One Identity Active Roles 7.5.3

How-To Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Active Roles How-To Guide
Updated - April 2022
Version - 7.5.3

Contents

What's New

For detailed information about new features, see the latest *Active Roles What's New Guide*.

What's new in Active Roles 7.5.3

This section provides a summary of the new features included in Active Roles. For detailed information about new features, see the latest *Active Roles What's New Guide*.

Major new features in Active Roles Version 7.5:

- Support for Microsoft Modern Authentication in the Active Roles Synchronization Service. Active Roles version 7.5 adds support for Modern Authentication when configuring the O365 Connector or the Azure BackSync operation of the Active Roles Synchronization Service, superseding the former Azure Admin user name and password-based authentication.

  NOTE: Consider the following when using this feature:

  - The SharePoint Online and Microsoft Skype for Business Online services are deprecated and no longer supported by the O365 Connector.
  - After creating a new client secret in the Azure Admin Portal, it may take up to 15 minutes until the client secret is synchronized and can be queried by the Active Roles Synchronization Service when creating the new O365 Connector.

Major new features in Active Roles Version 7.4.4:

- Support for cloud-only users and cloud-only contacts.
- Support for Microsoft SQL Server 2019.

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.

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, confirming 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 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 environment 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.

Enhancements

- Support for the **multiSubnetFailOver** feature of MS SQL Server to maximize internal availability.
- Support for Archive Mailbox-Exchange Online functionality.
- Support for the Security Identity Mappings functionality as available in Active Directory Users and Computers (ADUC) Snap-in.
- 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.

- Restrict MMC interface access to users, by enabling the MMC Interface access settings using the Configuration Center. By default, on installing Active Roles, all users are enabled to log in to the MMC interface. You can now enable the MMC interface access setting to restrict users from accessing the MMC interface.
- Enhancement of SPML operation to get ObjectSid to retrieve the value in the SID format along with the base64Binary format.
- Creation of OneDrive for Azure AD users using OneDrive Provisioning Policy.
- Configuring secure communication for Active Roles Web interface using Force SSL Redirection.

What's new in Active Roles 7.3

This section provides a summary of the new features included in Active Roles Version 7.3. For detailed information about new features, see the *Active Roles 7.3 What's New Guide*.

Major new features in Active Roles Version 7.3:

- Support for One Identity Hybrid Subscription
- Support for Hybrid Directory Mailbox Management
- Support for Microsoft SQL Server 2017
- Support for connecting to One Identity Starling, the Software as a Service (SaaS) solution of One Identity through Active Roles
- Integration of Starling Two-factor Authentication with Active Roles through the Web interface
- Support for customizing Microsoft Office 365 license related operations on User provisioning and deprovisioning
- Enhancements
    - Display the number of members in a Group in the Web interface
    - SPML Extension Enhancement to Modify Shared Mailbox User permissions
    - Back Sync Improvements
    - Sync Service enhancements
    - Password generation policy enhancement
    - Web interface security enhancements
    - Enhanced Web interface accessibility for disabled users

What's new in Active Roles from version 7.0

The following features are new in Active Roles as of version 7.0

- Web Interface has been redesigned for greater clarity and ease of use, to ensure consistent look and feel, improve user experience, and simplify and streamline management tasks.
- A new component, Synchronization Service, performs data synchronization and replication tasks to enable user, group, or recipient management across various on-premises systems and in the cloud.
- Integrated administration of users and mailboxes in Exchange resource forest environments, with the ability to create and administer mailboxes by managing mailbox users in external forests.
- Integrated administration of Lync Server users in single and multi-forest environments, with the ability to enable, disable or re-enable users for Lync Server and administer Lync Server user properties.
- Various improvements to Active Roles workflow, including new activities to help access and modify workflow data context at run time, new activity options, and workflow scripting capabilities.
- Support for Exchange 2010 remote Shell removes the need to install the Exchange 2010 Management Tools on the computer running the Active Roles Administration Service.
- Active Roles Configuration for Hybrid Environment.
- Azure AD /Office 365 Object Management in Hybrid Environment.
- Microsoft Office 365 License Management.
- Support for Microsoft Windows Server 2016.
- Support for Microsoft SQL Server 2016.
- Support for Microsoft Exchange 2016.
- Support for Microsoft .Net 4.6.2.
- Active Roles facilities a new attribute namely '**OperationInitiatorSid**' under the $Request object, which provide the SID of the initiator who requested the operation. This enhances the current Active Roles - Change Auditor integration capability to display the correct initiator information.
- Support for managing Skype for Business through Active Roles.
- Active Roles in-place upgrade enhancements.
- Limited support for Exchange Online.
- Management of Azure AD Contacts.
- Management of Azure AD Distribution groups.

- Enhancements to Azure Active Directory and Office 365 functionality:
  - Azure License Reporting.
  - Visual indicator for Azure configuration status.
  - Granular license customization.
  - Support for synchronized identity environments.
  - Azure Application permissions enhancements.
  - Support for creating users, groups, and contacts in Azure/Office 365 through SPML.

Changes to Setup and Installation

Active Roles introduces the following changes to Setup and Installation:

Unified Setup Wizard

Table 1: Changes to Unified Setup wizard

Version 6.9 and earlier	Version 7.3 or later
Numerous MSI files	Single ActiveRoles.EXE
The components must be installed in the correct order.	

Silent Install

The Active Roles installer, **Setup.exe** has command-line options for a silent installation. For more details, refer to KB 185799

Example:

```
Setup.exe /quiet /install ADDLOCAL=Service,Console /IAcceptActiveRolesLicenseTerms
```

Configuration Center

The Configuration Center unifies management of core configuration for the Active Roles Administration Service and Web Interface, which allows administrators to perform the core configuration tasks from a single location.

Highlights include:

- Initial configuration tasks such as creation of Administration Service instances and default Web Interface sites.
- Import of configuration and management history from earlier Active Roles versions.
- Management of core Administration Service settings, such as the Active Roles Admin account, service account, and database connection.

- Creation of Web Interface sites based on site configuration objects of the current Active Roles version or site configuration objects imported from earlier Active Roles versions.
- Management of core Web Interface site settings, such as the site's address on the Web server and configuration object on the Administration Service.
- Scriptable Configuration Center operations using Windows PowerShell command-line tools provided by the Active Roles Management Shell.

The following two methods are available for configuring the Active Roles instance:

- Graphical User Interface (Active Roles Configuration Center)
- PowerShell (Active Roles Management Shell)

Management Shell Integration

The Active Roles Management Shell, which provides Windows PowerShell based command-line tools (cmdlets) for executing and automating administrative tasks in Active Roles, is a part of the Management Tools component included in the Active Roles Setup.

Modules:

- ActiveRolesManagementShell
- ActiveRolesConfiguration

ActiveRolesManagementShell

- Provides cmdlets for managing users, group, computers, and other objects in Active Directory via Active Roles; managing digital certificates; and administering certain Active Roles objects.
- Cmdlets are prefixed with QAD or QARS, such as `New-QADUser`, `Add-QADCertificate`, or `New-QARSAccessTemplateLink`.

