CASE STUDY

Building better identity security across campuses

The George Washington University simplifies and automates critical identity administration and privileged access management processes for more than 26,000 students across multiple campuses building a strong foundation for a future larger-scale identity platform.

Key Facts

- **Company**
  The George Washington University
- **Industry**
  Education
- **Country**
  United States
- **Website**
  www.gwu.edu

Challenges

- Aging identity management system leads to failed tasks
- Inefficient directory access
- Time-sensitive Active Directory consolidation initiative

Results

- Simple, automated account lifecycle management for thousands of students, faculty and staff
- Password reset time cut from 10 minutes to near-real time
- Solid foundation for future deployment of larger-scale identity platform

Solutions

- Active Roles

The George Washington University (GWU) sought to streamline account lifecycle management and improve security to support an Active Directory centralization initiative. Tasks such as managing access for alumni were complex and time-consuming.

GWU partnered with XMS Solutions to build upon current One Identity Active Roles, using the Active Roles Sync Service to add orchestration functions to automate role creation. The university has simplified and automated identity and access management for more than 26,000 undergraduate and graduate students and 6,500 employees (includes faculty and staff). GWU has reduced password reset times from 10 minutes to near-real time, and now has a strong foundation for a planned future implementation of a wider identity platform on campus.

Seeking a streamlined account administration solution

Founded in 1821, The George Washington University (GWU), in Washington, D.C., is one of the nation's leading research universities. More than 26,000 students attend and nearly 6,500 staff and faculty work in the university's 10 schools and colleges.

Identity and access management(IAM) had become a major challenge for the GWU IT team, because the university relied on an aging Oracle-based identity management system that was no longer being supported. "The system was really slow, so a lot of identity and access management tasks were failing," says Becky Phares, IAM senior business analyst for GWU. As a result, a task like managing access for alumni, for example, was a complex process. "If an IT director wanted to reset alumni passwords, the only thing we could do was give them the same access everyone else at the university had. They could then technically reset anyone's passwords, which was a big security concern," Phares says.

> **"Active Roles is a powerful tool that reduces risk by giving us stronger security, more clarity and visibility, and automatic provisioning. It gives us a solid identity and access management foundation we can really build on."**
>
> Naveed Yousaf, Associate Director, Middleware and Identity Services, The George Washington University

The lack of system support was especially concerning because GWU was about to consolidate seven separate directories into a central Active Directory. “We wanted to offer Active Directory as a service, but we knew all the school’s IT directors wouldn’t want to give up control of their own directory system,” says Naveed Yousaf, associate director of middleware and identity services at GWU. “Our challenge was how to let them have that control. We knew it would take too much development effort to do it ourselves on the existing system.”

Automating user and group management tasks with One Identity Active Roles

Although the IT team had less than one year to move to a new identity platform, it decided on an interim solution: One Identity Active Roles, a single, unified tool that automates and streamlines user and group management tasks in hybrid Active Directory environments.

Working with technology partner XMS Solutions, GWU implemented One Identity Active Roles, taking advantage of features such as Active Roles Sync to add orchestration functions to enable the creation of roles. “One Identity Active Roles is not just an Active Directory administration tool. We pushed it far beyond that to include automated role provisioning,” Yousaf says. “No other existing solution gave us that ability.” The GWU IT team used Active Roles to create specific roles, including IT Support, that are automatically granted to specific departments across the university.

Simplifying account lifecycle management across campus

Using Active Roles, GWU has simplified user account management and provisions new users with the right access to learning applications, email and other systems. As a result, GWU has eliminated most of the failed tasks that were common on the previous identity management platform. “Previously, we were unable to provide automated role-based access,” Phares says. “Now, when someone new is onboarded, they will automatically get the level of access they need within the Active Roles system. Granting access to a new person used to involve mimicking a previous employee’s access, which was not ideal from a security perspective.”

“Previously, we were unable to provide automated role-based access. Now, when someone new is onboarded, they will automatically get the level of access they need within the Active Roles system.”

Becky Phares,
IAM Senior Business Analyst,
The George Washington University

GWU Identity Services Team that made all this possible

Tielor Robinson - Identity Engineer

Becky Phares - Senior Identity Analyst

Dhina Ramaian - Identity Engineer

Sheema Begum - Identity Engineer

Andy Navarrete - Identity Engineer

Chuck Moore - Project Manager

Frank William - Identity Admin

"We expect One Identity Active Roles to reduce operational time and errors, resulting in improved service to all users, from students to faculty to IT."

Naveed Yousaf,
Associate Director,
Middleware and Identity
Services, The George
Washington University

A better experience for students, faculty and IT

With the new solution, GWU will also be able to offer users a better overall experience. "We expect Active Roles to reduce operational time and errors, resulting in improved service to all users, from students to faculty to IT," says Yousaf. As an example, password resets typically took 10 minutes for each user. Using Active Roles, resets can be performed in near-real time, because resets occur in the cloud on Microsoft Azure and then propagate down to Active Directory.

Additionally, GWU IT administrators are notified immediately when a task fails. "We have an employee who spends up to two hours a day on failed tasks," says Phares. "Now, instead of waiting until the next day for a report telling you tasks failed, the administrator will go into Active Roles and see the failed tasks right away, restarting the task before it becomes an issue."

A solid foundation for the future

For GWU, the Active Roles solution goes beyond being a bridge to a broader identity platform. "This tool is much more than just a stopgap before we deploy a larger solution," says Yousaf. "Active Roles is a powerful tool that reduces risk by giving us stronger security, more clarity and visibility, and automatic provisioning. It gives us a solid identity and access management foundation we can really build on."

About One Identity

One Identity, a Quest Software business, lets organizations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. With our uniquely broad and integrated portfolio of identity management offerings including account management, identity governance and administration and privileged access management, organizations are empowered to reach their full potential where security is achieved by placing identities at the core of a program, enabling proper access across all user types, systems and data. Learn more at OneIdentity.com