

Active Roles™

Active Directory, simple and secure

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

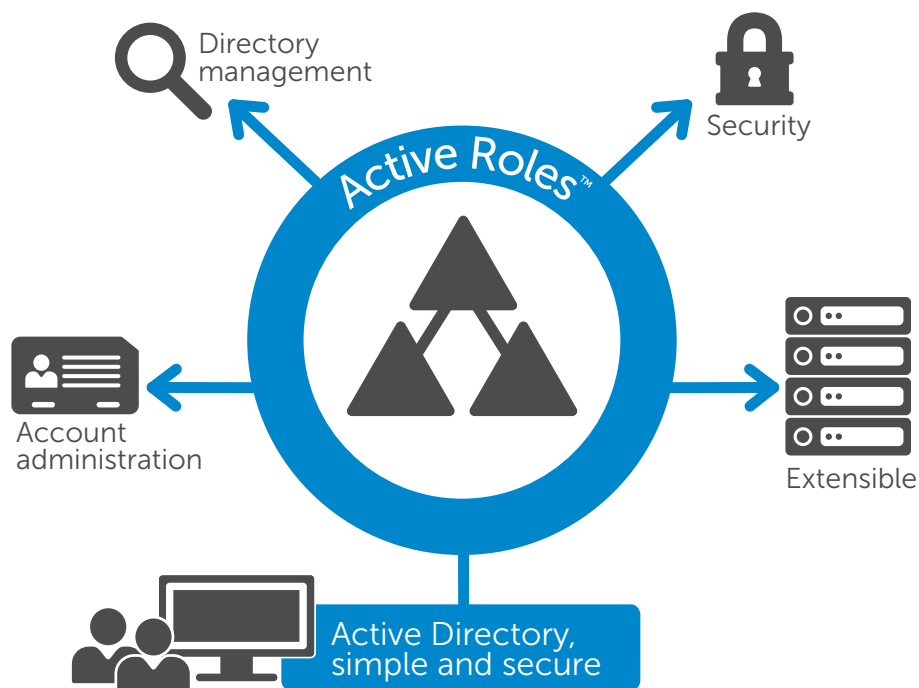
But with the frantic pace of today's businesses, administrators struggle to keep up with requests to create, change or remove access to AD, and they face security issues like terminated employees retaining access to valuable intellectual property, along with long days (and nights) struggling to support business requirements and satisfy auditors' requests for reports. Add the need to tightly delegate control of Active Directory among various

administrative groups and involve key people in IT processes through change approval, and today's Active Directory administrators need help!

Thankfully, help has arrived. With Active Roles™, you can solve your security issues and meet those never-ending compliance requirements by securing and protecting Active Directory simply and efficiently. Active Roles delivers automated tools for user and group account management that overcome the native shortcomings of Active Directory, so you can do your job faster. Active Roles is designed with a modular architecture, so your organization can afford to meet your business requirements today and in the future.

Benefits:

- Protects critical Active Directory data by strictly enforcing policies, eliminating unregulated access to resources, and regulating administrative privileges through a least-privilege model
- Automates account creation and deletion for secure and efficient user and group management in AD and AD-joined systems, as well as Exchange, Lync, SharePoint and Office 365
- Provides all tools necessary to securely and efficiently manage AD and overcome its native shortcomings, reducing IT workload and errors
- Reduces Active Directory administrative costs by giving help-desk personnel and data owners an intuitive, universally accessible console for Active Directory
- Eliminates security loopholes with tools and processes that generate audit-ready reports
- Deploys in weeks, for rapid time-to-value
- Delivers a standardized change approval process for AD administration, so you know who made what change and when
- Offers an integrated solution with a modular architecture, so you can meet your business needs today and in the future



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

For a complete list of system requirements, [click here](#).

Features

Secure access

Active Roles acts as a virtual firewall around 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 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 creation

Active Roles automates a wide variety of tasks, including:

- Creating user and group accounts in AD
- Creating mailboxes in Exchange
- Populating groups
- Assigning resource in Windows

It also automates the process of reassigning and removing user access rights in AD 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 in AD, Exchange, SharePoint, OCS, Lync and Windows, as well as any AD-joined systems such as Unix, Linux and Mac OS X.

Day-to-day directory management

With Active Roles, you can easily manage all of the following:

- 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

Active Roles also includes intuitive interfaces for improving day-to-day administration and help-desk operations via both an MMC snap-in and a web interface.

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.

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

About One Identity

The One Identity family of identity and access management (IAM) solutions, truly offers IAM for the real world including business-centric, modular and integrated, and future ready solutions for identity governance, access management, and privileged management.

One Identity

4 Polaris Way Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

© 2016 Quest Software Inc. ALL RIGHTS RESERVED. Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at www.quest.com/legal. All other trademarks, servicemarks, registered trademarks, and registered servicemarks are the property of their respective owners. Datasheet-ActiveRoles-US-CW-26207