Active Roles

Put security first to protect your hybrid identity environment

Extend native identity security and management capabilities with visibility across all Microsoft AD and M365 domains and Entra ID tenants from a single pane of glass with One Identity Active Roles. Protect, automate and unify administration across your entire hybrid environment and synchronize identity data across directories to increase security and simplify administration.

Implement a least privilege Zero Trust strategy with Active Roles using fine-grained privileged access and delegation for users and objects With Active Roles, you can focus on other IT tasks knowing your critical data, user permissions and privileged access are under control.

Overview

With One Identity Active Roles Tedious and error-prone administrative tasks are a thing of the past. Active Roles automates and unifies user and group administration, across AD/Entra ID/M365 synchronizing policies across platforms while securing and protecting privileged administrative access, driving efficiency and accuracy.

Features

Hybrid AD-ready

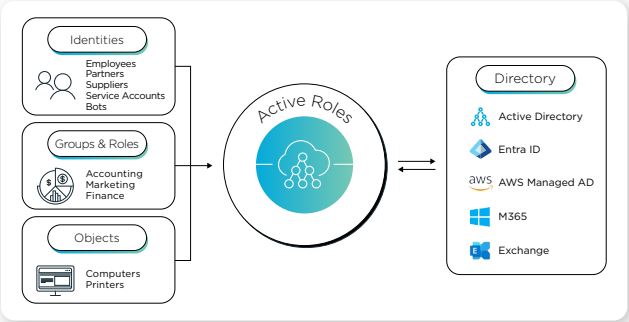
Active Roles consolidates visibility and serves the needs of both on-prem AD, Entra ID and M365 in a hybrid deployment. Via a single console, you can unify workflows and provision consistently across all domains and tenants across your entire hybrid environment.

Benefits

- **Protects** critical Active Directory, Entra ID and M365 data
- **Regulates administrative access** via a least-privilege model
- **Overcomes native-tools limitations**
- **Automates** users/group account creation and deletion
- **Provides a single, intuitive tool** for hybrid identity security and management
- **Generates audit-ready history and activity tracking** so you know when changes are made and by whom
- **Deploys quickly** for rapid time-to-value
- **Expands AD-centered identity management** to many non-Windows and SaaS systems

Secure access

With Active Roles you can use an RBAC model to delegate granular privileges and ensure identities and objects have the privileges they should.You can also deprovision those privileges to reduce standing privilege and thereby reduce risk to your organization.



Automate account administration

Active Roles automates a wide variety of tasks, including:

- **Creating user and group accounts** in AD, Entra ID and M365
- **Easily extending AD/Entra ID/M365-based account administrative actions** to SaaS apps and non-Windows systems
- **Creating mailboxes** in Exchange
- **Populating groups** across your identity landscape
- **Assigning resources** in Windows

It also automates the process of reassigning and removing user access rights in AD, Entra ID and AD-joined systems. When a user's access needs to be updated, automated workflows synchronize that change across all relevant systems and applications including any AD-joined systems, across your hybrid AD/Entra ID environment such as UNIX, Linux and Mac OS X.

Day-to-day directory management

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

- **Exchange recipients**, including mailbox/OCS assignment, creation, movement, deletion, permissions and distribution list management
- **Dynamic Groups**, Distribution Groups
- **Computers**, including shares, printers, local users and groups
- **Virtual Attributes** of Users
- **All other** AD, Entra ID or M365 Directory Objects

Active Roles consolidates security and administration onto a single console to optimize day-to-day administration and help-desk operations of a hybrid AD/Entra ID/M365 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.

Extend the administrative scope

Active Roles provides account and group administration of any SCIM-enabled SaaS application (via One Identity Starling Connect).

Manage groups and users in a hosted environment

Active Roles enables user and group account management from the client domain to the hosted domain, while also synchronizing attributes and passwords. Out-of-the- box connectors synchronize your on-premises AD accounts to Microsoft 365, Teams and SharePoint.

Consolidate management points through integration

Active Roles ensures integration with many One Identity products, including Identity Manager, Safeguard, Authentication Services, Password Manager, and Change Auditor. Active Roles also automates and extends the capabilities of PowerShell, ADSI, SPML and customizable web interfaces.

Active Roles:

- Oracle Database
- Oracle Unified Directory
- Exchange
- OneDrive
- SharePoint
- AD LDS
- Microsoft 365
- Entra ID
- Microsoft SQL Server
- Flat file

About One Identity

One Identity delivers comprehensive cloud and on-premises identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to their business. Our Unified Identity Platform brings together best-in-class identity governance and administration (IGA), access management (AM), privileged access management (PAM) and Active Directory management (AD Mgmt) capabilities. This holistic approach enables organizations to increase the visibility, control and protection over all their identities. Proven and trusted on a global scale, One Identity manages more than 500 million identities for more than 11,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest