International retailer, JYSK, eliminates AD issues with Active Roles

Denmark-based international home goods retailer brings elegance, style and efficiency to its Active Directory infrastructure

"Before we implemented Dell Security Active Roles, our Active Directory management was quite chaotic. Access rights were not under control."

Michael Gorm Jensen,
System Administrator IT Server Operations,
JYSK Nordic

Customer profile

JYSK

Company	JYSK Nordic
Industry	Home Goods Retailer
Country	Denmark
Employees	10,000+
Website	www.JYSK.com

Business need

To streamline and gain control of a complex Active Directory infrastructure that included an unruly number of domain admins, unstandardized naming conventions, and encompasses 10,000 users in 1,000 retail shops, located in 19 countries.

Solution

JYSK implemented Dell Active Roles into its Active Directory (AD) environment, which immediately paid off by delivering enhanced management, tighter controls – and facilitated approval workflows that ensured requested changes are necessary and that all required parties sign off on them. Plus, it reduced domain-admin access by more than 90 per cent.

Benefits

- Reduced call volume to service centre
- Accelerated change-management capabilities
- Delivered the ability for a four-person staff to more easily manage a 450-server environment
- Eliminated haphazard overprovisioning of access rights
- Ensured appropriate AD access to the right people.

Solutions at a glance

- Identity & Access Management

"Before we implemented Dell Security Active Roles, our Active Directory management was quite chaotic. Access rights were not under control," said Michael Gorm Jensen, System Administrator IT Server Operations, for Denmark-based international home goods retailer, JYSK Nordic. "We had trouble identifying all the domain admins across our network. And more frustrating was that we didn't know why someone was given access or why someone possessed a domain admin account at all."

With more than 10,000 employees and 1,000 stores in 19 countries, JYSK Nordic is a massive enterprise — and still growing. Managing the far-flung Active Directory infrastructure was a challenge to say the least. The local IT teams in each country implemented their own unique naming convention, so there was no standardization. In addition, there were few controls over the domain-admin approval process. JYSK's IT Server Operations team eliminated multiple unnecessary domain admin accounts on their system.

Jensen said, "As a team, we were asking ourselves, 'Is this request necessary? How is this access being used?' We needed to find a system that could give us complete control over Active Directory roles and access credentials."

To manage the sprawling, international enterprise, the IT Server Operations team were using a combination of native AD management utilities, as well as a cumbersome third-party solution that required hiring consultants to update and make changes. The third-party solution should have handled all Active Directory (AD) user creation, and access-group and distribution-group permissions. It did centralize much of the AD administrative work, but it was so inflexible that it required constant coordination between managers and regional service centres and the HQ service centre (support centre) in Denmark. The country-based centres

were unable to provision, change or de-provision users or domain admins.

Much of the time, the process consisted of multiple phone calls from a contact in the country requesting user access changes. The technicians in the service centres were unable to access user information and had to ask who the person was, why they needed access and then ultimately take the caller's word that the information was accurate and the request was legitimate.

"So it was just whatever way the wind blew, there was no real control over it," said Jensen.

On top of this, if any mistakes were made with user information or domain admin entries — or not entered exactly matching the unique country naming convention — the access did not work. Then the service techs would have to delete the user completely and start all over again. It was a huge time sink and a hassle.

Secure but unmanaged

Despite JYSK's AD management situation, they were better off than many enterprises of their size and scope. Due to a commitment to rock-solid security

Products & Services

Software

Dell Active Roles

practices, their overall IT infrastructure was protected and had experienced no breaches. The Active Directory architecture was a completely closed system.

The IT Server Operations team recently upgraded all the hardware in their server room to support approximately 450 virtual servers, the backup systems and other resources located in the 19 countries that made up their operating region. Each country has a physical administration server that runs several virtual servers in the country, including print, file and salary servers. If the country is large enough, it also has a dedicated anti-virus server, with smaller markets sharing a centralized anti-virus server.

