



[One Identity Active Roles](#)

[What's New Guide](#)

## Copyright 2021 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](http://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.

Active Roles What's New Guide  
Updated - May 2021  
Version - 7.4.4

# Contents

<b>Summary</b> .....	<b>5</b>
<b>Key new features</b> .....	<b>6</b>
Additional Hybrid Directory features .....	8
Office 365 Group CRUD activities .....	8
Office 365 roles management for hybrid users .....	9
Support for Exchange Online Mailbox Properties for Office 365 users in Federated and Synchronized environment .....	9
Support for provisioning objects in SaaS products .....	9
Upgraded database configuration and installation .....	10
Support for Azure AD Graph 1.6 for Active Roles Synchronization Services .....	10
Support for Group Managed Service Account (gMSA) for Active Roles Service account .....	10
Bulk attributes operations for multiple users .....	11
Reset password for multiple users at a time .....	11
Support for Solution Intelligence .....	11
Support for logging in to MMC interface through 2FA authentication .....	12
Support for federated authentication .....	12
Support to provide product feedback from the Web Interface .....	12
Support for cloud-only Azure objects .....	12
Support for cloud-only Azure object policies .....	13
Enhancements .....	13
<b>Upgrade issues</b> .....	<b>18</b>
Impact on Active Roles replication .....	18
Impact on custom solutions .....	18
Impact on unmanaged domains .....	19
Impact on add-ons .....	19
Impact on management history data .....	19
Impact on SSL and Federated Authentication configuration .....	20
<b>Glossary</b> .....	<b>21</b>
<b>About us</b> .....	<b>34</b>
Contacting us .....	34

Technical support resources .....34

# Summary

Active Roles (formerly known as ActiveRoles®) simplifies and streamlines creation and ongoing management of user accounts, groups, and contacts in Windows Active Directory (AD) and Azure Active Directory environments.

Active roles automates:

- Creating user, groups, and contacts in Active Directory and Azure AD
- Creating and managing Office 365 groups
- Managing Office 365 roles for hybrid users
- Creating mailboxes on Exchange Server and assigning licenses in Office 365
- Managing on-premise Exchange and Exchange Online properties
- Creating Remote Mailbox for hybrid users
- Provisioning OneDrive for hybrid users
- Provisioning users in Starling Connectors
- Support for Federated Authentication
- Support to configure Web Interface for secure communication
- Support to provide product feedback from the Web Interface

It provides strictly enforced security, rich capabilities for automating directory management tasks, change approval and easy-to-use Web interfaces, to achieve practical user and group account management for the Windows enterprise.

Active Roles also facilitates administration and provisioning for Active Directory, Exchange, and Azure Active Directory (Azure AD) in a hybrid environment.

Active Roles supports connecting to One Identity Starling and accessing Starling Services such as Two-factor Authentication, Starling Connect, and Identity Analytics and Risk Intelligence.

## Key new features

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

### Major new features in Active Roles Version 7.4.4:

- Support for Azure SQL database.
- Support for cloud-only Azure objects (Azure Users, Azure Guest Users, Azure Contacts).
- Support for Azure Multi-Factor Authentication.

### Major new features in Active Roles Version 7.4.3:

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

### 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 provisioning objects in SaaS products through Starling Connect.
- 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 Federated authentication feature.
- Support to provide product feedback from the Web Interface

Major enhancements Active Roles Version 7.4:

- New built-in workflow and script added for the following
  - Create Office 365 shared mailbox
  - 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.
- 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.
- In Active Roles, the Fine-Grained policy takes precedence over Domain policy in evaluating the User account and password information. The User account information and Account Policies are displayed based on the Fine-Grained policy applied on the container.
- Auto-shrink option can be customized for new Active Roles database (configuration and management history) during the configuration of Active Roles.
- In ERFM policy, the substitute attribute, mail can now be used optionally instead of using it as a hard-coded attribute.
- Support for new connectors through Synchronization Service. For more information, refer *Enhancements*.
- Supports installation of Synchronization Service Management Shell component individually via command prompt. For more details refer How to install Synchronization Service Management Shell in Synchronization Service Admin Guide
- Builtin Azure policy is enhanced with the additional provisioning of the attribute **edsvaAzureOffice365Enabled**.
- Support for Modern Authentication while communicating with Exchange Online from Active Roles service.
- Optimized policy evaluation for license management, Office 365 roles management.
- Support for the **multiSubnetFailOver** feature of MS SQL Server to maximize internal availability.
- 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.
- Support to modify the following Exchange Online properties in Synchronized Identity and Federated environments using the Active Roles Web interface:
  - Mail Flow Settings properties: Message Size Restrictions and Delivery Options
  - Mailbox Feature properties: Exchange ActiveSync, Outlook Web App, MAPI, IMAP, POP3, and Archive
  - Delegation: Send As, Full Access
  - Mail Settings: Messaging records Management
- Creation of Remote Mailbox for hybrid users
- Support for Federated Authentication.
- Support for new connectors through Synchronization Service. For more information, refer *Enhancements* topics.
- Restructured product documentation that consolidates content in lesser number of documents.  
For more information, see *Enhancements* topic.