ActiveRolesConfiguration

- Provides cmdlets for configuring Active Roles Administration Service instances and Web Interface sites.
- Available on 64-bit (x64) systems only. It requires the Active Roles Administration Service or Web Interface to be installed; otherwise, the module does not provide all cmdlets.
- The cmdlets provided in this module have their noun prefixed with AR, such as `New-ARDatabase`, `New-ARService`, or `New-ARWebSite`.

3

Changes to System requirements and Supported platforms

Active Roles introduces the following changes to system requirements:

- Active Roles can no longer be installed on Window Server 2008.
- Microsoft SQL Server 2005 is no longer supported. Microsoft SQL Server versions 2012 and later including 2019 are supported. The Configuration Center may be used to import Active Roles databases from SQL Server 2012 to a later SQL Server version. For details, see "Upgrading the Administration Service" in the Active Roles Quick Start Guide.
- Active Roles supports Google Chrome, Mozilla Firefox, and Microsoft Edge web browsers only. Internet Explorer is no longer supported.
- Web Interface is optimized for screen resolutions of 1280 x 800 or higher. The minimum supported screen resolution is 1024 x 768.

Active Roles 7.3 introduces the following changes to supported platforms:

- Exchange 2010 and earlier versions are no longer supported.
- Microsoft Exchange 2013 CU11 is not supported.

System Requirements

For the complete system requirements, please refer the latest *Active Roles Release Notes*. The following are the important system requirements for Active Roles installation:

- Operating Systems Supported for Active Roles installation: Microsoft Windows 2008 R2 and later, including 2019
- SQL Server requirements: Microsoft SQL 2012 through SQL 2019
- Microsoft .NET Framework: .NET 4.7.2
- Other software required for Active Roles may be installed from the Redistributables folder on the installation media.

Resource Usage

The sizing of disk space and the SQL database capacities are best planned out by using the **Resource Usage Calculator**, which is found in the Documentation folder on the installation disk or image.

The **Resource Usage Calculator** is included with the installation media and can be found under:

Documentation\ ActiveRoles_7.4_ResourceUsageCalc.xls

For more information on the system requirements, please see the Pre-Installation and Upgrade section for the Active Roles Diagnostic and System Readiness Checker tools.

Ports Used by Active Roles

If the environment managed by Active Roles is located behind a firewall, then the following ports must be open between Active Roles Administration Service and the managed environment:

Access to DNS Servers

- Port 53 TCP/UDP Inbound/Outbound

Access to domain controllers

- Port 88 (Kerberos) TCP/UDP Inbound/Outbound
- Port 135 (RPC endpoint mapper) TCP Inbound/Outbound
- Port 139 (SMB/CIFS) TCP Inbound/Outbound
- Port 445 (SMB/CIFS) TCP Inbound/Outbound
- Port 389 (LDAP) TCP/UDP Outbound
- Port 636 (LDAP SSL) TCP Outbound
- Port 3268 (Global Catalog LDAP) TCP Outbound

This port is required if Active Roles is configured to access the domain by using SSL.

- Port 3269 (Global Catalog LDAP SSL) TCP Outbound

This port is required if Active Roles is configured to access the domain by using SSL.

- The TCP port allocated by RPC endpoint mapper for communication with the domain controller

Active Directory domain controllers can be configured to use specific port numbers for RPC communication. For instructions, see http://support.microsoft.com/kb/224196.

Access to Exchange servers

- Port 135 (RPC endpoint mapper) TCP Inbound/Outbound
- The TCP port allocated by RPC endpoint mapper for communication with the Exchange server

Exchange servers can be configured to use specific port numbers for RPC communication. For instructions, see http://support.microsoft.com/kb/270836.

Computer resource management

- Port 139 (SMB/CIFS on the managed computers) TCP Inbound/Outbound
- Port 445 (SMB/CIFS on the managed computers) TCP Inbound/Outbound

Computer restart

- Port 139 (SMB/CIFS on the managed computers) TCP Inbound/Outbound
- Port 137 (WINS) UDP Outbound
- Port 138 (NetBIOS datagrams) UDP Outbound

Home folder provisioning and deprovisioning

- Port 139 (SMB/CIFS on the servers that host home folders) TCP Inbound/Outbound
- Port 445 (SMB/CIFS on the servers that host home folders) TCP Inbound/Outbound

Access to SMTP server for e-mail integration

- Port 25 (Default SMTP port) TCP Outbound

Active Roles uses SMTP port 25 by default. The default port number can be changed in the properties of the Mail Configuration object in the Active Roles console. If Mail Configuration specifies a different port, open that port rather than port 25.

Access to AD LDS instances

- The TCP port specified when registering the AD LDS instance with Active Roles

Access to SQL Server

If SQL Server that hosts the Active Roles database is located behind the firewall, open the following ports between Active Roles Administration Service and SQL Server:

- Port 1433 (Default SQL Server instance) TCP Inbound/Outbound

Open this port if the Active Roles database is on the default instance of SQL Server. If a different port is assigned to the default instance, open that port rather than port 1433.

- Port 1434 (SQL Server Browser service) UDP Inbound/Outbound

Open this port if the Active Roles database is on a named instance of SQL Server. In this case Active Roles uses UDP port 1434 to determine the port assigned to the named instance, open port 1434 along with the TCP port assigned to the named instance.

Access to Active Roles Administration Service

If a firewall is required between Active Roles clients, such as MMC Interface, Web Interface, ADSI Provider or Management Shell, and Active Roles Administration Service, open the following ports in the firewall:

- Port 15172 TCP Inbound/Outbound

Access to Web Interface

If the Active Roles Web Interface will be accessed through a firewall, open the following ports:

- Port 80 (Default HTTP) TCP Inbound/Outbound
- Port 443 (Default HTTPS) TCP Inbound/Outbound

The Web Interface normally runs over port 80, or over port 443 if SSL is enabled (off by default).

Synchronization Service

The Synchronization Service requires the following port to be open:

- Port 15173 TCP Outbound

The Capture Agent requires this port to be open (on the Domain Controller):

- Port 7148 TCP Inbound

Required Permissions and Access

As Active Roles performs operations on objects on behalf of delegated users, the Active Roles service account requires adequate permissions. It is recommended that the Active Roles proxy account be given the Domain Admin membership to ensure that Active Roles has all the required access.

It is possible to separate the tasks managed by the service account from Domain management by specifying distinct accounts for the service and for managing the Domain.

The service account credential has five main roles, two of which are optional:

- Accessing local resources on the Active Roles Administration Service host
- Creating the Service Connection Point in Active Directory - This functionality is not critical and does not prevent the service from functioning as expected, instead, Active Roles clients does not automatically discover the Active Roles Administration Service. Active Roles Clients will still be able to connect if the service name or IP address is available.
- All script modules are executed under the security context of the Active Roles Service Account.
- Connecting to the Microsoft SQL database - This is optional, as an SQL Authentication credential can also be specified.
- Synchronizing native permissions to Active Directory - This is required only if Active Roles is configured to do so.

