

One Identity Active Roles 7.4.3

Release Notes

October 2020

These release notes provide information about the One Identity Active Roles release.

- [About One Identity Active Roles 7.4.3](#)
- [New features](#)
- [The following is a list of enhancements implemented in Active Roles Version 7.4.x versions.](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [Product licensing](#)
- [Upgrade and installation instructions](#)
- [Globalization](#)

About One Identity Active Roles 7.4.3

NOTE: If you are currently utilizing the Office 365 Add-on, uninstall the add-on before performing the Active Roles upgrade to version 7.4.3. 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 7.4.3 is a service pack release, with new features and functionality. See [New features](#) for details.

Supported Platforms

Active Roles 7.4.3 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, and 2017.
- You can use Active Roles to manage Exchange recipients on Exchange Server 2019, 2016, 2010, or 2013.
NOTE: Microsoft Exchange 2013 CU11 is no longer supported. Refer [KB article 202695](#).
- To manage Exchange recipients on Exchange Server 2010, Active Roles no longer requires the Exchange 2010 Management Tools on the computer running the Administration Service.
- Internet Explorer 7, 8, 9, and 10 are no longer supported for the Web Interface access. You can use the following Web browsers to access the Web Interface: Internet Explorer 11; Google Chrome; Mozilla Firefox; Microsoft Edge on Windows 10.
- Web Interface is optimized for screen resolutions of 1280 x 800 or higher. The minimum supported screen resolution is 1024 x 768.
- Active Roles console requires Internet Explorer 11.

See also [System requirements](#).

New features

The new release of Active Roles extends and enhances the capabilities of the product .

Major new features in Active Roles Version 7.4.3:

- Support for multiple Azure tenants.
- Support for Modern Authentication.

NOTE: Modern authentication for exchange online properties is included as a preview feature in this release. The feature is tested and included in the product as a supplement to Basic authentication. One Identity reserves the right to provide limited support to this feature as defined in the [One Identity Support Guide](#).

Major new features in Active Roles Version 7.4.1:

- Additional Hybrid Directory features:
 - Support for Office 365 Group CRUD activities.
 - Support for Office 365 roles and reporting for Office 365 users.
 - Support for Exchange Online Mailbox Properties for Office 365 users in Federated and Synchronized environment.
- Support for provisioning objects in SaaS products.
- Separate configuration and management history databases during installation or in-place upgrade, conforming to Microsoft standards and best practices for replication.
- Support for Azure AD Graph 1.6 for Active Roles Synchronization Services.
- Use of Group Managed Service Account (gMSA) for Active Roles Service account.
- Bulk attribute operations for multiple users.
- Reset the password for multiple users at one time.
- Solution Intelligence for Active Roles.
- Log in to MMC interface through 2FA authentication.
- Support for Transport Layer Security (TLS) 1.2 in Synchronization Service.
- Support for remote mailbox creation and modification.

NOTE: The 'Remote mailbox migration (RemoteMailbox.ps1)' script has been provided as a sample script only, to illustrate the steps required, and should not be used as-is in a production situation without modification and enhancement. The use of security credentials within a script in clear text should never be considered appropriate or secure. In testing this script, care and consideration should be given to the authentication and use of credentials, and clear text credentials should not be left in the script once testing is complete. For more details refer the KB article: <https://support.oneidentity.com/kb/310525>.

- Support for Federated authentication feature.
- Support to provide product feedback from the Web Interface.

See also [Resolved issues](#).

The following is a list of enhancements implemented in Active Roles Version 7.4.x versions.

Major enhancements in Active Roles Version 7.4.3:

Table 1: General enhancements

| Enhancement | Issue ID |
|--|----------|
| Support to add multiple Azure tenants | 115765 |
| New builtin workflow and script added for: <ul style="list-style-type: none">• Create Office 365 shared mailbox | 169656 |

| Enhancement | Issue ID |
|---|----------|
| <ul style="list-style-type: none"> • Enabling Azure Roles. | |
| Edit or update exchange or extension properties of the Master account even in the absence of the corresponding shadow account in the Exchange Forest. | 172000 |
| Automate the process of copying the database users, permissions, SQL logins, and roles from the old SQL database to a new database during the in-place upgrade and import database. | 90779 |
| Active Roles now give precedence to Fine-Grained policy over Domain policy while evaluating the User account and password information. The User account information and Account Policies are displayed based on the configured policy applied on the container. | 90776 |
| Autoshrink option can be customized for new Active Roles database (configuration and management history) during the configuration of Active Roles. | 90999 |
| The substitute attribute, mail can now be used optionally instead of using it as a hard-coded attribute. | 100642 |
| Enable Modern Authentication while communicating with Exchange Online from ARS. | 153509 |
| edsvaAzureOffice365Enabled is automatically set to true, if azure policy is applied. | 99213 |
| Optimized policy evaluation for license management, Office 365 roles management type policies, and check policy compliance. | 90953 |
| Add multiple users to a group in ARS change workflow based on specific criteria. | 91024 |
| Active Roles Synchronization Service Management Shell is extended to install component separately. | 91061 |
| Active Roles Synchronization Service enhancements | |
| <ul style="list-style-type: none"> • Support for Oracle Database User Accounts (version 19.3) | 166918 |
| <ul style="list-style-type: none"> • Support for Oracle Database Connector (version 19C) | 166923 |
| <ul style="list-style-type: none"> • Support for Oracle Unified Directory (version 12.2.1.3) | 166925 |
| <ul style="list-style-type: none"> • Support for Micro Focus NetIQ Directory (version 9.2) | 166920 |
| <ul style="list-style-type: none"> • Support for IBM AS/400 connector (version v7r1) | 218409 |

Major enhancements in Active Roles Version 7.4.1:

Table 2: General enhancements

| Enhancement | Issue ID |
|--|----------|
| Support for the multiSubnetFailOver feature of MS SQL Server to maximize internal availability. | 90802 |
| Support for the Security Identity Mappings functionality as available in Active Directory Users and Computers (ADUC) Snap-in. | 90767 |
| Workflow enhancements that enable you to add Azure or Office 365 modules in PowerShell and run the Office 365 services such as Skype for Business, Azure AD, Azure RM, AZ, and Sharepoint Powershell scripts within existing Active Roles workflows. | 114132 |
| Support to restrict MMC interface access for a user. On installing Active Roles 7.4 on a computer, any user is enabled to log in to the MMC interface. You can now set the Active Roles MMC interface user access using the Active Roles Configuration Center. | 90765 |
| Enhancement of SPML operation to get ObjectSid to retrieve the value in the SID format in addition to the base64Binary format. | 90764 |
| Support for creation of OneDrive for Azure AD users using OneDrive Provisioning Policy. | 90797 |
| Support for configuring secure communication for Active Roles Web interface using Force SSL Redirection. | 90768 |
| In-place upgrade enhancements | 102832 |
| Support for federated authentication | 90820 |
| Support has been added for the following connectors through the Synchronization Service: | 124068 |

Table 3: New connectors and supported versions

| Connectors | Supported version |
|------------------------|--|
| Generic LDAP Connector | Version 3 |
| MY SQL Connector | MySQL database hosted on MySQL Community Server MySQL 8.0.12 |
| Open LDAP Connector | Version 3 |
| IBM DB2 Connector | IBM Db2 11.5 Edition for Windows |

| Connectors | Supported version |
|-----------------------|---|
| Salesforce Connector | Internet access to the data system you want to participate in data synchronization operations |
| Service now Connector | Internet access to the data system you want to participate in data synchronization operations |
| IBM RACF Connector | Version 1.13 or later. Optionally with LDAPX exit version 2.10 or later |

| | |
|--|-------|
| Support to modify the following Exchange Online properties in Synchronized Identity and Federated environments using the Active Roles Web interface: | 90758 |
| <ul style="list-style-type: none"> • Archive mailbox • Message records management • Mail flow settings • Email address | |

| | |
|--|-------------------------|
| Active Roles Sync Service enhancements | |
| <ul style="list-style-type: none"> • Support for Microsoft Share Point 2019 • Support for Microsoft Exchange 2019 • Support for Microsoft Skype for Business 2019 | 99916 99897 99910 |

| | |
|---|-------|
| Restructured product documentation for Active Roles. Documentation set now consists of the following guides: | 90791 |
| <ul style="list-style-type: none"> a. Administration Guide b. Evaluation Guide c. Feature Guide d. Predefined Access template guide e. Quick Start f. Release Notes g. Solutions guide h. Synchronization Service Guide i. User's Guide j. Web Interface Admin Guide k. Web Interface User's Guide l. Whats New Guide | |

- m. Diagnostics Tools Release Notes
- n. How-to Guide
- o. Add-on Manager Readme

The following guides from earlier releases are deprecated and the content is made available in the documents available for the current release:

- Management Pack for SCOM
- Configuration transfer Wizard Guide
- Exchange Resource Forest Management Guide
- Skype for Business Guide
- SPML Guide
- Azure AD and Office 365 Administration Guide
- Replication Guide
- Product Overview Guide

Resolved issues

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

Table 4: Administration Service, ERFM, Configuration Center, and Management Shell

| Resolved issue | Issue ID |
|---|----------|
| <p>Currently, Active Roles does not detect or overrides Native Active Directory schema modification performed for All extended rights ACE on default security for 'Computer' object type.</p> <p>To enable the fix on a system running Active Roles Service:</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start->Run and typing regedit on the machine where Active Roles Service is installed. 2. Navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles. 3. Right click and select New DWORD (32-bit) Value. 4. Enter the registry key name as DisableExtendedRightsACE. 5. Double click on the registry key name | 642572 |

| Resolved issue | Issue ID |
|--|----------|
| <p>and in the Value Data field, set the registry key value to 1 and click OK.</p> <p>6. Setting this value to 0 or deleting the key disables the fix.</p> <p>7. Re-start the Active Roles Administration Service.</p> | |
| <p>In Active Roles modifying the equipment mailbox or Room mailbox to include an user as "Send As trustee" fails with error message "Set-CASMailbox , 'ActiveSyncMailboxpolicy' may not be performed on resource mailbox"</p> <p>To enable the fix on a system running Active Roles Service:</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start->Run and typing regedit on the machine where Active Roles Service is installed 2. Navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles 3. Create a new DWORD entry named CASMailBoxExch and set the value to '1' 4. Setting this value to 0 or deleting the key disables the fix. | 667425 |
| <p>Active Roles VA processing throttles SQL CPU usage and may not function as expected in some environments.</p> <p>This fix optimizes the SQL lookups for Virtual Attributes in Active Roles.</p> <p>To enable this fix, set up a registry key as follows:</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start->Run and typing regedit on the machine where Active Roles Service is installed. 2. Navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles\Configuration\Service. 3. Right click and select New DWORD (32-bit) Value. 4. Enter the registry key name as Disable500VA. 5. Double click on the registry key name Disable500VA, and in the Value Data field set the registry key value to "1" and click OK. 6. Setting this value to 0 or deleting the key disables the fix. 7. Restart the Service to enable or disable the fix. <p>NOTE: The Event ID 2508 generated in the Event Viewer, during Service startup, displays the following message if the fix is enabled</p> | 726038 |

| Resolved issue | Issue ID |
|---|----------|
| successfully: Disable500VA registry value set to 1. | |
| <p>Currently in Active Roles exchange related operation is failing when trying to change Master account of a linked mailbox. Active Roles user is unable to change Master Account on Exchange 2013 linked mailboxes in an environment where exchange servers coexist on multiple sites.</p> <p>Create the following Registry key in the system Registry where Active Roles Service is installed.</p> <ul style="list-style-type: none"> • Registry Path = "HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles\7.4\Service" • Registry Key = "SetRegistryFor508214" • Registry Type = REG_DWORD • Registry value = 1 | 508214 |
| <p>In Active Roles, Performance issues may be noticed in large Exchange environments.</p> <p>This fix contains an alternate codepath which attempts to improve performance and generate additional logging.</p> <p>Enable the fix by setting a registry key as follows:</p> <ol style="list-style-type: none"> 1. Navigate to path, HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\ActiveRoles\Configuration. 2. Create a DWORD value with name PerformanceFlag and set data to '1'. 3. Setting PerformanceFlag to '1' will enable the fix. 4. Setting PerformanceFlag to '0' will disable the fix. <p>This value must be set on machines with the Administrative service and the Web Interface installed.</p> <ol style="list-style-type: none"> 5. Re-start the Service and IIS to enable or disable the fix. <p>The EventViewer will contain an event with Event ID 2508 which will have the following text if the fix is enabled successfully, Performance flag value set to 1.</p> | 724362 |
| <p>When Active Roles 6.9 and 7.x are working in parallel, Group family members are being removed by a dynamic group process if the cross domain membership is enabled for the dynamic group built-in policy.</p> <p>The fix is enabled by setting up a registry key as below:</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start->Run and typing regedit. | 668247 |

Resolved issue**Issue ID**

2. Navigate to the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles\7.4\Service**.

3. Create a new DWORD (32-bit) entry named "RebuildDG_CoExist" and set the value to '1'.

4. Setting this value to '0' or deleting the key disables the fix.

In Active Roles, Home folder is not shared when creating new user accounts with NetApp Filer.

699437

The fix is enabled by setting up a registry key as below:

1. After installation, open the **Registry Editor** by navigating to **Start->Run** and typing regedit.

2. For ARS 6.9, navigate to the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Aelita\EnterpriseDirectory Manager**.

3. For ARS 7.2 onwards, navigate to the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles**.

4. Create a new DWORD(32-bit) entry named **EnableHomeShareDelay** and set the value to an integer greater than '0'.

For example, **Setting EnableHomeShareDelay** to a value of '20' introduces a 20 second delay between user creation and home share creation.

5. Setting this value to '0' or deleting the key will disable the fix.

Active Roles currently does not accept LDAP expressions containing the "Extended Match Operator" for Dynamic Groups.