## Additional Hybrid Directory features

Active Roles supports the following additional features for hybrid directory support:

- Support for Office 365 Group CRUD activities.
- Support for Office 365 roles and reporting for Office 365 users.

## Office 365 Group CRUD activities

Active Roles provides the facility to perform administrative tasks such as create, read, update, and delete groups in Office 365 through the web interface. You can also perform other operations such as add and remove members to Office 365 groups. Some of the group operations can be performed using the Management Shell in addition to the web interface. For more information on managing Office 365 groups using the Active Roles web interface and Management Shell, see the following sections in the latest *Active Roles Administration Guide*.

- Office 365 Group management tasks using the Web interface
- Office 365 Group management tasks using Management Shell interface



# Office 365 roles management for hybrid users

Active Roles provides the facility to assign or modify the Microsoft Office 365 roles assigned to on-premises users synchronized to Office 365. You can perform the following Office 365 roles management tasks for hybrid users:

- Assign Office 365 roles to new hybrid users
- Assign Office 365 roles to existing hybrid users
- Modify or remove Office 365 roles assigned to hybrid users

**NOTE:** For more information on the Office 365 roles management see the latest *Active Roles Administration Guide*.

## Support for Exchange Online Mailbox Properties for Office 365 users in Federated and Synchronized environment

Exchange Online Mailbox Properties for Office 365 users were previously enabled for editing in Non-federated environment only. Active Roles supports editing of the following Exchange Online Mailbox Properties for Office 365 users in Federated and Synchronized environment also:

- **Mail Flow Settings properties:** Message Size Restrictions and Delivery Options
- **Mailbox Feature properties:** Exchange ActiveSync, Outlook Web App, MAPI, IMAP, POP3, and Archive
- **Delegation:** Send As, Full Access
- **Mail Settings:** Messaging records Management

## Support for provisioning objects in SaaS products

Active Roles provides support to connect to Starling Connect to manage the user provisioning and deprovisioning activities for the registered connectors. Using the Starling Join feature in Active Roles, you can connect to One Identity Starling.

On joining to Starling, the registered connectors for the user are displayed if the Starling Connect subscription exists. If the subscription does not exist, visit the Starling site for Starling Connect subscription. The displayed connectors are available for provisioning or deprovisioning of users or groups through Active Roles.

## Upgraded database configuration and installation

Active Roles provides default configuration of separate Management History and Configuration databases during installation of Active Roles. During Active Roles upgrade, if the Active Roles database is not split into configuration and management history databases, then the upgrade process by default creates a management history database. However, the management history data is not imported by default, and if required you may import the data from the earlier Configuration database. For more information on the impact, see *Upgrade issues* topic.

## Support for Azure AD Graph 1.6 for Active Roles Synchronization Services

Active Roles Synchronization Service now supports Directory schema extensions for Azure Graph API version 1.6. This enables you to view and select the extension attributes registered in the Azure subscription while selecting the attributes of an Azure object to perform the various CRUD activities.

## Support for Group Managed Service Account (gMSA) for Active Roles Service account

Active Roles now allows you to administer group Managed Service Accounts. Introduced in Windows Server 2012, group Managed Service Account (gMSA) is a domain security principal whose password is managed by Windows Server 2012 domain controllers and can be retrieved by multiple systems running Windows Server 2012. Having Windows services use gMSA as their logon account minimizes the administrative overhead by enabling

Windows to handle password management for service accounts. Group Managed Service Accounts provide the same functionality as Managed Service Accounts introduced in Windows Server 2008 R2 and extend that functionality over multiple servers.

**NOTE:** Exchange operations cannot be performed on the on-premises Exchange Server environment using the gMSA account. For example, Remote mailbox, User mailbox, or Contact.

Active Roles supports usage of Group Managed Service Account as Active Roles Service Account. For more information about using gMSA as a service account, see *Configuring gMSA as an Active Roles Service account* in the *Active Roles Administration Guide*.

## Bulk attributes operations for multiple users

Active Roles allows you to perform operations on bulk attributes for multiple users at a time. The Web interface provides you the **Update object attributes** to perform bulk operations on selected attributes for multiple Active Roles users.

