One Identity Active Roles 7.4.4

Release Notes

May 2021

These release notes provide information about the One Identity Active Roles release. For the most recent documents and product information, see Active Roles online product documentation.

About One Identity Active Roles 7.4.4

NOTE: If you are currently utilizing the Office 365 Add-on, uninstall the add-on before performing the Active Roles upgrade to version 7.4.4. For more information regarding the changes to Office 365 support see Impact on Office 365 add-on.

Before proceeding with the upgrade ensure to perform a database backup.

Active Roles (formerly known as ActiveRoles®), provides out-of-the-box user and group account management, strictly enforced administrator-based role security, day-to-day identity administration and built-in auditing and reporting for Active Directory and Azure Active Directory (AD) environments. The following features and capabilities make Active

Roles a practical solution for secure management of objects in Active Directory and Active Directory-joined systems:

- **Secure access** Acts as a virtual firewall around Active Directory, enabling you to control access through delegation using a least privilege model. Based on defined administrative policies and associated permissions generates and strictly enforces access rules, eliminating the errors and inconsistencies common with native approaches to AD management. Plus, robust and personalized approval procedures establish an IT process and oversight consistent with business requirements, with responsibility chains that complement the automated management of directory data.
- **Automate object creation** Automates a wide variety of tasks, including:
  - Creating user, groups, and contacts in Active Directory and Azure AD
  - Creating mailboxes on Exchange Server and assigning licenses in Office 365
  - Managing on-premise Exchange and Exchange Online properties
  - Provisioning objects in SaaS products

  Active Roles also automates the process of reassigning and removing user access rights in AD and AD-joined systems (including user and group deprovisioning) to ensure an efficient and secure administrative process over the user and group lifetimes. When a user's access needs to be changed or removed, updates are made automatically in Active Directory, Azure AD, Exchange, Exchange Online, SharePoint, Skype for Business, and Windows, as well as any AD-joined systems such as Unix, Linux, and Mac OS X.

  NOTE: Mailboxes can be created only for **Users**, enabling mailbox for a **Contact** is not allowed.
- **Day-to-day directory management** Simplifies management of:
  - Exchange recipients, including mailbox assignment, creation, movement, deletion, permissions, and distribution list management
  - Groups
  - Computers, including shares, printers, local users and groups
  - Active Directory, Azure AD, Exchange Online and AD LDS

  Active Roles also includes intuitive interfaces for improving day-to-day administration and help desk operations via both an MMC snap-in and a Web interface.
- **Manage users, groups, and contacts in a hosted environment** Provides Synchronization Service to operate in hosted environments where accounts from client AD domains are synchronized with host domains. Active Roles enables user, group, and contact management from the client domain to the hosted domain, while also synchronizing attributes and passwords.
- **Consolidate management points through integration** Complements your existing technology and identity and access management strategy. Simplifies and consolidates management points by ensuring easy integration with many One Identity products and Quest products, including One Identity Manager, Privileged Password Manager, Authentication Services, Defender, Password Manager,

ChangeAuditor, and GPO Admin. Active Roles also automates and extends the capabilities of PowerShell, ADSI, SPML and customizable Web interfaces.

Active Roles 7.4.4 is a service pack release, with new features and functionality. See New features for details.

Supported Platforms

Active Roles 7.4.4 introduces the following changes to system requirements from those for Active Roles 6.9.0:

- 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, see Knowledge Base Article 202695.
- Internet Explorer is no longer supported for the Web Interface access. You can use the following Web browsers to access the Web Interface: Google Chrome, Mozilla Firefox, and Microsoft Edge on Windows 10.
- The Web Interface is optimized for screen resolutions of 1280 x 800 or higher. The minimum supported screen resolution is 1024 x 768.

See also System requirements.

New features

Active Roles 7.4.4 contains the following new features:

Azure AD configuration changes

In Active Roles 7.4.4, the process of setting up Azure tenants and configuring Active Roles as a consented Azure application for administering objects in Azure tenants has changed:

- In the Active Roles Configuration Center, a new **Azure AD Configuration** option has been added, allowing you to:

- Configure Active Roles as a consented Azure application with a secure client ID and secret ID-based authentication.
- Add or remove Azure tenants to or from your organization.

