BitLocker Recovery** tab in the **Properties** dialog of the computer object, in the Active Roles Console. It is also possible to perform domain-wide searches for BitLocker recovery passwords.

SQL Server permissions

This section discusses the SQL Server permissions required to:

- Configure the Active Roles Administration Service ([Configuration permissions](#)).
- Run the Active Roles Administration Service ([Operation permissions](#)).
- Configure replication in Active Roles ([Replication configuration permissions](#)).
- Run Active Roles replication ([Replication Agent permissions](#)).

Configuration permissions

IMPORTANT: Starting from version 8.2, Active Roles supports (and its installer is shipped with) Microsoft OLE DB Driver 19.x for SQL Server. However, Active Roles still supports earlier OLE DB Driver versions as well (18.4 or newer).

- If you perform a clean installation of Active Roles 8.2.1 and want to use Microsoft OLE DB Driver 19.x (bundled with the Active Roles installer) due to security concerns, then verify that your SQL Server has SSL configured and the necessary trusted certificate set. Otherwise, Active Roles cannot communicate with the SQL Server and the Active Roles Administration Service might not start.

To use SSL with your SQL Server, configure a valid certificate. For more information on installing or viewing certificates for SQL Server via SQL Server Configuration Manager, see [Certificate management](#) in the *Microsoft SQL Server documentation*.

For general information about the encryption and certificate requirements of Microsoft OLE DB Driver 19.x, see [Encryption and certificate validation in OLE DB](#) and [Certificate requirements for SQL Server](#) in the *Microsoft SQL Server documentation*.

When configuring the SSL connection, consider the following:

- Microsoft OLE DB Driver 19.x for SQL Server requires a certificate from a Certificate Authority and no longer accepts self-signed certificates. For more information on how to access a Certificate Authority, see [Certification Authority Guidance](#) in the *Microsoft Windows Server documentation*.
- The Service Account running the SQL Server service must have permission to view the private key from the server certificate. For more information, see [Configure SQL Server Database Engine for encrypting connections](#) in the *Microsoft SQL Server documentation*.
- Microsoft OLE DB Driver 19.x for SQL Server requires specifying the Service Principal Names (SPNs). For more information, see the following *Microsoft SQL Server documentation* resources:
 - [Service Principal Name \(SPN\) Support in Client Connections](#)
 - [Service Principal Names \(SPNs\) in Client Connections \(OLE DB\)](#)
 - [Service Principal Names \(SPNs\) in Client Connections \(OLE DB\) in SQL Server Native Client](#)
- You might need to change your SQL connection string to match the certificate and the SPN. For more information, see [Using Connection String Keywords with OLE DB Driver for SQL Server](#) in the *Microsoft SQL Server documentation*.
- If you perform a clean installation of Active Roles 8.2.1 but you want to use an earlier supported version of Microsoft OLE DB Driver (18.4 or newer) instead of version 19.x that is bundled with the Active Roles installer, you must perform

additional configuration steps in your environment. For more information, see [Rolling back to a previous Microsoft OLE DB Driver for SQL Server version](#).

To assign a valid and trusted certificate to SQL Server, in the SQL Server Configuration Manager, navigate to **SQL Server Network Configuration > Protocols for MSSQLSERVER**.

The account that you use when configuring the Administration Service must have sufficient rights on SQL Server to perform the configuration tasks.

Which account is used to access SQL Server during configuration of the Administration Service depends upon the SQL Server connection option you select in the wizard for configuring the Administration Service. If you select the option to use Windows authentication, the wizard accesses SQL Server with the Windows user account under which the wizard is running. If you select the option to use SQL Server authentication, then the wizard accesses SQL Server with the SQL login and password that you specify in the wizard.

NOTE: Windows authentication is not applicable for configuring Active Roles on Azure database server.

The required rights of the account that is used to access SQL Server during configuration vary depending on your configuration scenario:

- The wizard can create a new database for the Administration Service only if the account is a member of the **dbcreator** fixed server role.
- For Azure SQL database variants, Azure SQL database and Azure SQL on elastic pool **dbmanager** role must be provided to the Server Admin to create databases.
- However, for variant Azure SQL Managed instance, the **dbcreator** fixed server role should be provided.
- If you want the wizard to import data from the Active Roles database of an earlier version, then the account must be a member of the **db_datareader** fixed database role in the source database.
- If you want the wizard to configure the Administration Service to use an existing database of the current version, then the account must be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.
- If you want the wizard to use an existing blank database for the Administration Service, then the account must be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.

Operation permissions

The Administration Service accesses its database with the account specified during configuration:

- If you select the option for Windows authentication to configure the Administration Service, then the Administration Service uses its service account to access the database.

- If you select the option for SQL Server authentication, then the Administration Service accesses the database with the SQL login and password supplied in the configuration wizard.

In either case, the account must have sufficient rights on SQL Server to retrieve data from, and make changes to, the database. The required rights vary depending on the role of the Administration Service's database server in the Active Roles replication environment.

| NOTE: Active Roles does not support replication on Azure SQL databases.

Standalone mode

When initially installed, the Administration Service database is configured not to participate in Active Roles replication. This configuration is known as "standalone Administration Service". The account that the standalone Administration Service uses to access the database must be, at minimum, the member of the **db_owner** fixed database role and must have the default schema of **dbo** in that database.

Publisher mode

If the Administration Service's database server holds the role of the Publisher in Active Roles replication, then the account the Administration Service uses to access the database must at a minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database. Additional rights are required if you want to see the replication status information and error messages in the Active Roles console. These additional rights are as follows:

- Default schema of **dbo** in the **msdb** system database.
- **SELECT** permission on the **sysjobs**, **sysjobsteps** and **MSagent_parameters** system tables in the **msdb** system database.
- **SELECT** permission on the **sys.servers** system view in the **master** system database.
- **EXECUTE** permission on the **xp_sqlagent_enum_jobs** system extended stored procedure in the **master** system database.
- **SELECT** permission on the **MSmerge_agents**, **MSmerge_history**, **MSmerge_sessions**, **MSsnapshot_agents** and **MSsnapshot_history** system tables in the distribution database (**AelitaDistributionDB** database by default).

Subscriber mode

If the Administration Service's database server holds the role of a Subscriber in Active Roles replication, then the account that the Administration Service uses to access the database requires the same rights as in standalone mode: The account must at a minimum be a member of the **db_owner** fixed database role and have the default schema of **dbo** in that database.

Replication configuration permissions

After you install and configure two or more Administration Service instances, each with its own database, you can deploy replication, if necessary, to synchronize the databases so that all your Administration Service instances have the same configuration and management history. Replication deployment begins when you configure the Publisher. Once the Publisher has been configured, the next step is to configure Subscribers. The task of configuring the Publisher or a Subscriber requires more rights on SQL Server than the Administration Service needs for normal operation. To elevate the rights of the Administration Service, Active Roles prompts for an alternative account. The following topics elaborate on the permissions needed to create the Publisher or add a Subscriber.

Permissions for creating or removing the Publisher

To create the Publisher, the Administration Service needs **sysadmin** rights on SQL Server. If the Administration Service's account for database access does not belong to the **sysadmin** role, then Active Roles prompts you to supply an alternative account. The alternative account must be a member of the **sysadmin** fixed server role on the database server you are going to make the Publisher.

Active Roles does not store the login name and password of this account. It only uses the login name and password of this account to configure the Publisher.

The same permissions are required for removing (demoting) the Publisher.

Permissions for adding or removing a Subscriber

To add a Subscriber, the Administration Service's database server must hold the Publisher role. When adding a Subscriber, the Administration Service makes changes on the Publisher database server and on the database server being configured as a Subscriber (Subscriber database server). Therefore, the Administration Service needs sufficient rights on both database servers.

On the Publisher database server, the Administration Service needs **sysadmin** rights. If the Administration Service's account for database access does not belong to the **sysadmin** role, then Active Roles prompts you to supply an alternative account for connection to the Publisher database server. The alternative account must be a member of the **sysadmin** fixed server role on the Publisher database server.

Active Roles does not store the login name and password of this account. It only uses the login name and password of this account to configure the Subscriber.

On the database server you are going to make a Subscriber, the Administration Service needs **db_owner** rights in the Active Roles database. If the Administration Service's account for database access does not have sufficient rights on the Subscriber database server, then Active Roles prompts you to supply an alternative account for connection to the Subscriber database server. The alternative account must:

- Be a member of the **db_owner** fixed database role in the Active Roles database on the database server you are going to make a Subscriber.
- Have the default schema of **dbo** in that database.

Active Roles does not store the login name and password of this account. It only uses the login name and password of this account to configure the Subscriber.

The same permissions are required for removing a Subscriber.

Replication Agent permissions

In Active Roles replication, SQL Server Replication Agents (Merge Agents) are used to synchronize data between the Publisher and Subscriber databases. Each Subscriber has a dedicated Replication Agent running on SQL Server that hosts the Publisher database. Since the agent's role is to maintain the Publisher and Subscriber databases in sync with each other, the agent needs sufficient rights to access both the Publisher and Subscriber database servers.

The Administration Service creates and configures a Replication Agent when adding a Subscriber. In terms of SQL Server, this is a Merge Agent for a push subscription. According to SQL Server Books Online (see [Replication Agent Security Model](#)), Merge Agent for a push subscription requires the following permissions.

The Windows account under which the agent runs is used when it makes connections to the Publisher and Distributor. This account must:

- At a minimum be a member of the **db_owner** fixed database role in the distribution database (**AelitaDistributionDB** database by default).
- Be a member of the publication access list (PAL).
- Be a login that is associated with a user in the publication database (the Active Roles database on the Publisher).
- Have read permissions on the snapshot share (by default, this is the **ReplData** folder on the administrative share C\$).

The account used to connect to the Subscriber must at minimum be a member of the **db_owner** fixed database role in the subscription database (the Active Roles database on the Subscriber).

By default, the security settings of a Merge Agent configured by Active Roles are as follows:

- The account under which the Merge Agent runs and makes connections to the Publisher and Distributor is the Windows service account of the SQL Server Agent service.
- The account the Merge Agent uses to connect to the Subscriber is the account under which the Merge Agent runs.

This means that, by default, Active Roles requires that the account of the SQL Server Agent service have all permissions the Merge Agent needs to make connections both to the Publisher/Distributor and to the Subscriber.

When adding a Subscriber, you have the option to supply a separate login for connection to the Subscriber. If you choose that option, the Merge Agent will use the login you supply (rather than the account of the SQL Server Agent service) to make connections to the Subscriber. In this case, it is the login you supply that must have **db_owner** rights in the subscription database. The SQL Server Agent service does not need to have any rights in

the subscription database. However, it still must have all permissions the Merge Agent needs to make connections to the Publisher and Distributor.

Installing Active Roles

You can install Active Roles by launching the installation wizard on the downloaded .iso file, provided that your environment meets all prerequisites.

Prerequisites

Make sure that all installation prerequisites are met. For more information on the hardware and software requirements for each component, see [System requirements](#).

NOTE: Installing the required Active Roles components to an offline Active Roles server (with no internet connection available) requires manual installation steps. For more information, see [Knowledge Base Article 4292417, Active Roles PowerShell Module prerequisites](#).

To install Active Roles and its components

1. Log in with a user account that has administrator rights on the computer.
2. Mount the Active Roles installation .iso file.
3. To start installation, double-click **ActiveRoles.exe**.
4. Accept the license agreement and click **Next**.
5. Based on the components selected by default, the setup wizard installs the Administration Service, Configuration Center, Web Interface, Management Shell, Console, and ADSI Provider components on the system. Change the selected components according to your needs, or review the default selection and follow the instructions of the wizard to proceed with the installation.

TIP: You can also install these components separately by launching their installers from their respective component directories in the Components folder.

NOTE: You will need to configure and run the Administration Service to configure and start any other Active Roles components later.

- For more information on installing and configuring the Administration Service, see [Deploying the Administration Service](#).
- For more information on installing and configuring the user interfaces, see [Deploying user interfaces](#).

6. In addition to the Active Roles default components, you can install and configure the following additional tools provided by Active Roles:

- Add-in for Outlook
- Add-on Manager
- Administrative Template
- Data Collector and Report Pack
- Configuration Transfer Wizard
- Diagnostic Tools
- Management Pack for SCOM
- SPML Provider
- Synchronization Service Capture Agent

For more information on installing and configuring these additional tools, see [Installing optional tools and components](#).

Rolling back to a previous Microsoft OLE DB Driver for SQL Server version

Starting from version 8.2, Active Roles supports (and its installer is shipped with) Microsoft OLE DB Driver 19.x for SQL Server. However, Active Roles still supports earlier OLE DB Driver versions as well (18.4 or newer).

If you want to use a previous supported version of Microsoft OLE DB Driver for SQL Server with your Active Roles installation instead of version 19.x, you can roll back your Microsoft OLE DB Driver for SQL Server installation.

Prerequisite

You must have Active Roles 8.2.1 and Microsoft OLE DB Driver 19.x for SQL Server installed via clean installation.

To roll back to a previous supported Microsoft OLE DB Driver for SQL Server version

1. Download and install any supported version of Microsoft OLE DB Driver for SQL Server (18.4 or newer).
2. Stop the Active Roles Administration Service. To do so, in the Active Roles Configuration Center, navigate to **Administration Service**, then click **Stop**.
3. In the Windows Registry Editor, modify the Microsoft OLE DB Driver for SQL Server version entries. To do so:

- a. In the Registry Editor, navigate to the following node:
HKEY_LOCAL_MACHINE > SOFTWARE > One Identity > Active Roles > Configuration > Service
 - b. In the **CHDatabaseConnectionString** and **DatabaseConnectionString** nodes, change the **Provider** key from **MSOLEDBSQL19** to **MSOLEDBSQL**.
4. Start the Active Roles Administration Service. To do so, in the Active Roles Configuration Center, navigate to **Administration Service**, then click **Start**.

NOTE: Consider the following if you use a Microsoft OLE DB Driver for SQL Server version older than 19.x with Active Roles:

- In the Active Roles Configuration Center, you can specify the database server hosting the Active Roles databases either with its short name (for example, ActiveRoles) or with its FQDN (for example, ActiveRoles.roles1.net).
- If you install Microsoft OLE DB Driver 19.x for SQL Server later on the machine (outside of the Active Roles installer), the OLE DB Driver installer will automatically update the **Provider** keys from **MSOLEDBSQL** to **MSOLEDBSQL19** in the Windows Registry. If you want to keep using Active Roles with a Microsoft OLE DB Driver for SQL Server version older than 19.x, make sure to revert this change.

