Active Roles On Demand

Release Notes

30 May 2022

These release notes provide information about the 30 May 2022 release of Active Roles On Demand. For the most recent documents and product information, see the Active Roles On Demand documentation on the *One Identity Support Portal*.

About this release

One Identity Active Roles On Demand is a complete Active Roles installation, provisioned in the One Identity cloud and connected to your network through a virtual private network (VPN). One Identity operates and monitors the runtime environment for you.

This Active Roles On Demand release is a patch release with new features and functionality based on Active Roles 7.5.3.

New features

NOTE: This document lists only the On Demand-specific changes of Active Roles On Demand. For more information on the new features of Active Roles 7.5.3, see New features in the *Active Roles 7.5.3 Release Notes*.

The 30 May 2022 release of Active Roles On Demand has the following new features:

- Support for the Active Roles 7.5.3 release.

Enhancements

NOTE: This document lists only the On Demand-specific changes of Active Roles On Demand. For more information on the enhancements of Active Roles 7.5.3, see Enhancements in the *Active Roles 7.5.3 Release Notes*.

The 30 May 2022 release of Active Roles On Demand has no enhancements compared to the previous release.

Resolved issues

NOTE: This document lists only the On Demand-specific changes of Active Roles On Demand. For more information on the resolved issues of Active Roles 7.5.3, see Resolved issues in the *Active Roles 7.5.3 Release Notes*.

The 30 May 2022 release of Active Roles On Demand has no resolved issues compared to the previous release.

Known issues

NOTE: This document lists only the On Demand-specific changes of Active Roles On Demand. For more information on the known issues of Active Roles 7.5.3, see Known issues in the *Active Roles 7.5.3 Release Notes*.

The 30 May 2022 release of Active Roles On Demand has the following known issues:

Table 1: Active Roles On Demand known issues

Known Issue	Issue ID
When opening the **Logging** settings of the Active Roles Configuration Center, the **Logging** page will be blank. **Workaround** Contact the One Identity Cloud Operations Team if you need to change your logging settings.	294755

Active Roles On Demand system requirements

One Identity Active Roles On Demand provides its core features in a SaaS-delivered model. Therefore, you do not need to install the Active Roles Administration Service and the Active Roles Web Interface components on-premises.

However, to access, configure and maintain the Active Roles On Demand solution, you must install certain client-based Active Roles components on-premises with the indicated system requirements.

Before using the 30 May 2022 release of Active Roles On Demand, ensure that you meet the following requirements.

Active Roles Management Tools

Active Roles Management Tools is a composite component, providing the following client-based tools to configure and manage your Active Roles deployment:

- Active Roles Configuration Center

  NOTE: Active Roles Configuration Center is available on 64-bit systems only.
- Active Roles Management Shell
- Active Roles SDK
- ADSI Provider

Table 2: Active Roles Management Tools system requirements

CPU	Intel x86, Intel 64 (EM64T) or AMD64 processor, 1 GHz or faster.
RAM	1 GB or more.
Disk space	100 MB
Supported OS	• Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition). • Microsoft Windows 8.1 or 10 (Professional or Enterprise edition, 32-bit or 64-bit). NOTE: Active Roles is not supported on Windows Server Core installations.
.NET Framework	4.7.2
Windows Management Framework	5.1

Miscellaneous	• Visual C++ 2017 Redistributable • Microsoft Windows Remote Server Administration Tools (RSAT) for AD is required to manage Terminal Services user properties with Active Roles Management Shell or Active Roles Management Tools.

Configuration Center

Active Roles Configuration Center provides a single solution for configuring the Active Roles Administration Service instances and Active Roles Web Interface sites, allowing administrators to perform the core configuration tasks from a single location. These include the following:

- Creating and configuring the Active Roles Administration Service and the default cloud-based Active Roles Web Interface sites.
- Managing the core Active Roles Administration Service settings, such as the Active Roles administrator account, service account, and database connection.
- Managing the core Active Roles Web Interface settings, such as the site address on the web server and its configuration object in the Active Roles Administration Service.
- Logging options for troubleshooting Active Roles components.