For more information, see *Configuring an Azure tenant and Active Roles as an Azure application* in the *Active Roles Administration Guide*.

NOTE: Azure Multi-Factor Authentication (MFA) is enforced by default for all users and guest users in newly-created Azure tenants. To disable Azure MFA for the Azure tenant, sign in to the Azure portal and navigate to **Tenant** > **Properties** > **Manage Security defaults** and set **Enable Security defaults** to **No**.

- In the Active Roles Web Interface, the following Azure tenant and Azure application-specific settings and configuration containers have been removed from the **Directory Management** > **Tree** > **Azure** > **Azure Configuration** node:
  - The **Azure Applications** and **Azure Domains** configuration containers.
  - The **Add Azure Tenant** and **Add Azure Application** options on the right-side pane when selecting the **Azure Tenants**, **Azure Applications** or **Azure Domains** configuration containers.
  - The **General** tab when viewing the properties of an existing Azure tenant.

  To access and configure the settings of these removed components, use the **Azure AD Configuration** option of the Active Roles Configuration Center.

  NOTE: The **Directory Management** > **Tree** > **Azure** node of the Active Roles Web Interface still retains the following Azure-specific features:
  - The **Azure Tenants** configuration object remains in the Web Interface, and provides access to the **Azure AD Tenant Type** and MFA security settings of the selected Azure tenant. These allow you change the type of the Azure tenant (non-federated domain, federated domain or synchronized identity domain) even after the Azure tenant has been created, and enable or disable Azure MFA for the users and guest users of the tenant.
  - Configured Azure tenants (and their directory objects) are still listed in the **Directory Management** > **Tree** > **Azure** node of the Active Roles Web Interface, allowing you to administer their O365 Groups, Azure users, Azure contacts and Azure guest users.
  - The **Azure Configuration** node still provides access to the **Azure Health Check**, **Azure Licenses Report** and **Office 365 Roles Report** pages.

Azure SQL database support

Active Roles now supports the administration of Azure SQL databases.

Cloud-only Azure object support

Active Roles now supports the administration of cloud-only Azure users, guest users and contacts in a configured Azure tenant. For more information, see the following topics of the *Active Roles Administration Guide*:

- For details on cloud-only Azure users, see *Managing cloud-only Azure users*.
- For details on cloud-only Azure guest users, see *Managing cloud-only Azure guest users*.
- For details on cloud-only Azure contacts, see *Managing cloud-only Azure contacts*.

Cloud-only Azure object policy support

The following Active Roles provisioning policies have been updated to support cloud-only Azure objects as well:

- **Property Generation and Validation**: This policy now also supports specifying object property rules for cloud-only Azure objects. For more information, see *Property Generation and Validation* in the *Active Roles Administration Guide*.
- **Group Membership AutoProvisioning**: This policy now also supports specifying group membership rules to automatically assign (or unassign) cloud-only Azure objects to (or from) O365 Groups of the same Azure tenant. For more information, see *Group Membership AutoProvisioning* in the *Active Roles Administration Guide*.
- **Script Execution**: This policy now also supports PowerShell and other custom scripts for provisioning cloud-only Azure objects. For more information, see *Script Execution* in the *Active Roles Administration Guide*.

In addition, as part of extending policy support for cloud-only Azure objects, Active Roles also received the following new built-in Policy Object and Script Module:

- **Azure CloudOnly Policy - Default Rules to Generate Properties**: Provides provisioning rules for the properties of cloud-only Azure objects, specifying whether they are mandatory or optional, along with their supported values. Find the policy in the **Configuration** > **Policies** > **Administration** > **BuiltIn** node of the Active Roles MMC interface, and use it as a template for creating your own custom policies.
- **Generate User Password - Azure only**: Provides a new PowerShell script to generate passwords for cloud-only Azure users that fulfill Azure password policy conditions. Find the script module in the **Configuration** > **Script Modules** > **BuiltIn** node of the Active Roles MMC interface, and use it as a template for creating your own password generation policy for cloud-only Azure users.