Deploying the Administration Service

After configuring access to the SQL Server, install the Active Roles Administration Service. This section describes how to install and configure a new instance of the Administration Service. For instructions on how to upgrade an existing Administration Service instance of an earlier version, see *Upgrading the Administration Service* in the *Active Roles Upgrade Guide*.

Installing the Administration Service

To create a new Administration Service instance, you must install the Administration Service and then perform the initial configuration.

To install the Active Roles Administration Service

1. Log in with a user account that has administrator rights on the computer.
2. Mount the Active Roles installation .iso file.
3. To start installation, double-click **ActiveRoles.exe**.
4. Accept the license agreement and click **Next**.
5. On the **Component Selection** page, clear all check boxes except **Administration Service**, then click **Next**.
6. On the **Ready to Install** page, review the summary and click **Install**.
7. On the **Completion** page, make sure that **I want to perform configuration** is selected. Then, to launch the Configuration Center, click **Finish**.

The setup wizard only installs the files. After you have completed the installation, you must configure the newly-installed Administration Service instance via the Active Roles Configuration Center that opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the setup wizard.

Alternatively, you can open the Configuration Center by selecting **Active Roles 8.2.1 Configuration Center** on the **Apps** page or **Start** menu, depending on the version of your Windows operating system.

Configuring the Administration Service

After installing Active Roles, perform the initial configuration of the Administration Service by specifying its service account, Active Roles Admin account, and database settings.

To configure the initial Administration Service

1. In Configuration Center, under **Administration Service**, click **Configure**. The Configure Administration Service wizard appears.
2. On the **Service Account** page, enter the name and password of the domain user account or the service account details of the Group Managed Service Account (gMSA) to be used as the Administration Service account. Then, click **Next**.

NOTE: Make sure that the service account has the minimum required permissions. For more information, see [Minimum required permissions for the Active Roles service account](#).

3. On the **Active Roles Admin** page, accept the default account, or click **Browse** and select the group or user to be designated as Active Roles administrator. Then, click **Next**.
4. On the **Configuration Database Options** page, select **New Active Roles database** or **Existing Active Roles database**. Then, click **Next**.
5. On the **Connection to Configuration Database** page, specify a database type, SQL Server instance and database name. Then, select the authentication option for the configuration database:
 - a. Select the required **Database Type**.
 - b. In **Database Server name**, specify an SQL Server instance in the form **<Computer>\<Instance>** (for named instance) or **<Computer>** (for default instance), where **<Computer>** stands for the FQDN of the computer running SQL Server or the name of the Azure SQL database server.

The wizard will create the database on the SQL Server instance that you specify.
 - c. In **Database name**, enter a name for the database that will be created.
 - d. Under **Connect using**, select the appropriate authentication option.
 - If your Windows logon account has sufficient rights to write data to the destination database, click **Windows authentication**.
 - If you have a SQL Server login with sufficient rights, click **SQL Server authentication** and enter the login name and password.

- If you have an Azure AD login with sufficient rights, click **Azure Active Directory authentication** and enter the login name and password.
6. On the **Management History Database Options** page, select **New Active Roles database** and click **Next**.
 7. On the **Connection to Management History Database** page, perform the same sub-steps for configuring the Management History database that you did for [configuring the Configuration database](#). Then, click **Next**.
 8. On the **Encryption Key Backup** page, perform the steps as described in [Backing up the encryption key](#).

NOTE: This window appears only if the Administration Service is configured with the **New Active Roles database** option for either the configuration or management history database.

9. Click **Next**, and follow the instructions in the wizard to complete the configuration.

If required by your organization and/or security policies, you can change the credentials of the Active Roles Administration Service account in the Active Roles Configuration Center immediately after performing the first-time configuration of the Administration Service.

(Optional) To change the Active Roles Administration Service account

1. Launch the Active Roles Configuration Center.
2. Click **Administration Service**.
3. On the Service Account, click **Change**.
4. Enter the new credentials and click **Change**.
5. To apply your changes, click **Finish**.
6. To start using the new credentials, restart the Active Roles Administration Service.

Backing up the encryption key

When you configure the initial Administration Service, the Active Roles Configuration Center creates a database along with a secret key that the Administration Service will use to encrypt and decrypt sensitive data in the database. This data can include, for example, credentials of the override accounts for managed domains and Azure administrator user passwords.

The secret key (or encryption key) is stored in the database using asymmetric cryptography, meaning that it has a private and public key pair. The secret key can only be retrieved and decrypted by the Administration Service instance that has the private key of the asymmetric key pair. Storing the secret key in this way ensures the optimal level of protection for security-sensitive data in the Active Roles database.

To retrieve the secret key, the private key that is the pair of the public key that was used for encrypting the secret key is required. Additional Administration Service instances that were configured for Active Roles after setting a secret key might not be able to retrieve the secret key and use the Active Roles database. This can occur if you:

- Configure a new Administration Service instance for an Active Roles database that is used by another instance of the Administration Service, and there is no running instance that could decrypt the secret key.
- Import Active Roles configuration data from another database (for example, the Configuration database of an earlier Active Roles version). In this case, you need the secret key that is used for data encryption in the source database. Otherwise, you cannot import the encrypted data.

If the Administration Service cannot retrieve the secret key from the database, you need a backup copy of the secret key. Configuration Center prompts you to create a backup of the secret key when you perform the initial configuration of the Administration Service via creating a new database.

On the **Encryption Key Backup** page, the Configure Administration Service wizard specifies a file to store a backup copy of the secret key. You can encrypt the backup by protecting the file with a password.

NOTE: Consider the following regarding encryption keys:

- The encryption key is only used to encrypt passwords for domain override accounts (including AD LDS instances). It does not encrypt any other data.
- By default, the encryption is saved to the following folder with the following default name:
C:\ProgramData\One Identity\Active Roles\ARServiceEncryptionKey-dj-ars<version>.bin
- If you lose your encryption key, you can still use Active Roles with one of the following workarounds:
 - As the encryption key is used for Managed Domain password encryption, you can reinstall Active Roles, and configure a new database by importing the settings from the old database. In this case, the wizard will prompt you to create a new encryption key file.
 - Configure an additional Administration Service instance, as it can retrieve the encryption key from an already running Administration Service instance.
 - If you are not using the latest available version of Active Roles, upgrade to the newest version and (optionally) create a new key when instructed.
 - If you have multiple Administration Service instances sharing the same database, Active Roles can fetch the encryption information from the other Administration Service instance.
- You must configure an Active Roles encryption key if you:
 - Add another Administration Service instance to an existing shared database.
 - Have no services connected to the same database that is up and running.
 - Cannot afford retyping passwords for managed domains.

Additional considerations for Active Roles database encryption

Active Roles encrypts some data, stored in the Active Roles database.

To use the encrypted data, you need the encryption key as the file is password protected. Active Roles stores the encryption key inside the Active Roles database using asymmetric cypher. As such, Active Roles can get the value of this key from the database. Active Roles also has a logic that allows the service to share this key with other services (like several services per single database). If the key is lost, you must retype the passwords for the managed domains.

You only need this file if you want to use an existing Active Roles database but cannot retype passwords for Managed Domains.

To back up the Active Roles database encryption key

1. (Optional) To change the name or location of the backup file, click **Browse**, then specify the desired file name and location. The wizard will save a copy of the secret key to the file specified.
2. (Optional) To encrypt the backup, select **Protect the backup file with a password**, then type and confirm a password. To retrieve the key from the backup file later, you must enter the specified password.

⚠ CAUTION: Do not lose or forget the password, as it cannot be recovered.

Configuring an additional Administration Service instance

This section covers the database-related steps of the Configure Administration Service wizard in a scenario where:

- At least one instance of the Administration Service version Active Roles is up and running in your environment.
- You are installing one more Administration Service instance for load distribution and fault tolerance.

To configure an additional Administration Service

1. On the **Database Options** page in the Configure Administration Service wizard, select one of the following options, depending on how you want to synchronize the configuration of the new Administration Service instance with the configuration of the existing Administration Service instances:
 - **Existing Active Roles database:** Configures the new Administration Service instance to use the database of an existing Administration Service instance so that the new Administration Service instance has the same configuration as the existing instance.
 - **New Active Roles database:** After configuring the new Administration Service instance, you will need to set up Active Roles replication for the new

Administration Service instance to have the same configuration as the existing instances.

2. If you have selected the **Existing Active Roles database** option, see [Using a common database for the Administration Service](#).
3. If you have selected the **New Active Roles database** option, complete the wizard as described in [Configuring the Administration Service](#).

The database created by this option holds the newest configuration of the Administration Service. To update and synchronize the new database with the configuration data of the Administration Service instances that were earlier deployed in your environment, you need to use the replication function. For instructions on how to set up replication of configuration data, see *SQL Server replication* in the *Active Roles Administration Guide*.

Using a common database for the Administration Service

If you select the **Existing Active Roles database** option on the **Database Options** page, the Configure Administration Service wizard causes the new Administration Service instance to connect to the database of an existing Administration Service instance. The new instance automatically becomes a replica of the existing one.

This option allows you to centralize the Active Roles configuration storage. You can deploy multiple Administration Service instances of the same configuration without having to synchronize them via replication. Rather, you have the option for multiple Administration Service instances to share configuration data held in a single database on centrally deployed SQL Server.

This option also ensures that the newly-deployed Administration Service instance can immediately be used as a replacement for the existing one. Switching between Administration Service instances is transparent to Active Roles users as both instances of the Administration Service have the same configuration.

To configure the Administration Service to share a database

1. On the **Database Options** page in the Configure Administration Service wizard, select the **Existing Active Roles database** option, and then click **Next**.
2. On the **Connection to Database** page, specify Database type, Database Server name, and Database fields. Specify the SQL Server instance and the name of the database being used by an existing instance of the Administration Service version Active Roles.

Specify the SQL Server instance in the form <computer>\<instance> (for named instance) or <computer> (for default instance). In these formats, <computer> stands for the FQDN of the computer running SQL Server.

3. On the **Connection to Database** page, under **Connect using**, select the appropriate authentication option:
 - To have the Administration Service connect to the database using the service account, click **Windows authentication**.
 - To have the Administration Service connect to the database using an SQL Server login, click **SQL Server authentication** and enter the login name and password.
4. On the **Connection to MH Database** page, specify the database type, database server name, and the name of the database, and select the desired authentication option for the Administration Service connection to the Management History database.
5. If you want to configure advanced database properties, click on the link displayed, and select one or both of the following options, based on the requirement, and then click **Apply**.:
 - On the **Advanced Database Properties** dialog box, in the **Connection Timeout** text box, enter the time in seconds. This value indicates the amount of time trying to establish a connection before terminating the attempt and generating an error.

NOTE:

- Default connection time out is as per the SQL OLEDB connection timeout.
- A value of 0 indicates no limit as attempt to connect will wait indefinitely and hence input value is permitted starting from 1 second.
- If any value populated in the field cannot be made null or empty once settings are saved and another valid value must be entered.
If you enter a value less outside the specified range, an error is displayed.
- To enable MultiSubnetFailover, select the **Enable faster failover for all Availability Groups and Failover Cluster instances** check box.
- The settings available on Advanced Database properties are not applicable for Azure databases.

6. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Using the database of an earlier Administration Service installation

When you deploy the Administration Service, you may need to configure it to use the database of an earlier installation of the Administration Service instead of creating a new database. You may need to do so in the following scenarios:

- Restoring the Active Roles database from a backup, and then configuring the Administration Service to use the restored database.

- Repairing the Active Roles installation by using **Programs and Features** in Control Panel.
- Installing a maintenance release of Active Roles to update the existing Administration Service instance.

NOTE: All these scenarios assume that the database has the same version as the Administration Service you are configuring. If the Administration Service version is greater than the database version, choose the option to create a new database and import data from the existing database. For more information, see *Importing configuration data* in the *Active Roles Upgrade Guide*.

Provided that the database is of the same Active Roles version as the Administration Service you are configuring, you can use the following steps to make the Administration Service use that database.

To use the database of an earlier Administration Service installation

1. On the **Database Options** page in the Configure Administration Service wizard, select the **Existing Active Roles database** option, and then click **Next**.
2. On the **Connection to Database** page, specify the Database type, Database Server name, and the name of the database. Select the desired authentication option for the Administration Service connection to the configuration database.
3. On the **Connection to MH Database** page, specify the Database type, Database Server name, and the name of the database. Select the desired authentication option for the Administration Service connection to the management history database.
4. If you want to configure advanced database properties, click on the link displayed, and select one or both of the following options, based on the requirement, and then click **Apply**:
 - On the Advanced Database Properties dialog box, in the **Connection Timeout** text box, enter the time in seconds for the database connection to get timed out.
If you enter a value less outside the specified range, an error is displayed.
 - Select the check box **Enable faster failover for all Availability Groups and Failover Cluster instances** to enable `MultiSubnetFailOver`.

NOTE:

- Default connection time out is as per the SQL OLEDB connection timeout.
 - A value of 0 indicates no limit as attempt to connect will wait indefinitely and hence input value is permitted starting from 1 second.
 - If any value populated in the field cannot be made null or empty once settings are saved and another valid value must be entered.
5. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Using a pre-created blank database

When you choose the option to create a new Active Roles database, the Configure Administration Service wizard uses default values for database properties, such as the location and other parameters of the database files and transaction log files. If you need specific database properties, then you can use SQL Server tools to create a blank database with the properties that meet your requirements, and have the wizard create the new Active Roles database by adding the Active Roles tables and data to that blank database. The following steps assume that you have a blank database already created.

To use a pre-created blank database

1. On the **Database Options** page in the Configure Administration Service wizard, select the **New Active Roles database** option, select the **Use a pre-created blank database** check box, and then click **Next**.
2. On the **Connection to Database** page, specify the Database type, Database Server name and the name of the database. Select the desired authentication option for the Administration Service connection to the configuration database.
3. If you want to configure advanced database properties, click on the link displayed, and select one or both of the following options, based on the requirement, and then click **Apply**.
 - On the Advanced Database Properties dialog box, in the **Connection Timeout** text box, enter the time in seconds. This value indicates the time to wait while trying to establish a connection before terminating the attempt and generating an error.

