One Identity Active Roles 7.4.5

Release Notes

September 2021

These release notes provide information about the changes, enhancements, and known or resolved issues of the latest One Identity Active Roles release, 7.4.5.

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 7.4.5

Active Roles 7.4.5 is a service pack release containing new features 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 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 7.4.5, see Upgrade and installation instructions

Supported platforms

Active Roles 7.4.5 supports the following software platforms:

- Windows Server 2012 or a later version of the Windows Server operating system is required to run the Administration Service or 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 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 7.4.5:

Modern Authentication Support in Active Roles Synchronization Service

Active Roles 7.4.5 supports Modern Authentication in Azure BackSync workflows of the Active Roles Synchronization Service, replacing the previous Azure Admin user name and password-based authentication.

NOTE: Consider the following when using this feature:

- If you previously had an Azure BackSync workflow configured, you will be prompted to reconfigure it in the Active Roles Synchronization Service Console.
- If you previously had an Azure BackSync workflow configured, and you use more than one Azure Active Directory (Azure AD) in your deployment, you must specify the Azure AD for which you want to configure BackSync in the Active Roles Synchronization Service Console. For more information, see Upgrade and installation instructions and Knowledge Base Article 334291.
- The SharePoint Online and Microsoft Skype for Business Online services are deprecated and no longer supported by the O365 Connector.
- After creating a new client secret in the Azure Admin Portal, you may need to wait up to 15 minutes until the client secret is synchronized and can be queried by the Active Roles Synchronization Service when creating the new O365 Connector.

Enhancements

The following is a list of enhancements implemented in Active Roles 7.4.5.

Table 1: Synchronization Service enhancements

Enhancement	Issue ID
Starting with Active Roles 7.4.5, when configuring Azure BackSync in the Active Roles Synchronization Service Console, you can now: • Indicate whether the Azure tenant contains multiple Azure AD services. • If you have multiple Azure AD services in your Azure tenant, you can specify the Azure AD for which you want to set up back-synchronization. For more information, see *Configuring automatic Azure BackSync* in the *Active Roles Synchronization Service Administration Guide*.	288302

Resolved issues

Active Roles 7.4.5 addresses the following reported issues.

Table 2: Resolved Issues – Active Roles Installer

Resolved issue	Issue ID
Previously, when installing Active Roles, the installation of the Microsoft Teams PowerShell module could cause confusion, as the module could not be installed	275276

Resolved issue	Issue ID
on computers that already had the Skype for Business PowerShell module installed. To solve this problem, the Active Roles Installer has been updated with a note instructing users to remove the Skype for Business PowerShell module before installing the Microsoft Teams PowerShell module.	
Previously, when users installed only the client-side components (that is the Active Roles Console, the Active Roles Web Interface, or the Active Roles Synchronization Service) of the product (for example, because Active Roles had already been running on another computer in the domain), the installer indicated the Azure Az and Microsoft Teams PowerShell modules as required components, even though their installation was not necessary for the client-side components. This issue is now fixed, and the Azure Az and Microsoft Teams PowerShell modules are no longer required for installing client-side Active Roles components.	275274

Table 3: Resolved Issues – Active Roles Configuration Center

Resolved issue	Issue ID
Previously, Active Roles Configuration Center could display the following error message when attempting to add an Azure tenant: `The term 'Connect-QADService' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.` This issue could occur on fresh Active Roles installations if the Active Roles Management Shell PowerShell module has not yet been imported. The issue is now solved, and the error message no longer appears.	275669
Previously, Active Roles Configuration Center could display a **`Task was cancelled`** error message when adding an Azure tenant. The issue occurred because Azure AD could not always reach a consistent state immediately after creating an Azure application, and while the Azure application object was created with the client secret, it could not be used immediately for OAuth 2.0 authentication. The issue has been resolved, and the error message no longer appears.	275439
Active Roles had several minor deficiencies due to the implementation of Microsoft Modern Authentication: • Administrators could not assign roles to Azure users due to the lack of	275268