Duo and Okta integration support

Duo and Okta are both cloud-based identity management services offering identity, authentication, and access control functions as a service. Active Roles can be integrated with Duo Multi-Factor Authentication (MFA) or Okta MFA to complement and extend identity and access management.

For more information, see the following topics of the *Active Roles Administration Guide*:

- *Appendix G: Active Roles integration with Duo MFA*.
- *Appendix H: Active Roles integration with Okta MFA*.

Other changes

- Cloud-only objects have a uniqueness policy check upon creation.
- Support for creating and managing B2C guest user accounts.
- Support for SQL Server 2019.
- Granular built-in access templates for Azure-only objects that allow delegating control.
- Internet Explorer is no longer supported.
- PowerShell modules AzureRM, MSOnline and SharePoint are no longer supported.

Resolved issues

The following is a list of issues addressed in the release.

Table 1: General Resolved Issues

Resolved issue	Issue ID
User Logon Name in Web Console not displaying the correct information. This has now been fixed.	91823
In Active Roles 7.4 and 7.4.1 Web interface, the images used as icons in the Web Interface do not use transparency and display a white box around them. This has now been fixed.	215903
Uninstalling and reinstalling of sync service from command mode automatically picks old configuration. This has now been fixed.	222327
"All Objects - Full Control" taking precedence over deny of several attributes regardless of expected precedence behavior. This has now been fixed.	231144
Error is thrown on clicking Force SSL Redirection button after enabling or disabling Starling. This has now been fixed.	232529
Azure configuration components were previously not audited in the Change History and in the Active Roles Event Log. This has now been fixed.	235530

Resolved issue	Issue ID
Minor issues in the MultiSubnetFailOver documentation and UI. This has now been fixed.	235786
The Starling 2FA page loaded with an error message when TLS1.2 was enforced, and the user could not be authenticated. This issue has been fixed, the Starling 2FA page loads correctly and the user receives the authentication text message.	240574
ManagedObjectStatistics.exe Azure-only option failing with federated admin. This has now been fixed.	242443
Azure SQL support: Database validation should be there for the database type selected. This has now been fixed.	243478
No database validation was performed for the selected database type This has now been fixed.	243655
SaaS provisioning failed users also counted in Managed object statistics. This has now been fixed.	244182
Azure SQL: Database Type getting changed to Azure SQL Managed instance post in-place upgrade. This has now been fixed.	244492
Azure SQL: Discrepencies in error displayed in Configuration center. This has now been fixed.	245083
Database Migration failed in the Management history database with the Azure AD Credentials. This has now been fixed.	245270
Azure SQL: Discrepancies in Collector configuration. This has now been fixed.	245275
Azure SQL: Initial configuration for existing database gives incorrect MH Database server name for on-premises scenario. This has now been fixed.	245662
Azure SQL: Initial configuration for existing database gives incorrect authentication error for MH Database.	245663

Resolved issue	Issue ID
This has now been fixed.	
Ready to Upgrade page: Version to be changed. This has now been fixed.	245959
Azure SQL: Copy database permission selected for Azure SQL databases. This has now been fixed.	246061
Azure SQL: Change database option do not carry the default Database type. This has now been fixed.	246085
Azure SQL: Multi subnet settings in Advanced database properties are enabled for Azure SQL database type. This has now been fixed.	246418
Azure SQL support: Database validation error messages are not correct for the database connection with AAD and validation failed for "sa" account. This has now been fixed.	246624
Azure SQL: Review page tables overlapping when database names are long. This has now been fixed.	246634
During an in-place upgrade of the Active Roles Review upgrade page displayed a database upgrade even if there was no database upgrade. This issue has now been resolved, the Review upgrade page does not display the database upgrade if the in-place upgrade does not contain a database upgrade.	246639
Azure SQL: MH database prepopulated with SQL short name while configuring an existing database. This has now been fixed.	246805
Azure SQL: Collector database expecting dbmanager permission for user. This has now been fixed.	246879
Documentation about Modern Authenticaton should contain Windows Remote management (WinRM) explicitly instead of Microsoft links. This has now been fixed.	246887
Error messages are not logged correctly on SQL Server checks for ARS System checker.	247083