NOTE: CONSIDER THE FOLLOWING WHEN YOU ARE SPECIFYING THE CONNECTION TIMEOUT

- The default connection will time out as per the SQL OLEDB connection timeout.
- A value of 0 indicates no limit as attempt to connect will wait indefinitely and hence input value is permitted starting from 1 second.
- If any value populated in the field cannot be made null or empty once settings are saved and another valid value must be entered.

If you enter a value outside the specified range, an error appears.

4. Select the check box **Enable faster failover for all Availability Groups and Failover Cluster instances** to enable MultiSubnetFailover.
5. On the **MH Database Options** page, select the **New Active Roles database** option, and select the **Use a pre-created blank database** check box, then click **Next**.
6. On the **Connection to MH Database** page, specify the Database type, Database Server name and the name of the database. Select the desired authentication option for the Administration Service connection to the management history database.
7. Click **Next**, and follow the instructions in the wizard to complete the configuration.

Deploying user interfaces

Active Roles provides user interfaces for the Windows system and the Web, allowing users with appropriate rights to perform administrative activities. The user interfaces include:

- Web Interface: A customizable web application for directory administration.
- MMC Interface: A desktop console for Active Roles configuration and directory administration.

By default, the Active Roles setup wizard installs all core Active Roles components, including the Console (MMC Interface) and the Web Interface. You can choose to install individual components, if needed.

Installing the Active Roles Console

The Active Roles Console can be installed on any computer that meets the system requirements and has a reliable network connection to a computer running the Administration Service. It can also be installed on the computer running the Administration Service instance.

To install the Active Roles Console

1. Log in with a user account that has administrator rights on the computer.
2. Mount the Active Roles installation .iso file.
3. To start installation, double-click **ActiveRoles.exe**.
4. Accept the license agreement and click **Next**.
5. On the **Component Selection** page, clear all check boxes except **Console (MMC Interface)**, then click **Next**.
6. On the **Ready to Install** page, review the summary and click **Install**.
7. To close the setup wizard, on the **Completion** page, click **Finish**.

Once you have installed the console, you can start it by selecting **Active Roles 8.2.1 Console** on the **Apps** page or the Windows Start menu, depending on the version of your operating system.

Restricting access to the Active Roles Console

By default, after installing Active Roles, every user can log in to the Active Roles Console. You can allow or restrict access either for all users or to users you specify.

Allowing or restricting access to the Active Roles Console for all users

Use the **MMC Interface Access** setting of the Active Roles Configuration Center. This setting lets you restrict Console access only to Active Roles Admin users (or allow Console access again for all users, if the access is restricted).

To allow or restrict access to the Active Roles Console for all users

1. On the Configuration Center **Dashboard** page, in the **MMC Interface Access** area, click **Manage Settings**.
2. On the **MMC Interface Access** page that opens, in the **Settings** area, click **Component**, then click **Modify** or double-click the **Component** item.
3. On the **MMC Interface Access** wizard that appears, select one of the following options:
 - **Allow Console (MMC Interface) access for all users:** Enables the user to log in to Active Roles Console.
 - **Restrict Console (MMC Interface) access for all users:** Restricts all non-Active Roles Admin users from using the Console. This affects all delegated users, but does not apply to Active Roles Admin users.
4. Click **OK**.

Active Roles then configures the Console access settings successfully. When ready, a message appears prompting you to restart the Administration Service and disconnect all Console user sessions, so that the updated settings can be validated.

Allowing access to the Active Roles Console for selected users

If Console access is already restricted to Active Roles Admin users, you can give Console access to individual users by assigning them to the **User Interface Management - MMC Full control** Access Template (AT). This AT gives access permission to the **Server Configuration > User Interfaces > MMC Interface** object.

To allow access to Active Roles Console for selected users

1. In the Console tree, expand **Active Roles > Configuration > Server Configuration**.
2. Under **Server Configuration**, locate the **User Interfaces** container, right-click it, and click **Delegate Control**.

3. On the **Users or Groups** page, click **Add**, then select the users or groups to which you want to delegate the control. Click **Next**.
4. On the **Access Templates** page, expand the **Active Directory > User Interfaces** folder, and select the check box next to **User Interface Management-MMC Full control**.
5. Click **Next** and follow the instructions in the wizard, accepting the default settings.
6. After you complete these steps, the users and groups you selected in Step 3 are authorized to log in to the Active Roles Console.
7. Click **OK** to close the **Active Roles Security** dialog.

Deploying the Web Interface

You can deploy the Active Roles Web Interface on any computer that meets the product system requirements and is running Internet Information Services (IIS) 7.5 or later.

NOTE: You do not need to deploy the Web Interface component on the same computer that runs the Active Roles Administration Service. However, the computer (or computers) hosting the Web Interface must have a reliable network connection to the computer (or computers) running the Administration Service component.

Prerequisites

For the prerequisites of deploying the Web Interface, see [System requirements](#).

- The Web Interface setup configures the **Web Server (IIS)** server role to meet the Web Interface requirements. You can use Server Manager to verify that the server role is configured properly.
- Web Interface requires Internet Information Services to provide **Read/Write** delegation for the following features:
 - Handler Mappings
 - Modules

To confirm that these features have delegation set to **Read/Write**, in the Internet Information Services (IIS) Manager tool, use **Feature Delegation**.

Installing the Web Interface

When installing and initially configuring the Web Interface, you first use the Setup wizard to install the Web Interface files and then use Active Roles Configuration Center to choose the Administration Service and create the Web Interface sites.

To install the Web Interface

1. Log in with a user account that has administrator rights on the computer.
2. Mount the Active Roles installation .iso file.
3. To start installation, double-click **ActiveRoles.exe**.
4. On the **Component Selection** page, clear all check boxes except **Web Interface**, then click **Next**.
5. By default, all components are selected. If you only want to install the Active Roles Web Interface, clear the check boxes of the other components.
6. On the **Ready to Install** page, review the summary and click **Install**.
7. On the **Completion** page, make sure that **I want to perform configuration** is selected. Then, to launch the Configuration Center, click **Finish**.

The setup wizard only installs the files. After you have completed installation, you must configure the newly-installed Web Interface instance via the Active Roles Configuration Center that opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the setup wizard.

Alternatively, you can open the Configuration Center by selecting **Active Roles 8.2.1 Configuration Center** on the **Apps** page or **Start** menu, depending on the version of your Windows operating system.

The procedure for configuring the Web Interface includes two stages:

- [Performing the initial configuration of the Web Interface](#): During initial configuration, the Administration Service is selected, and three Web Interface sites are created based on the default configuration templates.
- [Creating or modifying a Web Interface site](#): You can create additional sites, and modify or delete existing sites.

Performing the initial configuration of the Web Interface

After installing the Web Interface component, perform its initial configuration by specifying how it should select the Administration Service instance to use.

Prerequisites

The Active Roles Administration Service must be configured and running. If the Administration Service is not running, you will not be able to configure the Web Interface component.

TIP: You can view the state of the Administration Service on the **Administration Service** of the Configuration Center.

To perform the initial configuration of the Web Interface

1. Log in with a user account that has administrator rights on the computer.
2. Open Active Roles Configuration Center.
Configuration Center opens automatically if you select the **I want to perform configuration** check box on the **Completion** page in the Setup wizard. Alternatively, to open Configuration Center, select **Active Roles 8.2.1 Configuration Center** on the **Apps** page or **Start** menu, depending on the version of your Windows operating system.
3. In the Configuration Center main window, under **Web Interface**, click **Configure**.
This starts the wizard that will perform initial configuration of the Web Interface.
4. On the **Administration Service** page, specify how you want the Web Interface to select the Active Roles Administration Service. You can choose from the following options:
 - **Administration Service on the computer running the Web Interface**
 - **Administration Service on this computer**
Supply the fully qualified domain name of the computer running the desired Administration Service instance.
 - **Any Administration Service of the same configuration as this one**
Specify any Administration Service whose database holds the desired configuration, by supplying in the fully qualified domain name of the computer running that Administration Service. If Active Roles replication is used to synchronize configuration data, this must be any Administration Service whose database server acts as the Publisher for the configuration database.
5. Click the **Configure** button to start the configuration process.
6. Wait while the wizard completes the configuration.

Configuration Center creates three Web Interface sites based on the following configuration templates:

- **Default Site for Administrators:** Supports a broad range of tasks, including the management of directory objects and computer resources.
- **Default Site for Help Desk:** Handles typical tasks performed by Help Desk operators, such as enabling or disabling accounts, resetting passwords, and modifying select properties of users and groups.
- **Default Site for Self-Administration:** Provides User Profile Editor, allowing end users to manage personal or emergency data through a simple-to-use Web Interface.

Each configuration template provides an individual set of commands installed by default. Once a Web Interface site has been created, you can customize its configuration by adding or removing commands, and by modifying Web pages (forms) associated with commands. The customization procedures are covered in the *Active Roles Web Interface Administration Guide*.

After initial configuration, you can modify Web Interface site parameters, such as the Web application alias, create new Web Interface sites, or delete existing Web Interface sites.

Creating or modifying a Web Interface site

After deploying the Web Interface, you can use the Configuration Center to create new Web Interface sites, or modify the existing ones.

You can create any number of Active Roles Web Interface sites, either with each site having its own configuration, or sharing the configuration with other sites. For more information about Web Interface site configuration, see *Create a Web Interface site* in the *Active Roles Feature Guide*.

When creating Web Interface sites, you can apply the configuration of an existing Web Interface site to the newly created one. If you have the Web Interface site tailored to meet your requirements, and need to deploy its instance on another web server, this option ensures that the new Web Interface site has the same set of menus, commands and pages as the existing one.

To create or modify a Web Interface site

1. In the Active Roles Configuration Center, on the **Dashboard** page, click **Web Interface > Manage Sites**.
Alternatively, on the side bar, click **Web Interface**.
2. On the Web Interface page, click the applicable button:
 - To create a new site, click **Create**.
 - To modify an existing site, select it from the list, then click **Modify**.
3. (Optional) In the **Web Application** step, configure the following settings:
 - **IIS Web site**: Specifies the IIS website containing the web application that implements the Web Interface site. The list is populated from the websites defined on the web server.
 - **Alias**: Specifies the alias of the web application that implements the Web Interface site. The alias defines the virtual path used in the address of the Web Interface site on the web server.
4. (Optional) In the **Configuration** step, specify how to set the configuration of the new website. The website configuration contains all customizable settings of the user interface elements, such as the website menus, commands, and web page forms that appear on the Web Interface.
 - **Keep the current configuration**: Uses the configuration currently assigned to the site. Select this option if you do not want to assign a different configuration to the site.
| NOTE: This setting is only available when modifying an existing site.
 - **Create from a template**: Creates a new configuration for the Web Interface site based on a template. When selected, you must specify a unique **Configuration name** and must also select a **Template** used as a baseline for the new configuration. Active Roles contains a default template for Administration, Helpdesk and Self-Service sites.

TIP: Select this option if you want the Web Interface site to use a separate configuration that is initially populated with the default template data and settings.

- **Use an existing configuration:** Assigns an existing configuration to the Web Interface site. When selected, you must specify the desired configuration from a list of saved configurations stored by the Administration Service.

NOTE: The list includes configurations compatible with the currently installed Active Roles version only.

- **Import from an existing configuration:** Creates a new configuration for the Web Interface site by importing data from an existing configuration. When selected, you must specify a unique **Configuration name** for the new configuration and must also select the desired **Configuration to import** from the list of supported configurations stored by the Administration Service.

NOTE: The list includes configurations compatible with the currently installed Active Roles version only.

TIP: Select this option if you want the Web Interface site to use a separate configuration that is:

- Populated with data imported from the configuration of an earlier Active Roles version, or
- Copied from an existing configuration of the current Active Roles version.

- **Import from a file:** Creates a new configuration for the Web Interface site by importing data from an exported configuration file. When selected, you must specify a unique **Configuration name** for the new configuration and must also select the **File to import**.

TIP: Select this option if you want the Web Interface site to use a separate configuration that is:

- Populated with data imported from the exported configuration file of an earlier Active Roles version.
- Copied from an existing exported configuration file of the current Active Roles version. You can export existing configurations with the **Web Interface > Export Configuration** option of the Configuration Center after selecting a web site.

5. (Optional) To commit your changes when creating or modifying a site, click **Create** or **Modify**, respectively. The Configuration Center then performs the configured changes, and will indicate the results.

After you configured a new site or modified an existing one, you can access it from your browser by using the specified web application alias in the following format:

`http://<website>/<alias>`

In this alias, <website> identifies the IIS website containing the web application that implements the Web Interface site, while <alias> is the alias of the web application as specified in the Configuration Center. For example, if the web application is contained in the default website, the address will be the following:

`http://<computer>/<alias>`

In this example, <computer> is the network name of the computer (web server) running the Web Interface.

NOTE: By default, you can connect to Web Interface sites via HTTP. To encrypt the data transferred from the web browser to the Web Interface with SSL protection provided by the web server, in the Active Roles Configuration Center, configure the **Web Interface > Manage Sites > Force SSL Redirection** settings.

For more information on how to enable SSL on your web server, see [How to Set Up SSL on IIS 7 or later](#) in the *Microsoft Learn IIS documentation*.

For more information on how to configure SSL redirection in the Active Roles Configuration Center, see [Configuring the Web Interface for secure communication](#).

Configuring the Web Interface for secure communication

By default, you can connect to Web Interface sites via HTTP. To encrypt the data transferred from the web browser to the Web Interface with SSL protection provided by the web server, in the Active Roles Configuration Center, configure the **Web Interface > Manage Sites > Force SSL Redirection** settings.

TIP: One Identity strongly recommends using HTTPS to transfer data securely on local or remote servers.

Prerequisites

Make sure that SSL is enabled on your web server. For more information, see [How to Set Up SSL on IIS 7 or later](#) in the *Microsoft Learn IIS documentation*.