Resolved issue	Issue ID
required Azure application permissions. • While adding Azure tenants, Active Roles Configuration Center could display a **Task was cancelled** error message. The likelihood of this error varied in different Active Roles server hardware configurations. • While the ability to add new Azure tenants to Active Roles and the ability to set the type of those new Azure tenants have been moved from the Active Roles Web Interface to the Active Roles Configuration Center in Active Roles, the type of existing Azure tenants could still be modified only in the Active Roles Web Interface. These issues are now fixed, so that users now can: • Assign roles to Azure users. • Register Azure tenants in Active Roles without the **Task was cancelled** error message appearing. • Modify the type of already registered Azure tenants in the Active Roles Configuration Center.	

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

Resolved Issue	Issue ID
Previously, the **Product Usage Statistics** table of the Active Roles Console (available by clicking the Active Roles node at the top of the console tree) has counted Azure guest user licenses twice. This issue was caused by the incorrect filtering of cloud-only Azure members, fetching both Azure users and Azure guest users in the row of Azure users instead of just Azure users. The issue is now solved, and the table lists the number of Azure user and Azure guest user licenses correctly in their respective rows.	276954
Previously, workflow scripts run inside an If-Else branch conditional of the Active Roles Console Workflow Designer did not have access to any of the constructed objects, including **$workflow**, resulting in the **$workflow.FoundObjects()** method not working properly.	90784

Table 5: Resolved Issues – Active Roles Web Interface

Resolved issue	Issue ID
In the Active Roles Web Interface, adding a new user to the Exchange Online Mailbox delegation appeared to be successful, but failed in the back-end due to an unexpected exception.	283031

Resolved issue	Issue ID
The issue is now resolved, and you can add a new user to the Exchange Online Mailbox delegation.	
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, Proxy Objects added to a Group in a configured Managed AD LDS Instance (ADAM) partition were not recognized in the Active Roles Web Interface when performing object searches. This issue is now fixed, and Proxy Objects appear properly in searches after adding them to Groups from the **Members** menu.	280524
Previously, attempting to remove a user from one or more groups in the **Member of** page of the Active Roles Web Interface failed, as the **Remove** button remained disabled, even if one or more groups have been selected from the list. This is now fixed, and the **Remove** button works properly.	279053
Previously, when attempting to perform a main search or a quick search in the Active Roles Web Interface with an on-premises user that had the **All Objects - Read All Properties** Access Template assigned to it, the search returned an **`Object reference not set to an instance of an object`** error. This issue occurred because searches in the Active Roles Web Interface triggered the Azure Health Check to which non-administrator users have no access. The issue has been resolved by creating a new **Azure Health Check for Search** Access Template that gives read permission to the Azure Health Check service to let non-administrator users search for Azure objects. NOTE: Currently, the **Azure Health Check for Search** Access Template appears only if Active Roles 7.4.5 is installed with a clean installation. For more information, see the description of bug 285456 in Known issues.	277598
Previously, when running a global search in the Active Roles Web Interface, the search could return Azure-only Security Groups if they have been configured previously in the Azure tenant.	277502

