One Identity Active Roles 7.5

Release Notes

December 2021

These release notes provide information about the changes, enhancements, and known or resolved issues of One Identity Active Roles 7.5.

For the most recent documents and product information, and for the release notes and documentation of earlier product releases, see the online Active Roles technical documentation on the One Identity Support Portal.

About One Identity Active Roles 7.5

Active Roles 7.5 is a major release with new features, enhancements and resolved issues. For an overview of the current release, see the following topics:

- For the list of new features, see New features.
- For the list of enhancements, see Enhancements.
- For the list of resolved issues, see Resolved issues.
- For the list of known issues, see Known issues.

IMPORTANT: For more information about the changes you must consider before and after installing Active Roles 7.5, see Upgrade and installation instructions.

Supported platforms

Active Roles 7.5 supports the following software platforms:

- Windows Server 2012 or a later version of the Windows Server operating system is required to run the Active Roles Administration Service or the Active Roles Web Interface.
- The following SQL Server versions are supported: Microsoft SQL Server 2012, 2014, 2016, 2017, and 2019.
- You can use Active Roles to manage Exchange recipients on Exchange Server 2019, 2016, or 2013.

  NOTE: Microsoft Exchange 2013 CU11 is no longer supported. For more information, refer to Knowledge Base Article 202695.

- Internet Explorer 7, 8, 9, and 10 are no longer supported for the Web Interface access.

  You can access the Active Roles Web Interface using:

  - Firefox 36 or newer on Windows.
  - Google Chrome 61 or newer on Windows.
  - Microsoft Edge 79 or newer (based on Chromium) on Windows 10.

  You can use a later version of Firefox and Google Chrome to access the Web Interface. However, the Web Interface was tested only with the browser versions listed above.
- Active Roles Web Interface is optimized for screen resolutions of 1280 x 800 or higher. The minimum supported screen resolution is 1024 x 768.

For more information, see System requirements.

New features

The following is a list of new features implemented in Active Roles 7.5:

Support for Exchange Online resource mailboxes

You can create, manage and delete room mailboxes in the Active Roles Web Interface. Room mailbox is a type of Exchange Online resource mailbox assigned to a physical location, such as a meeting room. Using room mailboxes that an administrator creates,

users can reserve rooms by adding room mailboxes to meeting requests.

For more information, see *Managing room mailboxes* in the *Active Roles Administration Guide*.

OneDrive storage support in consented Azure tenants

Active Roles 7.5 reintroduces support for configuring Microsoft OneDrive storage for hybrid and cloud-only Azure users in consented Azure tenants. Find the new OneDrive configuration settings in the **Azure AD Configuration** > **Modify** (**Tenant details**) window of the Active Roles Configuration Center. With the new implementation, the former OneDrive settings on the Active Roles Web Interface have been removed.

For more information, see *Enabling OneDrive in an Azure tenant* in the *Active Roles Administration Guide*.

Azure Security Group support

Active Roles 7.5 introduces support for Azure AD Security Groups, allowing you to create, read, update or delete Azure AD Security Groups via the Active Roles Web Interface.

- For more information on Azure AD Security Groups, see Groups in Microsoft 365 and Azure in the *official Microsoft 365 documentation*.
- For more information on how to create, modify or delete an Azure AD Security Group, see *Managing Azure Security Groups* in the *Active Roles 7.5 Administration Guide*.

My Managed Resources support

In the Active Roles Web Interface, in **Settings**, you can now enable **Show objects owned by inheritance or secondary ownership**. Selecting this check box allows Self-Administration Web Interface users to view objects in **My Managed Resources** even if the user is not assigned to the objects as the primary owner (manager), but as a secondary or inherited owner.

Previously, administrators had to select this check box every time the Web Interface home page displayed to make **My Managed Resources** appear for users with secondary or inherited ownership, but now once it is selected, it remains the default setting.

Enhancements

The following is a list of enhancements implemented in Active Roles 7.5.

Table 1: Synchronization Service enhancements

Enhancement	Enhancement ID

Azure O365 groups received two enhancements:
• You can now configure dynamic membership rules for new and existing O365 groups in the Active Roles Web Interface, enabling Active Roles to automatically add or remove members based on the configured attribute-based rules.
  • For more information on setting up a new dynamic O365 group, see *Creating a new O365 group* in the *Active Roles 7.5 Administration Guide*.
  • For more information on modifying an existing O365 group to dynamic membership, see *Viewing or modifying an O365 group* in the *Active Roles 7.5 Administration Guide*.
• You can now view the change history of existing O365 groups in the Active Roles Web Interface. For more information, see *Viewing the change history of an O365 group* in the *Active Roles7.5 Administration Guide*.
	282832

Resolved issues

Active Roles 7.5 addresses the following reported issues.