Resolved issue	Issue ID
This has now been fixed.	
Collector page authentication label to be corrected. This has now been fixed.	248552
Azure SQL: Enable auto Shrink option getting displayed for existing database and pre-configured blank database options. This has now been fixed.	248663
Sync Service: Mailbox resource type in the O365 AuditOwner attribute is missing. This has now been fixed.	249045
Previously, the Web Interface upgrade failed with SSL connection when Federated Authentication was configured in the source database. This has now been fixed.	249150
Azure Cloud Only: In Federated or Synchronized Identity environment the property fields are greyed out and cannot be updated. This has now been fixed.	250457
Azure Cloud Only:[Event log Error] General error occurred when retrieving the cloud-only Azure user objects (InteropServices.SEHException). This has now been fixed.	250476
Azure Cloud only: Account options can be both selected, when only one should be set. This has now been fixed.	250488
You are allowed to set "Sign-In with MFA", but not enable MFA on the previous screen. This has now been fixed.	250489
Action pane displays the objectID, not the user name. This has now been fixed.	250492
Post Creation bugs. This has now been fixed.	250493
Previously, when setting up a new Azure user, the property fields were disabled if any of the Azure tenants in the Azure node were set to Federated Authentication Domain or Synchronized Identity Domain type. This has now been fixed.	250658

Resolved issue	Issue ID
Previously, cloud-only Azure users were not listed immediately after an Azure tenant has been configured. This has now been fixed.	250660
Previously, configured Multi-Factor Authentication settings were not set when creating a new user. This has now been fixed.	250671
Previously, the Generate Password button was sometimes disabled in the Active Roles Web Interface and the Active Roles MMC Console. This has now been fixed.	251048
OneDrive: Eventlog message to be changed. This has now been fixed.	251268
Previously, Microsoft OneDrive configuration was not working in an Azure multi-tenant environment. This has now been fixed.	251269
Previously, the details of the Microsoft OneDrive configuration were not displayed in the Azure properties window of the selected Azure users. This has now been fixed.	251270
Azure Cloud Only: Discrepency in OneDrive properties. This has now been fixed.	252707
Azure Cloud Only: Quick Search is case sensitive. This has now been fixed.	252924
Fix Azure User icons. This has now been fixed.	253190
AzureOneDrive ProcessGetOnedriveStorage is not logged correct information for the OneDrive storage account. This has now been fixed.	254345
The OneDrive Site URL and Storage Info were visible even if the User had no SharePoint license. This issue has been fixed, OneDrive Site URL and Storage Info are only visible if the User has a SharePoint license, otherwise hidden, because OneDrive is a SharePoint-dependent.	255602
When creating a new cloud-only Azure contact or updating an existing one, it may take up to 15 minutes for the changes to appear on the Active Roles Web Interface. This is due to a replication delay present between PowerShell and the Microsoft Graph API.	255841

Resolved issue	Issue ID
The user interface and the documentation has been updated to inform you on this issue.	
On the installation screen, there was an unnecessary white row appearing between the prerequisite downloadable softwares, on the Ready to Upgrade page. This white row has now been removed.	256811
Azure Tenant container GUID did not persist. This has now been fixed.	257576
Missing Azure Active Directory icons added to MMC Console.	258710
Previously, Policy Objects set up for Azure user containers were not enforced on the New User form of the Active Roles Web Interface. This issue has been resolved, the policy is enforced as expected on the form.	258737
Previously, Active Roles logs could unintentionally display privileged credentials. This issue is now resolved.	258850
Previously, it was not possible to assign Azure users and guest users to Office 365 Groups directly from the user form on the Active Roles Web Interface. This issue has been resolved, you can now assign group membership to users and guest users from the Azure User/Azure Guest User form via the Azure Member Of option from the right-hand side menu.	259281
After configuring Azure, attempting to update and rename User resulted in an error message. This issue has now been resolved, users can be renamed and properties can be updated properly.	260938
When creating a Guest User, if the Open properties for this object when I click Finish checkbox was checked, an error message appeared. This issue has now been fixed, the option has been removed, as it had no useful function for Guest Users.	260940
In the Synchronization Service UI, after filling in the necessary fields and checking the "Load Workday schema" checkbox on the "Add Connection" view of SCIM Connector, after clicking "Finish" or "Test Connection", the following error messages were displayed "Cannot connect using the specified connection settings" and "Bad Request". The issue has now been fixed, so that you can connect to a SCIM	262373

Resolved issue	Issue ID
compatible Web API via SCIM Connector with or without Workday schema.	
When trying to delete a group in the Active Roles MMC Console, the following error message was displayed: Cannot find any resource for Active Roles. This issue has now been fixed, groups can be deleted.	264323
When trying to create a new Azure Contact, the new contact wasn't created properly and was not displayed. This issue has been fixed, a new contact can be created.	264326
When attempting to add a group in the MMC, the following Error message was displayed: Cannot find any resource for Active Roles. This issue has now been fixed, new groups can be added.	264666
Completion of back sync configuration was not possible due to an outdated log component. This issue has been resolved, the component has been replaced.	264830
Due to a SonarCloud security hotspot issue, privileged credentials could be unintentionally displayed. This issue has been fixed	265020
Exclude from Managed Scope policy did not work on Azure objects. This has now been fixed, if the policy can be enabled, to grant the user only read-only rights. In the Product Usage Statistics page of the Active Roles MMC Console the license count was calculated incorrectly for Azure. This has now been fixed, the license count is calculated correctly.	265443
When setting up Active Roles with Federated login via Azure ADFS the Act as Part of the Operating System privilege was required. This has now been changed, you can use the Federated login without these privileges.	266197
Previously, the Change History page did not show the invitation date of the guest user as the creation of the user account. This issue has now been fixed, so that the Change History page now correctly displays the time of invitation as the time of creation.	267162
When configuring Federated Authentication for the Web Interface, the following error message was displayed after a timeout delay (5 minutes by default): Unable to uniquely identify the user using provided claims. Please contact your Active Roles Administrator.	268891

Resolved issue	Issue ID
This issue has been resolved and Federated Authentication now revalidates without error.	
Previously, Azure guest users were not shown in the Active Roles MMC console in some cases. This has now been fixed.	269277
Office 365 Groups without a description attribute were not synced to the Active Roles database and as a result did not show up as children in the Office 365 Groups container. This issue has now been fixed, now the Office 365 Groups that do not have a description are displayed correctly.	270166
There were several password-related input fields, buttons and check-boxes on the Guest User invitation form, which were unnecessary, as the password must be specified by the user when accepting the invitation. These, along with the Account tab that contained them, have been removed.	270183
The global search of the Active Roles Web Interface does not search in Office 365 Groups container. This issue has now been resolved, the names displayed in Office 365 Groups are also involved in the search results.	270184
There were several inpud fields missing from the New Azure User form. The following attributes have been added: • Job Title • Department • Enable Sign-In	270339
On the New Azure User and Invite Guest form, the Allow user to sign in and access services checkbox had no effect, the created account was always enabled. This issue has now been resolved, the checkbox works properly.	270471

Table 2: Resolved Documentation Issues

	Issue ID
Added missing information to the Active Roles Administration Guide about SQL permission level required for migrating database users, permissions, logins and roles during an in-place upgrade. The required permissionsResolved issue are the db_owner and	232869