664258

The fix can be enabled by setting up a registry key as below:

1. After installation, open the **Registry Editor** by navigating to **Start->Run** and typing regedit.

2. Navigate to the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles**.

3. Create a new DWORD entry named **BypassValidationForMatchingRuleOID** and set the value to '1'.

4. Setting this value to '0' or deleting the key will disable the fix.

When the active directory group object attribute

684127

"**msExchHideFromAddressLists**" is modified on environments with migrated exchange mailboxes and running Active Roles 6.9 Patch 4 without on-premises exchange servers, the following error is displayed:

| Resolved issue | Issue ID |
|---|----------|
| <p>"Operation could not be performed due to the current state of the object."</p> <p>The fix is enabled by setting up a registry key as follows:</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start->Run and typing regedit. 2. Navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles. 3. Create a new DWORD (32-bit) entry named EnableHideMailAddress and set the value to '1'. 4. Setting this value to '0' or deleting the key will disable the fix. | |
| When you run the commandlet Get-Qaduser -includeallproperty , an error is displayed. | 109578 |
| In an ERFM environment, the error <i>Unable to create user mailbox due to Unable to connect to Exchange Server</i> is logged in to the change history of the newly copied user. | 91639 |
| <p>In any error scenario in Azure Active Directory, the following error is logged in the Active Roles Web interface and Event Viewer:</p> <p><i>Administrative Policy returned an error. Could not find any resources appropriate for the specified culture or the neutral culture. Make sure "ActiveRoles.Service.Azure.Errors.resources" was correctly embedded or linked into assembly "ActiveRoles.Service.Exchange" at compile time, or that all the satellite assemblies required are loadable and fully signed."</i></p> | 91651 |
| <p>In Active Roles with a large number of computer objects with Bitlocker enabled, Bitlocker key search does not display search results in the Web interface and takes a long time to display the results in the MMC console.</p> <p>To enable the fix on a system where Active Roles 7.4 Web interface and MMC console are being used</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start->Run and typing regedit on the machine where Active Roles Service is installed. 2. Navigate to the registry key HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Active Roles. 3. Right click and select New DWORD (32-bit) Value. 4. Enter the registry key name as BitlockerSearch. 5. Double click on the registry key name BitlockerSearch and in the Value Data field, set the registry key value to 1 and click | 97931 |

| Resolved issue | Issue ID |
|--|----------|
| OK. | |
| 6. Setting this value to 0 or deleting the key disables the fix. | |
| In Active Roles when the Description attribute for a group is modified, the ' edsaAzureGroupDescription ' attribute is also modified, though the Azure policy is not enabled. | 101068 |
| In Active Roles, after an Azure User, Group, or Contact is created, the ' edsvaAzureObjectID ' attribute does not get populated in the change history. | 105368 |
| In Active Roles Web interface, the Azure tabs are hidden while copying a non-Azure user. | 106415 |
| In Active Roles, inconsistencies exist in the change history of the User properties modification, if an Approval activity exists and the task is approved post escalation in the Change workflow. | 106618 |
| In Active Roles, when a separate notification activity is configured to send an email to persons who approved the operation, the notification email is not sent out after the Approval activity. | 110932 |
| In Active Roles Management Shell, the New-qaduser commandlet with an attribute ' UserPassword ' passed, throws an error: <i>Unknown error 0x80041070</i> . | 102616 |
| In Active Roles Management Shell, for the attribute " edsvaSecondaryOwners ", clear operation through putEx does not work as expected. | 101221 |
| In Active Roles Management Shell, updating the attribute edsvaSecondaryOwners fails with an error. | 97215 |
| In Active Roles Management Shell, the Set-QADUser or Set-QADGroup commandlet does not update Authorig or unAuthOrig Exchange attributes, when the Append keyword is used. | 91656 |
| In Active Roles, performance issue is experienced in large environments, when an LDAP query is used to get user information in the Exchange Online properties Delegation tab. | 97214 |
| Currently, when connection to the Active Roles Service Domain Controller is lost the Get-QADUser command reads "passwordLastSet" or "pwdLastSet" attribute value as empty instead of not returning user data or any properties. | 781507 |
| In Active Roles Service, update to a multi-valued attribute using ADSI does not work as expected while using PutEx . | 776700 |
| In Active Roles Service, for the Workflow with "Modify Requested Changes" activity, the Create User operation fails and displays the | 775818 |

| Resolved issue | Issue ID |
|--|----------|
| error: <i>Nullable object must have a value.</i> | |
| In an ERFM environment, on the Active Roles MMC Console, changing the attribute value "msExchRecipientTypeDetails" of the shadow account deletes the master account email attribute value and removes the Exchange tabs from the Properties page. | 762902 |
| In Active Roles Service configured with Azure, Active Roles Service start does not complete successfully if connection to Azure is lost. | 709345 |
| In Active Roles integrated with Change Auditor, Deprovision reports are not sent successfully and display the error message: <i>Root element is missing and Specified method is not supported.</i> | 706844 |
| Active Roles Service looks for Exchange Servers in the current domain only even though Exchange Servers exist in other domains in the same forest. This fix adds additional logs and allows you to set the " Set-AdServerSettings " commandlet's ForceViewEntireForest value to true that enables the scope of the current session to the entire forest. Create the following Registry key in the system Registry to set " SetAdServerSettings " commandlet's ForceViewEntireForest value to true. <ul style="list-style-type: none"> • Registry Path = "HKEY_LOCAL_MACHINE\Software\One Identity\Active Roles" • Registry Key = "ForceViewEntireForest"; • Registry Type = REG_DWORD • Registry value = 1 Instructions to enable the fix: <ol style="list-style-type: none"> 1. Create and set the value of Registry key ForceViewEntireForest to 1 in the registry path HKEY_LOCAL_MACHINE\Software\One Identity\Active Roles. 2. Apply the fix. 3. Restart the Active Roles Service. | 603025 |
| In Active Roles, when the user Creation form is customized, Azure User Password from the Change History of the Azure user is displayed as plain text. | 773881 |
| Active Roles Management Shell displays an error during successful operations involving ChangeParentDN policy handlers when running Create Object Commandlets. | 749380 |

| Resolved issue | Issue ID |
|--|----------|
| <p>In Active Roles, when we enable Built-In policies for Exchange Resource Forest Management and Skype on any container, the "The directory object not found in cache" error is encountered during the following operations:</p> <ul style="list-style-type: none"> • Adding user to a group through SPML • Retrieving the properties for the container's objects through VB scripts | 748864 |
| In the Exchange Online, when Azure configuration is performed in Active Roles, properties are editable under Federated or Synchronized identity environment. | 754071 |
| In Active Roles, group properties modification workflow with two level approvers gives error in the Change History when 'edsaSecondaryOwners' is modified" | 759766 |
| In Active Roles Federated Authentication feature, all the menu options are displayed for some users, though required permissions are not granted in the applied access template. | 200332 |
| Upgraded RapidJson version from version 1.0.2 to 1.1.0 due to functionality issue. | 216245 |
| Upgraded Bootstrap version from version 3.2 to 3.4.1 due to functionality issue. | 216257 |
| In Active Roles, the User object copy operation does not copy Secondary Owners (edsaSecondaryOwners) attribute even when it is set as a mandatory option. | 223979 |
| ARS change workflow should be able to add multiple users to a group with specific criteria on users. | 122372 |
| Import/In-place upgrade from Active Roles 6.9 to 7.x versions provisioned with options to configure Execute On services for Dynamic Groups, Scheduled Tasks and Group Family. | 100716 |

Table 5: Console (MMC Interface) and Collector and Report Packs

| Resolved issue | Issue ID |
|--|----------|
| <p>In Active Roles, when the column size for attributes of the type string is less than the length of the attribute value, Active Roles Collector logs the following error:</p> <p><i>The given value of type String from the data source cannot be converted to type nvarchar of the specified target column. String or binary data</i></p> | 91885 |

| Resolved issue | Issue ID |
|--|----------|
| <i>would be truncated.</i> | |
| <p>In Active Roles Console with Deny permission Access Template applied on the edsaAzureSubscribedSkus attribute, creating mailbox for user from Exchange task fails with an error: <i>Access denied</i>.</p> <p>To enable or disable the fix:</p> <ol style="list-style-type: none"> 1. After installation, open the Registry Editor by navigating to Start Run and typing regedit. 2. Navigate to the registry key HKEY_LOCAL_MACHINE\Software\One Identity\Active Roles\Configuration. 3. Create a new DWORD entry named "SkipGeneratedAttribute" and set the value to '1'. 4. Setting this value to '0' or deleting the key will disable the fix. | 98401 |
| In Active Roles MMC Console and Web interface, when the Country or region is set, white spaces are added to the end of the country name for some countries. | 662476 |
| In Active Roles Console, workflow approval mails are not being sent to the mail enabled group members when the approver is a non mail enabled group. | 745948 |
| In Active Roles Console, setting message delivery restrictions for a dynamic distribution list gives the error "Index was outside the bounds of the array". | 731190 |
| In Active Roles Console, when an approval workflow, with the configuration setting "Split Membership Change Requests" applied, is triggered by adding more than one member to a group, multiple approval mails are sent. | 720242 |
| Currently, in Active Roles Console, an error is encountered when you attempt to use the ChangeParentDN method on a pre-create policy event handler for computer objects. | 745541 |
| In the Active Roles MMC interface, when creating a Group Family and using the Fine-Tune option while configuring the Group Naming Rules, any space that is part of the DISPLAY NAME field is ignored. | 756663 |
| The Active Roles MMC crashes when a user performs an undo deprovision by selecting the Reset the password check box and selects the User must change password at next logon option. | 769465 |
| In Active Roles Collector and Report Packs, the operation logs warning message "[Warning] Cannot find record with: GatheringComputer = [ComputerName], EventLog = ARAdminService, | 764633 |

| Resolved issue | Issue ID |
|--|----------|
| RecordNumber = [REcordNumber], GMT = [TimeValue in GMT]" which leads to empty reports in the report server. | |
| Incorrect error message is displayed for the Office 365 Roles Management policy violation. | 113962 |
| Active Roles service stops after modification operation is executed through a workflow or policy when the SaaS provisioned policy is enabled on the organizational unit. | 167708 |
| The MSONline cmdlets fails when the Office 365 script execution configuration activity in automation workflow is executed. | 167845 |
| In Active Roles MMC, the country names in the Country drop-down menu (co-attribute) for a user object are displayed without a white space. | 201475 |
| Collector fails when group hierarchy is enabled and Active Directory has a group containing curly braces. | 217928 |
| In Active Roles MMC Console, some of the virtual and AD attribute values are not displayed in Advanced Properties for all the object types, except Users. | 220298 |
| Active Roles Management Shell does not update Authorig Exchange attributes using the Delete keyword. | 226066 |
| Multiple built-in scheduled tasks have a blank value as default for edsvaServernameToExecute property. | 91827 |

Table 6: Web Interface, ADSI Provider, and Synchronization Service

| Resolved issue | Issue ID |
|---|----------|
| In Active Roles Web interface, when a new member is added to the Temporal group, the Temporary access dialog displays the member as Already Added instead of New . | 113224 |
| When copying a user in Active Roles, the UPNSuffix value is different in the Active Roles MMC Console and Web interface. | 105487 |
| In Active Roles Web interface, modifying any of the Exchange properties of Room or Equipment mailboxes fails with an error: <i>"Set-CASMailbox , 'ActiveSyncMailboxpolicy' may not be performed on resource mailbox"</i> . To enable or disable the fix: 1. After installation, open the Registry Editor by navigating to Start Run and typing regedit . | 99118 |

| Resolved issue | Issue ID |
|--|----------|
| <p>2. Navigate to the registry key HKEY_LOCAL_MACHINE\Software\One Identity\Active Roles\Configuration.</p> <p>3. Create a new DWORD entry named "BypassActiveSyncMailboxPolicy" and set the value to '1'.</p> <p>4. Setting this value to '0' or deleting the key will disable the fix.</p> | |
| In Active Roles Web interface, some properties with drop-down control do not get displayed as expected in some browsers like Internet Explorer and Firefox. | 91940 |
| <p>In Active Roles Web interface, the Remove button is disabled in the User and Group objects in the following tabs:</p> <ul style="list-style-type: none"> • Send As tab in the User object Exchange property. • Secondary owners tab in the User and Group object General property. | 91644 |
| In a federated or Synchronized Identity environment, deleting a contact from Active Roles fails with an error: <i>Administrative Policy returned an error. Could not find any resources appropriate for the specified culture or the neutral culture. Make sure "ActiveRoles.Service.Azure.Errors.resources" was correctly embedded or linked into assembly "ActiveRoles.Service.Exchange" at compile time, or that all the satellite assemblies required are loadable and fully signed.</i> | 91621 |
| In Active Roles Web interface, the Exchange Online properties form takes a long time to open or a time out error is displayed. | 786286 |
| In Active Roles Web interface, when viewing Exchange Online properties of an Azure user, the details of the previously selected user are displayed. | 787884 |
| In Active Roles Web interface, the Exchange Mailbox properties form has a performance issue, if the delegation properties (sendAs, SendOnbehalf, FullAccess) users have space in their display names. | 789710 |
| In Active Roles Web interface, the Exchange Mailbox properties form for Delivery Options has a performance issue, if the delegation properties (forwarding address) users have space in their display names. | 791191 |
| In Active Roles, adding new owners to an existing list of secondary owners causes previous owners to be deleted when operation is performed through SPML. | 690271 |
| <p>To enable this fix, you must configure the edsvaSecondaryOwners attribute into the SPMLSchema.config files:</p> <ol style="list-style-type: none"> 1. Browse to C:\Program Files\One Identity\Active Roles\7.4\SPML\Web, and open the SPMLSchema.config file. 2. Add the <attributeDefinitionReference name="edd- | |

| Resolved issue | Issue ID |
|---|----------|
| svaSecondaryOwners" required="false" /> into <ObjectClassDefinition name="group">. | |
| In Active Roles Web interface, the Properties button does not work, if MultiValued Attribute DNs contain special characters such as +,"<>. | 779518 |
| In Active Web interface, when the mailbox storage limits is updated and the Prohibit send and receive at (KB) attribute is set to zero, the operation reports success on screen but the changes to the settings are not done. However, the Active Roles MMC displays the updated settings. | 770044 |
| In Active Roles Web interface, when a user with Groups - Add/Remove Members Access template tries to add a member to a group, an Access Denied error message is displayed. | 765208 |
| In Active Roles Web interface, the Exchange properties' sub property page goes blank or does not get re-populated when you click Save . | 715563 |
| In Active Roles Web Interface, the setting for "Find In" for a customization is set to current domain even when we select "Active Directory" as the DN. | 730931 |
| In Active Roles Web Interface, some font colors, such as white on gray, lead to poor readability. NOTE: Perform IIS reset and clear browser cache to view the related changes. | 747079 |
| In Active Roles Web Interface, if the user has read only permissions, the radio buttons have an issue with their readability under certain scenarios. NOTE: Perform IIS reset and clear browser cache to view the related changes. | 747376 |
| In Active Roles Web Interface, User preview displays an error, <i>"Unable to display object properties, when Built-in policy Skype for Business - User Management is set on an OU."</i> | 749821 |
| Currently, Active Roles Web Interface is 508 non compliant. | 733133 |
| Currently, Active Roles does not load fonts locally in environments where access to Google font API is restricted. | 759016 |
| In Active Roles Web interface, when updating the Azure properties of a user, the Usage Location property and License assignment cannot be updated with a single request. | 675416 |
| When creating a group through Active Roles Web interface or PowerShell, Active Roles throws an error in event log with the following message: <i>Administrative Policy returned an error. Object reference not set to an instance of an object.</i> | 711277 |
| In Active Roles Web interface, inactive timeout occurs when a user is | 742153 |

| Resolved issue | Issue ID |
|---|----------|
| actively performing an operation on the objects within the same container such as an organizational unit. | |
| In Active Roles MMC and Web interface, it is not possible to set Mailbox Quota restrictions if the customer uses Exchange 2016. | 766791 |
| In Active Roles Web interface, the navigation bar 'hide' toggle (<) breaks or disappears, when navigating to Customize Customize Navigation Bar and name of the item is changed and is set to long characters. | 755871 |
| After upgrading the Synchronization Service to the current version, the Synchronization service logging is set Disabled. | 91696 |
| A delay in retrieving the objects is observed when the RSTS authentication is configured. | 139573 |
| Active Roles Web Interface exposes a potential vulnerability under very specific circumstances. | 142061 |
| On the Active Roles MMC console, SMS and Phone Calls options are displayed though it is disabled in the Starling 2FA settings. | 167719 |
| In Active Roles 7.4, When an user mailbox is created on the Microsoft Exchange 2016 server, selecting or clearing the selection Automatically update e-mail addresses based on email address policy displays an error. | 184339 |
| In Active Roles 7.4, unable to create an archive mailbox, when the mailbox is created on the Microsoft Exchange 2016 server. | 184342 |
| On the Active Roles Web Interface, Set As Reply button is unavailable after selecting the email addresses in exchange properties. | 169965 |
| On Active Roles Web Interface, the approval operation for Create user or Examine task is not working on Internet Explorer and Firefox browser. | 197562 |
| On Active Roles Web Interface, the Processing status tab in the Approval section is not closed though the operation is completed successfully. | 171737 |
| The Starling tab displays an Unjoined to Starling message after disabling Starling Two Factor Authentication. | 184448 |
| For a non-Azure user, Office 365 roles data was logged in Change History and event log. | 184311 |
| An error is logged at Azure User GetEffectivePolicy in ds log and Event Viewer when Office 365 is disabled and AzureObjectID is not set for the user. | 91752 |
| Learn more about approval workflow link not working as expected. | 187572 |
| The Azure roles are not removed after deprovisioning an Azure user with | 169473 |

| Resolved issue | Issue ID |
|--|----------|
| Azure roles. | |
| On Active Roles Web Interface, the group membership and the Azure Roles assigned to the user is displayed in the Azure Member Of tab. | 172657 |
| SaaS Notification is not displayed on the Web Interface for operations after an approval. | 198034 |
| An error is displayed when you perform a copy operation on an Azure user and subsequently try to create a remote mailbox. | 218394 |
| QuickConnect 5.5 pwdHash synchronization fails with ARS Synchronization Service Capture Agent 7.4. | 169064 |
| SignalR is unable to establish a connection with the server using FQDN and the notifications are not working as expected. | 218229 |
| In Active Roles Web interface, adding members to edsaLocalGroupMembers to manage computer objects is not working as expected. | 227530 |

Known issues

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

Table 7: Configuration Center known issues

| Known Issue | Issue ID |
|---|----------|
| Active Roles supports selection of custom installation path only during a fresh installation. During an in-place upgrade, Active Roles does not support changing the custom installation path. | 763071 |
| When Active Roles is uninstalled some Registry keys do not get removed. | 775437 |
| WORKAROUND | |
| Delete the old Registry keys before installing the latest Active Roles version. | |
| When you specify the SQL Server instance to host the database of the Administration Service, you may encounter the following error on the Connection to Database page in Configuration Center: "Invalid SQL Server computer name. Use the short computer name to specify the SQL Server instance, such as "computername" or "computername\instancename"." | 446759 |
| <ul style="list-style-type: none"> This error occurs in any of the following cases: <ul style="list-style-type: none"> Case 1. A data loss occurred in SQL Server system tables | |

- Case 2. The computer running the SQL Server instance was renamed
- Case 3. You have used an alias to identify the SQL Server instance

Examine the results returned by these queries:

1. If "select @@servername" returns NULL, you have encountered Case 1.
2. If "select @@servername" and "select serverproperty('servername')" return different non-null values, you have encountered Case 2.
3. If "select @@servername" and "select serverproperty('servername')" return the same non-null value, you have encountered Case 3.