Table 2: Resolved Issues – Active Roles Installer

Resolved issue	Issue ID
Previously, the Active Roles installer did not require Administrator privileges when launching it, resulting in the installation process unable to complete. This issue is now fixed, and the installer requests elevated privileges on start.	277310
During the installation of Active Roles, attempting to install the Microsoft Teams PowerShell module on a machine that has the PowerShell Module for Skype for Business installed results in an error. The error is caused by several factors: • The Microsoft Teams PowerShell module is a successor of the Skype for Business PowerShell module, with the majority of their commands being the same. Therefore, when installing the Microsoft Teams PowerShell module without uninstalling the Skype for Business PowerShell module first, the PowerShell installer will warn users to use the `-AllowClobbers` parameter to overwrite the shared commands.	275276

Resolved issue	Issue ID
• The obsolete commands of the Skype for Business PowerShell module can remain in the machine if the module is not uninstalled before installing the Microsoft Teams PowerShell module. To solve this problem, the **Ready to Install** page of the Active Roles installer has been updated with a Note that instructs users to remove PowerShell Module for Skype for Business Online before installing the Microsoft Teams PowerShell module.	

Table 3: Resolved Issues – Active Roles Configuration Center

Resolved issue	Issue ID
Due to the SharePoint Online PowerShell module not supporting client ID and client secret-based authentication, support for that PowerShell module has been deprecated in Active Roles 7.4.4, resulting in the various OneDrive configuration interfaces becoming unusable. This issue is now fixed, so Active Roles 7.5 reintroduces the OneDrive configuration settings in the Active Roles Configuration Center and the Active Roles Console. In addition, the Active Roles Web Interface now also displays the configured OneDrive storage provisioning settings for Azure users again. For more information on how to configure OneDrive provisioning, see *Configuring OneDrive in an Azure tenant* in the *Active Roles 7.5 Administration Guide*.	278521

Table 4: Resolved Issues – Active Roles Console (MMC Interface)

Resolved Issue	Issue ID
Previously, while Starling 2FA was configured for Active Roles, users attempting to open the Active Roles Console (also known as the MMC Interface) could receive the following error in the **Active Roles Starling 2FA Verify Token** pop-up: `One or more errors occurred: Failed while getting token from Starling: Could not load file or assembly 'Newtonsoft.Json'.` This error prevented users from accessing and using the Active Roles Console, forcing administrators to disable Starling 2FA as a workaround, whenever the Active Roles Console had to be used. The issue was caused by version conflicts among the external components of Starling 2FA, and is now fixed.	289723
Previously, configuring a dynamic group in the Active Roles Console with a	91690

Resolved Issue	Issue ID
, and using an LDAP query containing LDAP_MATCHING_RULE_TRANSITIVE_EVAL (1.2.840.113556.1.4.1941) resulted in the membership of the dynamic group not being updated. This issue is now fixed, and dynamic groups using LDAP matching rule 1.2.840.113556.1.4.1941 are now updated correctly.	

Table 5: Resolved Issues – Active Roles Web Interface

Resolved issue	Issue ID
Previously, when setting up the email account of the selected Azure user as a shared mailbox in the **Exchange Online Properties** > **Delegation** tab in the Active Roles Web Interface, the Send As permission could not be granted to the added users because they did not appear in the Send As list. The issue has been resolved and now the added users are correctly displayed in the Send As list.	284175
Previously, when selecting an Azure guest user in the Active Roles Web Interface, in Azure properties, the **Reset Password** option was available. Clicking **Reset Password** opened a window allowing you to specify and save a new password, but even if the operation failed, you got the following message: `The operation is successfully completed.` The issue is now fixed and the **Reset password** option is removed from the properties of Azure guest users. For more information, see the FAQ entry on *password reset support for Azure AD B2B collaboration users* in the *Microsoft Azure Documentation*.	277972
Previously, attempting to consent Active Roles as an Azure application in an Azure tenant could result in the following error message: `Could not create Application in Azure. Bad Request: Values of identifierUris property must use a verified domain of the organization or its subdomain: 'http://ActiveRoles` This issue was introduced because of a change in the Azure Active Directory (AAD) application creation system, introducing stricter requirements for identifierUris. This issue is now fixed, and Azure tenants can now be added or reauthenticated again.	291638
Previously, when creating a new Azure guest user in the Active Roles Web	288597