	Issue ID
sysadmin roles. For migrating the configuration settings and management history, the db_datareader role must also be set for the source database.	
Active Roles needs specific read access to be able to read fine-grained password policy objects in Active Directory. This has now been documented.	242347
Removed obsolete Password Manager references from Active Roles Web Interface Administration Guide. This has now been fixed.	250932
Missing information about setting the Transport Layer Security (TLS) version ha been added to the PowerShell Reference Guide. If importing Active Roles PowerShell modules fail, the TLS version of the operating system must be set to version 1.2 or higher.	252598
Added missing line $context.O365RemoveAllModulesSessions() to the sample Office 365 workflow script examples in the Active Roles Administration Guide. The $context.O365RemoveAllModulesSessions () allows users to clean up any open Azure PowerShell sessions, preventing high memory usage.	264234
The section about installing and configuring Redistributable STS (rSTS) has been rewritten in Appendix E in the Active Roles Administration Guide.	265434

Known issues

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

Table 3: Active Roles known issues

Known Issue	Issue ID
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**	275240

Known Issue	Issue ID
To avoid this issue, One Identity recommends configuring the Web Interface in the Active Roles Configuration Center only after importing any Active Roles configurations.	
After installing Active Roles and navigating to **Azure Guest Users** in the Web Interface, the list of guest users does not appear and the page is empty. NOTE: This issue only affects fresh installations of Active Roles. It does not occur after upgrading Active Roles from an older version. **Workaround** In the Active Roles Configuration Center, restart the Administration Service.	258904
In the Active Roles Web Interface, when creating passwords manually for cloud-only Azure users, there is no policy that validates the complexity of the password. If the administrator creates a password manually, the value is sent to Azure AD for user creation without explicitly checking the Azure AD password complexity requirements. If the password does not meet the requirements, the user creation request silently fails. **Workaround** Perform one of the following actions: • Generate a password instead of creating it manually because the built-in **Generate User Password - Azure only** PowerShell script generates a value for generated passwords that meet the Azure AD complexity requirements. • Create a password manually with a complexity that meets the Azure AD password complexity requirements. For more information, see Password policies and account restrictions in Azure Active Directory in the *Azure Active Directory Authentication documentation*.	270182

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 Modern Authentication and add **`/organizations`**. Example:
`<Tenants>`
`<Tenant Name="mytenant.OnMicrosoft.com"`
`ModernAuthentication="false"/>`
`/organizations`
	271447

Known Issue	Issue ID
`</Tenants>` • Roll back to Exchange Online Management module version 2.0.3.	
After running the **`get-qcworkflowstatus`** cmdlet in the Synchronization Service, the workflow status is not accurate.	125768
If a hybrid user is added as a member of the Office 365 Group, navigating to the **Member of** tab of the respective user, the Office 365 Group type is still displayed as a normal group.	101793
In the **Starling Connect Connection Settings** link, clicking **Next** displays progress, but the functionality is not affected, so the button is not required.	126892
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 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
Active Roles does not support creating Azure groups for existing groups.	117015
Tenant selection supports selecting only a single tenant.	229030
When configured for Group and Contacts, the **Office 365 and Azure Tenant Selection** policy displays additional tabs.	229031
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

Known Issue	Issue ID
BACKUP> to the current database <DBName>. NOTE: The PersonalSettings table contains the saved personal views. 3. Use the following SQL script 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].[Person-alSettings] ([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.	
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:	91977

Known Issue	Issue ID
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.	
Active Roles Web Interface does not support setting the **Exchange Online Property** of the **ProhibitSendQuota** value in **Storage Quotas**.	91905
After upgrading Active Roles, the pending approval tasks are not displayed in the Active Roles Web Interface.	91933
When a workflow is copied from built-in workflows, it may not be executed as expected.	153539
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
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

System requirements

Before installing Active Roles 7.4.4, 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

Table 4: 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

Requirement	Details
	Core mode setup.
Microsoft .NET Framework	Administration Service requires Microsoft .NET Framework 4.7.2 (see "Installing the .NET Framework" at http://go.microsoft.com/fwlink/?LinkId=257868).
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, the Administration Service requires Windows Management Framework 5.1 (see "Windows Management Framework 5.1" at https://www.microsoft.com/en-us/download/details.aspx?id=54616).
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. We recommend 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