WORKAROUND

Use the following instructions, depending on the case you have encountered, and then re-run Configuration Center to configure the Administration Service.

- Case 1: Run the following query against the Master database on the SQL Server instance in question, and then restart the SQL Server instance:

```
declare @sn sysname
select @sn = cast(serverproperty('servername') as sysname)
exec sp_addserver @sn, 'local'
```
- Case 2: Run the following two queries in succession against the Master database on the SQL Server instance in question, and then restart the SQL Server instance:

```
exec sp_dropserver @@servername, 'droplogins'

declare @sn sysname
select @sn = cast(serverproperty('servername') as sysname)
exec sp_addserver @sn, 'local'
```
- Case 3: Use the following syntax to identify the SQL Server instance when installing the Administration Service:
 "computername" - for the default instance
 "computername\instancename" - for a named instance
 In this syntax: "computername" stands for the short name of the computer running SQL Server; "instancename" stands for the name of the SQL Server instance.

Configuration Center is unable to configure the Administration Service if the name supplied for the Active Roles database on the Connection to Database page contains a single apostrophe ('). A symptom of the issue is the following error: "Incorrect syntax near '-'."

446843

WORKAROUND

Change the database name so that it does not contain a single apostrophe (').

When you configure the Administration Service on a domain controller, you may 37391

Known Issue

Issue ID

encounter the following error: "Service 'Active Roles Administration Service' (aradminsvc) failed to start. Verify that you have sufficient privileges to start system services."

WORKAROUND

Use the Services tool to manage the service named Active Roles Administration Service: Specify the logon name and password of the account that you want the service to log on as, and then start the service.

If an 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

While installing Active Roles on a new 2012 R2 Azure VM, intermittently an error is displayed asking to replace PkgMgr.exe with DISM.exe. 127497

In **Workflow activities and policy actions**, deprovision results has no information about O365 Licenses retention policy. 153665

On the **Starling Connect Connection Settings** link, clicking on **Next** shows progress, however, the functionality is not affected. 126892

Automation workflow with Office 365 script fails, if multiple workflows share the same script and it is scheduled to execute at the same time. 200328

WORKAROUND:

One Identity recommends to schedule the workflows with different scripts or at a different time.

edsvaAzureOffice365Enabled attribute is not present on the Container object. 90958

By design, it is not recommended to modify the default settings on the users and computers containers. One Identity recommends to create new OUs and move the user and computer objects from their default containers to the new OUs.

WORKAROUND:

In the event that there are non-default Container objects in the environment, the following workaround can be completed to allow Azure object creation within them. Do not perform this on the default Active Directory Containers such as Users, BuiltIn, Computers, and so on.

1. On the Active Roles console with Active Roles Admin credentials, expand **Configuration | Server Configuration | Virtual Attributes**.
2. Find the **EDSVA-Azure-Office365-Enabled** virtual attribute and double-click on it
3. On the **Classes** tab, uncheck **Container** and then click Apply.

| Known Issue | Issue ID |
|--|----------|
| <ol style="list-style-type: none"> Click OK. Click Reconnect on the Active Roles console and perform an IISRESET on the Active Roles Web Interface so that the schema change is detected. The edsvaAzureOffice365Enabled virtual attribute is present on the Container object. Set the value to TRUE and link the required Azure Policy and it will be possible to Azure-enable objects in that container. | |

Table 8: Administration Service known issues

| Known Issue | Issue ID |
|--|----------|
| <p>The Administration Service does not support querying for more than 200 different Custom Stored Virtual Attributes (CSVAs) within a single search request. When you query for more than 200 different CSVAs within a single search request so that the request is configured to retrieve the values of those attributes, you may experience performance degradation in the Administration Service and your query may return incorrect results.</p> <p>WORKAROUND</p> <p>If you need to query for a large number of CSVAs (so as to have your search request retrieve the values of those attributes), perform multiple search requests with a smaller number of attributes involved in each request. For best performance, a single search request should not query for more than 32 different CSVAs.</p> | 11990 |
| <p>The Administration Service incorrectly evaluates the delegated rights of the user account in the following scenario:</p> <ul style="list-style-type: none"> An organizational unit (OU) is configured so that a given user account is set as the manager of the OU (the "Managed By" property of the OU is assigned the DN of the user account). The Active Roles security settings on the OU are configured so that the "Primary Owner (Managed By)" built-in account has full control of the OU. <p>In this scenario, Active Roles does not permit the user account to modify objects in the OU. The expected behavior is as follows: since the user account is set as the manager of the OU, and full control of the OU is delegated to the "Primary Owner (Managed By)" account, the user account has full control of the OU and all objects held in the OU. The same issue occurs in the situation where a group is set as the manager.</p> <p>WORKAROUND</p> <p>Configure the Active Roles security settings on the OU so that the appropriate</p> | 18378 |

| Known Issue | Issue ID |
|--|----------|
| rights (for example, full control) are delegated to the user account (or group) itself rather than to the "Primary Owner (Managed By)" account. | |
| <p>The default Exchange mailbox database in which the Administration Service creates user mailboxes may differ from the mailbox database that Microsoft's native tools select for the mailbox creation operation by default.</p> <p>WORKAROUND</p> <p>When you use Active Roles to create a new mailbox-enabled user or create a mailbox for an existing user, verify the mailbox database selection, and choose the appropriate database if necessary. Another option is to configure and apply an Exchange Mailbox AutoProvisioning policy that would automatically choose the appropriate mailbox database.</p> <p>One more option is to configure and apply a script-based policy that would use the onGetEffectivePolicy handler to set the appropriate default value on the homeMDB attribute, which specifies the mailbox store:</p> <pre>Sub onGetEffectivePolicy(Request) Request.SetEffectivePolicyInfo "homeMDB", EDS_EPI_UI_GENERATED_VALUE, array(<desired value>) End Sub</pre> | 18419 |
| <p>When you use the "Handle changes from DirSync control" option in a script-based policy, you may encounter the following issue: The policy does not execute the onPostDelete handler. This issue occurs if the Policy Object containing the policy in question is applied (linked) to an Organizational Unit.</p> <p>WORKAROUND</p> <p>Apply the Policy Object to a domain rather than to an Organizational Unit.</p> | 22786 |
| <p>Creation, modification, or deletion of a custom display specifier has no effect on a given Administration Service until that Service is restarted. A symptom is that the directory management section of the Active Roles console does not reflect the changes to custom display specifiers until you restart the Administration Service the console is connected to.</p> <p>WORKAROUND</p> <p>Restart each Administration Service after you have made changes to custom display specifiers.</p> | 23848 |
| <p>When you export policy check results or change history results to a file in HTML format, and then send the file as an e-mail attachment, you may encounter the following issue: Opening the attachment in Outlook displays a corrupted HTML page, with extra spaces inserted between page sections.</p> <p>WORKAROUND</p> <p>Archive the file to which you have exported the results and then send the archive file as an attachment instead of sending the original file.</p> | 24227 |

| Known Issue | Issue ID |
|---|----------|
| <p>When configuring a Managed Unit to use a query-based membership rule, you may encounter the following issue: A membership rule based on a custom LDAP query may not work as expected if the query includes a right bracket (]). For example, the following query causes an error: (&(objectcategory=group)(accountNameHistory=*[DG]*)).</p> <p>WORKAROUND</p> <p>If possible, modify your query to eliminate the right brackets. In the above example, the query can be modified as follows, without loss of functionality: (&(objectcategory=group)(accountNameHistory=*[DG*]))</p> | 24229 |
| <p>The Administration Service may not provide its client applications with information about an Active Roles replication failure as expected. As a result, the Active Roles console or Management Pack for SCOM may not display an appropriate alert or status message on the Active Roles database servers that are experiencing replication problems.</p> <p>WORKAROUND</p> <p>Use the instructions given in the document "Active Roles Replication: Best Practices and Troubleshooting" to check the health of, and troubleshoot problems (if any) with, Active Roles replication.</p> | 24487 |
| <p>The policy compliance check in the Administration Service may inappropriately handle a policy configuration where values of certain object properties in the directory are dependent on other property values that are to be generated by a policy. Thus, when a "Property Generation and Validation" policy is configured to assign a certain property value based on a user logon name generated by a "User Logon Name Generation" policy, you encounter a policy violation error when creating a user account using the Active Roles console unless you have clicked the Generate button to have the Administration Service generate a user logon name.</p> <p>WORKAROUND</p> <p>If you have encountered a policy violation error when using a page that includes the Generate button, click that button to have the Administration Service generate a property value.</p> | 25236 |
| <p>When you apply an Access Template to a Managed Unit, with the option to enable synchronization of the resulting permission entries to Active Directory, you encounter the following issue: The resulting permission entries are inherited by the directory objects held in the Managed Unit, but not synchronized to Active Directory. The same problem occurs when you apply an Access Template to a Managed Unit container.</p> <p>Thus, you can check "Advanced Details Pane" on the View menu in the console, select a directory object held in the Managed Unit, and examine the permission entries on the "Native Security" tab in the lower sub-pane of the details pane, to</p> | 24486 |

see that the permission entries resulting from the Access Template you applied to the Managed Unit are marked as Absent, and displayed in red.

WORKAROUND

By default, for performance reasons, Active Roles does not sync permission settings to native Active Directory security that are configured by applying Access Templates to Managed Units or Managed Unit containers. If you need to sync permission settings from Active Roles security to native Active Directory security, we recommend that you apply Access Templates to Organizational Units. However, Active Roles provides the option to sync permission settings from the Managed Unit level. This option is enabled if the object "CN=Enable Sync to Native Security from Managed Unit,CN=ActiveRoles Server,CN=Services,CN=Application Configuration,CN=Configuration" exists and has the "edsaExtensionAttribute1" attribute set to TRUE. Otherwise, this option is not enabled. To enable this option, use the Active Roles console in Raw view mode as follows:

- In the "Configuration/Application Configuration/Services" container, create an object of the "EDS-Application-Settings-Container" object class with the object name "ActiveRoles Server".
- You can do this by using the "All Tasks | Advanced Create" command. In the "Configuration/Application Configuration/Services/ActiveRoles Server" container, create an object of the "EDS-Application-Setting" object class with the object name "Enable Sync to Native Security from Managed Unit".
- You can do this by using the "All Tasks | Advanced Create" command. On the "Enable Sync to Native Security from Managed Unit" object, set the "edsaExtensionAttribute1" attribute to TRUE.
- You can view or change the value of that attribute by using the "All Tasks | Advanced Properties" command. You can disable this option, if needed, by deleting the "Enable Sync to Native Security from Managed Unit" object, or by clearing the "edsaExtensionAttribute1" attribute of that object.

There is no option to configure an Active Roles policy for generating a user principal name (UPN) so that the UPN Suffix part of the name automatically changes if the generated name is in use by another user account. Normally, the UPN Prefix part of the name (the value of the edsUPNPrefix attribute) is the same as the pre-Windows 2000 user logon name (the value of the sAMAccountName attribute). This ensures the uniqueness of the user principal name regardless of the UPN Suffix setting.

25620

WORKAROUND

After the user account has been created with a valid (unique) user principal name, change the UPN Suffix and UPN Prefix parts of the name as needed using

| Known Issue | Issue ID |
|--|----------|
| the Active Roles console or Web Interface. | |
| In some limited scenarios, you may encounter corruption of attribute names (wrong characters) on the page that displays a report produced by the "Change History" command. For example, this problem may occur with the Change History report on a user account that was deprovisioned via the Active Roles Web Interface using the Web browser with a non-English locale. | 25728 |
| Incorrect behavior of a User Logon Name Generation policy that is configured to disallow certain (non-acceptable) characters in the user logon name: In the situation where the policy allows the generated name to be modified manually (for example, if the policy fails to generate a unique name), adding non-acceptable characters to the name in the New Object - User wizard causes a policy violation and then the field for entering the name gets unavailable so you cannot correct your input. | 25700 |
| WORKAROUND In the wizard, re-enter the value of any property based on which the user logon name is generated. This will enable the field for entering the user logon name so that you can remove the unacceptable characters from the name. | |
| With an Active Roles policy configured so that the value of a certain (dependent) property is based on another (master) property, the Administration Service may not force the Web Interface to change the dependent property in accordance with the changes that are made to master property. For example, with a policy that makes the user alias the same as the user logon name, changes to the user logon name may not cause the user alias to change accordingly. The issue may occur if the entries for the master property and the dependent property are located on different pages in the Web Interface. | 25902 |
| WORKAROUND To prevent this issue, modify properties of user accounts in the Active Roles console. | |
| Incorrect behavior of the console tree root page in the Active Roles console: Clicking Refresh at the top of the page may cause the following error: "Validation failed on XML." The issue may occur when you are repeatedly clicking Refresh while the Administration Service is busy loading information from a newly registered managed domain or AD LDS instance. | 26017 |
| WORKAROUND Click OK in the error message box and wait until the Administration Service has finished loading information from the managed domains and AD LDS instances. Then, click Refresh. | |
| While the Administration Service is busy loading information from the managed domains and AD LDS instances (for example, upon the startup to the | 26043 |

Known Issue

Issue ID

Administration Service), the Active Roles console may fail to connect to the Administration Service, returning the following error messages:

Message 4301: Failed to connect to Administration Service on '<servername>'

Message 1003: hr = 0x80131600

Interface: Unknown

WORKAROUND

Click Close in the error message box and wait until the Administration Service has finished loading information from the managed domains and AD LDS instances. Then, attempt to connect to the Administration Service.

The Administration Service may not send to the console the information that is required to populate the list of Administration Service instances in the "Management History Databases and Replication" section on the console tree root page in the details pane. As a result, the page does not display a list of the Administration Service instances that use a given Management History database.

26218

WORKAROUND

To view a list of the Administration Service instances that use a certain Management History database, go to the "Configuration/Server Configuration/Management History Databases" container in the console tree, open the Properties dialog box for the database you want to examine, and view the list on the "Administration Services" tab.

