

# Active Roles

Management and security for hybrid Active Directory and beyond

## Benefits

- Protects critical Active Directory and Azure Active Directory data
- Regulates administrative access via a least-privilege model
- Overcomes native-tools limitations
- Automates users/group account creation and deletion
- Manages accounts for Exchange Online, Lync, SharePoint Online, Office 365 and many more
- Provides a single, intuitive tool for hybrid environment
- Generates audit-ready reports
- Deploys quickly for rapid time-to-value
- Know who made what change and when
- Modular architecture to meet today and tomorrow's business needs
- Expands AD-centered identity management to many non-Windows and SaaS systems

## Overview

The challenges with managing accounts in Active Directory (AD) and Azure AD are many and varied. In addition, securing these critical systems is often a significant challenge. With native tools hybrid AD management and security is inefficient, disjointed, and error-prone.

With the frantic pace of today's businesses, organizations struggle to keep up with requests to create, change or remove access to the hybrid AD environment. Plus, they face security issues like terminated employees retaining access to valuable intellectual property, challenging business requirements and satisfying auditors' requests for reports. Then, add the need to tightly control Active Directory and Azure Active Directory administrative access as well as keeping up with the explosion of non-Windows and SaaS applications that must be also managed.

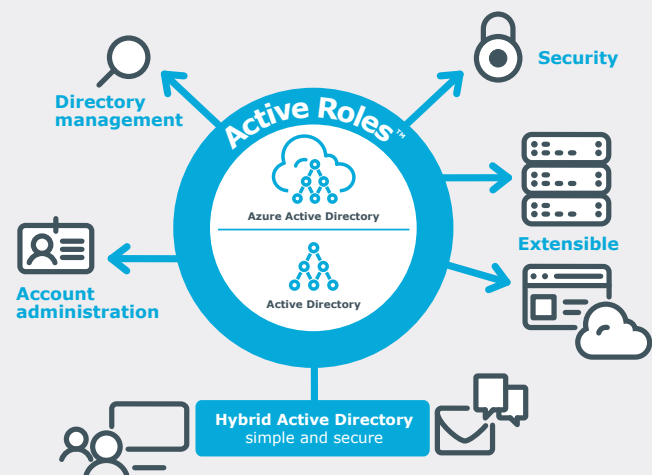
Thankfully, help has arrived. With One Identity Active Roles, you can automate these tedious and error-prone administrative tasks and solve your security issues. Active Roles automates and unifies account and group administration while securing and protecting all-important administrative access.

Active Roles delivers automated tools for user- and group-account management to overcome the shortcomings of native Active Directory and Azure Active Directory tools, which enables you to do your job more efficiently, more accurately, and with less manual intervention. Active Roles is designed with a modular architecture, so your organization can easily meet your business requirements today and in the future.

## Features

### Hybrid AD-ready

Active Roles is optimized to serve the needs of both on-prem AD and Azure AD in a hybrid deployment. It offers a single console, unified workflows and a consistent administrative experience across your entire hybrid environment. It eliminates the cumbersome, error-prone, and limited nature of using separate tools and manual processes.



## Secure access

Active Roles provides comprehensive privileged account management for Active Directory and Azure Active Directory, enabling you to control access through delegation using a least-privilege model. Based on defined administrative policies and associated permissions, it generates and strictly enforces access rules, eliminating the errors and inconsistencies common with native approaches to hybrid AD management. Plus, robust and personalized approval procedures establish an IT process and oversight consistent with business requirements, with responsibility chains that complement the automated management of directory data.

## Automate account administration

Active Roles automates a wide variety of tasks, including:

- Creating user and group accounts in AD and AAD
- Easily extend AD/AAD-based account administrative actions to non-Windows systems and SaaS applications.
- Creating mailboxes in Exchange and Exchange Online
- Populating groups across AD and AAD
- Assigning resource in Windows

It also automates the process of reassigning and removing user access rights in AD, AAD and AD-joined systems (including user and group de-provisioning) to ensure an efficient and secure administrative process over the user and group lifetimes. When a user's access needs to be changed or removed, updates are made automatically across all relevant systems and applications in the hybrid AD/AAD environment, as well as any AD-joined systems, such as Unix, Linux and Mac OS X as well as a rich and growing collection of many popular SaaS applications via the One Identity Starling Connect solution.

## Day-to-day directory management

With Active Roles, you can easily manage all of the following for both the on-prem and Azure AD environments:

- Exchange recipients, including mailbox/OCS assignment, creation, movement, deletion, permissions and distribution list management
- Groups
- Computers, including shares, printers, local users and groups
- Active Directory and Azure Active Directory

Active Roles includes intuitive interfaces to optimize day-to-day administration and help-desk operations of the hybrid AD/AAD environment via both an MMC snap-in and a web interface.

Active Roles also supports the most popular and relevant customization options such as PowerShell to deliver maximum

flexibility and the ability to use Active Roles in the manner that is most advantageous to your organization.

## Extend the administrative scope

Active Roles supports the SCIM standard, which allows any SCIM-enabled SaaS application (via One Identity Starling Connect) to be embraced in the AD-based account and group administration capabilities of Active Roles.

## Manage groups and users in a hosted environment

Synchronize AD domain clients with a host AD domain in hosted environments. Active Roles enables user and group account management from the client domain to the hosted domain, while



**When a user's access needs to be changed or removed, updates are made automatically in AD, AAD, Exchange Online, SharePoint Online, OCS, Skype for Business and Windows, as well as any AD-joined systems such as Unix, Linux and Mac OS X and SaaS apps.**

also synchronizing attributes and passwords. Utilize out-of-the-box connectors to synchronize your on-premises AD accounts to Microsoft Office 365, Lync Online / Skype for Business and SharePoint Online.

## Consolidate management points through integration

Active Roles complements your existing technology and identity and access management strategy. It simplifies and consolidates management points by ensuring easy integration with many One Identity products, including Identity Manager, Safeguard, Authentication Services, Password Manager, and ChangeAuditor. Active Roles also automates and extends the capabilities of PowerShell, ADSI, SPML and customizable web interfaces.

Active Roles comes with all the synchronization technology necessary to manage and secure:

- Lync / Skype for Business
- Exchange
- One Drive
- SharePoint
- AD LDS
- Office 365 (including roles and groups)
- Azure AD
- Microsoft SQL Server
- OLE DB (MS Access)
- Flat file

## About One Identity

One Identity, a Quest Software business, helps organizations achieve an identity-centric security strategy. With a uniquely broad portfolio of identity and access management offerings including identity governance, privileged access management and account management, all augmented by a hybrid cloud delivery strategy, One Identity helps organizations reach their full potential, unimpeded by security, yet safeguarded against threats. One Identity has proven unequalled in its commitment to its customers' long-term success. More than 7,500 organizations worldwide depend on One Identity solutions to manage more than 125 million identities, enhancing their agility and efficiency while securing access to their systems and data – on-prem, cloud or hybrid. For more information, visit [www.oneidentity.com](http://www.oneidentity.com)

© 2019 One Identity LLC ALL RIGHTS RESERVED. 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, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners.  
Datasheet\_2019\_ActiveRoles74\_US\_RS\_42104