NOTE: Contact One Identity Sales for any assistance in engaging One Identity Professional Services.

Access to the Administration Service Computer

The service account must be a member of the local Administrators group on the computer running Active Roles Administration service.

Service Publication in Active Directory

For Active Roles clients to discover available Active Roles services, the service account must be able to publish itself in Active Directory. On the One Identity sub-container, under the System container in the domain, grant the following rights:

- Create Container Objects
- Create ServiceConnectionPoint Objects

Access to Managed Domains

The service account must have at least Read Permissions in any Managed Domain. In addition, the service account must have Modify Permissions rights on the Active Directory objects and containers where the Active Roles security synchronization feature will be utilized.

Fine-Grained Password Policies

Active Roles needs specific read access to be able to read fine-grained password policy objects in Active Directory (AD). If it is unable to read them, it defaults to using the Default Domain Policy, for example, for password expiry information and password generation.

To enable Active Roles to read fine-grained password policies in AD, you must assign the **List**and **Read** permissions in each managed domain where passwords are managed, on the following container:

```
CN=Password Settings Container,CN=System,DC=<domain>
```

Access to Exchange Organizations

Exchange 2013, 2016, or 2019

To manage Exchange recipients on Exchange Server 2013, 2016, or 2019 the service account or the override account must be configured to have sufficient rights in the Exchange organization. The rights must be delegated to the service account if an override account is not used; otherwise, the rights must be delegated to the override account. For details, see the steps that follow.

To configure the service account or the override account

1. Add the account to the Recipient Management role group. For instructions, see "Manage Role Group Members" at http://technet.microsoft.com/library/jj657492 (exchg.150).aspx.
2. Add the account to the Account Operators domain security group.
3. Enable the account to use remote Exchange Management Shell. For instructions, see "Enable remote Shell for a user" in the topic "Manage Exchange Management Shell Access" at http://technet.microsoft.com/library/dd638078(exchg.150).aspx.
4. Ensure that the account can read Exchange configuration data (see Permission to read Exchange configuration data).
5. Restart the Administration Service after changing the configuration of the account: Start Active Roles Configuration Center (see "Running Configuration Center" in the Active Roles Administrator Guide), go to the Administration Service page in the Configuration Center main window, and then click the Restart button at the top of the Administration Service page.

Permission to read Exchange configuration data

To perform Exchange recipient management tasks, Active Roles requires Read access to Exchange configuration data in Active Directory. This requirement is met if the service account (or the override account, if specified) has administrator rights. For example the service account, is a member of the Domain Admins or Organization Management group. Otherwise, provide the account Read permission in the Microsoft Exchange container, using the ADSI Edit console.

NOTE: The following instructions apply to the ADSI Edit console that ships with Windows Server.

To provide Read access to the service account using the ADSI Edit console:

1. Open the ADSI Edit console, and connect to the Configuration naming context.
2. In the ADSI Edit console, navigate to the Configuration/Services container, right-click **Microsoft Exchange** in that container, and then click **Properties**.
3. On the **Security** tab in the Properties dialog box that appears, click **Advanced**.
4. On the Permissions tab in the Advanced Security Settings dialog box, click **Add**.
5. On the Permission Entry page, configure the permission entry:
    a. Click **Select a principal**, and select the desired account.
    b. Ensure that the **Type** box indicates **Allow**.
    c. Ensure that the **Applies** onto box indicates: **This object and all descendant objects**.
    d. In the Permissions area, select the **List** contents and **Read all properties** check boxes.
    e. Click **OK**.
6. Click **OK** to close the Advanced Security Settings dialog box, and then click **OK** to close the Properties dialog box.

Support for Exchange Remote Shell

When performing Exchange recipient management tasks on Exchange Server 2013 or later, Active Roles uses remote Exchange Management Shell to communicate with Exchange Server. Hence, it is not required to install the Exchange management tools on the computer running the Administration Service.

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

- Windows Server 2016 or a later version of the Windows Server operating system.
- Microsoft .NET Framework 4.5 installed (see "Installing the .NET Framework 4.5, 4.5.1" at https://msdn.microsoft.com/library/5a4x27ek%28VS.110%29.aspx).
- Windows Management Framework 3.0 installed (see "Windows Management Framework 3.0" at https://www.microsoft.com/en-us/download/details.aspx?id=34595).

Remote Shell also requires the following:

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

6

Product Licensing

After installing Active Roles 7.x (or upgrade to Active Roles 7.x), no additional steps are required to activate the purchased commercial license for Active Roles.

Product usage statistics may be used to verify Active Roles licensing compliance. For further details, see Evaluating Product Usage in the *Active Roles Administrator Guide*.

Pre-Installation and Upgrade

Active Roles 7.5.3 supports a direct upgrade from versions 6.9 and later, including 7.2.1.

NOTE: If customizations have been implemented by One Identity Professional Services, please contact One Identity Sales before proceeding with an installation or upgrade, as all customizations may not function with newer versions.

Installing Active Roles Diagnostic Tools

To install Active Roles Diagnostic Tools

1. Install the Active Roles Diagnostic Tools, which consists of Active Roles System Checker, which should be run in order to confirm that the server has adequate resources to host and run Active Roles. Navigate to the installation media.
2. Go to **Solutions** | **Diagnostic Tools**.
3. Double-click to run **ActiveRolesDiagnosticsTools_1.4.1.msi**.

   The Active Roles Diagnostic Tools Setup Wizard is displayed.
4. Click **Next**.
5. In the License Terms window, read and accept the license agreement and click **Next**.
6. In the Custom Setup window, select the appropriate tools to install. It is recommended to install the Active Roles Log Viewer, Directory Changes Monitor, and the Active Roles System Checker for later use. Click **Next**.
7. In the Ready to Install window, click **Install**.
8. After the tools are installed, click **Finish**.

Checking System Readiness

To check the system readiness

1. From the Windows Applications, **Start Menu**, select Active Roles System Checker.

   The Active Roles System Checker window is displayed.

2. Select **Computer** | **System Readiness Checks**.
3. In the Confirm System Readiness Checks window, select the appropriate components to check for and click **Check**.
4. In the System Readiness Checks window, review the summary and confirm that the computer has passed the required checks. Take appropriate action before installing Active Roles. For example, if there is a warning about insufficient Memory (RAM), then upgrade the Memory to the recommended amount.
5. In the Active Roles System Checker, select **SQL Server Checks** under **Environment**. Enter the SQL Server name and appropriate credentials for the Active Roles service account and click **Check**.
6. Review the summary to confirm that the SQL Server passed the checks.
7. In the Active Roles System Checker, select **Active Directory Checks** under **Environment**. Enter the Domain Controller name and appropriate credentials for the Active Roles service account and click **Check**.
8. Review the summary to confirm the account has adequate permissions in Active Directory.

   In this example, the checker found Exchange in the environment. Active Roles service account is not a member of the Exchange groups and therefore must be added appropriately in order to administer Exchange-related tasks in Active Roles.