When processing a query with an LDAP filter that specifies wildcard-based conditions on an Active Roles Custom Stored Virtual Attribute (CSVA) of the Integer type, the Administration Service may report the following error: "An unsupported conversion was attempted." This error may occur if the filter conditions include an asterisk wildcard character coupled with other characters, such as (edsvadeptcode=4*).

35396

WORKAROUND

Do not use filter conditions that include a combination of an asterisk with other characters. For example, you could use (edsvadeptcode>=4000) rather than (edsvadeptcode=4*).

When performing the Deprovision operation on a user object, the Administration Service may return the following error: "Failed to retrieve attributes of the object '<objectDN>'. XML document must have a top level element." The error occurs if the Administration Service performs the Deprovision operations concurrently with the "Change Tracking Cleanup" scheduled task.

37103

WORKAROUND

Click OK in the error message boxes that appear on the screen until you receive a message stating that the deprovision operation is completed. Then, open the

report on the operation results by using the Deprovisioning Results command in the Active Roles console.

The Administration Service may incorrectly process a Property Generation and Validation policy rule that includes a text string following the value of an attribute, such as "%<description> This user account was deprovisioned {@date(M/d/yyyy)}". If the attribute is empty (has no value set), the text string may be missing from the generated output. In this example, the output would not contain the text "This user account was deprovisioned".

WORKAROUND

Create a custom stored virtual attribute that holds the text string you want and modify the rule, replacing the text with that attribute. Thus, in the preceding example, you could create an attribute named edsVaDeprovisionTextConst on the domain object, set the attribute to the text string in question, and then apply the following rule: "%<description>%<domain.edsVaDeprovisionTextConst>{@date(M/d/yyyy)}"

Active Roles may fail to re-evaluate the membership of a Dynamic Group in a timely fashion after the membership rules of the Dynamic Group are modified. This issue can be caused by unavailability of the Administration Service that was designated to evaluate and apply the membership rule changes on the Dynamic Group.

WORKAROUND

On the Membership Rules tab in the Properties dialog box for the Dynamic Group in the Active Roles console, select the appropriate Administration Service from the "Service to evaluate and apply rule changes" list and click Apply. Alternatively, you may wait for Active Roles to correct the situation. For this purpose, Active Roles uses the "Dynamic Group Checker" scheduled task, located in the "Configuration/Server Configuration/Scheduled Tasks/Builtin/" container. The "DG update latency threshold" parameter on that task specifies the maximum period of time (5 days by default) after which the re-evaluation of the Dynamic Group membership is forced and the appropriate Administration Service is automatically designated to evaluate the membership.

The Administration Service may fail to execute a policy based on a script that calls the EventLog.ReportEvent method, returning the "Object doesn't support the action" error.

WORKAROUND

In Active Roles policy scripts, use the Request.ReportEvent method rather than EventLog.ReportEvent to record events to the event log, if necessary.

When managing user accounts in the Windows Server 2008 Active Directory Domain Services, the Administration Service fails to properly consider the password policy settings that are configured by using Password Settings objects

(PSOs). As a result, Active Roles may generate user passwords that do not meet the password policy requirements that are in effect (for example, it may generate a password of an inappropriate length). Only the password policy settings that originate from Group Policy objects are considered by the password generation algorithm.

WORKAROUND

Ensure that the password policy requirements imposed via Group Policy are the same as those specified by using Password Settings objects.

The Management History records that were received through Active Roles replication or imported using the Management History Migration Wizard may be unavailable to the Administration Service for a significant time period. The cause of this issue is as follows. In order to support Change History related queries and Approval Workflow functionality, Active Roles keeps certain non-replicated data in the Management History database. When new Management History records are added to the database from an external source (for example, via replication or data migration), the new records cannot be accessed until after the non-replicated data is properly updated. The time it takes to update that data depends upon various factors, including:

- The total number of records in the Management History database
- The number of records that were received from an external source
- CPU and disk performance of the SQL Server computer that hosts the Management History database

Depending on these factors, the average time to update a single Management History record may range from 0.1 seconds to 1 second.

WORKAROUND

Reduce the number of records in the Management History database in order to reduce the time it takes to complete the process of updating the non-replicated Management History data. For example, when importing Management History data by using the Management History Migration Wizard, you may choose not to transfer the records that are older than a certain date.

Incorrect behavior of the Approval Workflow function in the following scenario: 38246

While the operations are waiting for approval, the Active Roles environment is re-configured so that some instances of the Administration Service use a separate database to store the management history data, possibly synchronizing that data within a separate replication group of management history databases.

After the environment is re-configured, Active Roles fails to properly process the operations that were requested within the initial configuration. For example, when such an operation (say, creation of a user account) receives the Approve

action, the operation is marked as approved but it is not actually performed (the user account is not created). In addition, when approved on one of the Administration Service instances, the operation shows up as waiting for approval on another instance of the Administration Service.

WORKAROUND

Before re-configuring the Active Roles environment, ensure that no operations are waiting for approval. If any operations were requested but not completed before you re-configured the environment, have those operations re-initiated in the new environment. For example, if creation of a user account was started and was not approved or rejected in the initial environment, start creation of that user account again in the new environment.

- Initially, multiple instances of the Administration Service are configured to synchronize the configuration data and the management history data using Active Roles replication, with each instance storing all data in the configuration database.
- Within the initial configuration, certain operations (for example, creation of user accounts) that require approval are requested but not completed (neither approved nor rejected).

In an Active Roles replication environment where multiple Administration Service instances use the same database, execution of the 'Change Tracking Cleanup' task may fail with the following last run message: "Transaction (Process ID <number>) was deadlocked on lock resources with another process and has been chosen as deadlock victim. Rerun the transaction."

39140

WORKAROUND

Run the task again: In the Active Roles console tree, expand Configuration | Server Configuration | Scheduled Tasks | Builtin; then, in the details pane, right-click Change Tracking Cleanup and select All Tasks | Execute. When running the task, ensure that no data migration is being performed by the Management History Migration Wizard.

In certain rare conditions, the Administration Service may fail to properly configure a Subscriber database server: The New Replication Partner wizard in the Active Roles console reports that the operation is completed successfully, but the Subscriber database server configured by the wizard remains in standalone state and the Publisher database server does not recognize the newly configured Subscriber (the Subscriber's status on the Publisher is indicated as "unknown"). The Active Roles Admin Service event log contains a "ReplPartnerPolicy failed" error event in this case. Data synchronization between the Publisher and the newly configured Subscriber does not occur.

38646

WORKAROUND

Use the instructions that follow to delete the failed Subscriber record from the

Publisher's database, and then use the New Replication Partner wizard in the Active Roles console to add the Subscriber again.

To delete the failed Subscriber record, run the following SQL query against the Active Roles database on the Publisher database server (before running the query, replace the <datasasename> and <servername> placeholders with the name of the failed Subscriber database and the name of the SQL Server instance that hosts the failed Subscriber database, respectively):

```
delete from tblReplication where edsaSQLAlias = N'<servername>' and
edsaDatabaseName = N'<datasasename>'
```

Consider the following scenario. In your Active Roles environment, a Group Membership Removal policy is in effect that removes deprovisioned user accounts from groups. You use the Temporal Group Memberships feature of Active Roles to schedule addition of user accounts to groups. In this scenario, when you deprovision a user account that is scheduled to be added to a certain group, the Administration Service may not cancel that scheduled operation as expected. As a result, the deprovisioned account eventually becomes a member of that group, which violates the Group Membership Removal policy.

51063

WORKAROUND

If you are affected by this issue, please contact One Identity Support to obtain a fix for this version of the Administration Service.

Consider the following scenario. You have the Undo Deprovisioning policy configured so that it allows password reset on restored user accounts (this is the default policy setting). You delegate the right to restore deprovisioned accounts by applying the following Access Templates:

All Objects - Read All Properties

53491

Users - Perform Undo Deprovision Tasks

In this scenario, the delegated administrator receives the following error message when using the Undo Deprovisioning command: "Administrative Policy returned an error. Attempted to perform an unauthorized operation."

WORKAROUND

Create a new Access Template that contains the "Write properties" permission for these attributes on the User object class:

- edsaPassword
- userAccountControl
- edsvaUserMustChangePasswordAtNextLogon
- edsaUserCannotChangePassword
- edsaPasswordNeverExpires

Apply that Access Template in addition to those listed above, so as to give the

| Known Issue | Issue ID |
|--|----------|
| delegated administrator the rights to reset password and manage password options. | |
| <p>An Active Roles workflow that uses conditional branching based on the If-Else activity may cause duplicate occurrences of the EVENT_ACTIVITY_ALERT (ID=2711) event in the Active Roles Admin Service event log: "This activity is skipped because branch condition is not satisfied on any of its branches."</p> <p>WORKAROUND</p> <p>Disregard the duplicate occurrences of Event 2711 in the Active Roles Admin Service event log.</p> | 100584 |
| <p>Cyclic references within custom library scripts may cause the Administration Service to stop unexpectedly. Cyclic references occur when two different library scripts reference each other by calling the ScriptLib.Load() function. A typical example of a cyclic reference is as follows. Consider a library script module named LIB1 containing a script that loads a script module named LIB2 (Set LIB2 = ScriptLib.Load("LIB2")) whereas the script that is held in the module LIB2 loads the module LIB1 (Set LIB1 = ScriptLib.Load("LIB1")). In this case, saving changes to the module LIB1 or LIB2 may cause the Administration Service to stop unexpectedly.</p> <p>WORKAROUND</p> <p>Avoid cyclic references in Active Roles script module. In a situation where cyclic references may occur, consider copying the necessary functions from one script module to another instead of loading the module that contains those functions.</p> | 102049 |
| <p>When you deprovision and then un-deprovision a group, the temporary or pending members of that group may not be restored as expected. This issue may occur, for example, when you schedule a member to be added to a particular group at a certain time in the future, deprovision and then un-deprovision that group. As a result, the Administration Service loses the schedule setting for that member, so the member will not be added to the group as expected.</p> <p>WORKAROUND</p> <p>After you have un-deprovisioned a group, review the "Members" list of that group and, if necessary, add and configure the temporary or pending members by hand.</p> | 104474 |
| <p>When performing the Demote operation on the Publisher role holder, the Administration Service may cause a deadlock condition on SQL Server. In this case, the Administration Service returns an error message similar to the following: "Your transaction (process ID {#number}) was deadlocked on {lock communication buffer thread} resources with another process and has been chosen as the deadlock victim. Rerun your transaction." This issue is most likely to occur when the database server to demote is busy with other requests from</p> | 105507 |

the Administration Service, such as retrieving Active Roles configuration data requested through a custom script.

WORKAROUND

Ensure that the Administration Service is not performing any resource-intensive operations against the database, such as running scheduled tasks or custom scripts, and then try the Demote operation again.

When performing a request to un-deprovision a user account, the Administration Service may not restore the membership of the user account in a group that resides in a domain other than the domain of the user account. A symptom of the issue is the following error message: "The specified group type is invalid." The issue occurs if the domain of the group has the functional level of Windows Server 2003 and a Global Catalog server is unavailable in that domain.

WORKAROUND

Ensure that a Global Catalog server is up and running in the domain that holds the group.

If the domain has more than one domain controller, configure Active Roles to use a Global Catalog server for the operation requests initiated by the internal logic of the Administration Service (DirSync server). You can choose the appropriate DirSync server for a domain by using the Active Roles console:

1. Open the Properties dialog box for the domain registration object held in the container Configuration/Server Configuration/Managed Domains, and go to the DirSync Servers tab.
2. On the DirSync Servers tab, select the Administration Service in the list, and then click Change.
3. In the DirSync Server Selection dialog box, choose the option Only specified domain controller, click Browse, and select any domain controller that holds the role of a Global Catalog server.
4. Click OK to return to the Properties dialog box.
5. In case of multiple Administration Service instances, repeat Steps 2-4 for each instance.
6. Click OK to close the Properties dialog box.

Prior to performing the Undeprovision command, ensure that Active Roles uses a Global Catalog server for the operation requests initiated by the client application (Operational DC). You can choose the appropriate Operational DC by using the Change Operational DC command in the Active Roles console or Web Interface. Thus, in the Active Roles console, right-click the domain under the Active Directory node, select All Tasks | Change Operational DC, and then verify that the current domain controller is a Global Catalog server.

In a function within a PowerShell based policy script, the use of the "return" operator applied to a data array may cause the policy script not to perform as expected or may result in an error condition at run time. The root cause of the issue is that the service objects such as \$Request or \$DirObj may incorrectly

handle the input data conveyed by the "return" command. For example, the following policy script does not update the edsvaKeywords attribute as expected:

```
function onPostGet($Request)
{
    $var = ff
    $Request.Put("edsvaKeywords", $var)
}
function ff
{
    return @"("111", "222")
}
```

WORKAROUND

Avoid the use of the "return" operator in functions within Windows PowerShell based policy scripts when passing data to service objects. Thus, in the preceding example, you should remove the "return" operator from the function ff:

```
function ff
{
    @"("111", "222")
}
```

Active Roles may incorrectly process a scheduled task with the option "Execute on: All servers." The issue occurs in an environment where Active Roles replication is used to synchronize configuration of multiple Administration Service instances. Although the task option suggests that the task is to be run on each instance of the Administration Service, the task actually runs on only one instance.

120824

WORKAROUND

Use the Active Roles console to connect to each Administration Service instance and run the task on the connected instance by hand: Right-click the task and then select "All Tasks | Execute."

You may encounter the following issue in an environment where Active Roles replication is used to synchronize configuration of multiple Administration Service instances: If SQL Server Agent is not running on the Publisher SQL Server (which is a prerequisite for Active Roles replication to function), no diagnostic information is provided by Active Roles as to the replication problem caused by that condition. The only indication of the problem is the replication status of "Unknown" on the database objects in the "Configuration/Server Configuration/Configuration Databases" container in the Active Roles console.

120833

WORKAROUND

Known Issue**Issue ID**

If you encounter the replication status of "Unknown" on the database objects in the "Configuration/Server Configuration/Configuration Databases" container in the Active Roles console, verify that the SQL Server Agent service is up and running on SQL Server that hosts the Active Roles Publisher database.

The Administration Service may not stop a running scheduled task as expected: The Terminate command on the task in the Active Roles console either does not stop the task despite an information message stating that the operation was completed successfully, or fails with an error message stating that the specified method is not supported. The issue occurs with any scheduled task that uses a Windows PowerShell based script. 115880

WORKAROUND

To terminate the task, restart the Administration Service. Alternatively, wait for the task to finish running. Check the Active Roles Admin Service event log for an event indicating that the task has been completed.

The operation of adding an object to a group may cause a duplicate record in the Change History report for the group. The issue occurs when a given object is added to the group and then the same object is added to that group again (this could be accomplished, for example, by using two instances of the Active Roles console). In this scenario, the addition of the object to the group is recorded twice in the Change History report. A similar issue occurs with the operation of removing a member from a group. 122552

WORKAROUND

Disregard the duplicate Change History record regarding the addition or removal of an object from the group.

E-mail based approval cannot be used on Symbian OS based devices. With a Symbian OS e-mail client, the Approve/Reject links in Active Roles notification messages may not function as designed. 130043

WORKAROUND

Perform approval tasks using the Web Interface, or use a different e-mail client to work with Active Roles notification messages.

When populating the list of permissions on the "Native Security" tab in the advanced details pane in the Active Roles console, the Administration Service may incorrectly identify the domain of a built-in account, such as "Print Operators" or "Account Operators." As a result, in the list on the "Native Security" tab, the Name field may display an incorrect domain name for a built-in account (for example, it may display "PRODAM\Account Operators" instead of "PRODEU\Account Operators"). 137451

WORKAROUND

To view the correct names, use the Permissions dialog box which you can access

from the "Native Security" tab: Right-click a list entry on the "Native Security" tab and then click "Edit Native Security." In the Permissions dialog box that appears, the names are listed under "Group or user names."

