

Managing a 30-domain AD environment with Active Roles

Facing a complex Active Directory environment, Intercontinental Exchange simplified AD governance with Active Roles.



Country: **United States**

Employees: **13,000**

Industry: **Finance**

Website: www.ice.com

Overview

Facing a complex Active Directory environment, Intercontinental Exchange simplified AD governance with Active Roles, achieving faster deprovisioning, modern service account management and stronger compliance.

Challenges

Following its acquisition of Black Knight, Intercontinental Exchange needed to consolidate its identity operations across a 30-domain environment. Its previous AD management solution lacked key capabilities, including support for gMSAs, making it difficult to move toward a more secure and modern approach to service account management.

The team was also facing a critical security challenge: slow deprovisioning during employee offboarding. They needed a better way to quickly remove access and reduce the risk of unauthorized activity.

Benefits

- **Prompt and centralized deprovisioning** during offboarding
- **Secure and efficient service account management** with gMSAs
- Eliminated reliance on high-privilege native AD tools
- **Straightforward compliance workflows** through integration with Enterprise Reporter

Products Featured

- Active Roles by One identity

Solutions Featured

- Identity governance for Microsoft environments

Solutions

Intercontinental Exchange turned to Active Roles by One Identity to simplify its AD management across 30 domains – including legacy Black Knight and current domains. Active Roles provided the exact kind of gMSA support the team needed while giving administrators a centralized and secure way to provision, modify and remove access quickly.

In 2023, Black Knight – a leading software, data and analytics company – underwent a major transformation following its acquisition by Fortune 500 financial services company Intercontinental Exchange. The move brought the organization into a global enterprise spanning more than 12,800 employees across 21 countries. Bringing those environments together meant managing a complex AD landscape with multiple domains, heavy nesting and different operational requirements.

It also meant replacing its previous AD management tool with Active Roles by One Identity, a solution that aligned with the IAM team's need for gMSA support and faster provisioning and deprovisioning. The combined team needed to securely manage 30 domains across both organizations while reducing reliance on native AD tools and excessive permissions. Tammy Holland, IAM manager of distributed operations at Intercontinental Exchange, helped lead that transition.

“Our previous AD management tool had some flaws where it couldn't do gMSAs and other things that Active Roles can do,” Holland said.

One of the biggest drivers behind adopting Active Roles was the team's move toward gMSAs.

As organizations look for ways to reduce security risks tied to traditional service accounts, Intercontinental Exchange wanted to move away from accounts that require human interaction. Active Roles gave the team the flexibility to support that shift.

“Active Roles works so fluently with our Group Managed Service Accounts. It makes it so much easier.”

Tammy Holland, IAM manager of distributed operations at Intercontinental Exchange

Security around employee offboarding was another major driver. Before Active Roles, deprovisioning could experience delays, creating a gap between an employee's departure and the completion of access revocation.

“If we didn't have Active Roles, our company would be less secure.”

Active Roles gave the team a centralized way to manage provisioning and deprovisioning, helping administrators remove access more efficiently while maintaining tighter control across the environment. As Holland put it, she's “using Active Roles from the moment I log in to the moment I leave,” making it the team's primary tool for day-to-day AD management.

The move also reduced the team's reliance on native Active Directory tools for managing gMSAs. Without Active Roles, administrators would have needed more elevated permissions to perform routine tasks – a trade-off Holland said would have made the organization less secure.

Beyond day-to-day administration, Active Roles also supports the team's compliance efforts through its integration with Enterprise Reporter. Together, the solutions provide the visibility needed for reporting and audits and simplifies the work for administrators. “The two together just make life so much easier,” Holland said.

And for those harbouring doubt or thinking they can get by using native AD tools, Holland asserts they'll change their mind if they experience the possibilities for themselves.

“Try Active Roles and you won't say that again.”

About One Identity

One Identity delivers trusted identity security for enterprises worldwide to protect every identity, human and non-human. With flexible deployment options and subscription terms, from self-managed to fully managed, our solutions plug directly into an organization's identity fabric to strengthen the identity perimeter, reduce breach risk and keep governance and compliance aligned at scale. Headquartered in Cork, Ireland, and trusted by 80 of the Fortune 100, One Identity is a leading provider of integrated identity governance and administration (IGA) and privileged access management (PAM) for identity security without compromise. Learn more at www.oneidentity.com.