   A progress window is displayed. After completion, the summary is displayed.

9. On this screen, click the **Additional Resources** link to learn more about Active Roles. Click **Finish**.

Clean Installation

For an installation demonstration, please refer to the following knowledge base article:
https://support.oneidentity.com/kb/258459

Installing the Active Roles service

To install the Active Roles service

1. Run **ActiveRoles.exe**.
2. Accept the licensing agreement and click **Next**.
3. Select the desired components and click **Next**.
4. Review the summary and click **Install**.

   By default, the **I want to perform configuration** option is selected.
5. Click **Finish** to launch the Configuration Center.
6. Under the **Administration Service** option, click **Configure**.
7. Select a service account that will run the Active Roles service and click **Next**.
8. Choose the appropriate security group that will hold the role of the Active Roles Admin group and click **Next**.
9. If this is the first installation of Active Roles, select New Active Roles database and click **Next**.
10. Enter the appropriate SQL server, database name and credentials. Click **Next**.
11. After completing, click **Finish**.

Installing the Web interface

To install the Active Roles Web interface

1. Launch the Active Roles Configuration Center.
2. Click **Dashboard**.
3. Click **Configure** under the Web Interface section.
4. Select the appropriate service to connect to and click **Configure**.
5. After completing, click **Finish**.

Upgrade from Active Roles 6.9

Upgrading from Active Roles 6.9 to 7.x version is a side-by-side upgrade, which does not interrupt operations or affect the configuration of the currently installed Active Roles version. To ensure smooth upgrade to the new Active Roles version, upgrade the Administration Service first, and then upgrade the Web Interface.

Active Roles 6.9 components are not used in the upgrade and neither are any components from the earlier version uninstalled.

Before upgrading to the latest version of Active Roles, the add-ons of the earlier versions must be uninstalled.

Impact on Office 365 Add-On

- After an upgrade of Active Roles components to Active Roles 7.5.3, 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.
- Office 365 add-on is not supported on Active Roles 7.3 or later and must be uninstalled prior to the installation of Active Roles 7.1.
- Active Roles 7.5.3 manages Office 365 and Azure AD natively.

For an upgrade demonstration, please refer to the following knowledge base article:

https://support.oneidentity.com/kb/257995

Prerequisites for Active Roles 6.9 upgrade

Before any upgrade is performed, first consider the following:

- There is no need to break replication when upgrading to Active Roles 7.5.3 from 6.9 as Active Roles 7.3 or later does not support an in-place upgrade in this scenario. A

side-by-side installation of Active Roles must be performed and replication must be configured post installation on the new instance of Active Roles.

> NOTE: During and post-installation of Active Roles 7.5.3, the existing installation of Active Roles 6.9 will be available and fully functional. Hence, users will not be affected during the upgrade process with the exception of Dynamic Groups. For more details please review the knowledge base article, https://support.oneidentity.com/kb/211388.

- An upgrade of the Active Roles components may affect custom solutions. Custom solutions (such as scripts and other modifications), which work fine as expected with an earlier version of Active Roles may cease to work after the upgrade. Before starting an upgrade, test the existing solutions with the new version of Active Roles in a lab environment to verify that the solutions continue to work as expected after the upgrade.
- If ERFM (Exchange Resource Forest Management) is installed on the Active Roles 6.9 version, it must be uninstalled before installing 7.5.3 as ERFM is now part of the product. Failure to uninstall ERFM beforehand may result in conflicts and issues.
- If Lync Add-On is installed, it must be uninstalled before installing Active Roles 7.5.3 as Lync is now an integrated product feature.
- If Office 365 Add-On is installed, it must be uninstalled before installing Active Roles 7.5.3 as this functionality is replaced with the inbuilt Azure Active Directory Hybrid Integration.
- For additional information, please review Solution 111679:

  https://support.oneidentity.com/kb/111679
- Due to the design changes implemented in Active Roles 7.x in the Web Interface, any Web Interfaces and customizations from Active Roles 6.9 may not function in Active Roles 7.5.3. It is recommended not to import. Please refer to KB 189186 for additional information:

  https://support.oneidentity.com/kb/189186

To perform the Upgrade

1. From the installation media, run **ActiveRoles.exe**.
2. Accept the licensing agreement and click **Next**.
3. Select the desired components and click **Next**.
4. Review the summary and click **Install**.
5. By default, the **I want to perform configuration** option is selected. Click **Finish** to launch the Configuration Center
6. In the Configuration Center, under the Administration Service option click **Configure**.
7. Select a service account that will run the Active Roles service and click **Next**.
8. Choose the appropriate security group that will hold the role of the Active Roles Admin group and click **Next**.

9. If this is the first installation of Active Roles, select New Active Roles database and click **Next**.
10. Enter the appropriate SQL server, database name and credentials. Click **Next**.
11. After completing, click **Finish**.
12. In the Configuration Center, under Dashboard click **Import Configuration**, specify the Source SQL server, database and access credentials, and then click **Next**.
13. Click **Next**.
14. If the current version of Active Roles service is running, stop it and then click **Next** to continue.
15. If you have the encryption key, provide it. If not, select **Do not import encrypted data** and click **Next**.
16. If you do not have the encryption key, you must re-enter the credentials for any Managed Domains, which are not managed by the Active Roles Service account.

    The Add-On Advisor checks if there are any incompatible Add-Ons installed the Wizard will not proceed. Before continuing, uninstall the Add-Ons from the Active Roles 6.9 server.
17. Click **Next**.
18. Once ready, click **Import**.

Importing Change History

The Change History from Active Roles 6.9 database is not imported during the initial import, as the Change History may be extremely large and thus would take a long time for the initial Setup to complete. Active Roles provides a separate utility for importing Change History.

1. In the Active Roles Configuration Center, click **Import Management History** under **Administration Service**.
2. Enter the Active Roles 6.9 source database and appropriate credentials and click **Next**.
3. Select the destination database and click **Next**.
4. Choose the records to import and click **Next**.
5. Confirm the settings and click **Import**.

   The progress screen is displayed, and after completion, the summary is displayed.

In-place upgrade from Active Roles 7.x

This section describes the main steps of performing an in-place upgrade from an earlier version of Active Roles 7.x.

Backing up the Active Roles Database

Before upgrading, it is recommended to back up the Active Roles database. For general best practices, please refer to the following Microsoft article:

https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server

Prerequisites for in-place upgrade from Active Roles 7.x

It is recommended to back up the current Web Interfaces if any customizations have been implemented.

Any Web Interfaces that were created in Active Roles 7.2.x will continue to function in 7.5.3. However, it is recommended to thoroughly test before upgrading, as some customizations may not work as expected in newer versions of Active Roles.

To back up the Web Interface Configurations

1. Launch the Active Roles Configuration Center.
2. Click **Web Interface**.
3. Select the desired site(s) and click **Export Configuration**.

To upgrade Active Roles

1. Run **ActiveRoles.exe** from the installation media.
2. Click **Next** to continue.
3. Accept the license agreement and click **Next**.
4. Review the summary and warning. If the Office 365 Add-On is installed in the 7.0.x instance, uninstall it before continuing.