Resolved issue	Issue ID
, **Job Title**, **Department** or **Usage Location**) were not replicated to Azure AD by default. This issue is now fixed by making sure that the Azure guest user modify requests are sent appropriately from Active Roles to Azure AD.	
Previously, when opening the **Office 365 Groups** container of an Azure tenant in the Active Roles Web Interface, it could occur that the container appeared empty, with no Office 365 groups listed in it. This issue has been fixed.	282828
Previously, when opening the **Azure Users** container of an Azure tenant in the Active Roles Web Interface, it could occur that the Active Roles Web Interface did not list every Azure user managed in the Azure tenant. This issue was caused by an Active Roles caching mechanism problem, and has been fixed.	282182
Previously, objects whose `ShowInAdvanceViewOnly` property was set `true` were not shown in the Active Roles Web Interface, even when searching specifically for those objects. This issue has been fixed by removing the `ShowInAdvanceViewOnly` property from the LDAP search filters of the Active Roles Web Interface, ensuring that all directory objects now appear.	282169
Previously, when managing users with Exchange Online licenses (assigned either via Active Roles or the Microsoft Azure Portal), checking the **Exchange Online Properties** of users in the Active Roles Web Interface could result in an `Unable to retrieve Exchange Online Mailbox properties` error appearing after some time. Restarting the Active Roles Administration Service could resolve this issue for a while. This issue occurred because the Microsoft Modern Authentication access tokens (generated when first checking the **Exchange Online Properties** of the users) expired, as Active Roles did not request a new Exchange Online connection whenever the **Exchange Online Properties** option was used, resulting in a timeout over time. This issue is now fixed.	281545
Previously, after upgrading between major Active Roles versions, the Active Roles Web Interface Personal Views were lost, because they were not imported to the newly-created database. Instead, users had to import personal settings manually, requiring significant workaround. This issue is now fixed, and in-place Active Roles upgrades now import personal settings for configured websites.	91729
Previously, the **Licenses** step of the Azure (guest) user configuration process listed the Office 365 Content Explorer with the non-user friendly name **Content_Explorer**.	272301

Resolved issue	Issue ID
This issue is now fixed, and the list of licenses shows the resource as **Content Explorer**.	

Table 6: Resolved Issues – Active Roles Synchronization Service

Resolved issue	Issue ID
Previously, attempting to open the One Identity Manager (OneIM) Connector with the **OneIM** check box deselected resulted in the following error message: `D1IM web service is not connected.` The typo `D1IM` in the error message has been fixed to `One Identity Manager`.	91671
Previously, attempting to create the same user twice with an Active Directory (AD) and Active Directory Lightweight Directory Services (AD LDS) connection workflow resulted in the following error message: `An error occured while creating the object <object-name>. The object already exists.` The typo `occured` in the error message has been fixed to `occurred`.	92036

Table 7: Resolved Issues – Active Roles Collector and Report Pack

Resolved issue	Issue ID
Previously, specifying a blank **Azure SQL Database** with the **Specify Database** > **Use existing database** option of the Active Roles Collector and Report Pack returned the following error message: `Unable to use the specified database because the database is not empty and is not a Collector database.` Active Roles Collector and Report Pack returned this error because it considers an existing database empty only if it contains no tables at all. However, existing Azure SQL Databases always contain at least one system table, even if they are otherwise blank; therefore, Active Roles Collector and Report Pack cannot recognize them as usable empty databases. The error message received in this scenario has been clarified to make it clear that existing blank Azure SQL Databases cannot be selected when configuring the Active Roles Collector and Report Pack with the **Use existing database** option. TIP: In such cases, One Identity recommends selecting the **Create**	272581

Resolved issue	Issue ID
database option, and creating an empty Azure SQL Database during the configuration process.	

Table 8: Resolved Issues – Active Roles SPML Provider

Resolved issue	Issue ID
Previously, when using Constrained Delegation in the SPML Provider, submitting a modification request returned an Unsupported operation error because the SPLM Provider could not cast a com_object properly. The issue is now fixed and the data of the com_object returns without error.	289838

Known issues

The following is a list of issues in Active Roles 7.5, which are known to exist at the time of its release.