To enable secure communication for the Web Interface for the first time

1. In the Active Roles Configuration Center, navigate to **Web Interface > Manage Sites**.
The list of configured Web Interface sites appear.
2. To modify the secure communication settings for the sites, click **Force SSL Redirection**.
3. From the **Available Websites** drop-down, select the website for which you want to apply SSL redirection. If you only have the default Web Interface sites configured, this setting shows **Default Web Site** only.
4. Enable **Force SSL Redirection**.

NOTE: The **Manage SSL redirection settings** window shows the SSL redirection status as follows:

- If the website is not configured for secure communication, **Force SSL redirection** is set to **Off**, and the HTTPS configuration **Status** is shown as

Not configured.

- If the website is configured for secure communication, **Force SSL redirection** is set to **On**, and the HTTPS configuration **Status** is shown as **Configured**.
 - If the website is configured for secure communication, but the SSL bindings are deleted from the IIS site, the **Force SSL redirection** option is set to **On** by default, but the the HTTPS configuration **Status** is shown as **Binding Deleted**. In this case, you must reconfigure secure communication for the website.
5. From the **Available HTTPS bindings** drop-down, select the required binding for the website.
 6. To apply your changes, click **Modify**. The **Summary** page then appears, showing the results of the configuration and allowing you to check the configuration log.
 7. To exit the **Manage SSL redirection settings** window, click **Finish**.

TIP: If you need to disable secure communication later for your Web Interface sites for any reason, open **Web Interface > Manage Sites > Force SSL Redirection** again, and set **Force SSL redirection** to **Off**. To apply your change, click **Modify**, then click **Finish**.

NOTE: Consider the following when configuring security settings for the Web Interface:

- After making any changes to the SSL settings, always clear your browser cache.
- Active Roles supports accessing the configured Web Interface sites via federated authentication. For details, see *Configuring federated authentication* in the *Active Roles Administration Guide*.

Deleting a Web Interface site

After deploying the Web Interface, you can use the Configuration Center to delete existing Web Interface sites.

To delete a Web Interface site

1. In the Active Roles Configuration Center, on the **Dashboard** page, click **Web Interface > Manage Sites**.
Alternatively, on the side bar, click **Web Interface**.
2. On the Web Interface page, select an existing site from the list, then click **Delete**.
3. In the **Ready to Delete** step, review the site data, then click **Delete**. The Configuration Center then performs the configured changes, and will indicate the results.

Installing optional tools and components

In addition to the Administration Service, Console and Web Interface, Active Roles allows you to install the following components:

- **Active Roles Management Shell:** Provides commands based on the Windows PowerShell platform for managing users, group, computers and other objects in Active Directory via Active Roles; administering certain Active Roles objects; and configuring Active Roles Administration Service instances and Web Interface sites.
- **ADSI Provider:** Enables custom applications and scripts to access directory data via Active Roles by using standard COM interfaces. Documentation for ADSI Provider can be found in the Active Roles SDK.
- **Active Roles SDK:** Provides developers with documentation and samples to help them customize Active Roles by creating custom client applications and user interfaces, and implementing business rules and policies based on custom scripts.
- **Data Collector:** Gathers data required for reporting. Retrieves data from specified data sources through the Administration Service, and stores the data on database server.
- **Report Pack:** A comprehensive suite of report definitions that cover various administrative actions available in Active Roles.

Installing only the Management Shell, ADSI Provider and SDK

The Active Roles Management Shell, SDK and ADSI Provider tools are known as Management Tools. In the Active Roles installer, on the **Component Selection** page, the Active Roles Setup wizard automatically selects the **Management Tools** component if you have selected any core Active Roles components, such as the Administration Service, the Active Roles Console or the Web Interface.

This means that by default, the Active Roles Setup wizard installs the Management Tools together with any core component. However, you can also install them separately by selecting them individually.

To install the Active Roles Management Tools separately

1. Log in with a user account that has administrator rights on the computer.
2. Mount the Active Roles installation .iso file.
3. To start installation, double-click **ActiveRoles.exe**.
4. On the **Component Selection** page, clear all check boxes except **Management Tools**, then click **Next**.
5. On the **Ready to Install** page, review the summary and click **Install**.
6. To close the setup wizard, on the **Completion** page, click **Finish**.

After installing the Management Tools:

- To open the Active Roles Management Shell, in the Windows Start menu or the **Apps** page of the operating system, select **Active Roles 8.2.1 Management Shell**. To view a reference list of all commands available in the Management Shell, run **QuickRef**.
- To open the Active Roles SDK documentation, in the Windows Start menu or the **Apps** page of the operating system, select **Active Roles 8.2.1 SDK**.

Installing the Data Collector and Report Pack

Active Roles comes with a comprehensive suite of report definitions, contained in the Active Roles Report Pack. To work with reports, you must:

- Install the Active Roles Collector
- Use the Data Collector wizard to deploy the Report Pack.

Installing the Data Collector

You can use the Active Roles Data Collector to prepare data for reporting, allowing you to configure, schedule, and run data collection jobs. Data Collector stores report data in a database on an on-premises SQL Server or Azure SQL database. For best results, use Microsoft SQL Server 2012 or a later version of SQL Server to host the Data Collector's database.

| NOTE: Collector can now store data in Azure database.

To install the Collector

1. Install Active Roles Management Tools. For more information, see [Installing only the Management Shell, ADSI Provider and SDK](#).
2. In the Active Roles .iso, navigate to the **Tools > Collector and Report Pack** folder, and double-click the .msi file there.
3. Follow the instructions of the setup wizard.
4. Wait while the wizard completes the installation.

After you installed Collector, you can start the Data Collector wizard by selecting **Active Roles 8.2.1 Collector and Report Pack** on the **Apps** page or **Start** menu.

Deploying the Report Pack

Following the installation of the Active Roles Data Collector and Report Pack package, you can deploy the Report Pack component via the Data Collector wizard.

To deploy the Active Roles Report Pack

1. Start the Data Collector wizard. To do so, click **Active Roles 8.2.1 Data Collector and Report Pack** on the **Apps** page or the Windows Start menu, depending on the version of your operating system.
2. On the **Select Task** page, click **Deploy reports to Report Server**, then click **Next**.
3. On the **Report Server** page, enter the URL of your SSRS Report Server in the **Report Server Web Service URL** text box, then click **Next**.

By default, the URL is `http://<server-name>/ReportServer`. You can use the Reporting Services Configuration Manager tool to confirm the server name and URL. For more information about URLs used in Reporting Services, see [Configure Report Server URLs \(SSRS Configuration Manager\)](#).

4. (Optional) On the **Data Source** page, configure the data source for the Active Roles reports:
 - a. Click the **Configure Data Source** button.
 - b. Configure the data source settings by specifying:
 - The database server instance hosting the database you have prepared via Data Collector.
 - The name of the database.
 - The database type.
 - The authentication method that is used for connecting to the database.

TIP: If you do not have a database prepared by Data Collector, you can configure the data source after deploying the Report Pack. For instructions, see *Working with reports* in the *Active Roles Administration Guide*.

5. Click **Next** and wait while the wizard deploys the Report Pack.

After deploying the Report Pack, you can create and view Active Roles reports using the Report Manager, a web-based tool included with SSRS. For more information, see *Generating and viewing a report* in the *Active Roles Administration Guide*.

Installing the Add-on Manager

Use the Active Roles Add-on Manager to install and manage Active Roles add-ons, or create new ones with its Add-on Editor.

To install Add-on Manager

1. Mount the Active Roles installation .iso file.
2. In the .iso file, navigate to the **Tools > Add-on Manager** folder.
3. Run the .exe file and follow the on-screen instructions.
4. In the configuration wizard that appears after the installation is finished, select how to register Add-on Manager to the Active Roles Administration Service.
 - **Any available Administration Service:** Select this option to register Add-on Manager with the nearest Administration Service, connecting to that Administration Service instance with the credentials of your current login account. To apply this option, your current login account must be an Active Roles Admin.
 - **Administration Service on this computer:** Select this option to register Add-on Manager with the Administration Service that runs on the computer you specify. The wizard will then connect to that Administration Service with the user name and password you supply. Make sure that you specify the user name and password of the Active Roles Admin.
5. To apply your change, click **Register**.

Installing the Diagnostic Tools

The Active Roles Diagnostic Tools package provides the following tools:

- **System Checker:** Checks your computer, SQL Server, and the Active Directory domains to see if your environment meets the requirements of deploying Active Roles.
- **Log Viewer:** Examines Active Roles diagnostic logs and event logs. Use these logs when contacting One Identity Support for assistance.
- **Directory Changes Monitor:** Provides statistics for the directory changes that occurred in a particular Active Directory domain.

To install Diagnostic Tools

1. Mount the Active Roles installation .iso file, and navigate to the **Tools > Diagnostic Tools** folder.
2. Run the .msi file in the folder, and follow the on-screen instructions of the setup wizard.

Using the System Checker

To check if a computer and your organization environment supports installing Active Roles, use the Active Roles System Checker tool.

To check system readiness with Active Roles System Checker

1. From your operating system, launch Active Roles System Checker.
2. Select **Computer > System Readiness Checks**.
3. To check the computer specifications, in the **Confirm System Readiness Checks** window, select the appropriate components to check for and click **Check**.
4. In the **System Readiness Checks** window, review the summary and confirm that the computer has passed the required checks. Take appropriate action before installing Active Roles. For example, if there is a warning about insufficient memory (RAM), then upgrade the computer's memory to the recommended amount.
5. To check the SQL Server requirements of Active Roles, in the Active Roles System Checker, select **Environment > SQL Server Checks**.
6. Enter the SQL Server name and appropriate credentials for the Active Roles service account, then click **Check**.
7. Review the summary to confirm that the SQL Server passed the checks.
8. To check the Active Directory requirements, in the Active Roles System Checker, select **Environment > Active Directory Checks**. Enter the domain controller (DC) name and the appropriate credentials for the Active Roles service account, then click **Check**.

A progress window appears. Once the check completes, System Checker shows the summary.
9. Review the summary to confirm the account has adequate permissions in Active Directory.
10. To learn more about Active Roles, click **Additional Resources**. To finish the check, click **Finish**.

Silent installation of Active Roles components

Active Roles supports command line options for various installation procedures. The following is a list of command line options available with Active Roles 8.2.1.

Category	Command	Description
Installation type	ActiveRoles.exe	Launches the setup wizard in normal mode.
	ActiveRoles.exe /quiet [parameters]	<p>Launches the setup wizard in quiet mode (also known as silent mode or unattended installation) with no user interaction.</p> <p>Examples:</p> <ul style="list-style-type: none"> ActiveRoles.exe /quiet /install ADDLOCAL=Service,Console /IAcceptActiveRolesLicenseTerms ActiveRoles.exe /quiet /install ADDLOCAL=Console TARGETDIR=D:\Active Roles\ /IAcceptActiveRolesLicenseTerms
Parameter syntax	/parameter [properties]	Specifies additional installation parameters. Separate parameter properties with spaces.
Properties	ADDLOCAL=	<p>The comma-separated list of the Active Roles components to install.</p> <p>Example:</p> <p>ADDLOCAL=Service,Console</p>
	REMOVE=	<p>The comma-separated list of the Active Roles components to remove.</p> <p>Example:</p> <p>REMOVE=Web,Console</p>
	TARGETDIR=	<p>The path of the Active Roles installation folder.</p> <p>Example:</p>

Category	Command	Description
		TARGETDIR=D:\Active Roles\
Component names	ALL	Specifies all Active Roles components.
	Service	Specifies the Active Roles Administration Service.
	Web	Specifies the Active Roles Web Interface.
	Console	Specifies the Active Roles Console (MMC Interface).
	Tools	Specifies the Active Roles Management Tools.
	SyncService	Specifies the Active Roles Synchronization Service.
Parameters	/IAcceptActiveRolesLicenseTerms	Acknowledges that you have read and understood the terms of the Active Roles license agreement. This parameter is required if both the /quiet and /install parameters are specified. Example: ActiveRoles.exe /quiet /install /IAcceptActiveRolesLicenseTerms
	/install [properties]	Installs the Active Roles components specified by the ADDLOCAL property to the TARGETDIR folder. <ul style="list-style-type: none"> • If ADDLOCAL is omitted, it installs all Active Roles components, except Synchronization Service. • If TARGETDIR is omitted, it installs Active Roles to %programfiles%\One Identity\Active Roles\. <p>TIP: To install Active Roles Synchronization Service use the ADDLOCAL=SyncService parameter.</p> <p>Takes effect only if any Active Roles components are installed, otherwise disregarded.</p>

Category	Command	Description
		<p>Example:</p> <pre>ActiveRoles.exe /install ADDLOCAL=Web TARGETDIR=D:\Active Roles\</pre>
	/repair	<p>Repairs all installed components.</p> <p>Takes effect only if any Active Roles components are installed, otherwise disregarded.</p> <p>Example:</p> <pre>ActiveRoles.exe /quiet /repair</pre>
	/modify	<p>Installs the Active Roles components specified by ADDLOCAL property and removes the components specified by the REMOVE property.</p> <p>Takes effect only if any Active Roles components are installed, otherwise disregarded.</p> <p>Example:</p> <pre>ActiveRoles.exe /modify ADDLOCAL=Service,Console REMOVE=Web</pre>
	/uninstall	<p>Uninstalls all components. Error conditions may terminate uninstall.</p> <p>Takes effect only if any Active Roles components are installed, otherwise disregarded.</p> <p>Example:</p> <pre>ActiveRoles.exe /quiet /uninstall</pre>
	/forceuninstall	<p>Use this parameter to uninstall all components if errors prevent normal uninstall.</p> <p>Takes effect only if any Active Roles components are installed, otherwise disregarded.</p> <p>Example:</p> <pre>ActiveRoles.exe /quiet /forceuninstall</pre>

Category	Command	Description
	<code>/forcerestart</code>	<p>Auto-restarts the computer when a restart is required to complete the requested setup actions.</p> <p>Use this parameter to avoid having to restart the computer manually after running the Active Roles setup wizard (for example, if setup needs to update any files that are currently in use).</p> <p>Examples:</p> <ul style="list-style-type: none">• <code>ActiveRoles.exe /quiet /uninstall /forcerestart</code>• <code>ActiveRoles.exe /quiet /repair /forcerestart</code>

Uninstalling Active Roles

If Active Roles or any of its components are no longer used in the machine, you can remove it with Active Roles setup wizard.