5. If the system does not restart, click **Update Service Instance** in the Configuration Center.
6. If the system restarts and the Configuration Center does launch automatically, launch the Configuration Center and click **Update Service Instance**.

   Due to the update of the database schema, the 7.0 versions of the Websites are no longer compatible.
7. Click **Manage Sites** under **Web Interface** in the Configuration Center.
8. Make note of the current websites and configurations used (For example, ARWebAdmin, using configuration "Site for Administrators").
9. Delete all the sites and click **+Create.**
10. Enter the Alias of the site, for example ARWebAdmin and click **Next**.
11. On the Configuration screen, ensure **Create** from a template is selected.
12. Enter a Configuration name, select the original Template to import from (for example, "Site for Administrators 7.0"), and then click **Create**.
13. Click **Finish**.

11

Synchronization Service

Formerly a standalone product called Quick Connect, the Synchronization Service is now part of Active Roles 7.5.3.

With Synchronization Service, complete automation can be implemented to process data synchronization between the data systems.

Synchronization Service increases the data management efficiency by allowing automation of the creation, deprovision, and update operations between data systems. For example, when an employee joins or leaves the organization, the related information in the data systems managed by Synchronization Service is automatically updated, thereby reducing the administrative workload and getting the new users up and running faster.

In order to synchronize identity data between external data systems, Synchronization Service must be configured to connect to these data systems through connectors. A connector enables Synchronization Service to access specific data system to read and synchronize data in that system according its settings. Out of the box, Synchronization Service includes a number of built-in connectors:

- Active Roles versions 6.9 to 7.5.3
- Identity Manager version 8.1, 8.0, or 7.0
- Quest One Identity Manager version 6.1 or 6.0
- Delimited text files
- Microsoft Active Directory Domain Services
- Microsoft Active Directory Lightweight Directory Services
- Microsoft Azure Active Directory
- Microsoft Exchange Server
- Microsoft Skype for Business Server
- Microsoft Office 365
- Microsoft SharePoint
- Microsoft SQL Server
- OLE DB-compliant relational database
- Generic LDAP Directory service
- MY SQL Database

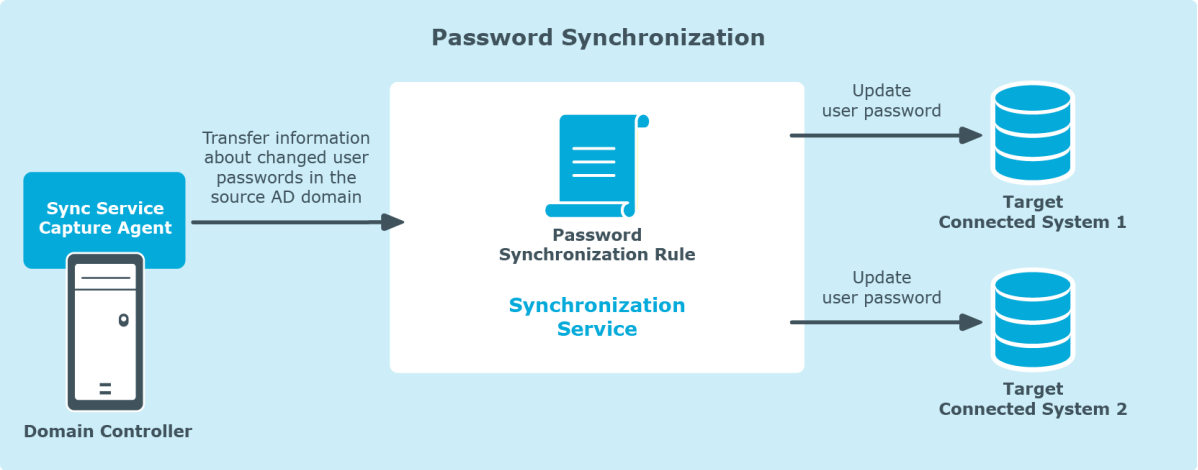
- OpenLDAP Directory service
- Salesforce
- ServiceNow
- IBM DB2 Database
- IBM RACF Connector
- Oracle Unified Directory Connector
- Oracle Database User Accounts Connector
- Oracle Database Connector
- Micro Focus NetIQ Directory Connector
- IBM AS/400 Connector

Figure 1: Technical Overview

Capture Agent

Synchronization Service Capture Agent allows password synchronization between Active Directory domains managed by Synchronization Service and other connected data systems. The following diagram shows how the Password Synchronization feature of Synchronization Service works:

Figure 2: Password Synchronization



Capture Agent tracks changes to user passwords in the source Active Directory domain and provides that information to Synchronization Service, which in turn synchronizes the changes with target connected data systems by using the configured password synchronization rules. To synchronize passwords, install a Capture Agent on each domain controller in the Active Directory source domain.

Upgrade from Quick Connect

If Quick Connect is configured with synchronization workflows that contain similar connector in Synchronization Service, then those synchronization workflows can be transferred to Synchronization Service.

The following synchronization workflows can be transferred from the following Quick Connect versions:

- Quick Connect Sync Engine 5.2.0, 5.3.0, 5.4.x, or 5.5
- Quick Connect Express for Active Directory 5.3.0, 5.4.0, 5.4.1, or 5.5.0
- Quick Connect for Cloud Services 3.3.0, 3.4.0, or 3.5.0
- Quick Connect for Base Systems 2.2.0 or 2.3.0

Limitations

Synchronization Service is unable to run synchronization workflows that employ connections to the following systems:

- ActiveRoles Server 6.5
- Google Apps
- Novell eDirectory
- ODBC-compliant data source
- OpenDS directory service
- Oracle Database
- Oracle User Accounts
- PeopleSoft HCM
- Red Hat Directory Server
- SAP Systems
- Sun One Directory Server
- Workday

If it is necessary to synchronize data held in these systems, continue using Quick Connect as not all connectors provided by Quick Connect are included with Synchronization Service. Alternatively, One Identity Manager may support these systems.

Synchronization Service upgrade

For an upgrade demonstration, please refer to the following knowledge base article:

https://support.oneidentity.com/kb/226332

To upgrade Synchronization Service

1. Install Synchronization Service on the computer running Quick Connect or on a different host.
2. Configure Synchronization Service to use a new database for storing configuration settings and synchronization data. To perform this step, use the Configuration Wizard

that appears when the Synchronization Service Administration Console starts for the first time after installation.

3. Import configuration settings from Quick Connect to Synchronization Service.

   NOTE: Before proceeding with this step, it is highly recommended to disable the scheduled workflows and mapping operations in Quick Connect. The scheduled workflows and mapping operations may be started after this step is completed.

   To import configuration settings:

   a. On the computer where the Synchronization Service is installed, start the Synchronization Service Administration Console.

   b. In the upper right corner of the Administration Console window, click the gear icon, and then click **Import Configuration**.

   c. In the wizard that appears, select the correct version of Quick Connect Sync Engine from which to import the configuration settings. Optionally, the **Import sync history** check box may be selected to import the sync history along with the configuration settings.

   d. Follow the steps in the wizard to complete the import operation. If the synchronization data to be imported is stored separately from the configuration settings, then, on the **Specify source SQL Server databases** step, select the **Import sync data from the specified database** check box, and specify the database.