Table 9: Active Roles known issues

Known Issue	Issue ID

Trying to reset the password of an Azure user in the Active Roles Web Interface returns the following error message:
`One or more errors occurred. Http Exception - Status Code Forbidden. Reason phrase Forbidden {"error":{"code":Authorization_ RequestDenied","message":"Insufficient privileges to complete the operation"}}`
This error occurs because of a Microsoft Graph API-related issue, described in the Authorization_RequestDenied error when you try to change a password using Graph API article of the *Microsoft Azure Troubleshooting* documentation.
Workaround
To solve this problem, assign the **Company Administrator** Office 365 administrative role to Active Roles with the following PowerShell cmdlets:
`Connect-MsolService`
`$displayName = "ActiveRoles"`
`$objectId = (Get-MsolServicePrincipal -SearchString $displayName).Ob-`
	293601

Known Issue	Issue ID
jectId $roleName = "Company Administrator" Add-MsolRoleMember -RoleName $roleName -RoleMemberType ServicePrincipal -RoleMemberObjectId $objectId	
Importing an Active Roles configuration with the **Administration Service** > **Active Roles databases** > **Import configuration** wizard of the Active Roles Configuration Center can result in an inconsistent Web Interface configuration state if the Web Interface has been previously configured with the **Dashboard** > **Web Interface** > **Configure** setting. This issue is caused by a discrepancy between the previously-configured Web Interface configuration and the imported Web Interface configuration. **Workaround** To avoid this issue, One Identity recommends configuring the Web Interface in the Active Roles Configuration Center only after importing any Active Roles configurations.	275240
When configured for Group and Contacts, the **Office 365 and Azure Tenant Selection** policy displays additional tabs.	229031
Tenant selection supports selecting only a single tenant.	229030
Automation workflow with Office 365 script fails, if multiple workflows share the same script and the script is scheduled to execute at the same time. **Workaround** One Identity recommends scheduling the workflows with different scripts or at a different time.	200328
In the Active Roles Web Interface, Azure roles are not restored automatically after performing an **Undo Deprovision** action on a user. **Workaround** After the **Undo Deprovision** action is completed, assign the Azure roles to the user manually.	172655
When a workflow is copied from built-in workflows, it may not be executed as expected.	153539
In the **Starling Connect Connection Settings** link, clicking **Next** displays progress, but the functionality is not affected, so the button is not required.	126892
After running the **get-qcworkflowstatus** cmdlet in the Synchronization Service, the workflow status is not accurate.	125768
Active Roles does not support creating Azure groups for existing groups.	117015

Known Issue	Issue ID
Azure Group Properties are not available if they are added to the Office 365 Portal or Hybrid Exchange Properties from the forwarding address attribute of Exchange online users.	98186
Activating the EnableAntiForgery key (`<add key="EnableAntiForgery" value="true"/>` in web.config) may cause the following error message: `Session timeout due to inactivity. Please reload the page to continue.` **Workaround** Update the **IgnoreValidation** key in the<appSettings> section by adding a property value in lowercase: 1. Open the IIS Manager. 2. In the left pane, under **Connections**, expand the tree view to **Sites** > **Default Web Site**. 3. Under **Default Web Site**, click on the Active Roles application (ARWebAdmin by default). 4. Double-click **Configuration Editor**. 5. From the **Section** drop-down, select **appSettings**. 6. Find the **IgnoreForValidation** key. 7. Append the comma-separated value to **IgnoreForValidation**, for example: `lowercasecontrolname`. 8. In the right pane, under **Actions**, click **Apply**. 9. Recycle the App pool.	91977
After upgrading Active Roles, the pending approval tasks are not displayed in the Active Roles Web Interface.	91933
Active Roles Web Interface does not support setting the **Exchange Online Property** of the **ProhibitSendQuota** value in **Storage Quotas**.	91905
In Active Roles with the **Office 365 Licenses Retention** policy applied, after deprovisioning the Azure AD user, the Deprovisioning Results for the **Office 365 Licenses Retention** policy are not displayed in the same window. **Workaround** To view the Deprovisioning Results after deprovisioning the Azure AD user: • In Active Roles MMC Console, right-click and select **Deprovisioning Results**. • In the right pane of the Active Roles Web Interface, click **Deprovisioning Results**. • To refresh the form, press **F5**.	91901

System requirements

Before installing Active Roles 7.5, ensure that your system meets the following minimum hardware and software requirements.