To uninstall Active Roles and its components

1. On the system where Active Roles is installed, open **Control Panel**, and navigate to **Programs > Programs and Features**.
2. In the list of installed programs, right-click on **One Identity Active Roles**, and click **Uninstall/Change**.
3. In the Active Roles setup wizard, click **Remove**.
4. To uninstall Active Roles, in the **Ready to Remove** dialog, click **Remove**.

TIP: If you want to fix a corrupted Active Roles installation, use the **Repair** option of the setup wizard to reinstall any corrupted Active Roles files.

Using Active Roles to manage Azure AD objects

You can use the Active Roles Configuration Center to perform Azure AD configuration tasks, such as adding, removing or modifying Azure tenants for managing their contents in Active Roles. Active Roles also supports the multi-tenant model.

NOTE: Administrative users or users with sufficient privileges only can view Azure configuration.

Configuring Active Roles to manage Azure AD using the Active Roles Configuration Center

You can add Azure tenants to manage their Azure AD resources in Active Roles with the Active Roles Configuration Center.

You can add an Azure tenant by two means:

- [Configuring a new Azure tenants.](#)
- [Importing an Azure tenant that you have used earlier in your organization.](#)

Configuring a new Azure tenant and consenting Active Roles as an Azure application

When installing Active Roles out-of-the-box, the **Directory Management > Tree > Azure** node of the Active Roles Web Interface only contains an empty **Azure Configuration** sub-node by default.

To manage Azure Active Directory (Azure AD) objects, you must specify an Azure tenant and configure Active Roles as a consented Azure application for it in the Active Roles Configuration Center.

NOTE: If you have already used an Azure tenant (or tenants) in a previous version of Active Roles, you can import and reconfigure them in two ways:

- If you perform an in-place upgrade of Active Roles (that is, you install the latest version without uninstalling the previous version of Active Roles first in one of the supported upgrade paths), you can reauthenticate the existing Azure tenants with the **Upgrade configuration** wizard upon launching the Active Roles Configuration Center after installation.

For more information on reauthenticating Azure tenants this way, see *Reconfiguring Azure tenants during upgrade configuration* in the *Active Roles 8.2.1 Upgrade Guide*. For more information on the supported upgrade paths, see *Upgrade and installation instructions* in the *Active Roles 8.2.1 Release Notes*.

- If you install a new version of Active Roles to a machine that does not have any earlier versions of the software installed (either because it has been already uninstalled, or it has been installed on another machine), you can import your existing Azure tenant(s) by importing your Azure AD configuration. Following the import, you can consent your Azure tenants manually.

For more information on importing existing Azure tenants this way, see [Importing an Azure tenant and consenting Active Roles as an Azure application](#).

Prerequisites

- The computer where Active Roles Configuration Center is running must already have all Azure-specific prerequisite software installed. If any of the prerequisite software required for Azure AD management are missing, install them with the following steps:
 1. Navigate to **Dashboard > Azure AD Configuration**.
 2. Click **Install Azure-specific Prereqs**.
 3. In the table that appears, install any components whose **Status** is not **Installed**.
 4. To apply your changes, click **Apply**.

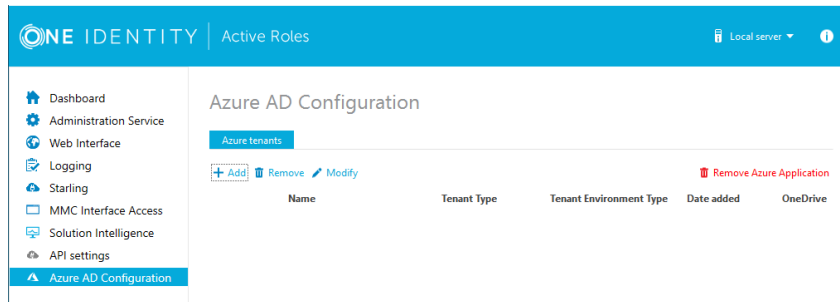
After all prerequisite software are installed, the **Install Azure-specific Prereqs** link will disappear, and the **Azure AD Configuration** option will appear.

- The Active Roles Administration Service must be already running. If Configuration Center indicates that the service is not running, then:
 1. In the Active Roles Configuration Center, navigate to the **Administration Service** page.
 2. Click **Start**.
- You must have the following administrator account roles and permissions at minimum:
 - Application Administrator
 - Privileged Role Administrator

However, One Identity recommends using an Azure AD administrator account with Global Administrator permission to perform the procedure.

To configure a new Azure tenant (or tenants) and set Active Roles as a consented Azure application

1. In the Active Roles Configuration Center, on the left pane, click **Azure AD Configuration**.



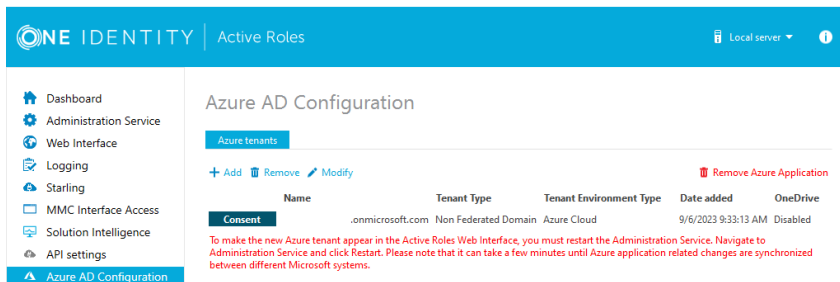
2. To start configuring a new Azure tenant, click **Add**.
3. From the **Tenant Type** drop-down, select the type of domain assigned to the new Azure tenant:
 - **Non-Federated Domain:** When selected, on-premises domains are not registered in Azure AD , and Azure AD Connect is not configured. Azure users and Azure guest users are typically created with the onmicrosoft.com UPN suffix.
 - **Federated Domain:** On-premises domains are registered in Azure AD and Azure AD Connect. Also, Active Directory Federation Services (ADFS) is configured. Azure users and Azure guest users are typically created with the UPN suffix of the selected on-premises domain.
 - **Synchronized Identity Domain:** On-premises domains may or may not be registered in Azure AD. Azure AD Connect is configured. Azure users and Azure guest users can be created either with the selected on-premises domain, or with the onmicrosoft.com UPN suffix.
4. From the **Tenant Environment Type** drop-down, select the type of environment you want to configure your Azure tenant in:
 - **Azure Cloud**
 - **Azure US Government** (for GCC and GCC-H tenants)

For the differences between Azure Cloud and Azure US Government tenants, see [Compare Azure Government and global Azure](#) in the *Microsoft Azure documentation*.

5. Click **Next**.
6. Authenticate your Azure AD administrator account.
 - If you already used one or more Azure AD administrator accounts on your PC, select your account from the **Pick an account** list, then provide the account password. If you do not find your account in the list, specify your account by clicking **Use another account**.

- If you have not used any Azure AD administrator accounts yet on the PC (for example, because you are configuring a fresh Active Roles installation), specify your account user name in the **Sign in** field, then provide your password.

Upon successful authentication, the new Azure tenant appears in the list.



7. To manage the Azure tenant and its contents in the Active Roles Web Interface, you must consent Active Roles as an Azure application. To do so, click **Consent** next to the Azure tenant.
8. Authenticate your Azure AD administration account again. Depending on the type of Microsoft pop-up that appears (**Pick an account** or **Sign in**), either select the Azure AD account you used for adding the Azure tenant, or specify its user name and password again.

NOTE: Make sure to specify the account used for adding the Azure tenant (that is, the account name listed under the **Name** column of the Azure tenant). Authenticating with another account will result in an error.

9. The standard Microsoft **Permissions requested** pop-up appears, listing all the permissions required for configuring Active Roles as an Azure application. To finish creating the Azure application, click **Accept**.

Active Roles then authenticates every Azure AD administrative operation performed in the Azure tenant with a set of generated client ID and client secret.

NOTE: Once you click **Accept**, Windows may show a **Security Warning** pop-up with the following message:

The current webpage is trying to open a site on your intranet. Do you want to allow this?

In such cases, clicking either **Yes** or **No** could freeze the pop-up dialog, but consenting the Azure tenant will finish without problem.

This issue can occur in case the computer running Active Roles has incorrect browser settings. As a workaround, to get an up-to-date status of the state of the Azure tenant, close and restart the Active Roles Configuration Center after clicking **Yes** in the **Security Warning** pop-up.

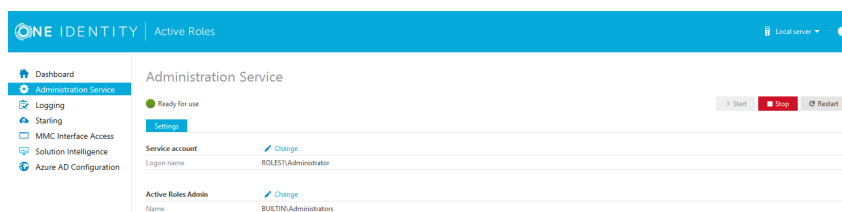
IMPORTANT: The Active Roles Administration Service creates the Entra ID application registration for Active Roles with the following required roles and permissions:

- **Privileged Authentication Administrator** role is necessary to reset password of Entra ID users and to update any additional sensitive information of Entra ID users.
- **User Administrator** role is necessary to create, update and delete an Entra ID user.
- **Exchange Administrator** role, and administrator-consented Exchange.ManageAsApp and full_access_as_app application permissions are necessary for EXO related operations
 - **Exchange.ManageAsApp** application permission is for other EXO related functionalities of Active Roles.
 - **full_access_as_app** application permission is for EXO EWS functionalities of Active Roles.
- **RoleManagement.ReadWrite.Directory** application permission is necessary to assign role to an Entra ID user.
- **Sites.FullControl.All** application permission is necessary for OneDrive site creation for Entra ID users.

The roles and permissions added by default are required for the Active Roles Administration Service to function as expected. Modifying these default roles and permissions might result in a configuration that is outside of the scope of the Active Roles Support Model.

You can add additional permissions to the Entra ID application or remove any of them by signing in to the Azure Portal. For more information, see the [Microsoft Entra ID application management documentation](#).

10. If you have additional Azure tenants to add and consent, configure them as described in the previous steps of this procedure.
11. To make the configured Azure tenant(s) appear in the Active Roles Web Interface, you must restart the Administration Service. To restart the Administration Service, open the Configuration Center, click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



TIP: After the Azure tenant or tenants are configured, and Active Roles is also set as a consented Azure AD application for it, you can view and modify the configured tenant(s) and their settings at the following locations:

- To change the domain type or OneDrive provisioning settings of an Azure tenant, in the Active Roles Configuration Center, navigate to **Azure AD Configuration**, select the Azure tenant, and click **Modify**. For more information, see *Viewing or modifying the Azure tenant type* in the *Active Roles Administration Guide*.

- To check the connectivity status of the Azure configuration, in the Active Roles Web Interface, navigate to **Directory Management > Tree > Azure > Azure Configuration > Azure Health Check**. For more information, see *Viewing the Azure Health status for Azure tenants and applications* in the *Active Roles Administration Guide*.
- To check the Azure Licenses Report, in the Active Roles Web Interface, navigate to **Directory Management > Tree > Azure > Azure Configuration > Azure Licenses Report**. For more information, see *Viewing the Azure Licenses Report of an Azure tenant* in the *Active Roles Administration Guide*.
- To check the Office 365 Roles Report, in the Active Roles Web Interface, navigate to **Directory Management > Tree > Azure > Azure Configuration > Office 365 Roles Report**. For more information, see *Viewing the Office 365 Roles Report of an Azure tenant* in the *Active Roles Administration Guide*.

NOTE: Azure Multi-Factor Authentication (MFA) is automatically enforced for Azure users and Azure guest users added to the configured Azure tenant. To disable Azure MFA for the Azure tenant, sign in to the Azure Portal and navigate to **Tenant > Properties > Manage Security defaults** and set **Enable Security defaults** to **No**.

Importing an Azure tenant and consenting Active Roles as an Azure application

If you previously managed an Azure AD deployment, but you are not upgrading from a previous version of Active Roles via in-place upgrade (for example, because the previous version of Active Roles has been uninstalled before installing the new version), you can import, reauthenticate and consent existing Azure tenants via the Active Roles Configuration Center.

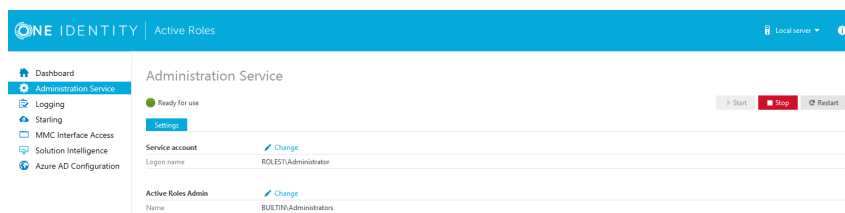
NOTE: Consider the following if you did not use any Azure tenants earlier, or if you installed the latest version of Active Roles via in-place upgrade:

- If you installed Active Roles out-of-the-box, and no Azure AD environment was used previously in your organization, you must specify a new Azure tenant to manage Azure directory objects (such as Azure users, guest users, contacts, M365 groups or Azure security groups). For more information, see [Configuring a new Azure tenant and consenting Active Roles as an Azure application](#).
- If you perform an in-place upgrade of Active Roles (that is, you install the latest version without uninstalling the previous version of Active Roles first in one of the supported upgrade paths), you can reauthenticate the existing Azure tenants with the **Upgrade configuration** wizard upon launching the Active Roles Configuration Center after installation.

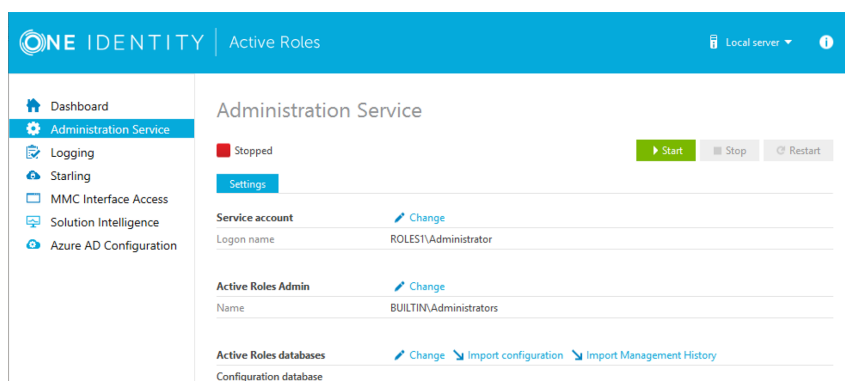
For more information on reauthenticating Azure tenants this way, see *Reconfiguring Azure tenants during upgrade configuration* in the *Active Roles 8.2.1 Upgrade Guide*. For more information on the supported upgrade paths, see *Upgrade and installation instructions* in the *Active Roles 8.2.1 Release Notes*.