Active Roles approval workflow may not function as expected in a scenario that needs conditional approval for adding members to a group and the condition of the approval is based on certain properties of objects being added to the group. The issue occurs with a workflow that starts upon a request to add objects to a group and analyzes certain object properties to determine if single-level approval (by a single person) or multi-level approval (by several persons in sequence) is required for the request to be performed.

The issue manifests as follows. Suppose Active Roles has been requested to add a batch of objects to a particular group, with the properties of some objects in the batch configured so that single-level approval will suffice, whereas the properties of others dictate multi-level approval. When processing such a request, Active Roles adds the entire batch of the objects to the group once it receives the approval to add any object found in the batch. As a result of this behavior Active Roles may add an object to the group despite the fact that all the necessary approvals are not received. Thus, upon receipt of the approval for an object that only needs single-level approval, Active Roles will add all objects to the group, including those for which multi-level approval is required.

WORKAROUND

To work around this issue, you should enable a policy that forces Active Roles to split requests for adding or removing objects from groups as needed in the case of approval workflow. For each object whose addition or removal from a given group requires approval, the policy creates a separate operation request, thereby ensuring the object is properly handled by approval workflow. If this policy is not enabled, a request to add multiple objects to a particular group (or remove them from that group) is performed as a single operation, which causes the operation to be completed for all objects once the request is approved, although additional approvals may be required for some of the objects involved in the operation.

The policy is enabled if the object "CN=Split Group Membership Change Requests,CN=ActiveRoles Server,CN=Services,CN=Application Configuration,CN=Configuration" exists and has the "edsaExtensionAttribute1" attribute set. Otherwise, this policy is not enabled. To enable the policy, use the Active Roles Server console in Raw view mode as follows:

1. In the "Configuration/Application Configuration/Services" container, create an object of the "EDS-Application-Settings-Container" object class with the object name of "ActiveRoles Server". You can do this by using the "All Tasks | Advanced Create" command.
2. In the "Configuration/Application Configuration/Services/ActiveRoles Server" container, create an object of the "EDS-Application-Setting" object class with the object name of "Split Group Membership Change Requests". You can do this

by using the "All Tasks | Advanced Create" command.

3. On the "Split Group Membership Change Requests" object, set the "edsaExtensionAttribute1" attribute to any non-null value. You can view or change the "edsaExtensionAttribute1" attribute value by using the "All Tasks | Advanced Properties" command.

You can disable this policy, if needed, by clearing the "edsaExtensionAttribute1" attribute or by deleting the "Split Group Membership Change Requests" object altogether.

When you uninstall an instance of the Administration Service, Active Roles may not remove the object representing that instance from the "Administration Services" container in the Active Roles console. The record of the uninstalled Administration Service is also present on the "Administration Services" tab in the "Properties" dialog box for the database object in the "Configuration Databases" and "Management History Databases" containers, with the "State" field indicating "Status unknown." The issue occurs if the uninstalled Administration Service was configured to use the database that is currently used by the Administration Service to which the console is connected.

197804

WORKAROUND

You may safely disregard the objects representing uninstalled Administration Service instances in the console. If you are sure that the given object in the "Administration Services" container applies to an uninstalled Administration Service, you might delete that object (right-click the object and click "Delete").

When you configure the Administration Service, you encounter the "Insufficient rights to access the Active Roles database. Ensure that your login has the default schema of "dbo" in the Active Roles database.

197815

SQL Server: <servername>

Database: <databasename>

Authentication mode: Windows Authentication

Login: DOMAIN\sAMAccountName" error if all of the following conditions are true:

- You are configuring the Administration Service with the option to use an existing database or import data from an existing database.
- Windows (integrated) authentication is used to connect to SQL Server.
- The Windows user account under which you run Configuration Center does not have a login on SQL Server.

The issue occurs even though the Windows user account in question is a member of a Windows domain group that has a login on SQL Server with sufficient rights, including membership in the "db_owner" database role.

WORKAROUND

If you use Windows (integrated) authentication to connect to SQL Server when installing the Administration Service, ensure that the Windows user account under which you run Configuration Center has a login on SQL Server mapped to

Known Issue

Issue ID

a database user with sufficient permissions to perform Administration Service installation tasks. For a list of permissions, see "SQL Server permission/Configuration permissions" in the Active Roles Quick Start Guide.

When you start the Administration Service, you encounter the "Account must have the default schema of dbo in the database" error if all of the following conditions are true:

- The Administration Service is configured to use Windows (integrated) authentication when connecting to SQL Server.
- The Windows user account under which the Administration Service is configured to run does not have a login on SQL Server.

The issue occurs even though the Windows user account in question is a member of a Windows domain group that has a login on SQL Server with sufficient rights, including membership in the "db_owner" database role.

197831

WORKAROUND

If you have the Administration Service configured to use Windows (integrated) authentication when connecting to SQL Server, ensure that the Windows user account under which the Administration Service is running has a login on SQL Server mapped to a database user with sufficient permissions in the Active Roles database. For a list of permissions, see "SQL Server permissions/Operation permissions" in the Active Roles Quick Start Guide.

Consider the following scenario. You create a mail-enabled Group Family in Active Roles, and select the "Hide group from the Exchange address lists" option on the "Exchange-related Settings" page in the Group Family configuration wizard. Then, you run the Group Family. In this scenario, the groups created by the Group Family do not have the "Hide group from the Exchange address lists" option selected by default.

203199

WORKAROUND

To ensure that the groups created by the Group Family have the "Hide group from the Exchange address lists" option selected, create a Policy Object containing a Script Execution policy based on the script that follows, and apply that Policy Object to the containers in which the Group Family is expected to create groups. Note that you should apply this policy before running the Group Family. The groups created before this policy is applied won't have the "Hide group from the Exchange address lists" option selected by default.

```
function onPostCreate($Request)
{
    if ($Request.Class -ne "group"){return}
    if ($request.Get("edsvaCGIsControlledGroup") -ne $true){return}
    if ($request.Get("msExchHideFromAddressLists") -ne $true){return}
    $DirObj.Put("msExchHideFromAddressLists", $true)
    $DirObj.SetInfo()
```

}

If multiple Administration Service instances share a single database, then updating the Active Roles schema on one of those Administration Service instances (for example, via installation of a patch) may have no effect on the other instances of the Administration Service. As a result, the consolidated Active Roles schema may not be updated as expected. Thus, it may occur that the attributes added to the Active Roles schema during update are missing from the consolidated schema, and are therefore not recognized by Active Roles clients.

204816

WORKAROUND

When applying a patch that updates the Active Roles schema, install the patch on all the instances of the Administration Service that use the same database. Then, restart one of the Administration Services you have updated. For instructions, see "Start, stop or restart the Administration Service" in the Active Roles Administration Guide.

Consider the following scenario. You choose the option that causes the Administration Service to access a particular domain using an override account. This is the "Access the domain using | The Windows account information specified below" option in the Properties dialog box for the domain object in the "Managed Domains" container in the Active Roles console. Then, you change the configuration by selecting the option for the Administration Service to access that domain using the service account. This is the "Access the domain using | The service account information the Administration Service uses to log on" option in the Properties dialog box for the domain object in the "Managed Domains" container. In this scenario, your change to the configuration may have no effect until you restart the Administration Service.

218147

WORKAROUND

After you have changed the Active Roles configuration so that the Administration Service must no longer use the override account to access the domain, restart the Administration Service for your changes to take effect. For instructions, see "Start, stop or restart the Administration Service" in the Active Roles Administration Guide.

When you use a multi-value workflow parameter to pass multiple values to a workflow activity, you encounter the following issue: The workflow activity receives one of the parameter values; the remaining values are disregarded. The issue occurs with parameters of DN, GUID or SID syntax when you use the "Object identified by workflow parameter" option to pass parameter values to a workflow activity.

226503

WORKAROUND

Use a script function to retrieve the parameter values and pass the array of

values to the workflow activity (in this script function, dnParameter stands for the name of the workflow parameter):

```
function GetParameterValues()
{
    $Workflow.ParameterEx("dnParameter")
}
```

For example, you can use this script function to assign the array of parameter values to a multi-value attribute, such as Secondary Owners (edsvaSecondaryOwners), within an "Update" activity:

1. Create a Script Module containing the "GetParameterValues()" function.
2. Open the "Target properties" page in the "Update" Activity Properties dialog box.
3. Click "Add property", and then click "Secondary Owners".
4. In the "Value" column, click "Define", and then click "Object identified by DN-value rule expression".
5. In the "Configure Rule Expression" dialog box, click "Add entry", and then click "Value generated by script".
6. In the "Configure Entry" dialog box, select the Script Module you created in Step 1, and then select script function "GetParameterValues()".

The "Pick a store containing the least number of mailboxes" option of an Exchange Mailbox AutoProvisioning policy may have no effect when you create Exchange mailbox-enabled users in a newly added managed domain with Exchange server.

227364

WORKAROUND

After you have added a new managed domain with Exchange server to Active Roles, wait for Active Roles to run the Scheduled Task "Mailbox Location Checker." Normally, that Task is scheduled to run on a daily basis at 2:00 AM. Alternatively, you could run that Task by hand: In the Active Roles console, go to the "Configuration/Server Configuration/Scheduled Tasks/Builtin" container, right-click the "Mailbox Location Checker" object in that container, point to "All Tasks" and then click "Execute."

After you click the Rebuild button on the Members tab in the Properties dialog box for a Dynamic Groups in the Active Roles console, Active Roles may not update the members list of the Dynamic Group as expected. The issue occurs if Active Roles has not completed the previous request to build the members list. For example, when you add a new membership rule, Active Roles receives, and starts processing, a request to build the members list in accordance with the new rule. If you change the rule and force the rebuilding of the members list before Active Roles has finished the ongoing build request, then you encounter the issue in question.

234922

WORKAROUND

Wait for Active Roles to finish building the members list of the Dynamic Group. Active Roles does not allow you to force the rebuilding of the members list while another request to build the members list is in progress.

When you block the "Dynamic Groups" policy on a particular container (organizational unit or domain), it may take 15 minutes or more for the block policy setting to take effect. The issue occurs if you've selected the "Blocked" check box next to "Built-in Policy - Dynamic Groups" in the dialog box displayed by the "Enforce Policy" command for a container in the Active Roles console.

249248

WORKAROUND

To ensure that the block policy setting is in effect, restart the Active Roles Administration Service. For instructions, see "Start, stop or restart the Administration Service" in the Active Roles Administration Guide.

The "Restricted characters" option of the User Logon Name Generation policy has no effect if the list of restricted characters contains a space character only. In this case, Active Roles may not remove space characters from the policy-generated logon name as expected.

284037

WORKAROUND

To ensure that space characters are removed from policy-generated logon names, configure the list of restricted characters to include any character in addition to a space character. For example, add an asterisk (*) to the list (note that asterisk characters are removed from policy-generated logon names anyway, regardless of whether or not the list of restricted characters includes an asterisk).

In Active Roles Replication environment, management of Azure objects from subscriber service does not work successfully post Azure configuration.

673381

WORKAROUND

In Active Roles Replication environment, restart the Subscriber Active Roles Service post Azure configuration, to enable management of Azure objects from Subscriber Service.

Active Roles provides limited workflow support for Azure AD Management.

682621

Currently after an in-place upgrade of Active Roles, the Active Roles Service cannot be upgraded remotely.

690207

WORKAROUND

Login to the system where Active Roles Service was upgraded, open Configuration Center and perform the "Upgrade Configuration Service" operation to upgrade the Service.

| Known Issue | Issue ID |
|---|----------|
| <p>Currently during an in-place upgrade of Active Roles, the earlier version of Active Roles is removed if the Upgrade process is canceled before completion.</p> <p>WORKAROUND</p> <p>On the Add or Remove Programs window, select the Active Roles component, and click the Modify component. This reverts Active Roles to the earlier version that was available on the system before starting the in-place upgrade.</p> | 690557 |
| <p>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 within the same window.</p> <p>WORKAROUND</p> <p>In Active Roles with the Office 365 Licenses Retention policy applied, after deprovisioning the Azure AD user, in Active Roles Console right-click and select click Deprovisioning Results, and in Web Interface click Deprovisioning Results in the Action Pane or press (F5) to refresh the form to view the deprovisioning results.</p> | 770629 |
| <p>Remote Mailbox creation note is displayed on the Azure tab, though the user has the on-premises presence.</p> | 140391 |
| <p>Navigating to Office 365 Roles report without configuring the Azure displays an error. However, the message displayed does not convey an appropriate meaning about the issue.</p> | 151013 |
| <p>Active Roles does not allow to create Azure Group for already existing Group.</p> | 117015 |
| <p>An error is displayed during the approval phase of the Pending Task after upgrading from a major version to a service pack version of the product.</p> | 186676 |
| <p>When you apply an Access Template to the "Active Directory" container in the Active Roles console, with the option to enable synchronization of the resulting permission entries to Active Directory, you encounter the following issue: The resulting permission entries are propagated from the "Active Directory" container to the managed domains held in that container, but not synchronized to Active Directory.</p> <p>Thus, you can check "Advanced Details Pane" on the View menu in the console, select a managed domain under the "Active Directory" node in the console tree, and examine the permission entries on the "Native Security" tab in the lower sub-pane of the details pane, to see that the permission entries resulting from the Access Template you applied to the "Active Directory" container are marked as Absent, and displayed in red. In this case, the synchronization can only be performed manually, by right-clicking such entries on the "Native Security" tab, and then clicking the "Resync from Active Roles Security" command.</p> <p>WORKAROUND</p> | 24439 |

| Known Issue | Issue ID |
|--|----------|
| Avoid using the synchronization option when applying Access Templates to the "Active Directory" container. If you need to synchronize permission entries from Active Roles security to native Active Directory security, apply Access Templates to managed domains or objects and containers within managed domains. | |
| O365 and Azure Tenant Selection policy when configured for Group and Contacts displays additional tabs. | 229031 |
| Tenant selection allows only one of the tenant to be selected. Instead of checkbox, a radio button should be used | 229030 |
| If a disabled workflow is copied and modified, Run workflow option is not available . | 231417 |

WORKAROUND

- Enable the built-in workflow and then Copy it and use it .Run workflow will be enabled.
- For any disabled workflow after we copy the workflow, to enable the **Run workflow** button we need to :
 - Enable the workflow.
 - Modify and save the workflow changes.
 - Reconnect the ARS console to ARS service.

Table 9: Web interface known issues

| Known Issue | Issue ID |
|--|----------|
| After upgrading between major Active Roles versions, Web Interface Personal Views are lost. | 91729 |
| WORKAROUND <ol style="list-style-type: none"> 1. Take a backup of the current database. 2. Copy the PersonalSettings data from the earlier database <DBName_BACKUP> to the current database <DBName>. <p> NOTE: The PersonalSettings table contains the saved personal views.</p> <ol style="list-style-type: none"> 3. Use the following SQL script to import the contents from the PersonalSettings table from the earlier database to the current database: <pre> DECLARE @SourceDB NVarChar(50) DECLARE @TargetDB NVarChar(50) </pre> | |

```

DECLARE @SQL NVarchar(max)

SET @SourceDB = 'ActiveRolesDB' -- Replace with old source database
name.

SET @TargetDB = 'ActiveRolesDB_repl' -- Replace with new target
database name.

SET @SQL = 'INSERT INTO [' + @TargetDB + '].[dbo].[PersonalSettings]
([rowId]
,[userId]
,[wiGuid]
,[settingName]
,[settingValue]
,[modified]) SELECT * FROM [' + @SourceDB + '].[dbo].
[PersonalSettings]'
EXEC(@SQL)

```

- Update the **wiGuid** of the **PersonalSettings** to reflect new **objectGUI** from the **WebInterface** table.
- Query 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.
- edsaWITemplateVersion** value for the Active Roles versions are:

| Active Roles Version | edsaWITemplateVersion value |
|----------------------|-----------------------------|
| 7.4.3 | 40 |
| 7.4 | 39 |
| 7.3 | 38 |
| 7.2 | 37 |
| 7.1 | 36 |

- In the **PersonalSettings** table of the current upgraded database, replace the respective Web interface site **objectGUID** to **wiGuid** for all rows.