Active Roles includes the following components:

- Administration Service
- Web Interface
- Console (MMC Interface)
- Management Tools
- Synchronization Service

This section lists the hardware and software requirements for installing and running each of these components.

Administration Service

This section lists the system requirements of the Active Roles Administration Service.

Table 10: Administration Service requirements

Requirement	Details
Platform	Any of the following: • Intel 64 (EM64T) • AMD64 • Minimum 2 processors • Processor speed: 2.0 GHz or faster NOTE: The amount of processors required depends on the total number of managed objects. Depending on the size of environment, the number of processors required may vary.
Memory	A minimum of 4 GB of RAM. NOTE: The amount of memory required depends on the total number of managed objects. Depending on the size of environment, the amount of memory required may vary.
Hard disk space	100 MB or more of free disk space.
Operating system	You can install Administration Service on a computer running: • Microsoft Windows Server 2019, Standard or Datacenter edition.

Requirement	Details
	• Microsoft Windows Server 2016, Standard or Datacenter edition. • Microsoft Windows Server 2012 R2, Standard or Datacenter edition. • Microsoft Windows Server 2012, Standard or Datacenter edition. NOTE: Active Roles is not supported on Windows Server Core mode setup.
Microsoft .NET Framework	Active Roles Administration Service requires Microsoft .NET Framework 4.7.2. For more information, see Installing .NET Framework for developers in the *Microsoft .NET documentation*.
SQL Server	You can host the Active Roles database on: • Microsoft SQL Server 2019, any edition. • Microsoft SQL Server 2017, any edition. • Microsoft SQL Server 2016, any edition. • Microsoft SQL Server 2014, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Pack. • Microsoft SQL Server 2012, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Pack. • Microsoft OLE DB Driver for SQL Server (MSOLEDBSQL).
Windows Management Framework	On all supported operating systems, Active Roles Administration Service requires Windows Management Framework 5.1 (available for download here).
Operating system on domain controllers	Active Roles retains all features and functions when managing Active Directory on domain controllers running any of these operating systems, any edition, with or without any Service Pack: • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 Active Roles deprecates managed domains with the domain functional level lower than Windows Server 2008 R2. One Identity recommends that you raise the functional level of the domains managed by Active Roles to Windows Server 2008 R2 or higher.
Exchange Server	Active Roles is capable of managing Exchange recipients on: • Microsoft Exchange Server 2019

Requirement	Details
	• Microsoft Exchange Server 2016 • Microsoft Exchange Server 2013 • Microsoft Exchange 2013 CU11 is no longer supported. For more information, see Knowledge Base Article 202695.
Azure Az PowerShell module	To use Modern Authentication, the Azure Az PowerShell module must be installed on the computer(s) running the Administration Service and the Synchronization Service. For installation instructions, see Install the Azure Az PowerShell module in the *Microsoft Azure PowerShell documentation*.
Partner Center PowerShell module	To manage Azure tenants in the Configuration Center, the Partner Center PowerShell module must be installed on the computer running the Administration Service. For installation instructions, see Install the Partner Center PowerShell module in the *Microsoft Partner Center documentation*.
Visual C++ Redistributables	Visual C++ 2017 Redistributable

Web Interface

This section lists the system requirements of the Active Roles Web Interface.

Table 11:
Web Interface requirements

Requirement	Details
Platform	Any of the following: • Intel 64 (EM64T) • AMD64 • Processor speed: 2.0 GHz or faster
Memory	At least 2 GB of RAM. The amount of memory required depends on the total number of managed objects.
Hard disk space	About 100 MB of free disk space.
Operating system	You can install Web Interface on a computer running: • Microsoft Windows Server 2019 Standard or Datacenter edition. • Microsoft Windows Server 2016, Standard or Datacenter edition. • Microsoft Windows Server 2012 R2, Standard or Datacenter edition.

Requirement	Details
	• Microsoft Windows Server 2012, Standard or Datacenter edition. NOTE: Active Roles is not supported on Windows Server Core mode setup.
Microsoft .NET Framework	Active Roles Web Interface requires Microsoft .NET Framework 4.7.2. For more information, see Installing .NET Framework for developers in the *Microsoft .NET documentation*.
Visual C++ Redistributable	Visual C++ 2017 Redistributable
Internet Services	On Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 Web Interface requires the **Web Server (IIS)** server role with the following role services: • Web Server/Common HTTP Features/ • Default Document • HTTP Errors • Static Content • HTTP Redirection • Web Server/Security/ • Request Filtering • Basic Authentication • Windows Authentication • Web Server/Application Development/ • .NET Extensibility • ASP • ASP.NET • ISAPI Extensions • ISAPI Filters • Management Tools/IIS 6 Management Compatibility/ • IIS 6 Metabase Compatibility Internet Information Services (IIS) must be configured to provide **Read/Write** delegation for the following features: • Handler Mappings • Modules Use **Feature Delegation** in Internet Information Services (IIS) Manager to confirm that these features have their delegation set to **Read/Write**.

