

Active Roles For Healthcare Organizations

Overview

Active Directory (AD) is the backbone of IT infrastructure in large healthcare organizations, and its efficient management is crucial for operational integrity and security. However, common customer problems often stem from the complexity and manual nature of traditional AD management. One Identity's Active Roles addresses these challenges head-on, providing a solution that not only simplifies administration but also enhances security and compliance.

Addressing Administration Challenges

The disjointed tools and manual processes prevalent in AD management lead to inefficiency and a high potential for human error. Active Roles combats this by offering a unified and automated approach to AD management. With Active Roles, tasks such as account lifecycle management become streamlined, reducing the administrative burden and minimizing the risk of mistakes.

Enhancing Security

Security concerns, such as shared admin access, persistent privilege, identity proliferation and convoluted solutions, create an environment ripe for breaches. Active Roles introduces clear accountability and role-based access, ensuring that only authorized personnel have access to sensitive information. For instance, Active Roles can automate the removal of users from access groups when they no longer need the privileges, addressing the common oversight and exposure inherent in manual processes.

Benefits

- Ensure data integrity and compliance
- Consolidate onto a single console
- Automate AD tasks and group management
- Integration with other Active Directory solutions
- Synchronize directories
- Deploy zero trust least privilege for AD, Entra ID, and Microsoft 365

Mitigating Risks in Hybrid AD Environments

In hybrid AD environments, the lack of visibility and control over user and admin rights poses significant risks. Active Roles provides comprehensive oversight and management capabilities for both AD and Entra ID, facilitating better communication between teams and reducing the chances of duplicate efforts and inconsistencies.

Data Sensitivity and Compliance

Healthcare organizations handle highly sensitive data (ex: patient records, research data) which need to be protected with strict access controls. Active Roles provides fine-grained privileges with delegation to ensure identities are accessing the appropriate resources at all times. In addition, Active Roles provides the ability to decommission

privileges which is valuable in addressing the variable user base in healthcare organizations. This strict control also assists with meeting compliance requirements including HIPAA, and for tighter application licensing control.

Cost-Effective License Management

Organizations often face financial losses due to inefficient license management. Active Roles can help reclaim licenses from orphaned accounts, ensuring that the organization only pays for what it needs. This proactive approach to account management can result in significant cost savings.

Streamlining Enterprise Identity and Access Management (IAM)

Enterprise IAM projects often struggle with the inclusion of hybrid AD due to its complexity. Active Roles simplifies this integration, making it less labor-intensive and more cost-effective. It ensures that IAM initiatives stay on track by providing a cohesive management experience across AD and Entra ID.

Reducing Operational Inefficiencies

Managing hybrid AD can be labor-intensive, especially when different teams are responsible for AD and Entra ID. Active Roles eliminates this siloed approach by offering a centralized platform for managing both environments, thereby improving efficiency and reducing delays.

Simplifying Compliance and Auditing

Proving compliance and conducting audits with native tools can be challenging. Active Roles provides detailed audit trails and reporting capabilities, making it easier to demonstrate compliance with regulations like HIPAA. It also offers visibility into changes made within the AD, ensuring that all actions are traceable and accountable.

Ensuring Consistent Policy Enforcement

With Active Roles, policies are applied consistently across the organization. It automates approvals and enforcement, ensuring that identities, objects and groups have access to the right resources based on their roles and attributes. This consistency is key to maintaining a secure and compliant IT environment.

Conclusion

In conclusion, One Identity Active Roles is an essential solution for healthcare organizations facing the myriad challenges of AD management. By providing a unified, automated, and secure approach to AD administration, Active Roles not only solves immediate problems but also positions Providers for future growth and success. It's a strategic investment that delivers tangible benefits in terms of security, compliance, and operational efficiency.

About One Identity

One Identity helps organizations strengthen cybersecurity, boost efficiency and control costs through the One Identity Fabric, a holistic approach to identity and access management (IAM). By unifying IAM tools, including identity governance and administration (IGA), access management (AM), privileged access management (PAM), and Active Directory management (AD Mgmt), it ensures optimal functionality and efficiency. This cohesive structure reduces identity sprawl and extends governance to the farthest endpoints of your IAM ecosystem. 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.