## Reset password for multiple users at a time

Active Roles allows you to perform password reset operation for multiple users at a time as part of the batch operations using the Web interface.

## Support for Solution Intelligence

Active Roles supports Solution Intelligence to monitor the web application and detect performance issues. Active Roles administrators can enable or disable the Solution Intelligence feature that supports intelligent collection of Active Roles solution usage data.

The telemetry data that is captured from Active Roles is sent to the Azure portal and can be accessed by the development team for analysis. In addition to the general telemetry data that is collected by Microsoft Azure, Solution Intelligence in Active Roles helps to capture the data about the Active Roles language pack usage by customers, referred to as

Language pack telemetry and the area of bugs and issues referred to as the diagnostic telemetry.

## Support for logging in to MMC interface through 2FA authentication

When a Starling 2FA enabled user tries to log in to the Active Roles MMC interface, the user is prompted to enter the Starling Two-factor token response. Based on the option selected by the user, the token response is provided through SMS, Phone Call or Push Notifications.

## Support for federated authentication

Federated authentication allows you to federate user access by authenticating them against a certain set of rules, known as claims. The authentication ticket or the token is used to validate the user across multiple application, web sites, or IT systems.

Claims-based authentication is a method to acquire the user identity related information on both on-premises and cloud-based products. A single token is created based on the predefined claims to identify the users trying to access the applications or web site. After the identification of the user is complete, a security token service is used to identify the type of user.

Active Roles supports federated authentication with Security Assertion Markup Language (SAML), through which you can sign in to an application once using the single sign-on option and you are authenticated to access multiple applications.

## Support to provide product feedback from the Web Interface

Active Roles now supports Feedback option on web site. Feedback option allows you to provide product feedback. This option is available only for Admin site and HelpDesk site. It can be enabled or disabled from **Global Settings**.

## Support for cloud-only Azure objects

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

*Active Roles Administration Guide:*

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

## Support for cloud-only Azure object policies

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

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

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

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

## Enhancements

This Active Roles release includes the following enhancements to the existing features:

### Enhancements in 7.4.4 Release

- The **Enable SQL auto shrink** option in the **Connection to Database > Advanced Database Properties** page of the Configure Administration Service wizard is now disabled by default, as enabling it may result in performance issues. For more information, see [Recommendations and guidelines for setting the AUTO\\_SHRINK database option in SQL Server](#) in the official *Microsoft SQL Server 2008 Enterprise* documentation.

### Enhancements in 7.4.3 Release

- New Builtin workflows and scripts are provided for **Create Office 365 shared mailbox** and **Enabling Azure Roles** . Initial template scripts are available under script modules that can be configured as per the user requirement for running the workflows.
- Active Roles now gives provision to **Edit or Update** exchange or extension properties of the Master account even in the absence of the corresponding shadow account in the Exchange Forest.
- In-place upgrade and import database process is enhanced with additional configurable option to copy database users, permissions, SQL logins, and roles from the old SQL database to a new database. For more details refer Upgrade section in *Active Roles Quick Start Guide*.
- 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 Fine-Grained policy applied on the container.
- Active Roles Configuration provides a new setting for enabling or disabling auto-shrink on SQL databases when configuring a new Configuration Database or Management History Database. The new **Enable SQL auto shrink** option is available in the **Connection to Database > Advanced Database Properties** page of the Configure Administration Service wizard.
- Active Roles now allow to use the substitute attribute **mail** as optional in ERFM policy so that we set different mail ids for master and shadow account.
- Support for new connectors through Synchronization Service:
  - Oracle Unified Directory Connector
  - Oracle Database User Accounts Connector
  - Oracle Database Connector
  - Micro Focus NetIQ Directory Connector
  - IBM AS/400 Connector

For details on the new connectors refer *Active Roles Synchronization Service Administration Guide*.

- Supports installation of Synchronization Service Management Shell component individually via command prompt. For more details refer How to install Synchronization Service Management Shell in *Active Roles Synchronization Service Administration Guide*.

- Builtin Azure policy is enhanced with the additional provisioning of the attribute **edsvaAzureOffice365Enabled**. This will automatically assign the attribute **edsvaAzureOffice365Enabled** on the OU on which the Azure policy is applied instead of manual assignment as done in earlier versions of Active Roles.
- Active Roles now provides support for Modern Authentication while communicating with Exchange Online from the service. The feature now gives the user option to configure Basic or Modern Authentication. By default, Modern Authentication is enabled in Active Roles Synchronization Service and administrators must enable Basic authentication manually.
- Optimized policy evaluation for Azure license management, Office 365 roles management.