Requirement	Details
Web browser	You can access the Active Roles Web Interface using: • Firefox 36 or newer on Windows. • Google Chrome 61 or newer on Windows. • Microsoft Edge 79 or newer (based on Chromium) on Windows 10. You can use a later version of Firefox and Google Chrome to access the Web Interface. However, the Web Interface was tested only with the browser versions listed above.
Minimum screen resolution	Active Roles Web Interface is optimized for screen resolutions of 1280 x 800 or higher. The minimum supported screen resolution is 1024 x 768.

Console (MMC Interface)

This section lists the system requirements of the Active Roles Console (MMC Interface).

Table 12: Active Roles Console requirements

Requirement	Details
Platform	Any of the following: • Intel x86 • Intel 64 (EM64T) • AMD64 • Processor speed: 1.0 GHz or faster
Memory	At least 1 GB of RAM. The amount required depends on the total number of managed objects.
Hard disk space	About 100 MB of free disk space.
Operating system	You can install Active Roles console on a computer running: • Microsoft Windows Server 2019, Standard or Datacenter edition. • Microsoft Windows Server 2016, Standard or Datacenter edition. • Microsoft Windows Server 2012 R2, Standard or Datacenter edition. • Microsoft Windows Server 2012, Standard or Datacenter edition. • Microsoft Windows 8.1, Professional or Enterprise edition, 32-bit (x86) or 64-bit (x64).

Requirement	Details
	• Microsoft Windows 10, Professional or Enterprise edition, 32-bit (x86) or 64-bit (x64). NOTE: Active Roles is not supported on Windows Server Core mode setup.
Microsoft .NET Framework	Active Roles Console requires Microsoft .NET Framework 4.7.2. For more information, see Installing .NET Framework for developers in the *Microsoft .NET documentation*.
Visual C++ Redistributable	Visual C++ 2017 Redistributable
Web browser	Active Roles Console requires Microsoft Edge 79 or newer, based on Chromium.

Management Tools

Active Roles Management Tools is a composite component that includes the Active Roles Management Shell, ADSI Provider, and SDK. On a 64-bit (x64) system, Active Roles Management Tools also include the Active Roles Configuration Center.

Table 13: Management Tools requirements

Requirement	Details
Platform	Any of the following: • Intel x86 • Intel 64 (EM64T) • AMD64 • Processor speed: 1.0 GHz or faster
Memory	At least 1 GB of RAM.
Hard disk space	About 100 MB of free disk space.
Operating system	You can install Management Tools on a computer running: • Microsoft Windows Server 2019, Standard or Datacenter edition. • Microsoft Windows Server 2012 R2, Standard or Datacenter edition. • Microsoft Windows Server 2012, Standard or Datacenter edition. • Microsoft Windows Server 2016, Standard or Datacenter edition. • Microsoft Windows 8.1, Professional or Enterprise edition, 32-bit (x86) or 64-bit (x64).

Requirement	Details
	• Microsoft Windows 10, Professional or Enterprise edition, 32-bit (x86) or 64-bit (x64). NOTE: Active Roles is not supported on Windows Server Core mode setup.
Microsoft .NET Framework	Active Roles Management Tools require Microsoft .NET Framework 4.7.2. For more information, see Installing .NET Framework for developers in the *Microsoft .NET documentation*.
Visual C++ Redistributable	Visual C++ 2017 Redistributable
Windows Management Framework	On all supported operating systems, Active Roles Management Tools require Windows Management Framework 5.1 (available for download here).
Remote Server Administration Tools (RSAT)	To manage Terminal Services user properties by using Active Roles Management Shell, Management Tools require 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 *Microsoft Documentation*.

Synchronization Service

This section lists the system requirements of the Active Roles Synchronization Service.