Resolved issue	Issue ID
This is now fixed, and Security Groups no longer appear in the search results, as they are currently not supported by Active Roles.	
Previously, the method of registering Active Roles Azure applications in Azure AD did not support connecting to and managing the same Azure tenant in the Active Roles Web Interface from multiple Active Roles instances that are not sharing the same database. This issue was caused by the properties of the identifier URI of the created Azure application: the URI must be unique, so every time a disconnected Active Roles instance attempted connecting with its own Azure application, it has done so with the same unique identifier URI. This fix enables using multiple Active Roles instances (that are not connected through the same database) to manage the same Azure tenant by using the same Azure application (named **`ActiveRoles`**) with the identifier URI **`http://ActiveRoles`** for accessing the Azure tenant. To access the Azure application, each Active Roles instance will generate and install its own client secret.	277119
Previously, when creating a new hybrid user on the Active Roles Web Interface, the **Properties** page of the user contained an **Enable Multi-Factor Authentication** setting that did not work. The issue has been solved by removing the setting.	275244
Previously, when Modern Authentication was enabled in Azure, the Active Roles Web Interface could not show cloud-only Azure users, the Azure properties of hybrid users, and the Exchange Online properties of hybrid users. To solve this issue, this fix implements Azure application-based authentication instead of Azure admin user-based authentication in Active Roles, so that users can manage Azure- and Exchange Online-related objects in Active Roles, regardless of whether Modern Authentication is enabled or disabled. NOTE: This change affects the procedure of adding Azure tenants and registering Azure applications for Active Roles. Therefore, these procedures are now available from the Active Roles Configuration Center instead of the Active Roles Web Interface.	269970
In the Active Roles Web Interface, resetting the password of a user did not work when the password was pasted into the password field and then confirmed using the mouse only. This issue was caused by a bug in the password application routine, which only registered keyboard input when applying the new password, but not mouse clicks. The issue is now fixed, and the password can be successfully reset even by using the mouse only.	139704

Table 6: Resolved Issues – Active Roles Synchronization Service

Resolved issue	Issue ID

Previously, when setting up Azure BackSync in Active Roles Synchronization Service with the **Settings** > **Configure Azure BackSync** option, the application sometimes returned the following error message while applying the configured Azure BackSync settings:
`Synchronization Service has returned an error`
 	
`Processing data from remote server <server-name> failed with the following error message:`
 	
`The role assigned to application <application-name> isn't supported in this scenario.`
This issue is now fixed.
	288440

Previously, when using a sync workflow step handler in workflows in Active Roles Synchronization Service, if a PowerShell script returned an empty ($null) value, the following value was written in the empty value's place, causing an error: `System.Collections.Generic.List`1[System.Object]` The issue has been resolved and now a PowerShell script returning an empty value is handled correctly.	286380
Previously, timeout in the Active Roles Synchronization Service was hard-coded to 6000 seconds (1 hour 40 minutes) that could cause long-running workflows to fail with a timeout error. The issue has been resolved by making the timeout setting modifiable with the following new registry key: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles\Configuration\SyncService\CommandTimeoutSeconds` This `CommandTimeOutSeconds` registry key appears after reconfiguring the Active Roles Synchronization Service with the **Settings** > **Configure Sync Service...** option. To modify the default value of 6000 seconds, just change the default value contained in the registry key. NOTE: The value of the **`CommandTimeoutSeconds`** registry key is not part of the Synchronization Service configuration, and therefore cannot be imported or exported with the configuration. You must set it manually after each synchronization service configuration import.	278183

Resolved issue	Issue ID
Previously, the Azure BackSync operation of the Active Roles Synchronization Service did not support Modern Authentication. Instead, users had to specify their Azure Admin user name and password to authenticate themselves toward Azure AD, and the PowerShell script behind the Azure BackSync configuration also used basic authentication. This fix implements Modern Authentication by adapting the PowerShell script to Modern Authentication, and removing the now-obsolete Azure Admin login fields from the **Configure BackSync operation in Azure with on-prem Active Directory objects** dialog.	273422
Previously, the O365 Connector of the Active Roles Synchronization Service did not support Modern Authentication, and instead required a user principal name and user password during configuration. This fix implements Modern Authentication for the O365 Connector when connecting it to the Exchange Online service. NOTE: • The SharePoint Online and Microsoft Skype for Business Online services are deprecated and no longer supported by the O365 Connector. • After creating a new client secret in the Azure Admin Portal, you may need to wait up to 15 minutes until the client secret is synchronized and can be queried by the Active Roles Synchronization Service when creating the new O365 Connector.	273420

Table 7: Resolved Issues – Active Roles Management Shell

Resolved issue	Issue ID
In the Active Roles Management Shell, running the **`Get-QAD*`** cmdlet with the **`-SearchRoot`** and **`-IncludeAllProperties`** parameters simultaneously resulted in failure. The issue has been resolved by removing attributes from the search that can only be searched with Base scope, but not in Subtree scope.	277063

Known issues

The following is a list of issues in Active Roles 7.4.5, which are known to exist at the time of its release.