  NOTE: Currently, when opening the **Logging** settings of the Active Roles Configuration Center, the **Logging** page will be blank. As a workaround, contact the One Identity Cloud Operations Team if you need to change your logging settings.
- The Starling Join feature, enabling Active Roles to connect to the One Identity Starling Cloud Platform and integrate with additional One Identity products for additional functionality.

Active Roles Management Shell

A set of Management PowerShell cmdlets, providing a means for executing and automating tasks in Active Roles and covering three key areas:

- Active Directory objects
- Active Roles configuration
- Active Roles Synchronization Service

Active Roles SDK

The Active Roles SDK, providing samples and documentation for developers to help them:

- Customize Active Roles by creating custom client applications and user interfaces.
- Expand the use of Active Roles by integrating it with the existing proprietary applications and network data sources.

ADSI Provider

The Active Directory Services Interface (ADSI) Provider enables custom user interfaces and applications to access Active Directory services through Active Roles. ADSI Provider translates client requests into DCOM calls and interacts with the Active Roles Administration Service.

The Active Roles ADSI Provider allows custom scripts and applications (such as web-based applications) to communicate with Active Directory, while taking full advantage of the security, workflow integration and reporting benefits of Active Roles.

The data exposed by Active Roles ADSI Provider is organized in a namespace identical to the namespace of the Windows system LDAP provider. The name of the Active Roles ADSI Provider namespace is `EDMS://`, instead of using the Microsoft `LDAP://` namespace).

Active Roles Console

Active Roles Console (also known as the MMC Interface) is a Microsoft Management Console (MMC) snap-in for a Microsoft Windows-based user interface.

Administrator users can use Active Roles Console to perform most Active Roles configuration actions while standard users can perform daily delegated administration and operations with it.

Table 3: Active Roles Console system requirements

CPU	Intel x86, Intel 64 (EM64T) or AMD64 processor, 1 GHz or faster.
RAM	1 GB or more. NOTE: The amount of memory required by Active Roles Console depends on the total number of managed objects.
Disk space	100 MB
Supported OS	• Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition). • Microsoft Windows 8.1 or 10 (Professional or Enterprise edition, 32-bit or 64-bit). NOTE: Active Roles is not supported on Windows Server Core installations.
.NET Framework	4.7.2
Web browser	Microsoft Edge 79 (or newer), based on Chromium
Miscellaneous	Visual C++ 2017 Redistributable

Active Roles Web Interface Access

The Active Roles Web Interface is a browser-based administration interface for Active Roles users and administrators. Certain Active Roles administration configuration actions (such as Microsoft 365 integration) is only available via the Web Interface.

The Active Roles On Demand solution hosts the Web Interface in a SaaS-delivered model, requiring no on-premises deployment. However, you need to meet the following requirements to access the Web Interface.

Table 4: Active Roles Web Interface access requirements

Web browser	• Internet Explorer 11 • Google Chrome 61 (or newer) • Microsoft Edge 79 (or newer), based on Chromium • Mozilla Firefox 36 (or newer)
Display resolution	The Active Roles Web Interface is optimized for screen resolutions of 1280x800 or higher. The minimum supported screen resolution is 1024x768.

Optional Active Roles Components

Active Roles On Demand provides several optional components that you can install on-premises for additional features. These components include:

- Active Roles Synchronization Service
- Active Roles Synchronization Service Capture Agent
- Active Roles Reporting (Data Collector and Report Pack)

Active Roles Synchronization Service

NOTE: If you plan to manage Azure AD or Office 365 operations in your environment, you must install the Active Roles Synchronization Service component.

The Active Roles Synchronization Service lets you:

- Synchronize identity information stored in data systems other than Active Directory (AD) and Active Directory Lightweight Directory Services (AD LDS) supported by the Active Roles Console.
- Automate identity information management among the various supported data systems (for example, by using workflows to create, read, update, delete, or deprovision identity information with Active Roles).

For more information on the Active Roles Synchronization Service, see Available Active Roles Reports.