**Table 1: New connectors and supported versions**

Connectors	Supported version
Oracle Database Connector	The computer running Synchronization Service must have the following software installed: <ul style="list-style-type: none"> <li>• Oracle Database version 19C.</li> </ul>
Oracle Database User Accounts Connector	The computer running Synchronization Service must have the following software installed: <ul style="list-style-type: none"> <li>• Oracle Database User Accounts version 19.3.</li> </ul>
Micro Focus NetIQ Directory Connector	Version 9.2
Oracle Unified Directory Connector	Version 12.2.1.3
IBM AS/400	Version 7 r1

### Enhancements in 7.4.1 Release

- Support for the **multiSubnetFailOver** feature of MS SQL Server to maximize internal availability.
- Support for the Security Identity Mappings functionality: Active Roles 7.4 Web interface is enhanced to support the Name Mappings functionality for Active Roles users, similar to the functionality 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. For example, you can extend Active Roles capability by adding new Exchange online capability which is not supported in Active Roles out of the box. For more information, see the *Office 365 workflows* section in the *Administration Guide*.

- 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. For security reasons, one more layer of access restriction is added for the MMC interface. You can now set the Active Roles MMC interface user access using the Active Roles Configuration Center.
- Enhancement of SPML operation to get ObjectSid to retrieve the value in the SID format along with the base64Binary format - In earlier versions of Active Roles, the SPML operation to retrieve properties of an object retrieved the ObjectSID properties in base64Binary format. The current release enables you to retrieve the ObjectSID properties in the SID format also.
- Creation of OneDrive for Azure AD users using OneDrive Provisioning Policy. Provisioning access to OneDrive for Azure AD users is controlled or restricted by creating a new provisioning policy and applying the policy to the Organizational Unit. Active Roles uses a scheduled task to provision OneDrive for Azure AD users for whom the OneDrive provisioning was not successful during user creation.
- Configuring secure communication for Active Roles Web interface: By default, Active Roles users connect to the Web interface using HTTP protocol, which does not encrypt the data during communication. However, it is recommended to use a HTTPS protocol to transfer data securely over the web. You can use the Force SSL Redirection option in the Configuration Center to enable secure communication over HTTPS for the Web interface on local or remote servers.
- Support to modify the following Exchange Online properties in Synchronized Identity and Federated environments using the Active Roles Web interface. In the previous versions, the Exchange online properties were restricted from modification in Federated and Synchronized Identity environments:
  - Archive mailbox
  - Message records management
  - Mail flow settings
  - Email address
- Creation and modification of Remote Mailbox for hybrid users
- Support has been added for the following connectors through the Synchronization Service:

**Table 2: New connectors and supported versions**

<b>Connectors</b>	<b>Supported version</b>
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
Salesforce Connector	Internet access to the data system you



Connectors	Supported version
Service now Connector	want to participate in data synchronization operations
IBM RACF Connector	Version 1.13 or later. Optionally with LDAPX exit version 2.10 or later

- Restructured product documentation for Active Roles. Documentation set now consists of the following guides:
  - 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

## Upgrade issues

The upgrade process of the Administration Service has impact on the following:

- Replication
- Custom Solutions
- Unmanaged domains
- Add-on components
- Management history data

### Impact on Active Roles replication

The upgrade process of the Administration Service does not preserve the replication settings. An upgrade can only be performed if the Administration Service is not configured for replication. Before upgrading the Administration Service, you should ensure that its database server is not configured as a Subscriber or Publisher. Replication for the new Administration Service needs to be configured after the upgrade.

### Impact on custom solutions

An upgrade of Active Roles components may affect custom solutions that build upon the functions of Active Roles. Custom solutions (such as scripts or other modifications) that work fine with the earlier version of Active Roles may cease to work after the upgrade. Prior to attempting 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. For any compatibility issues arising during the test process, contact One Identity Software Professional Services for paid assistance with those solutions.

# Impact on unmanaged domains

Upgrade of the Administration Service converts unmanaged domains to regular managed domains. If you have any domains registered as unmanaged domains with Active Roles version 6.8 or earlier, then, after the upgrade, you will need to make them unmanaged by applying the built-in Policy Object **Exclude from Managed Scope**. For further information and instructions, see "Configuring an unmanaged domain" in the Active Roles Administration Guide.

# Impact on add-ons

After an upgrade of Active Roles components to the latest version, the add-ons which were supported in the earlier versions of Active Roles, cease to work. Hence, it is recommended to uninstall the add-ons prior to the upgrade of Active Roles.