Table 14: Synchronization Service requirements

Requirement	Details
Platform	Any of the following: • Intel 64 (EM64T) • AMD64 • Processor speed: 2.0 GHz or faster One Identity recommends using a multi-core processor for the best performance.
Memory	At least 2 GB of RAM. The amount of memory required depends on the number of objects to synchronize.
Hard disk space	250 MB or more of free disk space. If SQL Server and Synchronization Service are installed on the same computer, the amount required depends on the size of the Synchronization Service database.

Requirement	Details
Operating system	You can install the Synchronization Service on a computer running: • Microsoft Windows Server 2019, Standard or Datacenter edition. • Microsoft Windows Server 2016, Standard or Datacenter edition. • Microsoft Windows Server 2012 R2, Standard or Datacenter edition. • Microsoft Windows Server 2012, Standard or Datacenter edition. NOTE: Active Roles is not supported on Windows Server Core mode setup.
Microsoft .NET Framework	Active Roles Synchronization Service requires Microsoft .NET Framework 4.7.2. For more information, see Installing .NET Framework for developers in the *Microsoft .NET documentation*.
Visual C++ Redistributable	Visual C++ 2017 Redistributable
SQL Server	You can host the Synchronization Service database on: • Microsoft SQL Server 2019, any edition. • Microsoft SQL Server 2017, any edition. • Microsoft SQL Server 2016, any edition. • Microsoft SQL Server 2014, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Pack. • Microsoft SQL Server 2012, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Pack.
Windows Management Framework	On all supported operating systems, Active Roles Synchronization Service requires Windows Management Framework 5.1 (available for download here).
Supported connections	The Synchronization Service can connect to: • Microsoft Active Directory Domain Services with the domain or forest functional level of Windows Server 2012 or higher. • Microsoft Active Directory Lightweight Directory Services running on any Windows Server operating system supported by Microsoft. • Microsoft Exchange Server version 2019, 2016, or 2013. NOTE: Microsoft Exchange 2013 CU11 is no longer supported. For more information, see Knowledge Base Article 202695. • Microsoft Lync Server version 2013 with limited support. • Microsoft Skype for Business 2019, 2016 or 2015.

Requirement	Details
	• Microsoft Windows Azure Active Directory using the Azure AD Graph API version 1.6. • Microsoft Office 365 directory. • Microsoft Exchange Online service. • Microsoft Skype for Business Online service. • Microsoft SharePoint Online service. • Microsoft SQL Server, any version supported by Microsoft. • Microsoft SharePoint 2019, 2016, or 2013. • Active Roles version 7.4.3, 7.4.1, 7.3, 7.2, 7.1, 7.0, and 6.9 • One Identity Manager version 7.0 (D1IM 7.0) • One Identity Manager version 8.0 • Support for Generic LDAP Connector, MySQL Connector, Open LDAP Connector, IBM Db2 Connector, Salesforce Connector, Service now Connector, and IBM RACF Connector. • Support for Oracle Database, Oracle Database User Accounts, Oracle Unified Directory, Micro Focus NetIQ Directory, and IBM AS/400 connectors. • Data sources accessible through an OLE DB provider • Delimited text files
Legacy Active Roles ADSI Provider	To connect to Active Roles version 6.9, the Active Roles ADSI Provider of the respective version must be installed on the computer running the Synchronization Service. For installation instructions, see the *Active Roles Quick Start Guide* for the appropriate Active Roles version.
Azure AD Module for Windows PowerShell Version 2	To connect to the Office 365 directory, the Azure Active Directory PowerShell module must be installed on the computer running the Synchronization Service.
Azure Az Power-Shell module	To use Modern Authentication, the Azure Az PowerShell module must be installed on the computer(s) running the Administration Service and the Synchronization Service. For installation instructions, see Install the Azure Az PowerShell module in the *Microsoft Azure PowerShell documentation*.
Windows PowerShell Module for Skype for Business Online	To connect to the Skype for Business Online service, Windows PowerShell Module for Skype for Business Online, now included in Microsoft Teams PowerShell, must be installed on the computer running the Synchronization Service. For installation instructions, see Install Microsoft Teams PowerShell in the *Microsoft Teams*

Requirement	Details
	documentation.
SharePoint Online Management Shell	To connect to the SharePoint Online service, SharePoint Online Management Shell must be installed on the computer running the Synchronization Service. Download the application here.
One Identity Manager API	To connect to One Identity Manager 7.0, One Identity Manager Connector must be installed on the computer running the Synchronization Service. This connector works with RESTful web service and SDK installation is not required.
Internet Connection	To connect to cloud directories or online services, the computer running the Synchronization Service must have a reliable connection to the Internet.