1. Retype access passwords in the connections that were imported from Quick Connect.

   This is required due to security reasons. The import of configuration settings does not retrieve the encrypted passwords from Quick Connect. Use the Synchronization Service Administration Console to make changes to each connection as appropriate, depending upon the data system to which the connection applies.

2. If the synchronization workflows involve synchronization of passwords, install the new version of Capture Agent on the domain controllers.

   The new version of Capture Agent replaces the old version. However, as the new version supports both Synchronization Service and Quick Connect, the password synchronization functions of Quick Connect will not be lost after the Capture Agent is updated.

Communication Ports

Table 2: Communication ports

Port	Protocol	Type of traffic	Direction of traffic
53	TCP/UDP	DNS	Inbound,

Port	Protocol	Type of traffic	Direction of traffic
			Outbound
88	TCP/UDP	Kerberos	Inbound, Outbound
135	TCP	RPC Endpoint mapper	Inbound, Outbound
139	TCP	SMB/CIFS	Inbound, Outbound
445	TCP	SMB/CIFS	Inbound, Outbound
389	TCP/UDP	LDAP	Outbound
3268	TCP	LDAP	Outbound
3269	TCP	SSL (only required if SSL is used to connect to AD)	Outbound
636	TCP	SSL	Outbound
15173	TCP	Synchronization Service	Inbound, Outbound
7148	TCP	Capture Agent (only if Synchronization Service is used to sync passwords to AD)	Inbound, Outbound

For further information regarding Synchronization Service, refer the latest *Active Roles Synchronization Service Administrator Guide* included with the Active Roles installation media.

Starling Two-Factor Authentication

Active Roles version 7.4.x supports integration with One Identity Starling services. The Starling Join feature in Active Roles now enables you to connect to One Identity Starling, the Software as a Service (SaaS) solution of One Identity. The Starling Join feature enables access to the Starling services through Active Roles thus allowing to benefit from the Starling services such as Two-factor Authentication and Identity Analytics and Risk Intelligence.

To start the wizard, click Configure in the One Identity Starling area on the Dashboard page in the Configuration Center main window. For further information and step-by-step instructions, see the "Initial configuration" topic in the "Installing and configuring the Web Interface" section in the *Active Roles Quick Start Guide*.

A video demonstration is available in the following knowledge base article:

https://support.oneidentity.com/kb/258341

In order to use Starling Two-Factor Authentication with Active Roles, you must first join One Identity Starling to Active Roles on the Active Roles Configuration Center. The Join to One Identity Starling wizard also includes links, which provide assistance for using Starling:

- The Online link displays information about the Starling product and the benefits you can take advantage of by subscribing to Starling services.
- The Trouble Joining link displays the Starling support page with information on the requirements and process for joining with Starling.

14

Reports

Reporting is an optional component of Active Roles. To use Active Roles reports, the following components are required:

- Microsoft SQL Server Reporting Services (SSRS) must be installed and configured.

  NOTE: If the SQL Server service and SRSS are on different hosts, a "Double-Hop" authentication issue may occur. For more information, see the knowledge base article, https://support.oneidentity.com/kb/69693.

- The Active Roles service account must have sufficient permissions to create and write to a database on the SQL Server.

  NOTE: The database cannot be pre-created, and must be created by Active Roles.

- The Active Roles service account must have sufficient permission to publish reports on the SRS server.

  NOTE: Quest Knowledge Portal is no longer included with Active Roles 7.x. To view reports, use the native SQL Server Report URL.

How to configure Reports

Please refer to Video Solution 156240, which demonstrates how to configure Reports in Active Roles:

https://support.oneidentity.com/kb/156240

Can Reports databases be re-used?

The Active Roles 7.x database structure is different than previous versions and therefore old Report databases, such as from Active Roles version 6.9, cannot be used directly.

However, the new Active Roles Collector and Report Pack wizard provides the ability to import events from an earlier database. Simply select Import events from an earlier database version and follow the prompts to import the older Collector database data.

15

Customizations

Custom solutions (scripts or other modifications) may not function properly after an upgrade due to compatibility issues. Prior to attempting an upgrade, test existing customizations with the new version of Active Roles in a lab or test environment to verify that the customizations function as expected. If compatibility issues arise during the test process, please contact One Identity Sales to arrange assistance from One Identity Professional Services.

16

Troubleshooting

The following sections provide information on troubleshooting Active Roles:

- Performance
- Safe Mode

Performance

For Active Roles performance, please refer to the following knowledge base article:

https://support.oneidentity.com/kb/185471

Safe Mode

Active Roles provides a troubleshooting option, referred to as safe mode, which starts the Administration Service in a limited state. When safe mode is enabled, the Administration Service disregards the following:

- Custom policies
- Workflows
- Scripts
- Scheduled tasks
- Other customizations that may block Active Roles from starting and operating normally, and rejects connections from any user other than an Active Roles Admin.

Active Roles Admin can connect to the Administration Service and make changes in order to fix or remove customizations that cause issues, and then disable safe mode.

How to use Safe Mode

1. Log on to the computer running the Administration Service with a user account that has administrator rights on that computer.

   NOTE: Local administrator rights are required to enable or disable safe mode.

2. Open Active Roles Management Shell on the computer running the Administration Service.
3. Click **Active Roles Management Shell** on the Apps page or **Start** menu depending upon the version of the Windows operating system.
4. To enable safe mode, enter the following commands at the Management Shell command prompt:
   - `Set-ARService -SafeModeEnabled $true`
   - `Restart-ARService`
5. To disable safe mode, enter the following commands at the Management Shell command prompt:
   - `Set-ARService -SafeModeEnabled $false`
   - `Restart-ARService`

Error and Log resources

Active Roles writes most events to its own Event log in Windows Event Viewer, under Applications and Services, called **Active Roles Admin Service**.

This event log can be used to help determine root causes for issues and typically provide more detailed error information if any issues are encountered within the console or Web Interface.

In addition to the Event log, there is a debug option for the Active Roles Administration service that is disabled by default. Enabling logging can be accessed either in the Active Roles MMC Console or via the Active Roles Configuration Center.

In addition to the Synchronization Center, the ADSI provider and MMC (console), it is recommended to use the Active Roles Configuration Center as it provides options to enable logging for the Web Interface component. The Log Viewer can then be launched directly from here for any of these logs.