**NOTE:** Office 365 add-on is not supported on the Active Roles 7.4.

# Impact on management history data

Configuration databases during installation of Active Roles. During Active Roles upgrade, if the Active Roles database is not split into configuration and management history databases, then the upgrade process by default creates a management history database. However, the management history data is not imported by default, and if required you may import the data from the earlier Configuration database.

**IMPORTANT:** The Management History data is not migrated to the new database during the upgrade. The data has to be imported manually into the database.

After you import the change history information, the Management History database has the following details:

- All managed objects change history includes the Properties modified during the operation, Workflow, and policy executed with operation
- User Activity information
- Automation Workflow Run history
- Temporal Group membership scheduler job status and its details to Add or Remove membership from the Temporal Group
- Workflow Approval tasks status includes Pending, Completed, and Paused
- Deprovision and UndoDeprovision object Results. If Deprovision object result does not exist in Management History database then UndDeprovision operation fails.

For more information on Upgrading to Active Roles 7.4 from 7.0.x or later using in-place upgrade method on the Active Roles Quick Start Guide.

**NOTE:** The reports produced by the Change History or User Activity command include information only about the changes made using a certain group of Administration Services, that share a common database from the connected management history database. If the Change History data is not imported from the previously available database, the data is not displayed in the new Management History database.

Operations that are dependent on Approval Workflow, Temporal Group Memberships, and Undo Deprovisioning features might not work consistently on the client interfaces. Without importing the information between the previously available Management History and the new Management History data, such as, a task created by one of the Old Administration Services may not be present on the new Administration Services.

## Impact on SSL and Federated Authentication configuration

SSL and Federated Authentication configuration settings are not retained post upgrade from version 7.4 or 7.4.1 to the current version. One Identity recommends to reconfigure the settings after the upgrade of Active Roles.

## Glossary

### A

#### **Access Control**

A security mechanism that determines which operations a user, group, service, or computer is authorized to perform on a computer or on a particular object, such as a file, printer, registry key, or directory service object.

#### **Access Control Entry (ACE)**

An entry in an object's discretionary access control list (DACL) that grants permissions to a user or group. An ACE is also an entry in an object's system access control list (SACL) that specifies the security events to be audited for a user or group.

#### **Access Control List (ACL)**

A list of security protections that apply to an entire object, a set of the object's properties, or an individual property of an object. There are two types of access control lists: discretionary and system

#### **Access Mask**

In an access control entry (ACE) of the access control list (ACL) associated with an object, a 32-bit value specifying the operations allowed, denied, or audited when the SID-holder accesses the object.

#### **Access Template**

Each access template represents a stand-alone collection of access masks. When an access template is applied to a network object in relation to a given trustee, the entire collection of access masks is translated into a set of access control entries in the object's access control list, with each entry containing the trustee's security identifier and one of the access masks extracted from the access template. When an access template is modified, all the access control entries created by applying that access template are modified accordingly.

## Active Directory

The Windows-based directory service. Active Directory stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects.

## Active Directory Schema

The Active Directory schema defines the set of all object classes and attributes that can be stored in the directory. For each object class, the schema defines what attributes an instance of the class must or may have and specifies the legal parents of the class. The Active Directory schema is stored in the directory as specific schema objects that are protected with access control. Schema objects can be accessed and updated dynamically.

## Administration Service

A core component of Active Roles, the Administration Service manages requests to network data sources. It validates requests, performs administrative tasks, and enforces administrative policies.

## Administrator

In the Windows Server family, a person who is responsible for setting up and managing local computers, stand-alone servers, member servers, or domain controllers. An administrator sets up user and group accounts, assigns passwords and permissions, and helps users with networking problems. Administrators can be members of the Administrators group on local computers or servers. A person who is a member of the Administrators group on a local computer or server has full access to that computer or server and can assign access control rights to users as necessary. Administrators can also be members of the Domain Admins group on domain controllers and have full control over user and computer accounts residing in that domain.

## C

### Cache

For Administration Service, a special pool in memory in which directory object data are held for quicker access. Administration Service updates the data in the cache immediately after a modification in Active Directory occurs, thereby ensuring that the cached data is always current and correct. For better performance, Administration Service only refreshes the data that is actually changed in Active Directory, achieving the real-time update of the cached data.

## Collection

A set of network objects defined by membership rules. For example, a Managed Unit is a collection. The same object can be a member of more than one collection.

## Computer Name

Computer names define computers to a network. Each computer name cannot be the same as any other computer or domain name in the network. A valid computer name contains letters (a-z, A-Z), numbers (0-9), and hyphens (-), but no spaces or periods (.). In addition, it may not consist solely of numbers.

## Computer Resource

A computer system itself, or a network component that resides on a computer system, such as a service, share, printer, print job, connected user, or open file.