Synchronization Service Capture Agent

This section lists the system requirements of the Active Roles Synchronization Service Capture Agent.

Table 15: Synchronization Service Capture Agent

Requirement	Details
Microsoft .NET Framework	Active Roles Synchronization Service Capture Agent requires Microsoft .NET Framework 4.7.2. For more information, see Installing .NET Framework for developers in the *Microsoft .NET documentation*.
Additional Requirements	To synchronize passwords from an Active Directory domain to some other connected data system, you must install the Sync Service Capture Agent on all domain controllers in the source Active Directory domain. The domain controllers on which you install Sync Service Capture Agent must run one of the following operating systems with or without any Service Pack (both x86 and x64 platforms are supported): • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 For more information, see the *Active Roles Synchronization Service Administration Guide*.

Product licensing

Use of this software is governed by the Software Transaction Agreement found at www.oneidentity.com/legal/sta.aspx. This software does not require an activation or license key to operate.

The product usage statistics can be used as a guide to show the scope and number of managed objects in Active Roles.

Upgrade and installation instructions

Starting from Active Roles 7.4, enhancements have been made for the in-place upgrade process.

- For general instructions on how to upgrade from an earlier version of Active Roles or how to install and initially configure Active Roles, see the *Active Roles Quick Start Guide*.
- For special considerations regarding the installation of Active Roles 7.5, see the following information.

IMPORTANT: Before installing Active Roles 7.5, make sure to perform a database backup.

Changes related to Azure tenants

NOTE: If your organization has any Azure tenants that are managed with Active Roles, you must reauthenticate and reconsent them after installing Active Roles7.5. Otherwise, Active Roles will not receive the required permissions for managing existing Azure tenants, and tenant administration in Active Roles7.5 will not work correctly. For more information, see *Reconfiguring Azure tenants during upgrade configuration* in the *Active Roles 7.5 Quick Start Guide*.

Changes related to Active Roles Synchronization Service

NOTE: Active Roles 7.4.5 introduced support for Modern Authentication in Azure BackSync workflows of the Active Roles Synchronization Service. After upgrading to Active Roles 7.5, if you previously had an Azure BackSync workflow configured, you will be prompted to reconfigure it in the Active Roles Synchronization Service Console.

CAUTION: If you previously had an Azure BackSync workflow configured in Active Roles Synchronization Service, and you use more than one Azure Active Directory (Azure AD) service in your deployment, you must specify the Azure AD for which you want to configure Azure BackSync. Failure to do so may either result in directory objects not synchronized at all, or synchronized to unintended locations.

For more information on how to specify the Azure AD used for back-synchronization, see *Configuring automatic Azure BackSync* in the *Active Roles Synchronization Service Administration Guide*.

Upgrade and compatibility

CAUTION: You must run the Active Roles Setup in Administrator Mode. Failing to do so will result in Active Roles not starting up at all.

For instructions on how to upgrade from an earlier version of Active Roles, see the *Active Roles Quick Start Guide*.

NOTE: Consider the following before upgrading to a new version of Active Roles:

- Components of an earlier Active Roles version may not work with the components of the new version you are upgrading to.
- Custom solutions (scripts or other modifications) that rely on Active Roles features may fail to work after an upgrade due to compatibility issues. Therefore, before starting the upgrade, test your existing solutions with the new version of Active Roles in a lab environment to verify that your custom solutions will continue to work.

TIP: When upgrading to a new Active Roles version, One Identity recommends to upgrade the Active Roles Administration Service first, and the client components (Active Roles Console and Active Roles Web Interface) afterwards.

Version upgrade compatibility chart

The following table shows the version upgrade path that you can take from one version of the product to another. *Source version* refers to the current product version that you have installed. *Destination version* refers to the highest version of the product to which you can upgrade.

Table 16: Version upgrade compatibility chart

Source version	Destination version
7.4.1	7.5
7.4.3	7.5
7.4.4	7.5
7.4.5	7.5

Additional resources

Join the Active Roles community at https://www.oneidentity.com/community/active-roles to get the latest product information, find helpful resources, test the product betas, and participate in discussions with the Active Roles team and other community members.

For the most recent documents and product information, see https://support.oneidentity.com/active-roles/.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

About us

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

Contacting us

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

Technical support resources

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

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

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

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.