When you add a number of Organizational Units to an Active Roles Managed

18427

Unit, and then open that Managed Unit in the Web Interface, you may encounter the following issue: The Organizational Units are not sorted by name in the Tree View pane.

WORKAROUND

When adding Organizational Units to the Managed Unit, add them in the order in which you want them to appear in the Tree View pane. For example, if you first add the "Groups" OU, then add the "Special Accounts" OU, and then add the "Users" OU, these three organizational units appear sorted by name in the Tree View pane.

When adding values to a multi-value attribute, the Active Roles ADSI Provider may add only the last value in a sequence of values. The problem occurs when you add values one by one, as in the following example:

```
obj.PutEx 3, "otherHomePhone", Array("123")
```

```
obj.PutEx 3, "otherHomePhone", Array("456")
```

```
obj.SetInfo()
```

When executing the code given in this example, the ADSI Provider will only add the "456" value and disregard the "123" value.

WORKAROUND

Use a single array containing all values to add, as in the following example:

```
obj.PutEx 3, "otherHomePhone", Array("123", "456")
```

```
obj.SetInfo()
```

When using the "Choose Columns" dialog box in the Web Interface, you may encounter the following issue with the "Hidden columns" list: Different list items have the same name. For example, for the object type User, the list includes two items with the same label - Name.

WORKAROUND

Click Add to move a list item to the "Displayed columns" list. This will allow you to view the LDAP display name which uniquely identifies the item. If you do not want to display the column represented by the item, use the Remove button to delete the item from the "Displayed columns" list.

When you use the Web Interface to create a network share, you may encounter the following issue on the "New Share" page: If you specify the path to the folder in the form "DiskLetter:/FolderName", and select the "Create folder if it doesn't exist" check box, the folder is created but a network share on that folder is not.

NOTE: You can access the "New Share" page as follows:

1. Select a computer object and click the Manage command to display a list

of computer resource categories.

2. In the list, click Shares to display a list of network shares found on that computer.
3. Click the "New Share" command.

WORKAROUND

In the Path field on the "New Share" page, specify the path in the form "DiskLetter:\FolderName" (use a backslash character (\) rather than a slash mark (/) as a separator in the path).

After submitting changes to a certain object for approval, the Web Interface may fail to display the appropriate page, returning the "Object reference is not set to an instance of an object" error. The problem occurs if the Web Interface user does not have the Read permission on the Active Directory container that holds the object. This scenario implies that the object is located by selecting a Managed Unit rather than an Active Directory container, so the Read permission on the container is not required to locate the object.

24713

WORKAROUND

If modification of a certain object requires approval, ensure that the Web Interface user has the All Objects - Read All Properties permission on the Active Directory container that hold the object.

When you use the Web Interface to view the members list of a group that is under the control on an Active Roles Group Family (controlled group), you may encounter the following error: "Exception has been thrown by the target of an invocation." The Web Interface returns this error when you select a controlled group and then click Members, if your logon account does not have the Read permission on the objectClass property of objects that belong to that group.

24740

WORKAROUND

Apply the "All Objects - Read All Properties" Access Template on a directory container that holds the members of the controlled groups so that that the Web Interface users have the Read permission on all properties, including the objectClass property.

When you use the Web Interface to configure permission settings on a network file share, you may encounter the following issue: The Web Interface fails to assign permissions to a local user account returning an error message that states "Value does not fall within the expected range."

25606

WORKAROUND

Use native Windows tools to perform that task.

When you use the Advanced Search option in the Approval section of the Web Interface to find an operation by completion date, you may encounter the

25913

following issue: The search results include some operations that are waiting for approval and therefore are not completed. This issue occurs with operations that have to be reviewed by multiple approvers. If such an operation is approved by some but not all of the approvers, the operation may appear in the search results list as if it were completed by the specified date.

WORKAROUND

When configuring a search for operations by completion date, specify an additional rule to ensure that the search returns only the completed operations: select the "Status" field, "Is (exactly)" condition, and "COMPLETED" value; then, select the AND option and click Add to include the new rule in the search filter.

| | |
|---|-------|
| Selecting the "Microsoft Exchange System Objects" container in the Web Interface displays a page for managing properties of the container instead of displaying a list of objects held in that container. | 26027 |
|---|-------|

WORKAROUND

Select the "Microsoft Exchange System Objects" container and then click "View Contents" to display a list of objects held in that container.

| | |
|--|-------|
| You may encounter incorrect behavior of a DN-syntax, single-value attribute entry after upgrading the Administration Service and Web Interface: If the Web Interface was customized so that such an entry was added to a custom form, then after the upgrade the entry behaves as if the attribute were multi-value. | 26046 |
|--|-------|

WORKAROUND

After the upgrade, use the Active Roles console to correct the configuration of the Web Interface:

1. Switch the console into Raw view mode: Select "View | Mode" and then select the "Raw Mode" option.
2. In the console tree, expand "Configuration | Application Configuration | Web Interface."
3. In the console tree, under "Web Interface," select a Web Interface site configuration item (each configuration item is identified by GUID, such as "662cf9fd-3985-431b-8b32-19ca436319d8").
4. In the details pane, double-click "Customization Settings".
5. Use the "All Tasks | Advanced Properties" command on the "CurrentCopy" and "WorkingCopy" objects in the details pane to modify the value of the "edsaWIEntries" attribute as follows:
 - a. Copy the attribute value from the Active Roles console into Notepad.
 - b. Use the Find command in Notepad to look for occurrences of the "FormEntry" XML element with the "Properties" attribute set to the LDAP display name of the attribute managed by the entry that

exhibits the incorrect behavior.

- c. If no occurrences of such an XML element can be found, leave the "edsaWIEntries" attribute value unchanged; otherwise, set the value of the "SingleValue" attribute in that XML element to "True" (SingleValue="True").
- d. Copy the text from Notepad to the "edsaWIEntries" attribute value in the Active Roles Restart Internet Information Services (IIS) on the Web server running the Web Interface (enter the iisreset command at a command prompt).console, to replace the attribute value.
- e. Repeat steps 3-5 for each of the configuration items located in the "Web Interface" container.

When two or more administrators simultaneously use the Customization section of the Web Interface to customize the same Web Interface site, the changes that were made by one of the administrators can be lost. 26135

WORKAROUND

Ensure that no more than one administrator uses the Customization section of the Web Interface at a time so that no more than one customization session is in progress at a time for each Web Interface site. The session begins when an administrator opens the Customization section of the Web Interface in the Web browser and ends when the administrator issues the Reload command and closes the Web browser window.

When you configure custom Web Interface pages for creating objects of a certain type (for example, Contact objects), you may encounter the following issue: If you have added the entry for the Name (name) property by creating a new entry (rather than selecting the existing entry), the pages do not work as expected. The object creation operation fails, returning an error. The error message reads "The 'Name' field cannot be empty." 36775

WORKAROUND

When configuring the object creation pages, select the existing entry for the naming property Name (name) instead of creating a new entry (on the Select Existing Entries page, select the check box that has the label 'Name' followed by 'name').

When modifying a user account, the Web Interface may fail to set the e-mail alias on the user account in accordance with the E-mail Alias Generation policy that is in effect. For instance, with a policy configured to set the e-mail alias to the user logon name (pre-Windows 2000), the Web Interface may not set the new alias when the pre-Windows 2000 logon name is changed. 36788

WORKAROUND

| Known Issue | Issue ID |
|---|----------|
| Customize the Web Interface to have the e-mail alias (mailNickname) entry and the pre-Windows 2000 logon name (sAMAccountName) entry located on the same Web Interface page (tab) for managing user account properties. | |
| <p>There is a limitation on the processing of Property Generation and Validation policy rules in the Web Interface. For a rule to generate a property value on a particular Web Interface form, the form must contain the entries for the properties based on which the value is to be generated. For example, since the form for creating AD LDS user objects does not contain entries for the First Name (givenName) and Last Name (sn) attributes, the Web Interface is unable to process a rule that generates the logon name based on those attributes when creating an AD LDS user object.</p> <p>WORKAROUND</p> <p>Customize the form so that it contains the entries for all the object attributes required by the policy rules that are in effect. In the preceding example, you should add the entries for the First Name (givenName) and Last Name (sn) attributes.</p> | 37870 |
| <p>If no Global Catalog servers are available in an Active Directory domain, then the Active Directory domain services fail to authenticate a domain user other than the built-in administrator account. In this situation, the Web Interface user may encounter one of the following errors:</p> <ul style="list-style-type: none"> • Error: Message 1003: hr = 0x80070005 Interface: Unknown Access is denied. • Error: Message 5202: The Active Roles Administration Service is not available. <p>WORKAROUND</p> <p>Ensure that at least one Global Catalog server is available in every Active Directory domain.</p> | 39209 |
| <p>When you select a built-in domain local group (for example, Administrators or Account Operators) in the Web Interface, and then navigate to the "Member Of" page for that group, you encounter the following issue: The "Add" button is available on the "Member Of" page. Clicking "Add" and selecting a group to add the built-in group to causes an error such as "A new member could not be added to a local group because the member has the wrong account type."</p> <p>WORKAROUND</p> <p>Do not use the "Add" button on the "Member Of" page for a built-in group: In Active Directory, built-in groups cannot be added to other groups.</p> | 39531 |
| When the Active Roles Administration Service cannot access the configuration database, you may receive an inappropriate error message in the Web Interface: "Client cannot use the selected Administration Service due to version | 39767 |

incompatibility."

WORKAROUND

If you receive that error message in the Web Interface, verify that the Administration Service is up and running. It is advisable to check for Event ID 2512 in the Active Roles Admin Service event log.

On the "General Properties/Managed By" page for a group in the Web Interface, the object name may not fit in the "Manager" field, so you cannot view the entire name. 46387

WORKAROUND

You can view the name by copying it to a text editor, such as Notepad: Click in the Manager field, press Ctrl+A, press Ctrl+C, switch to your text editor, and then press Ctrl+V.

The following Property Generation and Validation policy rule for computer objects may cause a policy violation when you create a computer account in the Web Interface: 47238

'Computer name (pre-Windows 2000)' must be '%<cn>\$' (default value) Upon object creation, this policy generates default value: Yes

WORKAROUND

Modify the rule by selecting the 'Computer name (pre-Windows 2000) is case-insensitive' option. As a result, the rule changes to: 'Computer name (pre-Windows 2000)' is case-insensitive and must be '%<cn>\$' (default value) Upon object creation, this policy generates default value: Yes

On the "Member Of" page in the Web Interface, the "Set Primary Group" button is available when you select a group that does not meet the standard requirement for the primary group setting: "A user's primary group must be in the same domain as the user's account and the primary group must be either a global or universal security group." 54638

WORKAROUND:

If clicking "Set Primary Group" has no effect, verify whether the group you selected meets the above-stated requirement. If not, change your selection.

Consider the following scenario. The DN of an AD LDS partition managed by Active Roles contains the DN of an Active Directory domain that is also managed by Active Roles. In this scenario, the Active Roles ADSI Provider may fail to locate the Administration Service when binding to a directory object. 55184

WORKAROUND

In a binding string, explicitly specify the name of the computer running the Administration Service (for example, "EDMS://server.company.com/CN=John Smith,OU=Research,DC=Gamp,DC=com").

| Known Issue | Issue ID |
|---|------------------|
| When you assign a secondary owner to a group by using the Web Interface, the "Select Object" dialog box allows you to choose an AD LDS user or group from a Managed Unit. The expected behavior is that only AD DS users or groups can be selected for the role of secondary owner. | 103650 103677 |
| WORKAROUND | |
| When using the "Select Object" dialog box in the Web Interface to select a user or group for the secondary owner role, verify that you do not select an AD LDS user or group. | |
| The Web Interface does not support Property Generation and Validation policy rules that control the "name (name)" property value. Thus, a policy rule such as "name=%1<givenName>%<sn>" has no effect on the name of an object when you administer that object in the Web Interface. | 104964 |
| WORKAROUND: | |
| When configuring a policy rule for a certain object class, choose the naming property of that object class rather than the "name (name)" property. The naming property for most object classes is "Name (cn)". The naming property for the Organizational Unit object class is "Name (ou)". So, to work around the issue with the "name=%1<givenName>%<sn>" policy rule on the User object class, you could replace that policy rule with the following one: "cn=%1<givenName>%<sn>" | |
| With the E-mail Alias Generation policy configured to set the e-mail alias to the "Name (cn)" property of the user account, the Web Interface fails to create a mailbox-enabled user account, returning an error such as "E-mail alias does not comply with the E-mail Alias Generation policy. A different e-mail alias must be assigned to this user account." | 105471 |
| WORKAROUND | |
| Select the "name (name)" property rather than "Name (cn)" when configuring the E-mail Alias Generation policy with the option "Set e-mail alias to other combination of user properties." | |
| When you use the Web Interface to create a new room or equipment mailbox by copying an existing room or equipment mailbox, you encounter the following issue: The settings on the "Resource Information" page are not copied from the original mailbox. | 106596 |
| WORKAROUND | |
| After you have copied a room or equipment mailbox, configure resource information settings for the new mailbox by hand as required. | |
| When you use the "Approval/Advanced Search" page in the Web Interface, you may encounter incorrect search results in case of a search rule with the following parameters: | 107621 |

| Known Issue | Issue ID |
|---|----------|
| <ul style="list-style-type: none"> Find: Operations Field: Type Condition: Is (exactly) Value: ModifyThe search does not return the operations that modify the members list of groups. <p>WORKAROUND:</p> <p>Add a search rule with the following parameters:</p> <ul style="list-style-type: none"> Find: Operations Field: Target object property Property to search: member Condition: Modified <p>Use the logical OR operator to combine the newly added rule with the existing rule.</p> | |
| <p>The Web Interface does not apply the Property Generation and Validation policy rules or Effective Policy Info settings to the property entries that are configured with the IsStatic attribute set to TRUE (IsStatic="true").</p> <p>WORKAROUND</p> <p>When configuring a property entry that is subject to the Property Generation and Validation policy rules or Effective Policy Info settings, avoid the use of the IsStatic attribute. Set the ReadOnly attribute to TRUE instead (ReadOnly="true"). For information regarding the entry configuration attributes, see topic "The Entries Settings" in the Active Roles SDK.</p> | 130826 |
| <p>Consider the following scenario. You select a domain or an Organizational Unit (OU) in the TREE pane in the Web Interface, choose the "New Organizational Unit" command, and create an OU. In this scenario, the newly created OU may not appear in the tree view, even after you click the "Refresh" button in the top-right corner of the TREE pane.</p> <p>WORKAROUND</p> <p>In the tree view, click the domain or the Organizational Unit to which you applied the "New Organizational Unit" command (this is the parent container of the newly created OU), and then click the "Refresh" button in the TREE pane. This will cause the tree view to display the newly created OU.</p> | 209882 |
| <p>Consider the following scenario. You open the "Approval" page in the Web Interface, click "Advanced Search" and configure a search condition to search for a certain property value, approver action, or approval task title. If you specify the value in quotation marks, then your search causes an error in the Web Interface. For example, the following search condition causes an error:</p> | 211135 |

Known Issue

Issue ID

- Find: Tasks
- Field: Approver action
- Conditions: Is (exactly)
- Value: "Approve"

WORKAROUND

Do not use quotation marks in the Value field. Thus, in the above example, you should type Approve instead of "Approve" in the Value field.

Consider the following scenario. You use a Web browser other than Windows Internet Explorer to customize the Web Interface. You open the "Customization | Directory Objects" page in the Web Interface, select any menu for AD LDS objects (for instance, "container - AD LDS Object"), select any form-based command (for instance, "Properties"), click "Edit Form" to start the Form Editor, and then choose "Add Entry | Create" or "Add Entry | Select" in the Form Editor to add an entry to the form. In this scenario, you encounter one of the following errors:

- Form with this FormID cannot be found.
- Object reference not set to an instance of an object.