Table 5: Active Roles Synchronization Service system requirements

CPU	Intel x86, Intel 64 (EM64T) or AMD64 processor, 1 GHz or faster. NOTE: One Identity recommends using a multi-core processor for the best performance.
RAM	2 GB or more. NOTE: The amount of memory required depends on the number of synchronized objects.
Disk space	250 MB
Supported OS	Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition). NOTE: Active Roles is not supported on Windows Server Core installations.
Supported databases	• Microsoft SQL Server 2019, 2017 or 2016, any edition. • Microsoft SQL Server 2014 or 2012, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Packs.
.NET Framework	4.7.2
Windows Management Framework	5.1
Miscellaneous	Visual C++ 2017 Redistributable
Supported connector versions	• Active Roles versions 7.4.3, 7.4.1, 7.3, 7.2, 7.1, 7.0, and 6.9. • Data sources accessible through an OLE DB provider. • Delimited text files. • Generic LDAP Connector. • IBM AS/400 Connector. • IBM Db2 Connector. • IBM RACF Connector. • Micro Focus NetIQ Directory. • Microsoft AD Domain Services with the domain or forest functional level of Windows Server 2012 (or higher). • Microsoft AD LDS running on any Windows Server operating system supported by Microsoft.

- Microsoft Exchange Server version 2019, 2016, 2013, or 2010.
- NOTE: Microsoft Exchange 2013 CU11 is not supported. For more information, see Knowledge Base Article 202695 on the *One Identity Support Portal*.
- Microsoft Lync Server version 2013 (with limited support).
- Microsoft Skype for Business 2019, 2016 or 2015
- Microsoft Windows Azure AD (using the Azure AD Graph API version 1.6).
- Microsoft Office 365 directory.
- Microsoft Exchange Online service.
- Microsoft Skype for Business Online service.
- Microsoft SharePoint Online service.
- Microsoft SQL Server (any version supported by Microsoft).
- Microsoft SharePoint 2019, 2016, or 2013.
- MySQL Connector.
- One Identity Manager version 7.0 (D1IM 7.0).
- One Identity Manager version 8.0.
- Oracle Database.
- Oracle Database User Accounts.
- Oracle Unified Directory.
- OpenLDAP Connector.
- Salesforce Connector.
- ServiceNow Connector.

NOTE: Data sources accessible through an OLE DB provider, delimited text files, and IBM RACF data systems are supported by Active Roles Synchronization Service without bi-directional support.

Active Roles Synchronization Service Capture Agent

Active Roles Synchronization Service provides a Capture Agent to synchronize user passwords between Active Directory (AD) domains managed by the Synchronization Service and other connected data systems.

NOTE: To synchronize passwords from an AD domain to other connected data systems, you must install the Synchronization Service Capture Agent on all domain controllers in the source AD domain.

Table 6: Active Roles Synchronization Service system requirements

.NET Framework	4.7.2
Supported OS on domain controllers	Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition). Both x86 and x64 platforms are supported, with or without any Service Packs.

Active Roles Reporting

Active Roles offers optional on-premises reporting capabilities with its Data Collector and Report Pack, allowing you to view Active Roles tracking logs for administrative roles, Managed Units (MUs), policy compliance, Policy Objects, and the state of key Active Directory (AD) objects.

Active Roles Data Collector and Report Pack facilitates the collection of environment data (stored in an SQL Server database) and the automated generation of reports on management activities. The Report Pack component is deployed on Microsoft SQL Server Reporting Services (SSRS) to view, save, print, publish, and schedule Active Roles reports. For more information on the available report, see Available Active Roles Reports.

Table 7: Active Roles Collector and Report Pack system requirements

.NET Framework	4.7.2
Supported OS on domain controllers	Microsoft Windows Server 2022, 2019, or 2016 (Standard or Datacenter edition). NOTE: Active Roles is not supported on Windows Server Core installations.
Supported databases	• Microsoft SQL Server 2019, 2017 or 2016, any edition. • Microsoft SQL Server 2014 or 2012, any edition, 32-bit (x86) or 64-bit (x64), with or without any Service Packs.
.NET Framework	4.7.2
Other Active Roles components	The Active Roles Management Tools must be installed and must have the same version as the Active Roles Administration Service, due to using the Active Roles ADSI Provider component.