Table 8: Active Roles known issues

Known Issue	Issue ID
When creating a new Azure guest user in the Active Roles Web Interface, licenses, roles and optional attributes (such as **First Name**, **Last Name**, **Job Title**, **Department** or **Usage Location**) are not replicated to Azure AD by default. **Workaround** After creating the new Azure guest user, modify any of its properties under **Directory Management** > **Tree View** > **<azure-tenant-name>** > **Azure Guest Users** > **Azure Properties**, then save your changes. Updating any attribute of the Azure guest user will replicate its properties to Azure AD.	288597
Currently, the **Azure Health Check for Search** Access Template is not created if Active Roles 7.4.5 is installed via an in-place upgrade. **Workaround** To ensure that the **Azure Health Check for Search** Access Template appears properly, install Active Roles 7.4.5 with a clean installation.	285456
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, resulting in the various OneDrive configuration interfaces becoming unusable. Because of this, all OneDrive configuration settings have been removed from the Active Roles Web Interface and the Active Roles Console.	278521
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
In Active Roles Synchronization Service, Exchange Online Management module version 2.0.4 enforces Modern Authentication, causing the O365 connector connections to fail, if Modern Authentication is not enabled for the Azure tenant. **Workaround** Perform one of the following actions: • In the **Office365ConnectorConfig.xml** configuration file, disable	271447

Known Issue	Issue ID

. Example:
`<Tenants>`
`<Tenant Name="mytenant.OnMicrosoft.com" ModernAuthentic-`
`ation="false"/>`
`/organizations`
`</Tenants>`
• Roll back to Exchange Online Management module version 2.0.3.	

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
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.`	91977

Known Issue	Issue ID
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.	
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
After upgrading between major Active Roles versions, Web Interface Personal Views are lost because they are not imported to the newly created database. **Workaround** 1. Take a backup of the current database. 2. Copy the **PersonalSettings** data from the earlier database <DBName_	91729

BACKUP> to the current database <DBName>.

NOTE: The PersonalSettings table contains the saved personal views.

3. Use the following SQL script (without line breaks) to import the contents from the PersonalSettings table from the earlier database to the current database:

```
DECLARE @SourceDB NVarChar(50) DECLARE @TargetDB NVarChar(50)
DECLARE @SQL NVarChar(max) SET @SourceDB =
'ActiveRolesDB' -- Replace with <old-source-database> name. SET
@TargetDB = 'ActiveRolesDB_repl' --
Replace with <new-source-database> name. SET @SQL = 'INSERT INTO ['
+ @TargetDB + '].[dbo].
[PersonalSettings] ([rowId] ,[userId] ,[wiGuid] ,[settingName] ,
[settingValue] ,[modified]) SELECT * FROM
[' + @SourceDB + '].[dbo].[PersonalSettings]' EXEC(@SQL)
```

4. Update the **wiGuid** of the **PersonalSettings** to reflect the new **objectGUI** from the **WebInterface** table.
5. Query the current upgraded database **WebInterface** table as: Select * from Webinterface where **edsaWITemplateVersion** = '37'.

   NOTE: **edsaWITemplateVersion** value is based on the current version of the Active Roles Web Interface.

   The **edsaWITemplateVersion** value for the Active Roles versions are the following:

   - 7.4.3 / 40
   - 7.4 / 39
   - 7.3 / 38
   - 7.2 / 37
   - 7.1 / 36.
6. In the **PersonalSettings** table of the current upgraded database, replace the respective Web Interface site **objectGUID** to **wiGuid** for all rows.