To import and reauthenticate an Azure tenant and set Active Roles as a consented Azure application

1. Stop the Active Roles Administration Service. To do so, in the Active Roles Configuration Center, navigate to **Administration Service**, then click **Stop**.



2. After the Active Roles Administration Service stopped, open the **Import configuration** wizard by clicking **Active Roles databases > Import configuration**.

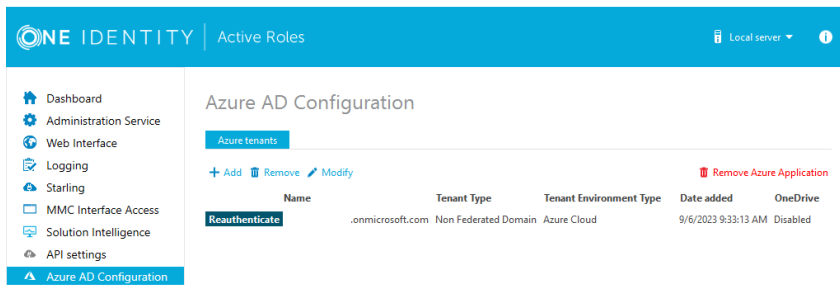


3. Perform the steps of the wizard. For more information, see *Importing configuration data* in the *Active Roles Upgrade Guide*, or [Deploying the Administration Service](#).

CAUTION: Importing a configuration will overwrite every Azure tenant currently listed in the **Azure AD Configuration** page with those included in the imported configuration.

4. After the import procedure finished, start the Active Roles Administration Service by clicking **Start** in the **Administration Service** page.
5. In the Active Roles Configuration Center, on the left pane, click **Azure AD Configuration**.

The list of imported Azure tenants appears.



6. To configure an imported Azure tenant, click **Reauthenticate**.
7. Authenticate your Azure AD administrator account.
 - If you already used one or more Azure AD administrator accounts on your PC, select your account from the **Pick an account** list, then provide the account password. If you do not find your account in the list, specify your account by clicking **Use another account**.
 - If you have not used any Azure AD administrator accounts yet on the PC (for example, because you are configuring a fresh Active Roles installation), specify your account user name in the **Sign in** field, then provide your password.
8. To manage the Azure tenant and its contents in the Active Roles Web Interface, you must consent Active Roles as an Azure application. To do so, click **Consent** next to the Azure tenant.
9. Authenticate your Azure AD administration account again. Depending on the type of Microsoft pop-up that appears (**Pick an account** or **Sign in**), either select the Azure AD account you used for adding the Azure tenant, or specify its user name and password again.

NOTE: Make sure to specify the account used for adding the Azure tenant (that is, the account name listed under the **Name** column of the Azure tenant). Authenticating with another account will result in an error.
10. The standard Microsoft **Permissions requested** pop-up appears, listing all the permissions required for configuring Active Roles as an Azure application. To finish creating the Azure application, click **Accept**.

Active Roles then authenticates every Azure AD administrative operation performed in the Azure tenant with a set of generated client ID and client secret.

NOTE: Once you click **Accept**, Windows may show a **Security Warning** pop-up with the following message:

The current webpage is trying to open a site on your intranet. Do you want to allow this?

In such cases, clicking either **Yes** or **No** could freeze the pop-up dialog, but consenting the Azure tenant will finish without problem.

This issue can occur in case the computer running Active Roles has incorrect browser settings. As a workaround, to get an up-to-date status of the state of the

Azure tenant, close and restart the Active Roles Configuration Center after clicking **Yes** in the **Security Warning** pop-up.

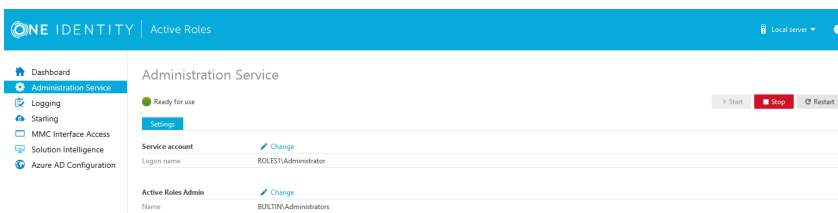
IMPORTANT: The Active Roles Administration Service creates the Entra ID application registration for Active Roles with the following required roles and permissions:

- [Privileged Authentication Administrator](#) role is necessary to reset password of Entra ID users and to update any additional sensitive information of Entra ID users.
- [User Administrator](#) role is necessary to create, update and delete an Entra ID user.
- [Exchange Administrator](#) role, and administrator-consented Exchange.ManageAsApp and full_access_as_app application permissions are necessary for EXO related operations
 - [Exchange.ManageAsApp](#) application permission is for other EXO related functionalities of Active Roles.
 - [full_access_as_app](#) application permission is for EXO EWS functionalities of Active Roles.
- [RoleManagement.ReadWrite.Directory](#) application permission is necessary to assign role to an Entra ID user.
- [Sites.FullControl.All](#) application permission is necessary for OneDrive site creation for Entra ID users.

The roles and permissions added by default are required for the Active Roles Administration Service to function as expected. Modifying these default roles and permissions might result in a configuration that is outside of the scope of the Active Roles Support Model.

You can add additional permissions to the Entra ID application or remove any of them by signing in to the Azure Portal. For more information, see the [Microsoft Entra ID application management documentation](#).

11. To make the configured Azure tenant(s) appear in the Active Roles Web Interface, you must restart the Administration Service. To restart the Administration Service, open the Configuration Center, click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



TIP: After the Azure tenant or tenants are configured, and Active Roles is also set as a consented Azure AD application for it, you can view and modify the configured tenant(s) and their settings at the following locations:

- To change the domain type or OneDrive provisioning settings of an Azure tenant, in the Active Roles Configuration Center, navigate to **Azure AD Configuration**, select the Azure tenant, and click **Modify**. For more information, see *Viewing or modifying the Azure tenant type* in the *Active Roles Administration Guide*.
- To check the connectivity status of the Azure configuration, in the Active Roles Web Interface, navigate to **Directory Management > Tree > Azure > Azure Configuration > Azure Health Check**. For more information, see *Viewing the Azure Health status for Azure tenants and applications* in the *Active Roles Administration Guide*.
- To check the Azure Licenses Report, in the Active Roles Web Interface, navigate to **Directory Management > Tree > Azure > Azure Configuration > Azure Licenses Report**. For more information, see *Viewing the Azure Licenses Report of an Azure tenant* in the *Active Roles Administration Guide*.
- To check the Office 365 Roles Report, in the Active Roles Web Interface, navigate to **Directory Management > Tree > Azure > Azure Configuration > Office 365 Roles Report**. For more information, see *Viewing the Office 365 Roles Report of an Azure tenant* in the *Active Roles Administration Guide*.

NOTE: Azure Multi-Factor Authentication (MFA) is automatically enforced for Azure users and Azure guest users added to the configured Azure tenant. To disable Azure MFA for the Azure tenant, sign in to the Azure Portal and navigate to **Tenant > Properties > Manage Security defaults** and set **Enable Security defaults** to **No**.

Configuring Active Roles to manage hybrid AD objects

You can use the Active Roles Configuration Center to perform Azure AD configuration tasks, such as adding, removing or modifying Azure tenants for managing their contents in Active Roles. Active Roles also supports the multi-tenant model.

NOTE: Administrative users or users with sufficient privileges only can view Azure configuration.

Configuring Active Roles to manage hybrid AD objects has the following main steps:

1. Configuring an Azure AD tenant.
2. Consenting Active Roles as an Azure AD application.
3. Providing the administrator consent for the Azure AD application.
4. Enforcing the **Built-in Policy - Azure - Default Rules to Generate Properties** Policy Object to the on-premises Active Directory containers, which are synchronized to Azure AD.

NOTE: After an upgrade, the **edsvaAzureOffice365Enabled** attribute will not be available for viewing or editing from **Organizational Unit > Advanced Properties**, or through the relevant Management Shell cmdlet. However, the Organizational Unit container will remain an Azure enabled container, as the Azure policy is already applied.

Active Roles availability on Azure and AWS Marketplace

Active Roles supports deployment on the Amazon Web Services (AWS) and Azure platforms via Active Roles Marketplace images, using your organization subscription.

The marketplace images contain Active Roles running on Windows Server 2022 Datacenter Edition.

NOTE: Amazon Marketplace does not offer AWS EC2 instances preinstalled with Active Roles. You must deploy the EC2 instances first, then install and configure Active Roles manually on them.

TIP: To install additional Active Roles components later, modify your existing installation. For more information, see [Installing optional tools and components](#).

AWS and Azure virtual environment recommendations

If you deploy Active Roles in an AWS or Azure virtual environment via its marketplace image, One Identity recommends using the following virtual environments to host your Active Roles installation.

TIP: Before choosing the Azure virtual machine (VM) or Amazon Elastic Compute Cloud (EC2) instance to use, see the following resources:

- For more information on Azure VMs, see [Windows virtual machines](#) in the *Microsoft Azure portal*.
- For more information on AWS EC2 instances, see [EC2 instance types](#) in the *Amazon Web Services portal*.

NOTE: One Identity offers limited support for the virtual environments recommended in this section, as the actual performance on the listed environments (and the optimal environment to choose) might depend on the number of dynamic groups, Managed Units (MU), policies, scripts, workflows and other resources managed in your organization.

One Identity reserves the right to withhold support until you adapt your virtual environment for optimal performance to manage your resources with Active Roles.

Recommended AWS EC2 instance types

The Active Roles marketplace image was tested to work with the following Amazon Elastic Compute Cloud (EC2) instances:

- **m5a.2xlarge**: 8 vCPU, 32 GB RAM, up to 10 Gbps network bandwidth, up to 2880 Mbps EBS bandwidth.
- **m5a.xlarge**: 4 vCPU, 16 GB RAM, up to 10 Gbps network bandwidth, up to 2880 Mbps EBS bandwidth.
- **m5.2xlarge**: 8 vCPU, 32 GB RAM, up to 10 Gbps network bandwidth, up to 4750 Mbps EBS bandwidth.
- **m5.xlarge**: 4 vCPU, 16 GB RAM, up to 10 Gbps network bandwidth, up to 4750 Mbps EBS bandwidth.
- **m4.2xlarge**: 8 vCPU, 32 GB RAM, EBS-only storage, high network performance.
- **m4.xlarge**: 4 vCPU, 16 GB RAM, EBS-only storage, high network performance.
- **m3.2xlarge** (previous generation): 2 vCPU, 30 GB RAM, non-EBS optimized SSD, high network performance.
- **m3.xlarge** (previous generation): 4 vCPU, 15 GB RAM, non-EBS optimized SSD, high network performance.

Recommended Azure VMs

One Identity recommends using the following Azure VMs with the Active Roles marketplace image:

- **Standard D8s v3**: 8 vCPU, 32 or 64 GB RAM, 12800 max IOPS, 64 GiB local storage.
- **Standard D4s v3**: 4 vCPU, 16 GB RAM, 6400 max IOPS, 32 GiB local storage.
- **Standard D3 v2**: 4 vCPU, 14 GB RAM, 0 max IOPS, 200 GiB local storage.
- **Standard DS3 v2**: 4 vCPU, 14 GB RAM, 12800 max IOPS, 28 GiB local storage.
- **Standard D2 v4**: 2 vCPU, 8 GB RAM, 3200 max IOPS, 16 GiB local storage.
- **Standard D2s v3**: 2 vCPU, 16 GB RAM, 3200 max IOPS, 16 GiB local storage.
- **Standard D2 v2**: 2 vCPU, 7 GB RAM, 0 max IOPS, 100 GiB local storage.

Supported AWS and Azure environment types

Active Roles supports the following virtual environment types:

- **Cloud-only**: Active Roles, its components, and all required third-party components are deployed on the same cloud platform. For more information on configuring this environment type, see [Configuring the Azure or AWS virtual machine](#).
- **Hybrid on-premises**: Some components required by Active Roles are deployed in your on-premises environment. For more information on configuring this

environment type, see [Configuring a hybrid on-premises environment for Active Roles](#).

NOTE: One Identity provides no support or assistance in the configuration of these environments, or troubleshooting connectivity and performance issues related to the Azure and AWS services.

Configuring a hybrid on-premises environment for Active Roles

In a hybrid on-premises setup, some Active Roles components are deployed in the cloud while others in your on-premises environment.

NOTE: Consider the following if you plan to deploy Active Roles and its resources in a hybrid on-premises environment:

- Active Roles supports hybrid on-premises environments using the Azure or AWS cloud platforms.
- For optimal performance, One Identity recommends hosting Active Roles and the SQL Server containing the Active Roles databases in the same region.

One Identity recommends configuring a site-to-site VPN connection between your cloud environment (Azure or AWS) and your on-premises environment. This connection will be used to connect your on-premises network to your cloud virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. The connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

Prerequisites

Before you start configuring the site-to-site VPN connection between your on-premises and cloud environments (Azure or AWS), make sure that the following conditions are met:

- Your organization has a compatible VPN device that you can configure.
- The VPN device has an externally-facing public IPv4 address.
- You are familiar with the IP address ranges located in the on-premises network configuration.
- All cloud (Azure or AWS) resources are located in the same region or location.

To configure a site-to-site VPN between Azure and your on-premises environment

1. In the Azure portal, create a new resource group in your desired region. For more information, see [Create resource groups](#) in the *Microsoft Azure documentation*.
2. Create a virtual network with required address space. For more information, see [Quickstart: Use the Azure portal to create a virtual network](#) in the *Microsoft Azure documentation*.

