BALASYS

One Identity Active Roles

Hybrid Active Directory, simple and secure

BENEFITS

- Protects critical Active Directory and Azure Active Directory data
- Regulates administrative access via a least-privilege model
- Automates users/group account creation and deletion
- Manages Identities for Exchange Online, Lync, SharePoint Online and Office 365 and many more
- Overcomes native-tools limitations
- 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

OVERVIEW

Microsoft® Active Directory® (AD) and Azure Active Directory (AAD) administrators are responsible for securing critical data, complying with internal policies and external regulations, and ensuring that users and groups have access to exactly the right resources and nothing more.

But with the frantic pace of today's businesses, administrators struggle to keep up with requests to create, change or remove access to the hybrid AD environment, and they face security issues like terminated employees retaining access to valuable intellectual property, along with long days (and nights) struggling to support business requirements and satisfy auditors' requests for reports. Add the need to tightly delegate control of Active Directory and Azure Active Directory among various administrative groups and involve key people in IT processes through change approval, and today's administrators need help!

Thankfully, help has arrived. With One Identity Active Roles, you can solve your security issues and meet those never-ending compliance requirements by securing and protecting Active Directory and Azure Active Directory simply and efficiently.

Active Roles delivers automated tools for user and group account management that overcome the native shortcomings of Active Directory and Azure Active Directory, so you can do your job faster. Active Roles is designed with a modular architecture, so your organization can easily meet your business requirements today and in the future.

FEATURES

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.

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

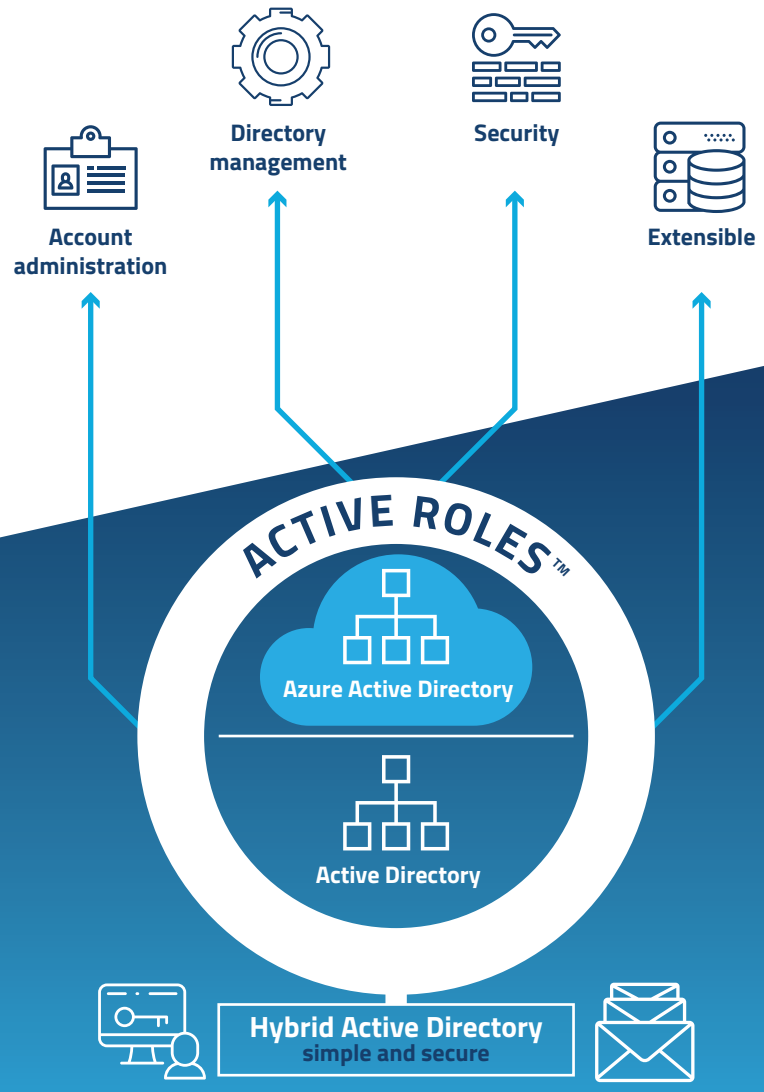
Active Roles also includes intuitive interfaces for improving day-to-day administration and help-desk operations of the hybrid AD/AAD environment via both an MMC snap-in and a web interface.

Automate account creation

Active Roles automates a wide variety of tasks, including:

- Creating user and group accounts in AD and AAD
- 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.



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 the entire hybrid environment. It eliminates the cumbersome, error-prone, and limited nature of using separate tools and manual processes.

Identity Analytics

Mitigate risks before an issue occurs through comprehensive insight into user entitlements in a hybrid AD environment. Starling Identity Analytics & Risk Intelligence (an add-on to Active Roles) provides an analysis of users' rights in Active Directory, Azure Active Directory, and Active Roles itself to highlight areas of unacceptable-risk where those rights may be out of line with peers, organizational policy, or role definitions.

One Identity Hybrid Subscription

Expand the capabilities of Active Roles with the One Identity Hybrid Subscription, which offers immediate access to cloud-delivered features and services. These include all-you-can-eat Starling Two-Factor Authentication to protect administrative access. and Starling Identity Analytics & Risk Intelligence so that you can pre-emptively detect risk; plus you get Active Roles access analysis, too. These offerings can also be extended to additional target systems and use cases. A single subscription enables all One Identity solution deployments.

When a user's access needs to be changed or removed, updates are made automatically in AD, AAD, Exchange Online, Share-Point Online, OCS, Lync and Windows, as well as any AD-joined systems such as Unix, Linux and Mac OS X.

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, Privileged Password Manager, Authentication Services, Defender, Password Manager, Cloud Access 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
- Exchange
- SharePoint
- AD LDS
- Office 365
- Azure AD
- Microsoft SQL Server
- OLE DB (MS Access)
- Flat file

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

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats.

ONE IDENTITY by Quest