System requirements

Before installing Active Roles 7.4.5, 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 9: 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. • 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.

Requirement	Details
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 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2013 • Microsoft Exchange 2013 CU11 is no longer supported. For more information, see Knowledge Base Article 202695.
Visual C++ Redistributables	Visual C++ 2017 Redistributable

Web Interface

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

Table 10:
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. • 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/

Requirement	Details
	• 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**.
Web browser	You can access 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 11: 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). • 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 12: 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). • 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 13: 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.
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.

Requirement	Details
	• 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. • 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	To connect to Active Roles version 6.9, the Active Roles ADSI Provider of

Requirement	Details
Roles ADSI Provider	*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 Module for Windows PowerShell module must be installed on the computer running the Synchronization Service.
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 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 14: 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

Requirement	Details
	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 in-place upgrade processes.

- 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 7.4.5, see the following information.

CAUTION: Hazard of data loss! Before installing Active Roles 7.4.5, make sure to perform the following steps in preparation. Failure to perform these steps before installing Active Roles 7.4.5 may result in unpredictable behavior, stability issues or data loss.

- **If Active Roles 7.4.4 hotfix SOL333618 is installed, remove it.**
- **Perform a database backup.**

Changes related to Azure tenants

NOTE: If your organization has any Azure tenants that are managed with Active Roles, you need to reauthenticate and reconsent them after installing Active Roles 7.4.5. Otherwise, Active Roles will not receive the required permissions for managing existing Azure tenants, and tenant administration in Active Roles 7.4.5 will not work correctly. For more information, see Reconfiguring Azure tenants during upgrade configuration.

Changes related to Active Roles Synchronization Service

NOTE: Active Roles 7.4.5 introduces support for Modern Authentication in Azure BackSync workflows of the Active Roles Synchronization Service. After upgrading to Active Roles 7.4.5, 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.

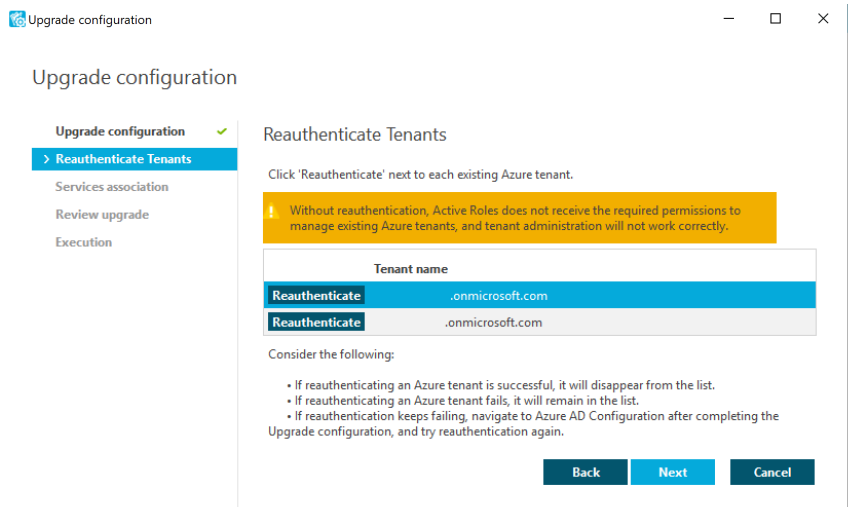
For more information on how to specify the Azure AD used for back-synchronization, see *Configuring automatic Azure BackSync* in the *Active Roles Synchronization Service Administration Guide*.

Reconfiguring Azure tenants during upgrade configuration

If your organization has any Azure tenants managed in Active Roles, you will need to reauthenticate and reconsent each Azure tenant after installing Active Roles 7.4.5. Otherwise, you may experience difficulties with Exchange Online connectivity and managing Azure AD resources (for example, assigning Azure AD roles).

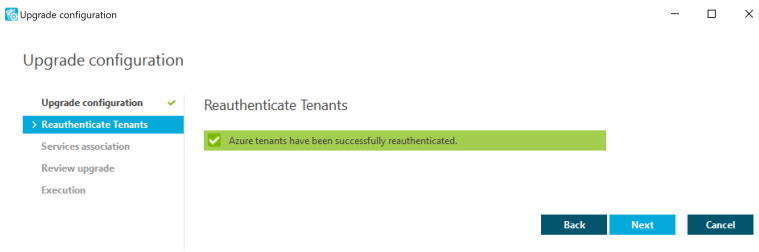
To reauthenticate and reconsent Azure tenants after installing Active Roles 7.4.5

1. Once Active Roles 7.4.5 is installed, open the Active Roles Configuration Center in Windows. The **Upgrade configuration** wizard will automatically appear.
2. To reauthenticate existing Azure tenants, proceed to the **Reauthenticate tenants** step and click **Reauthenticate** next to each Azure tenant.



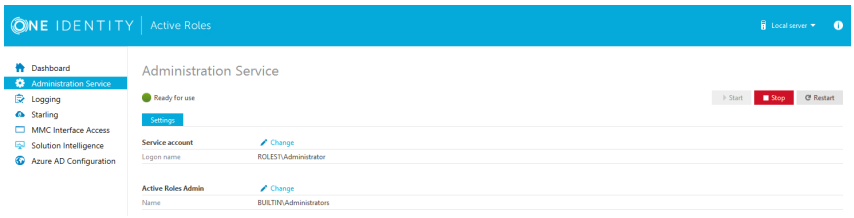
NOTE: Consider the following when reauthenticating existing Azure tenants:

- If reauthentication is successful, the Azure tenant will disappear from the list, and the **Reauthenticate tenants** step shows a confirmation message.

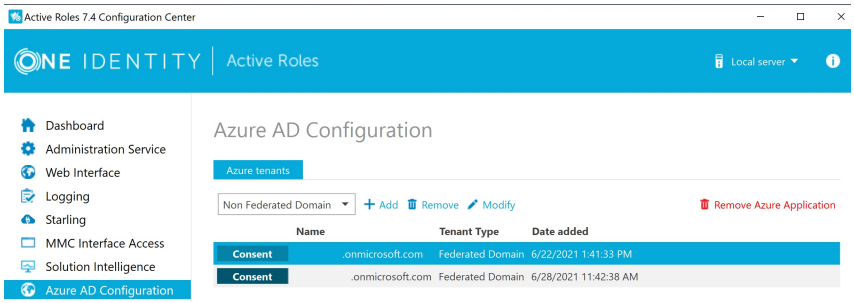


- If reauthentication fails, the Azure tenant will remain in the list. Reauthentication can typically fail if there is a service outage in Azure AD, or in case of internet connectivity issues in your network. If reauthentication keeps failing, try performing it later after completing the **Upgrade configuration** wizard by removing, readding and consenting the Azure tenants to Active Roles via the **Azure AD Configuration** tab of the Active Roles Configuration Center. For more information, see Reconfiguring Azure tenants manually.

3. Complete the rest of the steps in the **Upgrade configuration** wizard.
4. To make the reauthenticated Azure tenants appear in the Active Roles Web Interface, you must restart the Administration Service. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



5. Once the Active Roles Configuration Center has successfully restarted, navigate to **Azure AD Configuration**.



6. To reconsent Active Roles as an Azure application for the reauthenticated Azure tenants, click **Consent** in each tenant row.
7. To complete consenting, click **Accept** on the Microsoft **Permissions Requested** page that appears.