See also *Network Object* and *Directory Object*.

## Configuration

See *Directory Partition*.

## Console Tree

The left pane in Microsoft Management Console (MMC) that displays the items contained in the console. The items in the console tree and their hierarchical organization determine the capabilities of a console.

See also *Microsoft Management Console (MMC)* and *Details Pane*.

## Container

An object that can logically contain other objects. The objects created or placed in a container object are referred to as the container's child objects, and the container object is referred to as their parent object. For example, an Organizational Unit is a container object. An object can have only one parent container.

## Cross-Site Request Forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

## Cross-site Scripting (XSS )

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

## D

### Delegate Administrative Control

To assign responsibility for management and administration of a collection of network objects to an individual user or a group of users.

### Delegated Administrator

See *Trustee*.

### Details Pane

The right pane in Microsoft Management Console (MMC) that displays details for the selected item in the console tree. The details can be a list of items or they can be administrative properties, services, and events that are acted on by a snap-in.

See also *Console Tree*, *Microsoft Management Console (MMC)*, and *Snap-in*.

### Directory Database

The physical storage for each replica of Active Directory. Also called the *store*.

See also *Active Directory*.

### Directory Object

Any object stored in Active Directory or other directory service. A directory object is described by a distinct, named set of attributes. For example, the attributes of an Active Directory user object might include the user's first name, last name, and e-mail address.

See also *Network Object*.

### Directory Partition

Active Directory is made up of one or more partitions (naming contexts). Each partition represents a contiguous sub-tree that is replicated as a unit to other domain controllers in the forest. In Active Directory, a single server holds at least three directory partitions: schema (class and attribute definitions for the directory), configuration (replication topology and related metadata), and domain (sub-tree that contains the per-domain objects for one domain).



## Domain

In Active Directory, a collection of computer, user, and group objects defined by the administrator. These objects share a common directory database, security policies, and security relationships with other domains.

## Domain Controller

In an Active Directory forest, a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources. Administrators can manage user accounts, network access, shared resources, site topology, and other directory objects from any domain controller in the forest.

## Domain Local Group

A security or distribution group that can contain universal groups, global groups, other domain local groups from its own domain, and accounts from any domain in the forest. Domain local security groups can be granted rights and permissions on resources that reside only in the same domain where the domain local group is located.

See also *Group*.

## Domain Tree

In Active Directory, a hierarchical structure of one or more domains, connected by transitive, bidirectional trusts, that forms a contiguous namespace. Multiple domain trees can belong to the same forest.

See also *Forest*.

## E

### Explicit Permissions

Explicit permissions are those that are defined directly on an object. Explicit permissions are defined either automatically when the object is created, or by user action. For example, when a user account is created, the permissions on it are explicit permissions.

See also *Permissions* and *Inherited Permissions*.

## F

### Fault Tolerance

The ability of a software product to ensure data integrity when hardware failures occur. Active Roles provides fault tolerance through multi-master replication of the data individually stored by each of a number of Administration Services.

## Forest

One or more Active Directory domains that share the same class and attribute definitions (schema), site and replication information (configuration), and forest-wide search capabilities (global catalog). Domains in the same forest are linked with two-way, transitive trust relationships.

## G

### Global Catalog

A server that holds a partial replica of every user-naming context in Active Directory. The Global Catalog also contains the schema and configuration naming contexts. The attributes in the Global Catalog are those most frequently used in search operations and those attributes that are required to locate a full replica of the object. The Global Catalog enables users and applications to find objects in Active Directory given one or more attributes of the target object, without knowing what domain holds the object.

### Global Group

A global group can be granted permissions and rights for the domain controllers of its own domain, for other members of its own domain, and for trusting domains. A global group can become a member of local groups in any of these domains. However, it can contain user accounts only from its own domain. Only domain controllers maintain global groups.

See also *Group*.

### Group Name

A group name must be unique among groups and user accounts in the domain. A valid group name contains letters (a-z, A-Z), numbers (0-9), and special characters, except for the following:

/ \ [ ] : ; | = , + \* ? < >

### Group

A collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists.

See also *Domain Local Group*, *Global Group*, *Local Group*, and *Universal Group*.

## H

### Home Folder (Home Directory)

The home folder is a folder that is accessible to the user and can contain files and programs for that user. A network home folder can be assigned to an individual user or

can be shared by many users. If no local or network home folder is assigned, the default local home folder is located on the drive on the user's computer.

## Hybrid

Hybrid environment refers to an environment which uses a mix of on-premises Active Directory and Azure Active Directory and allows synchronization of objects from the on-premises AD to the Azure AD.