WORKAROUND

In the above scenario, use Windows Internet Explorer to customize the Web Interface.

When you use the Web Interface to start an automation workflow with a parameter name containing a quotation mark ("), you may encounter a script error stating "Unable to set property 'control' of undefined or null reference."

WORKAROUND

When configuring workflow parameters, ensure that the name of the parameter contains only alphanumeric characters (letters or digits). You may safely use non-alphanumeric characters, such as quotation marks, in the display name of the parameter.

When you use the Active Roles Web Interface to start an automation workflow with a parameter name containing a colon (:), comma (,) or dollar sign (\$), you may encounter an error condition. The reeoe message is one of the following:

WORKAROUND

When configuring workflow parameters, ensure that the name of the parameter contains only alphanumeric characters (letters or digits). You may safely use non-alphanumeric characters, such as a colon (:), comma (,) or dollar sign (\$), in the display name of the parameter.

| Known Issue | Issue ID |
|--|----------|
| <p>If you have any customizations of the Web Interface an earlier Active Roles version that use custom code or images stored in the CustomCode or CustomImages folder in the Web Interface installation directory, then you lose those customizations after upgrade to Active Roles 7.4, as the contents of the CustomCode and CustomImages folders are not copied to the new Web Interface version during upgrade.</p> <p>WORKAROUND</p> <p>After upgrade, copy the files held in the CustomCode and CustomImages folders to the corresponding folders in the Active Roles 7.4 Web Interface installation directory, and then restart the Web server running the Active Roles 7.4 Web Interface.</p> | 447158 |
| <p>After Enabling Request Validation(<add key="EnableRequestValidation" value="true"/>, the following error may be displayed even when an expected operation is performed:</p> <p><i>A potentially dangerous Request. Form value was detected from the client.</i></p> <p>WORKAROUND</p> <p>To solve this issue, update the IgnoreForValidation key in <AppSettings> section.</p> <p> NOTE: The values for the key must be in lowercase.</p> <p>To Modify the key:</p> <ol style="list-style-type: none"> 1. Open IIS Manager, expand default website, and click on Active Roles Application (Default is ARWebAdmin). 2. In the right pane, click Configuration Editor. 3. In the Section drop-down, select <appSettings>, and click on the button corresponding to (Count=*). 4. Find Key <i>IgnoreForValidation</i> and append the comma separated Value as <i>"lowercasecontrolname"</i>. <p>For example:</p> <pre>Error: A potentially dangerous Request.Form value was detected from the client (ctl00\$FormContentPlaceholder\$ObjectProperties Form\$ctl04\$ctl01\$ctl00\$hiddenXML="&lt;?xml version="1.0" ...").</pre> <p>In the above example, <i>"lowercasecontrolname"</i> value is <i>"hiddenXML"</i>, which appears after the last \$ sign and before "=" sign.</p> <ol style="list-style-type: none"> 5. Add "value" for <i>"IgnoreForValidation"</i> key as: <i>hiddenxml</i>. 6. In the right pane, in the Actions menu, click Apply. 7. Recycle the App pool. | 652470 |

| Known Issue | Issue ID |
|--|----------|
| <p>After Enabling EnableAntiForgery"(<add key="EnableAntiForgery" value="true"/>), the following error may be displayed in a new tab:</p> <pre>" {"State":1,"ErrorMessages":["Session timeout due to inactivity, Please reload the page to continue."],"Arguments":null} "</pre> <p>WORKAROUND</p> <p>To solve this issue, update the IgnoreValidation key in <AppSettings> section.</p> <p> NOTE: The values for the key must be in lowercase.</p> <p>To Modify the key</p> <p>Open IIS Manager, expand default website, and click on Active Roles Application (Default is ARWebAdmin).</p> <ol style="list-style-type: none"> 1. In the right pane, click Configuration Editor. 2. In the Section drop-down, select <appSettings>, and click on the button corresponding to (Count=*). 3. Find Key <i>IgnoreValidation</i> and append the comma separated Value as <i>"lowercasecontrolname"</i>. <p>For example, in the URL of a blank page where an error is displayed: /ARWebAdmin/Handlers/CustomizeForm.ashx?TaskId=NewSharedFolder&MenuId=organizationalUnit</p> <p><i>"lowercasecontrolname"</i> value is: <i>"CustomizeForm"</i>, which precedes .ashx</p> <ol style="list-style-type: none"> 4. Add "value" for "IgnoreValidation" key as: customizeform 5. In the right pane, in the Actions menu, click Apply. 6. Recycle the App pool. | 653530 |
| Active Roles Web interface supports exporting linear nested access templates only. Exporting circular nested access templates may cause errors. | 675024 |
| The Azure Password complexity does not match with Azure policy. | 672022 |
| <p>WORKAROUND</p> <p>The Azure password complexity requirement expects password length to be 8. Hence, you must set the minPwdLength attribute on the domain to 8.</p> | |
| <p>Active Roles uses graph API to communicate with Azure AD. However, Graph API is not supported in Federated environment to update Azure objects attributes.</p> <p>Hence, after any create or update operation through the Active Roles web interface, for example, Update attribute, Deprovision, undo-deprovision, and so on, the changes are not visible in Azure AD immediately.</p> | 675092 |

| Known Issue | Issue ID |
|---|----------|
| WORKAROUND You must wait for the delta sync (using AADConnect) to complete from local AD to Azure AD in order to see the updated information. | |
| Azure Configuration and Azure objects creation is not possible through HelpDesk and Self-Service portal. | 682586 |
| WORKAROUND To enable a help desk user to perform Azure related operation, he must be provided with delegated rights and use the Administrators site to perform the required operation. | |
| After in-place upgrade of Active Roles, Configuration to import drop-down does not display existing website configurations when trying to create a new website before completing service upgrade. | 690566 |
| WORKAROUND <ol style="list-style-type: none"> 1. Complete the upgrade service configuration operation before trying to create new website. 2. Close and launch the configuration center again to see the existing website configurations and create new websites. | |
| Currently, Active Roles Web interface does not support setting the Exchange online Property of ProhibitSendQuota value in Storage Quotas. | 728521 |
| In Active Roles, logout button works with ONLY the "Basic Authentication" which displays the login prompt to enter username and password(how to configure Basic Authentication https://technet.microsoft.com/en-us/library/cc733010(v=ws.10).aspx). | 691672 |
| After Active Roles upgrade, the pending approval tasks are not displayed in Web Interface. | 711492 |
| On Internet Explorer, intermittently the Starling notifications are not sent. | 142523 |
| The features on the Mailbox Features tab cannot be selected in Internet Explorer | 91631 |
| Intermittently, selecting and deleting multiple objects on the Web Interface will not delete all the selected objects. | 128045 |
| When a workflow is copied from built-in workflows, it may not be executed as expected. | 153539 |
| Deprovisioning proces is slow for users in Active Roles. | 113811 |
| Notifications are not sent when you configure Active Roles Web Interface for HTTPS. | 142059 |

| Known Issue | Issue ID |
|---|----------|
| WORKAROUND: Perform the following for notification to work as expected, if you are using ActiveRoles website over HTTPS- <ul style="list-style-type: none"> • Import a valid certificate into Trusted Root Certificate Authority in the machine where ActiveRoles Service is installed. • In the below command, substitute thumbprint of the newly added certificate to CERT_HASH. • In the below command, substitute a Unique GUID to APP_ID. • Execute the command below in PowerShell command interface: <pre>netsh http add sslcert ipport=0.0.0.0:7466 appid='{APP_ID}' certhash=<CERT_HASH></pre> | |
| In Active Roles Federated Authentication, if identical users are present across multiple domains, by using the credentials of domain1, a domain2 user can login to ARS, if claim is set to upn in RSTS. | 184313 |
| WORKAROUND: Configure RSTS with a custom claim. For more information, see the <i>Active Roles Administration Guide</i> . | |
| On Active Roles Web Interface, Azure Roles is not restored after an undo-deprovision operation. | 172655 |
| WORKAROUND: One Identity recommends to assign the roles to the user again. | |
| The Federated Authentication configuration settings are not retained after an upgrade from 7.4 or 7.4.1 to 7.4.3. | 200589 |
| The Force SSL Redirection configuration settings are not retained after an upgrade from 7.4 or 7.4.1 to 7.4.3. | 200666 |
| After enabling or disabling Starling, an error is displayed after clicking the Force SSL redirection button. | 232529 |

Table 10: MMC interface known issues

| Known Issue | Issue ID |
|--|----------|
| Consider the following scenario. You are using the Active Roles console to register an AD LDS instance with Active Roles. On the Active Roles Credentials page in the Add Managed AD LDS Instance wizard, you specify an incorrect account (for example, an account that does not have sufficient rights to access | 26019 |

the desired AD LDS instance). Then, you return back to the previous page of the wizard and click Next on that page. In this scenario, you may receive an error message stating "There is no such object on the server."

WORKAROUND

Close the wizard by clicking Cancel, and start registering the AD LDS instance again. Another option is to click Next again, without closing the dialog box that displays the error message, and then close that dialog box.

Consider the following scenario. You are using the Active Roles console to manage a mailbox-enabled user account that resides in a forest other than the forest in which the console is installed. In addition, the domain of your user account is not trusted by the domain of the account being managed. You open the Exchange Advanced tab in the Properties dialog box for that mailbox-enabled user and click Mailbox Rights. Then, you click Add in the Permissions dialog box to select users or groups for which you want to assign permissions. In this scenario, the "Select Users, Computers, or Groups" dialog box, which appears when you click Add, may not allow you to specify the desired location from which to select users or groups. The issue occurs if the domain of the users or groups you want to select does not trust the domain of the user account under which the console is running.

26398

WORKAROUND

In this scenario, you can use the Active Roles Web Interface to configure mailbox rights. The Web Interface would allow you to select users or groups from the location you want.

The Active Roles console incorrectly processes Property Generation and Validation policy rules that include any values containing a backslash character (\).

37815

WORKAROUND

To specify one backslash character (\) in a Property Generation and Validation policy rule, use a combination of two backslash characters (\\). For example, to specify a policy rule such as "Network path must begin with \\server\", enter \\\server\\ in place of \\server\.

For a Dynamic Group or Managed Unit with a membership rule based on a custom LDAP query, the Active Roles console may incorrectly display the query in the dialog box for editing the rule: A closing parenthesis character may get removed.

39592

WORKAROUND

When editing such a query, verify the query to ensure that the syntax is correct. If necessary, add the closing parenthesis character at the end of the string. Another option is to modify the query so as to change the order of sub-filter

| Known Issue | Issue ID |
|---|----------|
| strings. | |
| <p>Consider the following scenario. You have a Dynamic Group configured in Active Roles with complex membership rules (for example, using a complex query that returns a large number of objects). You open the Properties dialog box for that group, go to the Members tab, and click Rebuild. The console informs you of the fact that you are going to start a lengthy operation, without giving you the option to cancel the operation. When you click OK in the warning message box, the console may stop responding for a certain time period.</p> <p>WORKAROUND:</p> <p>Wait while Active Roles completes the rebuild operation.</p> | 55373 |
| <p>In the Active Roles console, when you right-click a selection containing a large number of objects (100+), you may experience a long delay before the shortcut menu is displayed.</p> <p>WORKAROUND:</p> <p>Wait while the console processes your selection. Consider using a selection of fewer objects.</p> | 55600 |
| <p>You may encounter a noticeable delay in the Active Roles console when you click the plus sign (+) to expand an Organizational Unit (OU) in the "Browse for Container" dialog box. This issue is most likely to occur if the OU holds a large number of other OUs.</p> <p>WORKAROUND:</p> <p>If you need to select the OU itself, avoid expanding the OU, only click the name of the OU in the "Browse for Container" dialog box. To select an OU that is held within another (parent) OU, you have to wait while the console expands the parent OU.</p> | 55919 |
| <p>You may encounter a noticeable delay in the Active Roles console when saving your changes to a Group Family configuration that were made from the Groupings tab in the Properties dialog box for the Group Family configuration storage group. Clicking OK or Apply on that tab may cause the console to "hang" for up to a minute. This issue is most likely to occur if the Group Family is configured to search within a large number of objects (50,000+), and has two or more group-by properties specified.</p> <p>WORKAROUND:</p> <p>When you specify the location of managed objects for Group Family, avoid choosing containers that hold a large number of objects.</p> | 55998 |
| <p>When you configure the "<attribute> must be <value>" policy rule for a Property Generation and Validation policy, you may encounter an issue in the following scenario. Suppose you have specified a list of acceptable values for a</p> | 64436 |

certain attribute and selected one of them to be the default value. Then, you choose the "Sort Items Ascending" or "Sort Items Descending" command from the shortcut menu to reorder the values. As a result, the default value setting may change: the value that now occupies the first position in the list is set as the default value.

WORKAROUND:

After the values have been reordered, right-click the value that you want to be default, and then click "Set as Default Value".

You may encounter an issue in the following scenario of configuring a workflow that includes an approval or notification activity. Suppose the workflow applies to the User object type ("User" is selected as the target object type in the workflow start conditions). You specify notification settings for a particular event so that the "Manager of operation target object" option is selected in the "Notification recipients" area. Then, you change the target object type in the workflow start conditions by selecting "Group" instead of "User". In this scenario, the "Manager of operation target object" option gets cleared (so notification e-mails will not be sent to the manager), but the event with that recipient remains in the "Events, Recipients and Messages" list. Re-selecting the "Manager of operation target object" causes the manager to be specified two times in the "Notification Recipient" field of the corresponding list entry under "Events, Recipients and Messages".

93007

WORKAROUND:

Prior to changing the target object type from User to Group, or vice versa, verify the notification settings for all events to ensure that the "Manager of operation target object" option is not selected.

The Active Roles console may return an error message stating that the console cannot use the Administration Service on a particular computer due to version incompatibility, although both the console and the Administration Service are of the same version. This issue occurs if the user account under which the console is running does not have sufficient rights to access the Administration Service. Under that condition the console attempts to contact the Administration Service with the credentials of the Guest user account, and fails to identify the version of the Administration Service. As a result, it displays an error message that informs of a version mismatch.

104085

WORKAROUND:

Disable the Guest user account.

When you use the "Select Objects" dialog box in the Active Roles console, you may encounter the following issue: If you type in a name and then click "Check Names", Active Roles fails to find any object if the name you supplied contains a backslash character (\).

118209

WORKAROUND:

Select the desired object from the list in the "Select Objects" dialog box.

When you use the Active Roles console to edit a PowerShell based script, you encounter the following issue: The "Include Library Script" command does not function as expected in the Script Editor.

134558

WORKAROUND:

To include a library script into a PowerShell based script, add the following code to the onInit function in that script:

```
function onInit($context)
{
    $context.UseLibraryScript("Script Modules/<name>")
}
```

Here Script Modules/<name> stands for the path and name of the Script Module containing the library script.

When you configure a Scheduled Task in the Active Roles console, you may encounter the following issue: The "All servers" item is missing from the "Execute on" list on the General tab in the Properties dialog box for the Scheduled Task object, so you cannot configure the Scheduled Task to be executed by all instances of the Administration Service in your Active Roles environment.

186054

WORKAROUND:

Use the following steps to enable the "Execute on all servers" option for a Scheduled Task:

1. Open the "Advanced Properties" dialog box for the Scheduled Task object (right-click the object in the console, point to "All Tasks", and then click "Advanced Properties").
2. In the "Advanced Properties" dialog box, select the "Show all possible attributes" and "Include attributes with empty values" check boxes; then, double-click "edsaServerToExecute" in the Property column to open the "Edit Value" dialog box.
3. In the "Edit Value" dialog box, paste the following string into the Value box: ffffffff-ffff-ffff-ffff-ffffffffffff.
4. Click OK to close the dialog boxes you opened.