NOTE: Consenting will be successful only if Active Roles can receive the following permissions:

- Manage Exchange as Application
- Read and write directory data
- Read and write all groups
- Read and write all directory RBAC settings
- Read and write all users' full profiles
- Sign in and read user profile

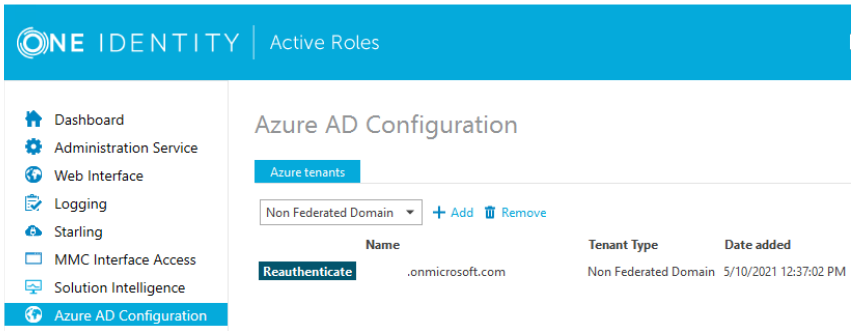
Reconfiguring Azure tenants manually

If your organization has any Azure tenants managed in Active Roles, you will need to reauthenticate and reconsent each Azure tenant after installing Active Roles 7.4.5. Otherwise, you may experience difficulties with Exchange Online connectivity and managing Azure AD resources (for example, assigning Azure AD roles).

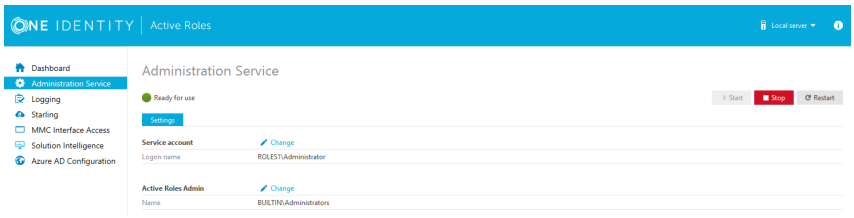
Azure tenant reauthentication is part of the **Upgrade configuration** process by default (for more information, see Reconfiguring Azure tenants during upgrade configuration). However, if reauthentication fails during that process for any reason, you can complete the reauthentication and reconsenting of existing Azure tenants with the following manual steps later.

To reconfigure Azure tenants after upgrading from Active Roles 7.4.1 or 7.4.3 to Active Roles 7.4.5

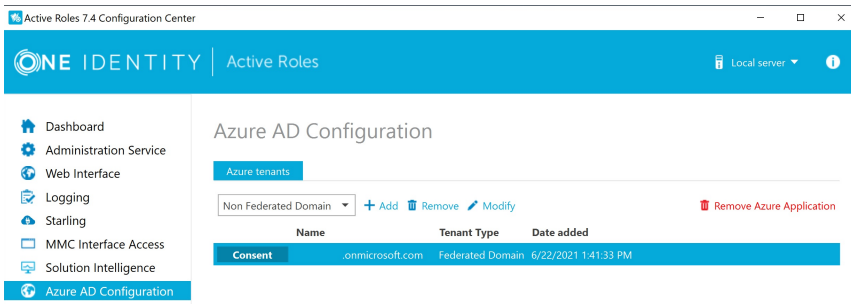
1. In the Active Roles Configuration Center, navigate to **Azure AD Configuration**.
2. To reconfigure the existing Azure tenants, select a tenant and click **Reauthenticate** in its row. Repeat the process for each existing Azure tenant.



3. To make the configured Azure tenant appear in the Active Roles Web Interface, you must restart the Administration Service. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



4. Once the Administration Service is restarted, consent Active Roles as an Azure application for each reconfigured Azure tenant. To do so, navigate again to **Azure AD Configuration**, select the Azure tenant and click **Consent**.