## I

### Inherited Permissions

Inherited permissions are those that are propagated to an object from a parent object. Normally, an object inherits the permissions from the container where that object is placed. For example, when an object is created or moved in an Active Directory organizational unit (OU), the object automatically inherits the permissions from that OU. Defined on a parent object, inherited permissions can only be modified by changing the parent object's permission settings.

In Active Roles, permissions defined on a managed unit or inherited by a managed unit are also inherited by all the members of that managed unit. Due to this inheritance feature, objects' permissions change as objects change their memberships in managed units, providing the ability to regulate permission settings by using membership rules.

See also *Explicit Permissions* and *Permissions*.

## L

### Local Group

A local group can be granted permissions and rights only for its own computer on which the group resides. However, it can contain user accounts and global groups from its own domain and trusted domains.

See also *Group*.

### Logon Script

A logon script allows an administrator to affect a user's environment without managing all aspects of it. When a logon script is assigned to a user account, it runs each time the user logs on. One logon script can be assigned to one or more user accounts. It can be a batch file (.cmd or .bat filename extension) or an executable program (.exe filename extension). When a user logs on, the computer authenticating the logon locates the logon script by following the logon script path.

## M

### Managed Domain

A domain registered for the management with Active Roles. Active Roles can be configured to manage multiple domains.

### Managed Unit

A collection of objects managed with Active Roles defined by using membership rules, for the purposes of distribution of administrative responsibilities. Managed units provide large organizations with the flexibility they need to delegate network administration, enforce administrative policies, and manage complex network environments.

### Member Server

A server that is joined to a domain but is not a domain controller. Member servers typically function as file servers, application servers, database servers, Web servers, certificate servers, firewalls, or remote access servers.

### Membership Rules

Membership rules are criteria by which Active Roles evaluates whether or not a network object is a member of a particular managed unit or view. Each managed unit or view only includes the objects whose properties meet the membership rules for that unit or view.

### Microsoft Management Console (MMC)

A framework for hosting administrative tools called *snap-ins*. A console might contain tools, folders or other containers, World Wide Web pages, and other administrative items. These items are displayed in the left pane of the console, called a *console tree*. A console has one or more windows that can provide views of the console tree. The main MMC window provides commands and tools for authoring consoles. The authoring features of MMC and the console tree itself might be hidden when a console is in User Mode.

See also *Console Tree*, *Details Pane*, and *Snap-in*.

### MMC Interface

A Active Roles user interface that network administrators and trustees use to administer Active Directory data. This interface provides access to all the capabilities of Active Roles. The MMC interface is implemented as an MMC snap-in.

See also *Snap-in*.

## N

### Naming Context

See *Directory Partition*.

### Network Object

A directory object or computer resource.

See also *Directory Object* and *Computer Resource*.

### Non-Transitive Trust Relationship

A trust relationship in a multiple-domain environment that is restricted to just two domains. For example, if domain A has a non-transitive trust with domain B, and domain B trusts domain C, then there is no trust relationship between domain A and domain C.

See also *Trust Relationship* and *Transitive Trust Relationship*.

## O

### Object

An object is a named set of attributes that represents something concrete, such as a user, a printer, or a computer system. The attributes hold data describing the subject that is identified by the object. For example, attributes of a user might include the user's given name, surname, and e-mail address.

### Organizational Unit (OU)

An Active Directory container object used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a Group Policy object (GPO) can be linked, or over which administrative authority can be delegated.

## P

### Permissions

Permissions represent authorization to perform certain operations on specific network objects, such as user accounts, groups, or computer resources. Unless permission to perform an operation is explicitly granted, it is implicitly denied. Permissions can also be explicitly denied. There are two types of permissions: explicit and inherited.

See also *Explicit Permissions* and *Inherited Permissions*.

## Policy Object

A policy object represents a collection of administrative policies. Active Roles enforces administrative policies by linking policy objects to managed units, individual directory objects, or container objects. When linked to a unit or container, a policy object affects all the member objects, including those that are located in the child containers.

## Primary Domain Controller

In a Windows NT domain, a domain controller that maintains the master copy of the Security Accounts Manager (SAM) database. The primary domain controller is the only computer that directly receives the changes made to the SAM database. Within a domain, the primary domain controller periodically replicates its data to the other domain controllers, known as backup domain controllers.

## Proxy Server

The service component of Active Roles operates as a permissions-based proxy server. When accepting requests from a client, the server component validates each request as against permissions the client has for network objects. If the client's permissions are sufficient to perform the requested operation, the service component performs it by the using the operating system facilities.

# S

## Schema

See *Active Directory Schema*.