3. Create a gateway subnet in virtual network you configured. For more information, see [Create a gateway subnet](#) in the *Microsoft Azure documentation*.
4. Specify a public IP address.
5. Create the VPN gateway using the public IP address you specified. For more information, see [Create a VPN gateway](#) in the *Microsoft Azure documentation*.
6. Create the local network gateway using the public IP address of the on-premises gateway and the address space of the on-premises network. For more information, see [Local network gateway configuration](#) in the *Microsoft Azure documentation*.
7. Configure your VPN device.
8. Create the VPN connection in the local network gateway configured earlier.
9. Make sure that the shared key provided in the **Connection** settings of Azure matches with that of the on-premises environment.
10. In Azure, check that the **Azure Connection** and **Connection Status** fields are updated and the status appears as **Connected**.
11. After the site-to-site VPN connection has been set, configure Active Roles with the on-premises domain controller (DC).

For more information about configuring site-to-site VPN connections with Azure, see [Tutorial: Create a site-to-site VPN connection in the Azure portal](#) in the *Microsoft Azure documentation*.

To configure a site-to-site VPN between AWS and your on-premises environment

1. Create a customer gateway using the public IP address of your on-premises network. For more information, see [Your customer gateway device](#) in the *AWS Site-to-Site VPN User Guide*.
2. Create a virtual private gateway, and attach it to your VPC. For more information, see [Creating a virtual private gateway](#) in the *AWS Direct Connect User Guide*.
3. In the route table, select **Route Propagation**. For more information, see [Configure route tables](#) in the *Amazon Virtual Private Cloud User Guide*.
4. Update your security groups. For more information, see [Work with security groups](#) in the *Amazon Virtual Private Cloud User Guide*.
5. Create a site-to-site VPN connection between the customer gateway and the virtual private gateway configured earlier. For more information, see the [AWS Site-to-Site VPN User Guide](#).
6. Once the configuration is ready, to save it in TXT format with the network details, click **Download Configuration**, then set the following options:
 - **Vendor: Generic**
 - **Platform: Generic**
 - **Software: Vendor Agnostic**
7. Configure your on-premises gateway and/or VPN device.

8. In the AWS Console, check that the **Tunnel** status of the site-to-site VPN connection appears as **UP**.
9. After the site-to-site VPN connection has been set, configure Active Roles with the on-premises domain controller (DC).

For more information about configuring site-to-site VPN connections with AWS, see [Getting started with AWS Site-to-Site VPN](#) in the *AWS Site-to-Site VPN User Guide*.

Creating Azure or AWS virtual machines for Active Roles

To deploy Active Roles in the AWS or Azure cloud with a marketplace image, you must:

1. Open all required communication ports. For more information, see [Opening communication ports for the Active Roles virtual machine](#).
2. Create the Active Roles virtual machine (VM) and deploy Active Roles on it with its marketplace image. For more information, see [Configuring the Azure or AWS virtual machine](#).

Prerequisites

Before you begin, make sure that the following prerequisites are met:

- Configure the domain controller (DC) before deploying the Active Roles VM in the cloud.
- Configure the SQL Server that will host the Active Roles databases before deploying the Active Roles VM in the cloud.

NOTE: When configuring your SQL Server, make sure that the Active Roles Administration Service has the necessary access permissions.

- For the list of required permissions, see [SQL Server permissions](#).
- For the additional SQL Server port requirements, see [Configure the Windows Firewall to allow SQL Server access](#) in the *Microsoft SQL documentation*.
- Make sure that the DC and your SQL Server are accessible from the Active Roles VM.
- If you use a **hybrid on-premises** environment type, add a DC to your environment and connect Active Roles to it. Also, make sure that your network is configured so that both the DC and your SQL Server are accessible to the Active Roles VM.
- If you use a **hybrid on-premises** environment type, make sure that your network is configured so that both the DC and your SQL Server are accessible to the Active Roles VM.

Opening communication ports for the Active Roles virtual machine

If a firewall protects the environment that is managed by Active Roles, you must open the required ports between Active Roles Administration Service and the managed environment.

For example, if you have a firewall configured between Active Roles and a DNS, you must open:

- Port **15172** (both inbound and outbound) on the Active Roles virtual machine (VM) and the firewall between Active Roles and Exchange Server.
- Port **53** on the DNS or the firewall between Active Roles and the DNS.

For the list of communication ports used by Active Roles, see *Communication ports* in the *Active Roles Administration Guide*. For more information on Active Roles communication ports in general, see [Knowledge Base Article 4227036](#) on the *One Identity support portal*.

Opening ports in Azure

To open ports in Azure or create an endpoint to your VM, you must:

1. Create a network filter on a subnet or a VM network interface.
2. Select the filters to control both inbound and outbound traffic on a network security group attached to the resource that receives the traffic.

For the steps of opening ports in Azure, see [Tutorial: Filter network traffic with a network security group using the Azure portal](#) in the *Microsoft Azure documentation*.

Opening ports in AWS

Amazon virtual environments use security groups that act as a virtual firewall, controlling the traffic for one or more instances. You can add rules to each security group to allow traffic to or from its associated instances.

If your organization has additional requirements that are not met by the Amazon security groups, you can maintain your own firewall on any of your instances instead of using the Amazon system-provided security groups.

If you plan to deploy Active Roles in AWS, make sure that the following ports are open:

- Port 3389 for Windows-based AMIs and RDP.
- Port 5985 for WINRM towards the required IP address.

For the steps of opening ports on AWS, see [Amazon EC2 security groups for Windows instances](#) in *Amazon Elastic Compute Cloud User Guide for Windows Instances*.

Configuring the Azure or AWS virtual machine

If you have [opened all required ports](#) and checked that [all prerequisites are met](#) for cloud deployment, configure the Azure virtual machine (VM) or Amazon Elastic Compute Cloud (EC2) instance that will host Active Roles.

To configure an Azure VM for Active Roles

1. Log in to the Azure Portal with the appropriate credentials.
2. Navigate to Azure Marketplace.
3. In the Azure Marketplace, search the **One Identity Active Roles** offer.
4. Select the marketplace image for deployment.
5. Create the Azure VM by following the on-screen instructions. For more information, see [Quickstart: Create a Windows virtual machine in the Azure portal](#) in the *Microsoft Azure documentation*.
6. After your VM is created and running, join it to your domain. For more information, see [Join a Computer to a Domain](#) in the *Microsoft Windows Server documentation*.
TIP: You can also use Azure Artifacts to join your VM to a domain. For more information, see the [Microsoft Azure Artifacts documentation](#).
7. Continue the configuration of Active Roles in the VM as described in the [Deploying the Administration Service](#) and later sections.

To configure an EC2 instance on AWS

NOTE: Amazon Marketplace does not offer AWS EC2 instances preinstalled with Active Roles. You must deploy the EC2 instances first, then install and configure Active Roles manually on them.

1. Log in to the AWS Console with the appropriate credentials.
2. Navigate to AWS Marketplace.
3. In the AWS Marketplace, search the **One Identity Active Roles** offer.
4. Select the marketplace image for deployment:
5. Launch an AWS EC2 instance.
NOTE: As a minimum recommended configuration, One Identity recommends using an **m3.xlarge** instance.
6. Once your EC2 instance is created and running, join it to your domain. For more information, see [Manually join a Windows instance](#) in the *AWS Directory Service documentation*.
7. Continue the configuration of Active Roles in the EC2 instance as described in the [Deploying the Administration Service](#) and later sections.

Deploying Active Roles on Microsoft Azure VM

This section describes how to deploy Active Roles in a [Microsoft Azure Infrastructure](#) environment. After you complete these steps, you have the following services deployed in Microsoft Azure using Microsoft Azure Virtual Machines (VMs):

- A supported version of SQL Server to host the Active Roles databases.
For the list of SQL Server versions supported by Active Roles, see *System requirements* in the *Active Roles Release Notes*.
- Active Roles Administration Service
- Active Roles Web Interface

Deploying Microsoft SQL Server on an Azure VM

If you deploy Active Roles in the Azure cloud, you must also deploy an SQL Server instance in an Azure virtual machine (VM), so that you can host the Active Roles databases.

For the list of SQL Server versions supported by Active Roles, see *System requirements* in the *Active Roles Release Notes*.

Prerequisites

- A Microsoft account with at least one valid, active Microsoft Azure subscription.
- At least one writable replica domain controller installed in your Microsoft Azure account.

For more information on how to install a replica domain controller, see [Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks](#).

To deploy SQL Server on an Azure VM

1. Create a VM based on an SQL Server image published in Windows Azure.
When creating the VM, on the **Virtual machine configuration** page, select the **Create a new cloud service** option and choose the Virtual Network used by your replica domain controller in Windows Azure.
For more information on how to deploy an SQL Server in Microsoft Azure, see [Create SQL Server on a Windows virtual machine in the Azure portal](#) in the *Microsoft Azure documentation*.
2. Join the SQL Server VM to your Active Directory domain.
3. Using SQL Server Management Studio, grant the **sysadmin** fixed server role to the domain user account that will be used as the service account for the Active Roles Administration Service.
4. Configure Windows Firewall to allow connections to TCP port **1433** from computers in your virtual network.

NOTE: As SQL Server will be accessed from within the virtual network, you do not need to create public endpoints in Windows Azure.

Deploying the Active Roles Administration Service on an Azure VM

Prerequisites

- A Microsoft account with at least one valid, active Microsoft Azure subscription.
- At least one writable replica domain controller installed in your Microsoft Azure account.

For more information on how to install a replica domain controller, see [Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks](#).

To deploy the Active Roles Administration Service on an Azure VM

1. Create a virtual machine (VM) based on a supported Windows Server image published in Microsoft Azure. For the list of Windows Server versions supported by Active Roles, see *System requirements* in the *Active Roles Release Notes*.

When creating the VM, on the **Virtual machine configuration** page, select the cloud service that you created for the SQL Server virtual machine in [Deploying Microsoft SQL Server on an Azure VM](#). This will automatically select the correct virtual network as this cloud service is already used to host the SQL Server virtual machine.

2. Connect the newly-created VM to your Active Directory domain.
3. Connect to the VM using Remote Desktop, and run the Active Roles Setup wizard to install the Active Roles Administration Service. For more information, see [Deploying the Administration Service](#).

When prompted for the service account, specify the appropriate user account defined in your Active Directory domain. Ensure that this user account is a member of the Administrators local group on the VM where you are installing the Administration Service. For example, this could be a domain user account that belongs to the Domain Admins group of your Active Directory domain.

When prompted for SQL Server, specify the name of the SQL Server you deployed in [Deploying Microsoft SQL Server on an Azure VM](#).

4. To configure the Windows Firewall, run the following Windows PowerShell command on the VM where you installed the Active Roles Administration Service:

```
$allowedClientSubnets = @('10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16');
New-NetFirewallRule -DisplayName "Active Roles" -Direction Inbound `
-Action Allow -Service 'aradminsvc' -RemoteAddress $allowedClientSubnets `
-Enabled True
```

Deploying the Active Roles Web Interface on an Azure VM

Prerequisites

- A Microsoft account with at least one valid, active Microsoft Azure subscription.
- At least one writable replica domain controller installed in your Microsoft Azure account.

For more information on how to install a replica domain controller, see [Install a Replica Active Directory Domain Controller in Windows Azure Virtual Networks](#).

To deploy the Active Roles Web Interface on an Azure VM

1. Create a virtual machine (VM) based on a supported Windows Server image published in Microsoft Azure. For the list of Windows Server versions supported by Active Roles, see *System requirements* in the *Active Roles Release Notes*.

When creating the VM, on the **Virtual machine configuration** page, select the cloud service that you created for the SQL Server virtual machine in [Deploying Microsoft SQL Server on an Azure VM](#). This will automatically select the correct virtual network as this cloud service is already used to host the Active Roles Administration Service and SQL Server VMs. For more information, see *Create Virtual Machine and Deploy to Virtual Network* in [Add a Virtual Machine to a Virtual Network](#).

2. Connect the newly-created VM to your Active Directory domain.
3. Connect to the VM using Remote Desktop, and run the Active Roles setup to install the Active Roles Web Interface. For more information, see [Installing the Web Interface](#) and [Performing the initial configuration of the Web Interface](#).

When prompted, choose the option to connect to the Administration Service on the specified computer, and specify the fully qualified domain name of the VM you deployed in [Deploying the Active Roles Administration Service on an Azure VM](#).

Configuring Active Roles for AWS Managed Microsoft AD

NOTE: This feature is officially supported starting from Active Roles 8.1.3 SP1 (build 8.1.3.10). It is not supported on Active Roles 8.1.3 (build 8.1.3.2) and earlier versions.

Active Roles supports deployment and configuration in the Amazon cloud to manage [AWS Managed Microsoft AD](#) instances hosted via AWS Directory Service.

This allows you to:

- Perform Active Directory management tasks in your AWS Managed Microsoft AD environment.
- Synchronize directory data from an on-premises AD environment to AWS Managed Microsoft AD.
- Synchronize passwords from an on-premises Active Directory to AWS Managed Microsoft AD (with certain limitations).

For more information about the Active Roles features supported with AWS Managed Microsoft AD, see *Support for AWS Managed Microsoft AD* in the *Active Roles Feature Guide*.

Supported AWS Managed Microsoft AD deployment configuration

To manage AWS Managed Microsoft AD environments, you must deploy Active Roles in Amazon Web Services (AWS) in the following configuration:

- Active Roles must be deployed on an Amazon Elastic Compute Cloud (EC2) instance or instances. For more information, see the [Amazon Elastic Compute Cloud documentation](#).
- The SQL Server required by Active Roles Administration Service must run on a separate Amazon Relational Database Service for Microsoft SQL Server (RDS for SQL Server) instance. For more information, see the [Amazon RDS documentation](#).
- The Active Directory environment must be hosted in AWS via AWS Directory Service. For more information, see the [AWS Directory Service documentation](#).

NOTE: Support for AWS Managed Microsoft AD by Active Roles was tested only in this configuration. Active Roles does not officially support managing AWS Managed Microsoft AD environments in a hybrid deployment, that is, using an on-premises Active Roles and/or SQL Server installation and hosting AD via AWS Directory Service.

Deployment requirements for AWS Managed Microsoft AD support

Before starting the deployment and configuration of Active Roles to manage AWS Managed Microsoft AD via AWS Directory Service, make sure that the following requirements are met.