Figure 3: Active Roles Console

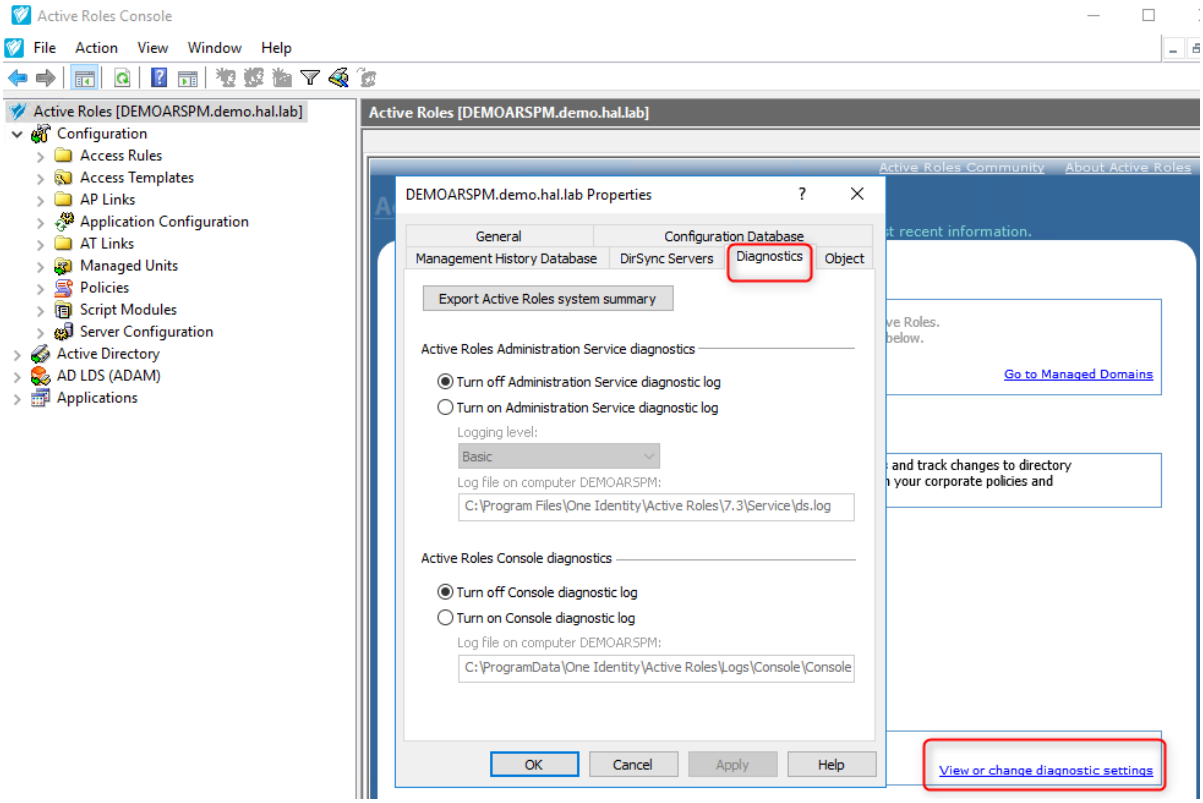
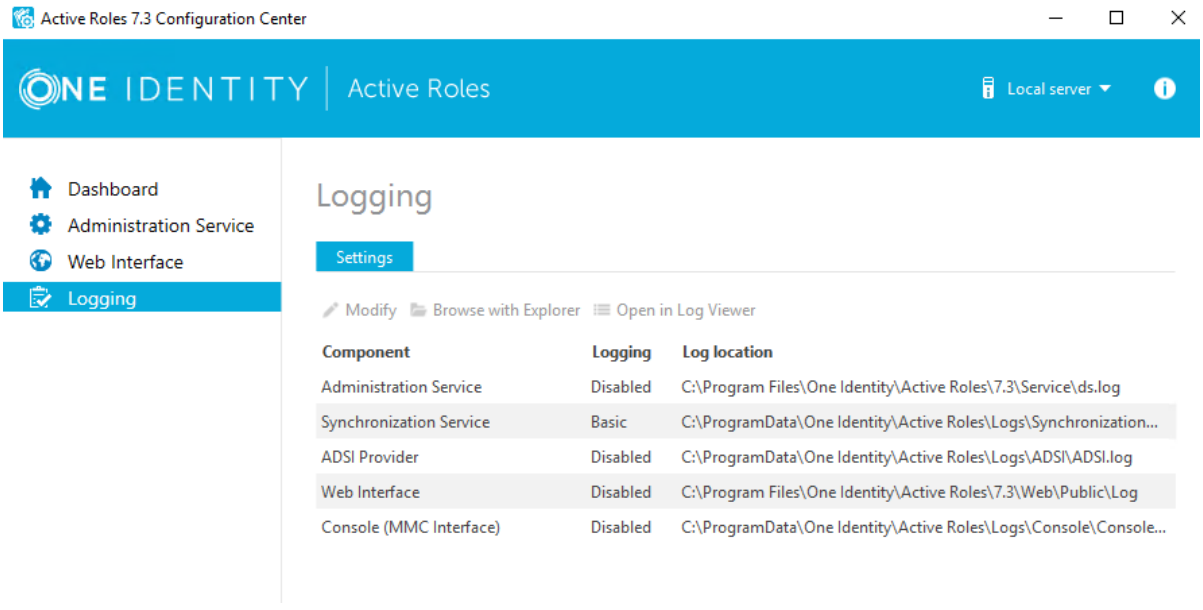


Figure 4: Active Roles Configuration Center



In versions earlier to Active Roles 7.0, after the logs are generated, the logs are sent to One Identity Support for analysis as the logs on their own can be difficult to read.

With Active Roles 7.0 we have provided a new tool called the Active Roles Log Viewer, which breaks down the log to a simple and readable format so that customers can review the logs on their own before engaging One Identity Support.

Active Roles Log Viewer

The Log Viewer tool provides the ability to browse and analyze diagnostic log files created by the Active Roles Administration Service, as well as event log files created by saving the Active Roles event log in Event Viewer on the computer running the Administration Service. Log Viewer helps to study the sequence or hierarchy of requests processed by the Administration Service, identify error conditions that the Administration Service encountered during request processing, and find Knowledge Articles that apply to a given error condition.

With Log Viewer, both Active Roles diagnostic log files (ds.log) or saved event log files (.evtx) can be opened, and the following can be viewed:

- Errors encountered by the Administration Service and recorded in the log file
- Requests processed by the Administration Service and traced in the log file
- All trace records found in the diagnostic log file
- All events found in the event log file

Select an error in the list, and choose a command to look for the solution in Knowledge Base. The command performs a search in One Identity Software Knowledge Base to list the Knowledge Articles that can provide helpful information on how to troubleshoot the selected error. Log Viewer can be used to:

- Search the list for a particular text string, such as an error message
- Filter the list by various conditions, to narrow the set of list items of interest
- View detailed information about each list item, such as error details, request details or stack trace

Log file size

The logs grow in size quickly. Therefore, it is recommended to enable logging right before and disable logging immediately after the issue has been reproduced.

The file captures any activity being performed by the service, including the tasks performed by connected users while debug logging is enabled.

In some scenarios, it may be required to leave the logging on for a specific period of time. Due to the logs getting stored on the computer running Active Roles, sufficient hard drive space may not be available. In this event, the following solution can help to set logging for a specific interval and move the logs to another drive or network share:

- How to automate Active Roles logging (debug):

https://support.oneidentity.com/kb/8617

For the Web Interface, there is a separate log file,<*name of Site*>.log.