The IT Server Operations team managed all the physical and virtual servers, plus were tasked with performing ongoing maintenance, development and any other work needed to keep the retailer's systems running smoothly.

Need for efficiency

But to bring a whole new level of efficiency to user and domain admin access, the retailer needed a tool that brought easy and simple structure that could be repeated across country borders. They needed one that provided a clear view of processes, user info and data resources, as well as support expansion that included cloud resources and federated credentials.

When Jensen joined JYSK three years prior, he immediately identified the need to gain control of the AD infrastructure. "I thought: 'This is not going to end well. It's going to crash as some point.' So, we needed to do something."

They looked at upgrading the existing tool but quickly eliminated it. They considered Microsoft Orchestrator, which would have incurred no additional expense to JYSK Nordic because of their enterprise licensing agreement with Microsoft, but Orchestrator didn't

have all the required capabilities. Team Manager Ander Harder, IT Server Operations, recommended Dell Active Roles to JYSK Nordic's CSO.

After assessing other tools, they started testing Active Roles in their HQ service centre. After successfully testing, it was rolled out to all JYSK Nordic's service centres. Now, the retailer has users that do all the AD tasks, such as creating users, de-provisioning, changing titles, passwords and locations on their own without the need for corporate intervention.

Jensen said, "It sounds so simple now, but before we implemented Active Roles that couldn't happen. Every time they wanted to change a password or needed to change a surname, the local service centres had to contact us."

Approval workflows

Now JYSK's IT Server Operations team has control over permission groups and distribution groups. There are workflows for any changes to ensure that the requester actually should have the access they have requested and that all approvals are obtained before access is allowed.

"We've created workflows so that nobody can go in and say 'I want access to this distribution group' or 'I want access to that security group' without the manager being notified," said Jensen. "If someone wants a title change, it goes straight to our service centre and our HR department reviews changes as part of the workflow."

Now, thanks to Active Roles, the service centres have access to all information about the user on one page. When a tech starts up Active Roles, they can see everything. They instantly know what user they are dealing with, including the type of computer they are using, the serial number, the user's location – and they can perform all administrative tasks quickly and easily in Active Roles.

"It sounds so simple now but before we implemented Active Roles, every time a password or a surname needed to be changed, the local service centres had to contact us."

Michael Gorm Jensen,
System Administrator IT Server
Operations, JYSK Nordic

DELL

> "Our service centre staff was so happy when we showed them the capabilities of Active Roles, the place erupted into a party mood."
>
> *Michael Gorm Jensen,*
> *System Administrator IT Server*
> *Operations, JYSK Nordic*

All changes regarding access rights are automatically sent to the relevant manager for approval as part of the workflow.

Control and Insight

"Active Roles made everything much easier for us and for the service centre – and even more so for the users out there," said Jensen. "Our managers now have more control over who has access to which resources. Most importantly for us and the users in the service center, we don't have to take sole responsibility for granting access the end user."

When we rolled out Active Roles to the HQ service centre, they instantly picked it up as if they've been using it for months. It's so easy and intuitive to use. Of course, they couldn't keep quiet. They had to tell some of the other service centres in the other countries and immediately they started calling us ... and calling us ... and calling us. 'When are we getting Active Roles?'"

"Now when a service center manager or store manager calls and asks for a new or automated feature (whatever it might be) – which happens about five times a day – we can do it. We don't have to bring in a consultant and wait three or four weeks and pay a fortune to make changes. We can actually go in and do it almost instantly.

"Our service centre staff was so happy when we showed them the capabilities of Active Roles, the place erupted into a party mood. We have Active Roles running in all the service centres now in the 19 countries. And they're very happy about it," said Jensen.

About Dell Security

Dell Security solutions help you create and maintain a strong security foundation with interconnected solutions that span the enterprise. From endpoints and users to networks, data and identity, Dell Security solutions mitigate risk and reduce complexity so you can drive your business forward. www.dell.com/security.

DEPARTMENT OF YES

View all Dell case studies at Dell.com/CustomerStories

DELL