When you rename a Policy Type object by using the Rename command in the Active Roles console, you encounter the following issue: The Rename command only changes the name of the object, leaving the object's display name intact.

218881

WORKAROUND:

You can change the display name of a Policy Type object on the General tab in

the Properties dialog box for that object.

After you have created a Policy Type object implementing a custom workflow activity (the Policy Type category is set to "Workflow activity"), the Workflow Designer may not display the new activity item in the toolbox.

227628

WORKAROUND:

To ensure that the Workflow Designer displays all activity items, including those based on the newly created Policy Type objects, click the "Refresh Toolbox" button next to the search box at the top of the left pane in the Workflow Designer.

When you configure a CRUD or Search activity, you encounter the following issue: The point-and-click interface in the Workflow Designer does not allow you to select an object or container from the Active Roles Configuration namespace. For example, when you configure a "Create" activity, you cannot select a sub-container of the Active Roles Configuration container so as to have the activity create objects in that sub-container.

228096

WORKAROUND:

You can use the "Object identified by DN-value rule expression" option to specify the Distinguished Name of the desired object or container, including the Distinguished Name of an object or container held in the Active Roles Configuration container. The following steps demonstrate how to specify the "Configuration/AT Links" container for a "Create" workflow activity:

1. Open the "Container" page in the "Create" Activity Properties dialog box.
2. Click "Define", and then click "Object identified by DN-value rule expression".
3. In the "Configure Rule Expression" dialog box, click "Add entry", and then click "Text string".
4. In the "Configure Entry" dialog box, in the "Text string" box, type the Distinguished Name of the desired container: CN=AT Links,CN=Configuration.

The Script Editor provided by the Active Roles console may change the letter case of certain words in comment strings within a PowerShell script. For instance, after you save a PowerShell script in the Script Editor, "FOR" changes to "for" (all lowercase) and "xml" changes to "XML" (all uppercase). The issue occurs with multi-line comments, that is, multiple lines enclosed in the "<#" and "#>" tags.

302897

WORKAROUND:

Use single-line comments where each comment line begins with a number sign (#).

| Known Issue | Issue ID |
|--|----------|
| <p>For Active Roles Server, Indexes are added to the database tables only when a new data base is chosen during installation. Indexing is not added in case of upgrade of the existing database installation.</p> <p>To resolve this issue, run the following script through sql:</p> <pre> use [<DataBaseName>] go CREATE CLUSTERED INDEX [_dta_index_CVSAValues_c_20_534292963__K1] ON [dbo].[CVSAValues] ([objectGUID] ASC)WITH (SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF, ONLINE = OFF) ON [PRIMARY] go CREATE STATISTICS [_dta_stat_534292963_1_3] ON [dbo].[CVSAValues]([objectGUID], [attributeSchemaIDGUID]) go CREATE NONCLUSTERED INDEX [_dta_index_CVSAIndexedValues_20_550293020__K2_5] ON [dbo].[CVSAIndexedValues] ([attributeValueGUID] ASC) INCLUDE ([isLongValue]) WITH (SORT_IN_TEMPDB = OFF, IGNORE_DUP_KEY = OFF, DROP_EXISTING = OFF, ONLINE = OFF) ON [PRIMARY]go </pre> | 651518 |
| Currently, in Active Roles, designating Approvers while escalating an approval request using a script function throws an error exception when we are using a persist-ent variable. | 705698 |
| Invalid LDAP filter error is displayed while performing "Find" operation on Active Directory using Extended Match operator in LDAP query. | 744483 |
| Issues observed while viewing the Active Roles help file from the MMC console on Windows 2010 and Windows 2019 operating systems. | 114736 |
| In Active Roles updating the value edsva-TemporalGroupMemberships-Service to desired service to execute on for temporal groups does not work as expected when set through Management shell cmdlet or from MMC Console Advanced Properties. | 231159 |

Table 11: Management Shell known issues

| Known Issue | Issue ID |
|---|----------|
| Containers other than Organizational Units do not show up on the OU-related reports. For example, such reports do not include information about the Users or Builtin container. | 23641 |
| WORKAROUND | |
| Create a Managed Unit that holds the container and then use Managed Unit-related reports to display data from that container. To create a Managed Unit that holds a given container, use the Active Roles console. When creating the Managed Unit, specify the membership rule with the following settings: | |
| <ul style="list-style-type: none"> • Type: Include by Query • Find: Custom Search • In: The container you want the Managed Unit to hold • LDAP query (enter this syntax on the Advanced tab): (objectClass=*) | |
| On domains with a large number of directory objects (typically 100,000 or more user accounts), you may encounter significant performance degradation of the Data Collector component. Thus, a data collection job may take more than 30 hours to finish running for a domain containing 100,000+ user accounts. | 24297 |
| When using SSRS Report Manager to export an Active Roles report in Excel format, you may experience the following problem: The report data in the resulting Excel book is incomplete. | 49955 |
| WORKAROUND | |
| Choose a different export format. | |
| In the Active Roles reports, the filter options that use the "like" operator (such as "Object name like") do not support the asterisk (*) wildcard character, which is expected to represent a string of zero or more characters. | 50295 |
| WORKAROUND | |
| Use the percent character (%) to represent any string of zero or more characters, or use the underscore character (_) to represent any single character. | |
| In the Active Roles reports, a filter option that uses the "like" operator (such as "Object name like") may cause an error if the option value contains an apostrophe or single quotation mark character ('). | 107520 |
| WORKAROUND | |
| In the "like" option value, enclose each of the apostrophe or quotation mark characters in brackets, such as [']. | |
| Get-QAD cmdlets such as, Get-QADObject, Get-QADUser, Get-QADComputer displays | 90968 |

| Known Issue | Issue ID |
|---|----------|
| <p>an Unknown error (0x80041070), if parentheses are used in property values section for LdapFilter with a proxy switch.</p> <p>WORKAROUND</p> <p>One Identity recommends to use escape sequence instead of parenthesis.</p> <p>For example, in the command <code>Get-QADComputer -LdapFilter "(description=server2 (Infra))"</code>, replace the parentheses exist for description value with escape sequences. Use the command, <code>Get-QADComputer -LdapFilter "(description=server2 \28Infra\29)" -Proxy</code>, where <code>\28</code> is equivalent to <code>(</code> and <code>\29</code> is equivalent to <code>)</code>.</p> | |
| Remove-QADGroupMember fails with an internal error. | 232788 |

Table 12: Group Managed Service Account known issues

| Known Issue | Issue ID |
|--|----------|
| <p>Group Managed Service Account (gMSA) is not validated if it is an indirect member of built-in Admins and Local Admins.</p> <p>WORKAROUND</p> <p>Add the Group Managed Service Account (gMSA) as a direct member of the local administrators group where the Active Roles service is running as well as the "Builtin administrators" group of the domain.</p> | 116422 |

Table 13: General known issues

| Known Issue | Issue ID |
|---|----------|
| <p>Azure group properties are not available if added in Office 365 Portal or Hybrid Exchange properties from Send on Behalf attribute for Exchange online Users.</p> | 91624 |
| <p>Azure group properties are not available if added in Office 365 Portal or Hybrid Exchange properties from forwarding address attribute for Exchange online Users.</p> | 98186 |
| <p>Bulk operation on attributes are not reflected immediately on the Web Interface list of objects pane after the operation.</p> <p>Workaround</p> <p>Refresh the page to view the values.</p> | 116287 |

| Known Issue | Issue ID |
|---|----------|
| In the Advanced Database Properties window of Configuration Center, when an invalid value is entered in the Connection timeout field, a validation error message box is displayed. It is not possible to close the message. | 98159 |
| Workaround | |
| Close the complete Advanced Database Properties window and re-open to ignore the error. | |
| An EXO V2 prerequisite warning is displayed in the ARS installer and system checker, if the default path %ProgramFiles%\WindowsPowerShell\Modules is missing in the PsModulePath environment variable. | 231231 |
| Workaround | |
| Add %ProgramFiles%\WindowsPowerShell\Modules in the beginning of the PsModulePath environment variable. | |
| By default, O365 License "Microsoft Search" is assigned to the user after assigning a license to that particular user. | 229032 |

Table 14: Synchronization service known issues

| Known Issue | Issue ID |
|---|-------------------|
| Requires a configured database and then try again error is displayed in Synchronization service when the box is rebooted. | 91738 |
| After executing the get-qcworkflowstatus cmdlet in the Synchronization service, the workflow status is not accurate. | 125768 |
| When Synchronization service is run from Command line with the option SyncService.msi INSTALLSYNCSHELL=0 or by running the SyncService.msi directly, some of the registry keys are not cleared even after uninstallation. | 222131 and 222327 |
| WORKAROUND | |
| Run the following script in PowerShell with administrative privileges where synchronization service is installed and restart the system: | |
| <pre>write-host "Clearing registry keys for sync service" if(Test-Path -Path "Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ARSyncSvc") { Write-Host 'Clearing sync service...'; Remove-Item -Path Registry::HKEY_LOCAL_</pre> | |

```
MACHINE\SYSTEM\CurrentControlSet\Services\ARSyncSvc
}

if (Test-Path -Path "Registry::HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Services")
{
Write-Host 'Clearing sync service configuration...';
set-itemproperty -path "Registry::HKEY_LOCAL_MACHINE\SOFTWARE\One
Identity\Active Roles\Configuration\SyncService" -Name "Configured" -Value
"0"
}

Write-Host -NoNewLine 'Press any key to continue...';
$null = $Host.UI.RawUI.ReadKey('NoEcho,IncludeKeyDown');
```

System requirements

Before installing Active Roles 7.4.3, 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 15: Administration Service requirements

| Requirement | Details |
|--------------------------|--|
| Platform | <p>Any of the following:</p> <ul style="list-style-type: none">• Intel 64 (EM64T)• AMD64• Minimum 2 processors• Processor speed: 2.0 GHz or faster <p>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.</p> |
| Memory | <p>A minimum of 4 GB of RAM.</p> <p>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.</p> |
| Hard disk space | 100 MB or more of free disk space. |
| Operating system | <p>You can install Administration Service on a computer running:</p> <ul style="list-style-type: none">• 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 <p>NOTE: Active Roles is not supported on Windows Server Core mode setup.</p> |
| 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 | <p>You can host the Active Roles database on:</p> <ul style="list-style-type: none">• Microsoft SQL Server 2019, any edition• Microsoft SQL Server 2017, any edition• Microsoft SQL Server 2016, any edition |

| Requirement | Details |
|--|---|
| | <ul style="list-style-type: none"> • 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 | <p>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:</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 <p>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.</p> <p>NOTE: Active Roles is not supported on Windows Server Core mode setup.</p> |
| Exchange Server | <p>Active Roles is capable of managing Exchange recipients on:</p> <ul style="list-style-type: none"> • Microsoft Exchange Server 2019 • Microsoft Exchange Server 2016 • Microsoft Exchange Server 2013 • Microsoft Exchange Server 2010 Service Pack 3 • Microsoft Exchange 2013 CU11 is no longer supported. Refer KB article 202695. |
| Visual C++ Redistributables | Visual C++ 2017 Redistributable |

Web Interface

Table 16:
Web Interface requirements

| Requirement | Details |
|----------------------------|--|
| Platform | Any of the following: <ul style="list-style-type: none">• 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 | <p>You can install Web Interface on a computer running:</p> <ul style="list-style-type: none">• 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 <p>NOTE: Active Roles is not supported on Windows Server Core mode setup.</p> |
| 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 |
| Internet Services | <p>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:</p> <ul style="list-style-type: none">• Web Server/Common HTTP Features/• Default Document• HTTP Errors• Static Content• HTTP Redirection |

| Requirement | Details |
|---------------------------|--|
| | <ul style="list-style-type: none"> • 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 <p>Internet Information Services (IIS) must be configured to provide Read/Write delegation for the following features:</p> <ul style="list-style-type: none"> • Handler Mappings • Modules <p>Use Feature Delegation in Internet Information Services (IIS) Manager to confirm that these features have delegation set to Read/Write.</p> |
| Web browser | <p>You can access Web Interface using:</p> <ul style="list-style-type: none"> • Firefox 36 on Windows • Google Chrome 61 on Windows • Windows Internet Explorer 11 • Microsoft Edge on Windows 10 <p>You can use a later version of Firefox, Google Chrome or Internet Explorer to access Web Interface; however, Web Interface 7.4.3 has been tested only against the browser versions listed above.</p> |
| Minimum screen resolution | <p>Web Interface is optimized for screen resolutions of 1280 x 800 or higher. The minimum supported screen resolution is 1024 x 768.</p> |

Console (MMC Interface)

Table 17: Active Roles Console requirements

| Requirement | Details |
|----------------------------|---|
| Platform | Any of the following: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 7 Ultimate, Professional, or Enterprise edition, 32-bit (x86) or 64-bit (x64) Service Pack 1 • Microsoft Windows 10, Professional or Enterprise edition, 32-bit (x86) or 64-bit (x64) <p>NOTE: Active Roles is not supported on Windows Server Core mode setup.</p> |
| Microsoft .NET Framework | Active Roles console 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 |
| Web browser | Active Roles console requires Internet Explorer 11. |

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 18: Management Tools requirements

| Requirement | Details |
|------------------------------|--|
| Platform | Any of the following: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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) <p>NOTE: Active Roles is not supported on Windows Server Core mode setup.</p> |
| 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 |

| Requirement | Details |
|---|--|
| | (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 19: Synchronization Service requirements

| Requirement | Details |
|------------------|--|
| Platform | Any of the following: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 |

| Requirement | Details |
|------------------------------|--|
| | <p>NOTE: Active Roles is not supported on Windows Server Core mode setup.</p> |
| 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 | <p>You can host the Synchronization Service database on:</p> <ul style="list-style-type: none"> • 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 | <p>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).</p> |
| Supported connections | <p>The Synchronization Service can connect to:</p> <ul style="list-style-type: none"> • 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, 2013, or 2010 <p>NOTE: Microsoft Exchange 2013 CU11 is no longer supported. Refer KB article 202695.</p> <ul style="list-style-type: none"> • 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. |

| Requirement | Details |
|---|---|
| | <ul style="list-style-type: none"> • 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, MY SQL 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 | <p>To connect to the Office 365 directory, the following module must be installed on the computer running the Synchronization Service:</p> <ul style="list-style-type: none"> • Azure Active Directory Module for Windows PowerShell <p>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.</p> |
| 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 must be installed on the computer running the Synchronization Service. For installation instructions, see |

| Requirement | Details |
|------------------------------------|---|
| | "Windows PowerShell Module for Skype for Business Online" at http://go.microsoft.com/fwlink/?LinkId=294688 . |
| 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 20: 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 | <p>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.</p> <p>The domain controllers on which you install Sync Service Capture Agent must run one of the following operating systems with or without any Service Pack (both x86 and x64 platforms are supported):</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 |

Requirement

Details

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 7.4.3 Synchronization Service Administration Guide*.

Upgrade and compatibility

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 21: Version upgrade compatibility chart

| Source version | Destination version |
|----------------|---------------------|
| 6.9.0 | 7.4.3 |
| 7.0 | 7.4.3 |
| 7.1 | 7.4.3 |
| 7.2 | 7.4.3 |
| 7.3 | 7.4.3 |

Impact on Office 365 add-on

After an upgrade of Active Roles components to the Active Roles 7.4.3, the Office 365 add-on which was supported in the earlier versions of Active Roles, ceases to work. Hence, it is recommended to uninstall the Office 365 add-on prior to the upgrade of Active Roles.

NOTE: Office 365 add-on is not supported on Active Roles 7.4.3 and must be uninstalled prior to the installation of Active Roles 7.4.3.

Active Roles 7.4.3 manages Office 365 and Azure AD natively. However, Active Roles 7.4 does not support the following feature of Office 365 add-on that were supported in earlier versions of Active Roles:

- Ability to manage and select Office 365 domains through policies.

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

Copyright 2020 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC.

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.



Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

-  **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.