NOTE: When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. For more information about environment virtualization, see [One Identity's Product Support Policies](#).

Connectivity requirements

You must have:

- Stable network connectivity to Amazon Web Services (AWS).
- Port **1433** open and available for the Amazon Relational Database Service (RDS) service.
- Access to the AWS service with the **AWSAdministratorAccess** permission.

NOTE: Make sure that you have **AWSAdministratorAccess** permission, as it is required for certain configuration steps. The **AWSPowerUserAccess** permission is not sufficient for completing the entire configuration procedure.

Infrastructure requirements

To deploy and configure Active Roles for AWS Managed Microsoft AD, you must have access to the following AWS services and resources:

- AWS Managed Microsoft AD deployed via AWS Directory Service.
- One or more Amazon Elastic Compute Cloud (EC2) instance(s) hosting the Active Roles services and components.

The EC2 instance(s) must have, at minimum:

- 2 vCPUs running at 2.0 GHz.
- 4 GB of RAM.

TIP: One Identity recommends hosting the main Active Roles services and components (the Active Roles Service and Console, and the Active Roles Web Interface) on separate EC2 instances. If you deploy all Active Roles services and components in a single EC2 instance, use a more powerful instance to ensure a better user experience for the product.

NOTE: AWS Managed Microsoft AD support was tested with a single **t2.large** EC2 instance.

- An Amazon Relational Database Service for SQL Server (RDS for SQL Server).

NOTE: AWS Managed Microsoft AD support was tested with an RDS instance running the latest version of Microsoft SQL Server.

Make sure that all these components are discoverable or visible to each other.

Main steps of configuring Active Roles for AWS Managed Microsoft AD

If your organization and environment meet the [Deployment requirements for AWS Managed Microsoft AD support](#), configuring Active Roles for managing AWS Managed Microsoft AD via AWS Directory Service has the following main steps:

1. [Creating your AWS Managed Microsoft AD environment.](#)
2. [Creating an Amazon Elastic Compute Cloud \(EC2\) instance for Active Roles.](#)
3. [Joining the EC2 instance to AWS Managed Microsoft AD.](#)
4. [Creating an Amazon Relational Database Service for SQL Server \(RDS for SQL Server\) instance](#) to host the Active Roles Management History and Configuration databases.
5. [Verifying the connectivity between the EC2 and RDS instances.](#)
6. [Installing and configuring Active Roles on the EC2 instance.](#)
7. (Optional) Installing and configuring Active Roles Synchronization Service on the EC2 instance. For more information, see *Installing and configuring Synchronization Service to manage AWS Managed Microsoft AD resources* in the *Active Roles Synchronization Service Administration Guide*.

Creating the AWS Managed Microsoft AD instance

To deploy and configure Active Roles in Amazon Web Services (AWS) for managing AWS Managed Microsoft AD, first you must create an AWS Directory Service instance hosting your AWS Managed Microsoft AD instance in the AWS console. For more information on configuring the service in the AWS console, see [Setting up AWS Directory Service](#) in the *AWS Directory Service documentation*.

NOTE: Consider the following when creating the AWS Managed Microsoft AD instance:

- Make sure that the connectivity requirements listed in [Deployment requirements for AWS Managed Microsoft AD support](#) are met.
- During the procedure, take note of the following values, as they will be required in later procedures:

- **Directory DNS name:** The fully qualified domain name (FQDN) of your AD service (for example, `activeroles.demo`).
 - **Directory NetBIOS name:** The NetBIOS name (or shortname) of your AD service (for example, `ARDEMO`).
 - **Admin password:** The password of the default admin account (named `admin`).
- After specifying all required settings, it takes approximately 30-40 minutes to create the AWS Managed Microsoft AD instance. If you run into any issues when creating the environment, see [Troubleshooting AWS Managed Microsoft AD](#) in the *AWS Managed Microsoft AD documentation*.

Creating the EC2 instance for Active Roles

To deploy and configure Active Roles in Amazon Web Services (AWS) for managing AWS Managed Microsoft AD, you must create an Amazon Elastic Compute Cloud (EC2) instance hosting your Active Roles installation.

Complete the procedure in AWS as described in [Set up to use Amazon EC2](#) in the *Amazon EC2 documentation*. If you run into any problems when configuring or connecting to the EC2 instance, see [Troubleshoot EC2 Windows instances](#) in the *Amazon EC2 documentation*.

NOTE: Consider the following when creating the EC2 instance:

- Make sure that the connectivity requirements listed in [Deployment requirements for AWS Managed Microsoft AD support](#) are met.
- For the operating system on the EC2 instance, select a **Microsoft Windows Server** AMI supported by Active Roles. For the list of supported Windows Server operating systems, see *System requirements* in the *Active Roles Release Notes*.
- Select an EC2 instance type that has, at minimum:
 - 2 vCPUs running at 2.0 GHz.
 - 4 GB of RAM.
- One Identity recommends setting the storage to a minimum of 60 GiB of gp2 root volume.

TIP: For consistency, after you logged in to the EC2 instance, rename the virtual machine to the same name that you originally defined for the EC2 instance in the AWS console.

Joining the EC2 instance to AWS Managed Microsoft AD

After you [created your AWS Managed Microsoft AD service](#) and [your EC2 instance\(s\)](#), you must join the configured Amazon Elastic Compute Cloud (EC2) instance(s) to AWS Managed Microsoft AD.

Complete the procedure in Amazon Web Services (AWS) as described in [Join an EC2 instance to your AWS Managed Microsoft AD directory](#) in the *AWS Directory Service documentation*.

NOTE: Consider the following when joining the EC2 instance(s) to AWS Managed Microsoft AD:

- Make sure that the connectivity requirements listed in [Deployment requirements for AWS Managed Microsoft AD support](#) are met.
- You need to use the fully qualified domain name that you configured during [Creating the AWS Managed Microsoft AD instance](#).

TIP: If the domain join process ends with an error, check the specified DNS addresses and Domain Admin credentials in the AWS console.

Creating the RDS instance for the Active Roles SQL Server

If you manage AWS Managed Microsoft AD with Active Roles in Amazon Web Services (AWS), you must store the Active Roles Management History and Configuration databases in an Amazon Relational Database Service (RDS) instance.

Configure the RDS instance in AWS as described in [Setting up for Amazon RDS](#) in the *Amazon RDS documentation*.

NOTE: Consider the following when creating the EC2 instance:

- Make sure that the connectivity requirements listed in [Deployment requirements for AWS Managed Microsoft AD support](#) are met.
- Select the SQL Server edition that suits your needs the most. For most Active Roles use cases, **SQL Server Standard Edition** is an optimal choice.
- Take note of the **Master username** and **Master password**, as these credentials will be required later.
- For **Storage type**, select **General Purpose SSD (gp2)**, and allocate a minimum storage of 60 GiB.
- Consider selecting **Enable storage autoscaling**. Selecting this setting is useful if the SQL Server is utilized with a heavy load most of the time, but it might incur additional operational costs.
- For **Certificate authority**, select the **rds-ca-2019** certificate, as it is required for Microsoft OLE DB Driver 19 for SQL Server to function properly.

Verifying connectivity between the EC2 and RDS instances

After you created the RDS instance, you can test in the EC2 instance with the telnet client or Microsoft SQL Server Management Studio (SSMS) if the RDS connectivity was successfully configured.

To verify RDS connectivity in the EC2 instance

1. Log in to the EC2 instance created for Active Roles.
2. To test connectivity to RDS, install the telnet client. To do so:
 - a. Open Windows Server Manager.
 - b. On the **Dashboard**, click **Add roles and features**.
 - c. In **Installation Type**, select **Role-based or feature-based installation**, then click **Next**.
 - d. In **Server Selection**, choose **Select a server from the server pool**, and make sure that the local server (the EC2 instance) is selected.
 - e. In **Server Roles**, just click **Next**.
 - f. In **Features**, select **Telnet Client**.
 - g. In **Confirmation**, click **Install**, then **Close** the application.
3. To verify connectivity to the RDS instance, open the Windows Command Prompt, and run the following command:

```
telnet <rds-server-endpoint> <port-number>
```

To find the RDS server endpoint and port to specify, open the entry of the RDS instance in the AWS console, and check the values under **Connectivity & Security > Endpoint & port**.

NOTE: If the command returns an empty prompt, that indicates connectivity between the EC2 instance and the RDS instance.
4. Download and install [Microsoft SQL Server Management Studio \(SSMS\)](#) on the EC2 instance.
5. To test the connection with SSMS, start the application, then in the **Connect to Server** dialog, specify the following attributes:
 - **Server type:** Select **Database Engine**.
 - **Server name:** The same RDS instance endpoint used in the telnet command.
 - **Authentication:** Select **SQL Server Authentication**, then specify the admin user name and password created when [configuring the RDS instance](#).
6. After you specified all connection properties, click **Connect**.

Installing and configuring Active Roles on the EC2 instance

After you [checked the connectivity between the EC2 and RDS instances](#), you can deploy and configure Active Roles on the EC2 instance.

Prerequisites

Before starting the procedure, make sure that the following requirements are met:

- The EC2 and RDS instances are connected.
- Microsoft SQL Server Management Studio (SSMS) is installed on the EC2 instance. If you followed the steps of [Verifying connectivity between the EC2 and RDS instances](#), SSMS must already be installed on the EC2 instance.

To install Active Roles on the EC2 instance

1. Download the Active Roles installation media to the EC2 instance.
2. Run the setup and install Active Roles with all required prerequisites as described in [Installing Active Roles](#).

NOTE: Starting from Active Roles 8.2, make sure that you install Microsoft OLE DB Driver 19 for SQL Server and all its prerequisites from the `Redistributables` folder of the installation media.

Also, to make sure that the connection to the SQL Server is properly encrypted, download and install the latest AWS RDS Root Certificate by adding it to the **Trusted Root Certification Authorities** container of the `certmgr` (Manage User Certificates) utility. For more information, see [Using SSL/TLS to encrypt a connection to a DB instance](#) in the *Amazon RDS documentation*.

After installing Active Roles, configure the Active Roles Administration Service.

To configure Active Roles Administration Service for managing AWS Managed Microsoft AD in SQL Server Management Studio

1. Start Microsoft SQL Server Management Studio (SSMS) and connect to the RDS for SQL Server instance as described in [Verifying connectivity between the EC2 and RDS instances](#).
2. Under the **Databases** node of the **Object Explorer**, create two new empty databases to be used later for configuring Active Roles:
 - A database for the Management History database. Name it, for example, **ARMH**.
 - A database for the Active Roles Configuration database. Name it, for example, **ARConfig**.
3. Create a new user that Active Roles will use to connect to the SQL database in the RDS instance. To do so, right-click the **Security > Logins** node of the **Object Explorer**, then select **New login** and specify the following details:

- a. Under **General** > **Login name**, enter the name of the user (for example, `sql-activeroles`). Then, select **SQL Server authentication**.
- b. Under **User Mapping**, select the databases that you [created](#) (in this example, `ARMH` and `ARConfig`), and assign the `db_owner` role to both of them.

To configure Active Roles Administration Service for managing AWS Managed Microsoft AD in Active Roles Configuration Center

1. Start the Active Roles Configuration Center.
2. On the **Dashboard**, under **Administration Service**, click **Configure**.
3. In **Service Account**, enter the user name and password of the Active Roles Service account. This can be, for example, the domain admin account supplied by Amazon Web Services (AWS).
4. In **Active Roles Admin**, specify the security group or administrator user in the EC2 instance who will hold Active Roles Admin permissions.
5. In **Configuration Database Options**, select **New Active Roles database** and **Use a pre-created blank database**.
6. In **Connection to Configuration Database**, configure the following settings:
 - **Database type**: Select **On Premise**. In the context of Active Roles, the Amazon RDS for SQL Server instance functions like an on-premises SQL Server.
 - **Database Server name**: Specify the endpoint URL of the RDS instance. This is the same endpoint you specified during [Verifying connectivity between the EC2 and RDS instances](#).
 - **Database name**: Specify the name of the blank database that you [created](#) as the Active Roles Configuration database (in this example, `ARConfig`).
 - **Connect using**: Select **SQL Server authentication**, and enter the user name and password of the user created as the owner of the database.
7. In **Management History Database Options**, select **New Active Roles database** and **Use a pre-created blank database**.
8. In **Connection to Management History Database**, specify the same **Database type**, **Database Server name** and connection settings that you set for the [Configuration database](#). However, for **Database name**, enter the name of the blank database that you [created for use](#) as the Active Roles Management History database (in this example, `ARMH`).
9. In **Encryption Key Backup**, specify the file name and save location of the Active Roles database encryption key.
10. (Optional) Still in **Encryption Key Backup**, specify a password for additional protection. To continue, click **Next**.
11. Review your settings. Then, to apply your changes, click **Configure**.

After you configured the Active Roles Administration Service, you can also configure the Active Roles Console to manage your AWS Managed Microsoft AD instance.

To configure Active Roles Console for managing AWS Managed Microsoft AD

1. Start the Active Roles Console.
2. Due to limitations with Service Connection Points (SCPs) in the Amazon cloud, Active Roles Console is likely unable to automatically discover the Administration Service instance you [configured previously](#).

To manually connect to the Administration Service, in the **Connect to Administration Service** dialog, under **Service**, specify `localhost`. Under **Connect as**, select **Current user**, then click **Connect**.

NOTE: If you cannot connect to the Administration Service by specifying `localhost`, then specify the full **Device name** as indicated in the **Settings > About** page of the operating system.

3. After you connected, in the Active Roles Console landing page, click **Add Domain**.
4. In the Add Managed Domain Wizard, in **Domain Selection**, click **Browse** and select the domain configured by AWS for the EC2 instance.
5. In **Active Roles Credentials**, select **The service account information the Administration Service uses to log on**.
6. To finish adding the domain, click **Next**, then **Finish**.
7. To make sure that the contents of the AWS Managed Microsoft AD domain appear in the Active Roles Console, click **Refresh** or right-click the Active Roles node, then click **Reconnect**.

NOTE: The connected AWS Managed Microsoft AD environment will contain several built-in and AWS-specific containers with read-only access. You can create and manage AD objects only in the Organizational Unit whose name matches the shortname of the connected domain's name (specified during [Creating the AWS Managed Microsoft AD instance](#)).

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