Available Active Roles Reports

Active Roles provides reporting services for the following Active Directory and Active Roles objects, components and events.

Active Directory Assessment

- Domains
  - Domain account SID resolution.
  - Domain Summary.
  - Domain Trusts.
- Group Membership
  - Group Membership by groups.
  - Group Membership by users.
  - Users with domain administration rights.
- Groups
  - Domain group statistics.
  - Empty groups.
  - Group hierarchy.
  - Group list with member statistics.
- Organization Units (OUs)
  - Member statistics by OU.
  - OU hierarchy.
  - OU membership.
- Other Directory Objects.
  - Active Directory object properties.
  - All discontinued computer accounts.
  - Computer accounts.
- Potential Issues
  - Cycled groups.
- Users
  - Account Information
    - Bad password information.
    - Password age information.
    - User account list.
    - User account options.

- Exchange 2000-2003 (or newer)
    - Email delivery options.
    - Email delivery restrictions.
    - Mailbox information by user.
    - Active Roles tracking log.
- Miscellaneous Information
    - Objects managed by a user.
    - Personnel hierarchy.
    - User profile information.
    - Users with specified properties.
- Obsolete Accounts
    - All discontinued user accounts.
    - Deprovisioned user accounts.
    - Disabled user accounts.
    - Expired user accounts.
    - Inactive user accounts.
    - Locked user accounts.
    - User accounts with expired password.

Active Roles Tracking Log

- Active Directory Management
    - Deprovisioning of user accounts.
    - Directory object management.
    - User attribute management.
- Active Roles Configuration Changes
    - Control delegation.
    - Policy enforcement.
- Active Roles Events
    - Active Roles events statistics.
    - Active Roles startup failures.
- Active Roles Workflow
    - Approvals and rejections.
    - Workflow monitoring.
- Dashboard
    - User account management.

Administrative Roles

- Access Template permissions.
- Access Template summary.
- Access Templates linked to Managed Units (MUs).
- Access Templates linked to OUs.
- Control delegation by object.
- Control delegation by object (with group hierarchy).
- Control delegation by trustee.
- Control delegation by trustee (with container hierarchy).

Managed Units

- MU members.
- MU membership rules.
- MU summary.
- MUs affected by policies.
- MUs with delegated control.

Policy Compliance

- Objects violating policy rules.
- Violated policy rules.

Policy Objects

- Linked property validation settings.
- Linked property validation settings (with inheritance).
- Linked script settings (with inheritance).
- Policy Object references.
- Policy Object settings.
- Policy Object summary.
- Policy Objects with securable objects.
- Securable objects (with inheritance).

Product licensing

Use of this software is governed by:

- The Software Transaction Agreement found at: http://www.oneidentity.com/legal/sta.aspx
- The SaaS Addendum found at: http://www.oneidentity.com/legal/saas-addendum.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 On Demand.

New organization instructions

One Identity Active Roles On Demand provides its core features in a SaaS-delivered model. Therefore, you do not need to install the Active Roles Administration Service and the Active Roles Web Interface components on-premises.

However, to access, configure and maintain the Active Roles On Demand solution, you must install certain client-based Active Roles components on-premises with the indicated system requirements.

Therefore, when deploying Active Roles On Demand in your organization the first time, the deployment procedure has 4 main steps:

1. Preparing the Active Roles server for an offline domain join.
2. Collecting all on-premises and cloud resource information required for the deployment procedure.
3. Sending the generated offline domain join file and the required configuration information to the One Identity Cloud Operations Team via the One Identity Starling portal (https://www.cloud.oneidentity.com).
4. Installing the on-premises components of Active Roles and performing the initial configuration of Active Roles On Demand.

For detailed instructions on how to deploy Active Roles On Demand in your organization, see *Active Roles On Demand Quick Start Guide* on the One Identity Support Portal.

More resources

Additional information is available from the following resources:

- For the most recent documents and product information, see the Active Roles On Demand documentation in the *One Identity Support Portal*.
- Join the Active Roles On Demand 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 On Demand team and other community members.

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 supports operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

About us

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

Contacting us

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

Technical support resources

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

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

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

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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