Requirement	Details
	• Microsoft Exchange Server 2013 • Microsoft Exchange 2013 CU11 is no longer supported. Refer KB article 202695.
Visual C++ Redistributables	Visual C++ 2017 Redistributable

Web Interface

Table 5:
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 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	Web Interface requires Microsoft .NET Framework 4.7.2 (see "Installing the .NET Framework" at http://go.microsoft.com/fwlink/?LinkId=257868).
Visual C++ Redistributable	Visual C++ 2017 Redistributable

Requirement	Details
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 delegation set to **Read/Write**.
Web browser	You can access Web Interface using: • Firefox 36 on Windows • Google Chrome 61 on Windows • Microsoft Edge on Windows 10 You can use a later version of Firefox and Google Chrome to access the Web Interface. However, the Web Interface has been tested only against the browser versions listed above.

Requirement	Details
Minimum screen resolution	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)

Table 6: 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 (see "Installing the .NET Framework" at

Requirement	Details
	http://go.microsoft.com/fwlink/?LinkId=257868).
Visual C++ Redistributable	Visual C++ 2017 Redistributable
Web browser	Active Roles console requires Microsoft Edge.

Management Tools

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

Table 7: 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

Requirement	Details
	Core mode setup.
Microsoft .NET Framework	Management Tools require Microsoft .NET Framework 4.7.2 (see "Installing the .NET Framework" at http://go.microsoft.com/fwlink/?LinkId=257868).
Visual C++ Redistributable	Visual C++ 2017 Redistributable
Windows Management Framework	On all supported operating systems, Management Tools require Windows Management Framework 5.1 (see "Windows Management Framework 5.1" at https://www.microsoft.com/en-us/download/details.aspx?id=54616).
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. See Microsoft's documentation for instructions on how to install Remote Server Administration Tools appropriate to your operating system.

Synchronization Service

Table 8: Synchronization Service requirements

Requirement	Details
Platform	Any of the following: • Intel 64 (EM64T) • AMD64 • Processor speed: 2.0 GHz or faster For best results, a multi-core processor recommended.
Memory	At least 2 GB of RAM. The amount required depends on the number of objects being synchronized.
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:

Requirement	Details
	• 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	Synchronization Service requires Microsoft .NET Framework 4.7.2 (see "Installing the .NET Framework" at http://go.microsoft.com/fwlink/?LinkId=257868).
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, the Synchronization Service requires Windows Management Framework 5.1 (see "Windows Management Framework 5.1" at https://www.microsoft.com/en-us/download/details.aspx?id=54616).
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

Requirement	Details
	NOTE: Microsoft Exchange 2013 CU11 is no longer supported. Refer KB 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 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 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 following module must be installed on the computer running the Synchronization Service: • Azure Active Directory Module for Windows Power-Shell

Requirement	Details
	For installation instructions, see "Install the Azure AD Module" at https://docs.microsoft.com/en-us/powershell/azure/active-directory/install-adv2?view=azureadps-2.0.
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" at https://docs.microsoft.com/en-us/microsoftteams/teams-powershell-install.
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. For installation instructions, see "SharePoint Online Management Shell" at http://go.microsoft.com/fwlink/?LinkId=255251.
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

Table 9: Synchronization Service Capture Agent

Requirement	Details
Microsoft .NET Framework	Synchronization Service Capture Agent requires Microsoft .NET Framework 4.7.2 (see "Installing the .NET Framework" at http://go.microsoft.com/fwlink/?LinkId=257868).
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

Requirement	Details
	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

In Active Roles 7.4, enhancements are made for in-place upgrade processes. For instructions on how to upgrade from an earlier Active Roles version, see the Active Roles Quick Start Guide. The Quick Start Guide also contains instructions on how to perform installation and initial configuration of Active Roles.

For instructions on how to install and configure the Synchronization Service, see 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 Active Roles, refer to 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 10: Version upgrade compatibility chart

Source version	Destination version
6.9.0	7.4.4
7.0	7.4.4
7.1	7.4.4
7.2	7.4.4
7.3	7.4.4

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.