## Secure Communication

In Active Roles, a network connection between the client and the server that requires packet privacy. When transmitting security-sensitive information, such as a user password, Active Roles uses standard DCOM mechanisms of data protection, including data encryption.

## Security Descriptor

A data structure associated with a protected object to specify security information, including who is permitted to access the object and in what way, who owns the object, and what types of access will be audited.

## Security ID (SID)

A data structure of variable length that identifies user, group, and computer accounts. Every account on a network is issued a unique SID when the account is first created. Internal processes in Windows refer to an account's SID rather than the account's user or group name.

## Security Principal

An account holder that is automatically assigned a security identifier (SID) to control access to resources. A security principal can be a user, group, service, or computer.

## Security Subsystem

A protected subsystem that authenticates and logs users on to the system, maintains information about the local security policy, and provides various services for translation between names and security identifiers.

## Service

A process that performs a specific system function and often provides an application-programming interface (API) for other processes to call.

## Service Account

The user account that a service uses to log on to the computer or network. The account must have the specific rights and permissions required by that service.

## Shared Resource (Share)

Refers to a computer resource that is made available to network users, such as a folder, file, or printer.

## Snap-in

A type of tool that you can add to a console supported by Microsoft Management Console (MMC). A stand-alone snap-in can be added by itself; an extension snap-in can be added only to extend the function of another snap-in.

See also *Microsoft Management Console (MMC)*.

## Standalone Server

A server that runs the Windows operating system, but does not participate in a domain. A stand-alone server has only its own database of users, and it processes logon requests by itself. A stand-alone server does not share account information with other computers and cannot provide access to domain accounts.

See also *Domain* and *Member Server*.

## Subtree

An unbroken path in the tree, including all child objects of any container in that path.

See also *Tree* and *Domain Tree*.

## T

### **Transitive Trust Relationship**

A trust relationship that flows throughout a set of domains, such as a domain tree, and forms a relationship between a domain and all domains that trust that domain. For example, if domain A has a transitive trust with domain B, and domain B trusts domain C, then domain A trusts domain C.

See also *Domain Tree, Forest, and Non-Transitive Trust Relationship*.

### **Tree**

Tree is usually used to describe a hierarchy of objects. Nodes in the tree (points at which the tree branches) are container objects. For example, a computer network or domain is a container object. A tree shows how objects are connected or the path from one object to another. A contiguous sub-tree is any unbroken path in the tree, including all child objects of any container in that path.

### **Trustee**

A group or user account that is authorized to perform specific administrative tasks for a specific set of network objects managed with Active Roles. Normally, Trustees are regular users or groups that have no rights to perform administrative tasks by directly accessing Active Directory. This ensures that the only way for the Trustees to perform their tasks is by using Active Roles.

### **Trust Relationship**

A logical relationship established between domains to allow pass-through authentication, in which a trusting domain honors the logon authentications of a trusted domain. User accounts and global groups defined in a trusted domain can be given rights and permissions in a trusting domain, even though the user accounts or groups don't exist in the trusting domain's directory.

### **Trusted Domain**

See *Trust Relationship*.

### **Trusting Domain**

See *Trust Relationship*.

### **Two-way Trust Relationship**

A link between two domains that allows each domain to trust user accounts in the other domain to use its resources. A user can log on from computers in either domain to the domain that contains the user's account.

See also *Trust Relationship*.



## U

### UNC Name

A full name of a shared resource on a network. It conforms to the `\\servername\sharename` syntax, where *servername* is the server's name and *sharename* is the name of the shared resource. UNC names of folders or files can also include the directory path under the share name, with the following syntax:

```
\\servername\sharename\directory\filename
```

UNC is also called Universal Naming Convention.

### Universal Group

A security or distribution group that can contain users, groups, and computers from any domain in its forest as members. Universal security groups can be granted rights and permissions on resources in any domain in the forest.

See also *Group*.

### User Account

In Active Directory, an object that consists of all the information that defines a domain user, which includes user name, password, and groups in which the user account has membership. User accounts can be stored in either Active Directory or on a local computer.

### User Profile

A file that contains configuration information for a specific user, such as desktop settings, persistent network connections, and application settings. Each user's preferences are saved to a user profile that Windows uses to configure the desktop each time a user logs on.

## W

### Wildcard Character

A character that represents one or more characters. The question mark (?) wildcard can be used to represent any single character and the asterisk (\*) wildcard can be used to represent any character or group of characters that might match that position in other names. Wildcard characters are especially instrumental in defining membership rules. For example, when defining a membership rule to include all servers with names that begin with X, you would specify X\* as the computer name. One more wildcard character, the number sign (#) represents any digit or the number sign itself.

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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product