ONE IDENTITY
by Quest

UK parliament optimises Active Directory (AD) management

UK Parliament
Digital Service

With Active Roles, PDS simplifies Active Directory management while increasing security and freeing up time for hybrid cloud migration

Customer:

Parliamentary Digital Service (PDS)

Industry:

Public Sector – Government

Country:

United Kingdom

Website:

www.parliament.uk

- Frees up time to work on strategic migration projects
- Automate JML and PAM to increase protection, efficiency and security
- Handles licensing challenges for Zoom conferences during pandemic
- Drives move to Active Directory and Azure Active Directory integration

Challenge

- Inefficient management of joiners, movers and leavers (JML) resulting in hours lost every month
- Increasing risk by manually controlling privileged access management (PAM)
- Lack of support for hybrid cloud

Solution

- One Identity Active Roles

The Parliamentary Digital Service (PDS) supports the UK's House of Commons and the House of Lords as well as parliamentary staff. Serving many purposes, PDS supports IT, manages the parliamentary network, develops applications and plans for future technological needs. It also runs the UK Parliament website and social media.

Whilst the crowd of tourists outside the UK Parliament's House of Commons or House of Lords may be large, the crowd of cybercriminals outside the parliamentary network is even larger. "The security threats are non-stop," says Cherry O'Donnell, head of identity and access management at PDS. "We are a major target, making network security a top focus."

Managing multiple changes

Keeping a network secure by carefully managing access is no easy task. For PDS, it's challenging because of the number and variety of accounts in Active Directory (AD).

There are those accounts for the members of parliament (MPs) and their personnel as well as the Lords and their employees. Then there are more than 2,000 permanent parliamentary staff, and accounts will have to be created or deleted for the 100 to 200 people who either join or leave the network each month. In addition, AD groups will need updating for the many existing network users who take up new parliamentary positions. Finally, among the AD groups, there are also the privileged accounts, which PDS has to control in order for administrators to gain access to hardware, including servers for tasks like patching.

> "With One Identity Active Roles we have a **clear view** of who has **permissions** at any one time as well as in the past. There is **no room for error**."
>
> Cherry O'Donnell, Head of Identity and Access Management, PDS

Time-consuming tasks

Whether it was managing joiners, movers and leavers (JML) or controlling privileged access management (PAM), the work in AD was largely manual. It consumed many hours a month that the PDS team could have used on strategic projects. The lack of automation meant a greater risk of human error, creating an increased chance of someone gaining access to something they shouldn't. Moreover, the legacy solution for access management wasn't optimised for Azure AD and a hybrid solution, featuring on-premises and cloud AD.

> "The hours we save allow us to press ahead with initiatives such as re-platforming for Active Roles 7.4."
>
> Cherry O'Donnell, Head of Identity and Access Management, PDS

PDS engaged One Identity to help enhance the management and security for a hybrid AD infrastructure. The organisation had an earlier version of One Identity Active Roles and wanted to optimise their solution to take advantage of the latest innovations in the product. With the support of the One Identity team, PDS began the improvement process, replacing thousands of lines of command-line shell and scripting language with Active Roles leveraging powershell modules and Active Roles workflows. "We had a One Identity consultant working with us," comments O'Donnell. "We all worked really hard on the project and delivered what we set out to do."

Saving hours a month on access management

JML management in AD is now fully automated, allowing the identity and access management team to recoup precious time. O'Donnell states, "The hours we save allow us to press ahead with initiatives such as re-platforming for Active Roles 7.4. Saving hours of time means we can now do important work like threat analysis. I'm surprised we found time to get things done in the past." There are no longer emails flying around with requests for account access when someone new begins or account termination when someone leaves. Integrations with human resources (HR) means that JML data is shared with Active Roles and accounts are activated or terminated automatically. "Access to the basic services such as email and OneDrive are in place when they start. They call us to set their password and they're ready to go," comments O'Donnell.

Making privileged access seamless and secure

PDS has also automated PAM, with time limits now enforced on access to servers for tasks such as patching. "Once the allocated time for a task is up, Active Roles automatically removes the permission," says O'Donnell. "There is no risk of anyone forgetting to do it." PDS is moving towards a Zero Trust model where every administrative action is authenticated uniquely. But for the time being, PAM is easy with admins requesting permission via a web portal with dropdown menus. Active Roles generates the permission unless the work is so sensitive it needs to be authorised by O'Donnell or another senior member of PDS.

Once permission is granted, emails are fired off to the PDS cybersecurity team and the identity and access management team to ensure there is visibility of any elevations. Plus, records of access are generated in Active Roles for auditors to see if required. "With One Identity Active Roles we have a clear view of who has permissions at any one time as well as in the past," says O'Donnell. "There is no room for error."

Enabling a powerful response to the pandemic

With Active Roles, PDS has also enabled the UK Parliament to respond in an effective way to the pandemic. MPs and government ministers have been using Zoom video communications for discussions and debates. However, with the UK Parliament holding a finite number of Zoom licenses, PDS needs to carefully manage access. "We are building a web form powered by Active Roles," states O'Donnell. "The form will give the name and the date of the discussion or debate and Active Roles then adds the MP or minister to the AD Zoom group. Access is then revoked automatically at the end of the day."

Going complete cloud on access management

The PDS team is now looking forward to adopting Active Roles 7.4. "It's pure cloud aware," says O'Donnell. "We'll be able to create a user in the cloud and give them access to SharePoint and One Drive all through a single workflow. It's a true one-stop solution." For O'Donnell, the improvements in 7.4 reflect the customer-centricity of One Identity. "Technology gives us new opportunities whilst creating new risks at the same time," she says. "One Identity provides the tools to make the most of the good while protecting us from the bad. It's peace of mind out of the box."

About One Identity

One Identity, a Quest Software business, lets organisations implement an identity-centric security strategy, whether on-prem, in the cloud or in a hybrid environment. Our uniquely broad and integrated portfolio of identity management offerings includes account management, identity governance and administration and privileged access management. Learn more at OneIdentity.com.