The default Location of the Web Interface log is here:

C:\Program Files\One Identity\Active Roles\7.4\Web\Public\Log

As with the ds.log file, the Web Interface log can grow quickly as well. It is recommended to turn it on while reproducing an issue only.

17

Replication

For a video demonstration, please refer to the following knowledge base article:

https://support.oneidentity.com/kb/234198

For additional information and troubleshooting, please refer the latest *Active Roles Administration Guide*.

Understanding Management History

The **Management History** feature provides information on who did what and when it was done with regard to the Active Directory management tasks performed using Active Roles.

This feature provides a clear log, documenting the changes that have been made to a given object, such as a user or group object. The log includes entries regarding actions performed, success or failure of the actions, as well as which attributes were changed.

The Management History feature can be used to examine:

- Change History Information on changes that were made to directory data via Active Roles.
- User Activity Information on management actions that were performed by a given user.

Both Change History and User Activity use the same source of information—the Management History log, also referred to as the Change Tracking log. For information on the configuration settings of the Change Tracking log, see the Management History configuration section.

Active Roles also includes reports to examine management history by collecting and analysing event log records. For more information on reports, see the Active Roles Reporting section. However, the process of retrieving and consolidating records from the event log may be time-consuming and inefficient.

NOTE: You must import the Management History from the old version after an upgrade in order to perform Deprovisioning operations and Undo Temporal Group operations.

Considerations and best practices

The **Management History** feature (also known as **Change History** or **Change Tracking**) is designed to help investigate promptly what changes were recently made to directory data, as well as when it was done and by whom. However, this feature does not provide for data change auditing exploring large volumes of data changes that occurred during a long period of time. For this reason, in addition to the Management History feature, Active Roles provides a suite of reports for change tracking and auditing, which is

part of the Active Roles Report Pack. Each of these options, Management History and Report Pack, has its own advantages and limitations. Follow the recommendations in this section to choose the one that is best suited.

The Management History feature can be used to examine changes that were made to directory data via Active Roles. The feature is designed to help answer the following typical questions:

- Who made the most recent changes to a given user or group object?
- Who modified a given user or group object during the last X days?
- What changes were made to a given user object last night (yesterday, the day before)?
- Have any planned modifications of a given user or group object actually been performed?
- What objects did a given delegated administrator modify during the last X days?

Management History can be accessed instantly whenever an investigation is required or troubleshoot a problem that results from inappropriate modifications of directory data. Management History includes a dedicated repository to store information about data changes, referred to as the Change Tracking log, and GUI to retrieve and display information from that repository. No additional tasks, such as collecting or consolidating information, are required to build Management History results. However, the advantages of the Management History feature also entail some limitations. Before using the Management History feature, consider the following recommended best practices and limitations of using this feature. The main factor to consider is the size of the Change Tracking log. To ensure real-time update of the log on all Administration Services, the log is normally stored in the Active Roles configuration database, but can be separated into its own database if required. This imposes some limitations on the log size. By default, the Change Tracking log is configured to store information about changes that occurred within last 30 days. If the setting is increased, do so carefully; otherwise, the following problems may be encountered:

- Excessive increase in the log size significantly increases the time required to build and display Change History and User Activity results.
- As the log size grows, so does the size of the configuration database. This considerably increases the time required to back up and restore the database, and causes high network traffic replicating the database when an additional Administration Service is joined to Active Roles replication.
- The GUI is not suitable to represent large volumes of Management History results in a manageable fashion. Since there is no filtering or paging capabilities, it may be difficult to sort through the results.

To address these limitations, Active Roles provides different means for change auditing, change-tracking reports, included with the Active Roles Report Pack. These reports are designed to answer the following questions:

- What management tasks were performed on a given object within a certain period of time?

- What management tasks were performed on a given object during the object's entire life time?
- When was a certain attribute of a given object modified?

Change-tracking reports are based on data collected from event logs. A separate log is stored on each computer running the Administration Service, and each log contains events generated by one Administration Service only. Therefore, to use reports, the events from all event logs need to be consolidated to form a complete audit trail. The process of consolidating events, referred to as the data collection process, is performed by a separate Active Roles component—Collector. The Collector wizard can be configured to execute data collection jobs, and schedule them to run on a regular basis. The main limitation of change-tracking reports is the fact that the information needs to be collected and consolidated in a separate database before the reports can be built. The data collection process exhibits the following disadvantages:

- Collecting data may be a very lengthy operation and the database size may grow unacceptable when collecting all events that occurred within a long period of time in a large environment.
- Collecting data is impossible over slow WAN links. This limitation is inherent to the Active Roles component intended to collect data for reporting.

Management History configuration

The configuration of Management History includes the following elements:

- Change-tracking Policy Builds the data pertinent to history of changes made to directory objects, and specifies what changes are to be included in the reports on change history and user activity.
- Change Tracking Log Configuration Specifies how many change requests are to be stored in the log.
- Replication of Management History Data Specifies whether to synchronize Management History data between Administration Services that use different databases.

Reference

Management History is being synchronized, the Active Roles service is unavailable:

https://support.oneidentity.com/kb/103363

Management History Wizard:

https://support.oneidentity.com/kb/90375

Important Considerations

The Management History Migration Wizard was designed for a "one-to-one" database migration for an Active Roles upgrade. It was designed to speed up the upgrade process as

the history migration can be quite lengthy - sometimes in excess of 25 hours (depending on history and environment).

The tool has never been tested in migrating several Management History databases to one. This type of scenario is not supported.

However, the tool can be re-run several times from the same source database in this upgrade scenario. The import for the Management History database is a Merge import and adds any changes to the target Active Roles database.

NOTE: The Configuration database import functionality performs a Replace action. This operation overwrites current settings.

Active Roles stores its configuration data in the Configuration database in SQL. It is recommended to backup Configuration and Management History databases prior to the upgrade.

For more information on upgrade paths, refer to the knowledge base article https://support.oneidentity.com/kb/111679.

Service Account

Active Roles 7.0 introduced the Configuration Center, which provides a simple method for changing or updating the Active Roles service account.

Changing Active Roles service account credentials

To change the Active Roles Administration Service account

1. Launch the Active Roles Configuration Center.
2. Click **Administration Service** tab.
3. Click **Change** on the Service Account.
4. Enter the new credentials and click **Change**.
5. After completing, click **Finish**.

To start using the new credentials, you must restart the service. Restart the service immediately or later, at a more convenient time.

Changing Service account credentials for SQL database connection

To change the account that is used to run the Active Roles Administration Service

1. Launch the **Active Roles Configuration Center**.
2. Click the **Administration Service** tab.
3. On the Active Roles database section, click **Change** .
4. Enter the new credentials and click **Next**.

5. Click **Change** to commit the changes.
6. Click **Finish**.

To start using the new credentials, you must restart the service. Restart the service immediately or later, at a more convenient time.

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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