5. To complete consenting, click **Accept** on the Microsoft **Permissions Requested** page that appears.

   NOTE: Consenting will be successful only if Active Roles can receive the following permissions:

   - Manage Exchange as Application
   - Read and write directory data
   - Read and write all groups
   - Read and write all directory RBAC settings
   - Read and write all users' full profiles
   - Sign in and read user profile

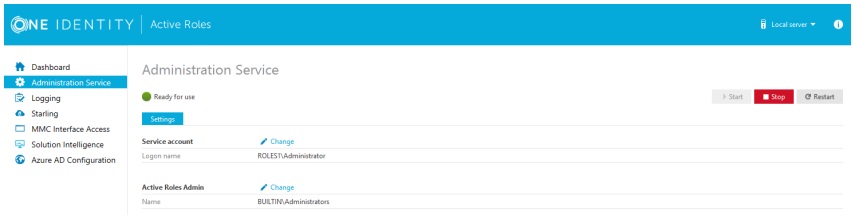
6. Repeat the previous two steps for each Azure tenant.

To reconfigure Azure tenants when upgrading from Active Roles 7.4.4 to 7.4.5

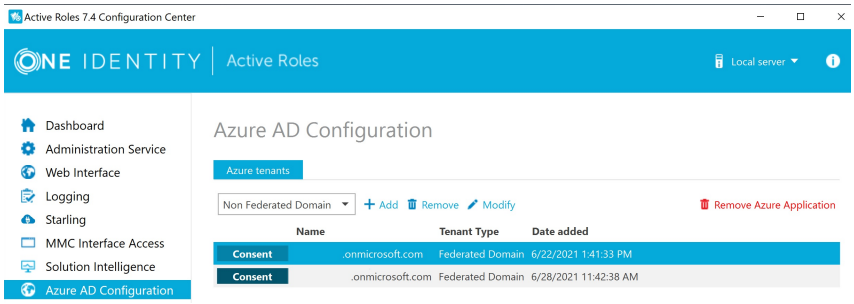
1. In the Active Roles Configuration Center, navigate to **Azure AD Configuration**.
2. Remove all Azure tenants. To do so, select an Azure tenant and first click **Remove Azure Application**, and then click **Remove**.
3. Repeat the previous step for each remaining Azure tenant.
4. Add the removed Azure tenants again to the list. To do so, use the drop-down box to select the type of domain assigned to the Azure tenant (**Non-Federated Domain**, **Federated Domain**, **Synchronized Identity Domain**), and click **Add**.

   Upon successful authentication, the new Azure tenant appears in the list.
5. Repeat the previous step for each Azure tenant that you previously removed.

6. To make the configured Azure tenants appear in the Active Roles Web Interface, you must restart the Administration Service. Click **Administration Service** on the left pane, then either click **Restart**, or first click **Stop** and then **Start**.



7. Once the Administration Service is restarted, consent Active Roles as an Azure application for the reconfigured Azure tenants. To do so, navigate to **Azure AD Configuration**, select an Azure tenant and click **Consent**.



8. To complete consenting, click **Accept** on the Microsoft **Permissions Requested** page that appears.

   NOTE: Consenting will be successful only if Active Roles can receive the following permissions:

   - Manage Exchange as Application
   - Read and write directory data
   - Read and write all groups
   - Read and write all directory RBAC settings
   - Read and write all users' full profiles
   - Sign in and read user profile

9. Repeat the previous two steps for each Azure tenant.

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*.

When performing the upgrade, keep in mind that the components of the earlier version may not work in conjunction with the components you have upgraded. To ensure smooth upgrade to the new version, you should first upgrade the Administration Service and then upgrade the client components (Console and Web Interface).

Custom solutions (scripts or other modifications) that rely on the functions of Active Roles may fail to work after an upgrade due to compatibility issues. Prior to attempting an upgrade, you should test your existing solutions with the new version of the product in a lab environment to verify that the solutions continue to work.

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 15: Version upgrade compatibility chart

Source version	Destination version
7.4.1	7.4.5
7.4.3	7.4.5
7.4.4	7.4.5

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.