CASE STUDY

Protecting the data of refugees and those who help them

Danish Refugee Council boosts security and efficiency by increasing control over IT access and cutting provisioning to an hour with One Identity

Key Facts

- **Company**
  Danish Refugee Council
- **Industry**
  Nonprofit
- **Country**
  Denmark
- **Employees**
  7,000
- **Website**
  www.drc.ngo

Challenges

- Consistently manage IT and data access for 7,000 global employees
- Boost efficiency and ensure quick access to IT resources
- Meet data-protection regulations
- Minimise costs

Results

- Increased control and insight over system access
- Achieved immediate and accurate provisioning processes
- Standardised and automated identity workflows
- Simplified compliance
- Boosted efficiency, saving at least 10,000 hours of effort annually

Solutions

- One Identity Active Roles

To protect refugees, employees and supply transports—plus minimise costs—the Danish Refugee Council (DRC) wanted to standardise the management of Active Directory.

After evaluating solution options, DRC deployed One Identity Active Roles. As a result, DRC established user templates and automated workflows for governing access for 7,000 global employees. Today, DRC can provision new users in an hour. IT staff have greater control over who can access which applications and data. And the organisation has increased staff efficiency, boosted savings and simplified regulatory compliance.

Every two seconds, a person is forcibly displaced from their home as a result of conflict or persecution. The numbers add up quickly. Today, there are 68.5 million refugees and displaced people around the globe. Besides physical protection and shelter, relief organisations provide a variety of services to help. However, as they deliver assistance, they must also protect data—about refugees and operations including aid shipments—from unauthorised access to minimise risks.

The Danish Refugee Council (DRC) is one of the leading global organisations helping displaced people rebuild their lives. Operating in more than 30 countries, including conflict-affected areas and refugee migration routes, DRC uses advanced security technologies to protect all its systems and data from unauthorised access.

To meet evolving threats and help more people, the organisation continually looks for ways to boost security, save money and improve efficiency. For these reasons, DRC replaced its disparate communication tools with Microsoft Office 365, migrated to Microsoft Dynamics 365 and adopted Microsoft Azure Active Directory. In addition, DRC centralised control over system-access privileges in one IT team at its corporate headquarters. Michael Schiøtt, senior Microsoft system administrator at DRC, says, “We went from managing just a subset of users to handling

> **“We are increasing security, reducing costs and saving at least 10,000 hours of administrative effort annually with Active Roles. It’s a smarter way of working.”**
>
> Michael Schiøtt,
> Senior Microsoft System Administrator,
> Danish Refugee Council

access for 7,000. To manage and delegate access for this many people, we needed a tool that could give us better insight into our Active Directory and allow us to automate processes like the creation of identities."

DRC reviewed technologies and chose One Identity Active Roles. "It was an easy choice," says Schiøtt. "Active Roles is a powerful management tool that allows us to manage our Active Directory in a very smart way."

Improves security and speeds user provisioning to one hour

The IT team used Active Roles to automate processes to provision and deprovision system access based on changes made to the organisation's HR system. "Automating these workflows ensures consistency and that nothing is forgotten," says Schiøtt. "Today, we are able to provision consistent, role-based privileged access for the IT community, which is raising the level of security. And new users are provisioned almost instantly now that we use Active Roles. This is much faster than the two to three days it used to take, when all of the processes were manual." The automated workflows also generate email messages that notify HR and managers about changes to identities in Active Directory and to system access.

Simplifies regulatory compliance

Today, DRC's corporate IT team can instantly see which global users have access to which systems, what changes have been made to Active Directory and who made them. "One of the biggest advantages we gain with Active Roles is being able to trace everything that's done in Active Directory," Schiøtt explains. "This makes it easier to comply with Europe's General Data Protection Regulation." DRC can also see information such as unused accounts. "Implementing Active Roles has been a process of cleaning things up as well as standardising roles and processes."

Supports delegation and saves money

DRC is now fine-tuning the solution to realise greater efficiencies. For example, IT staff are implementing even more detailed controls over the types of data people can access by using virtual attributes in Active Roles. They are also automating workflows such as delegation processes to ensure consistency in who can manage access for which users, including staff who work in a particular country, department or group. "The more we standardise things, the simpler the world is to handle," says Schiøtt. "We are increasing security, reducing costs and saving at least 10,000 hours of administrative effort annually with Active Roles. It's a smarter way of working that allows us to free up resources to help more people live dignified lives."

> "New users are provisioned almost instantly now that we use Active Roles. **This is much faster** than the two to three days it used to take."
>
> Michael Schiøtt,
> Senior Microsoft System Administrator, Danish Refugee Council

About One Identity

The One Identity family of identity and access management (IAM) solutions offers IAM for the real world including business-centric, modular and integrated, and future-ready solutions for identity governance, access management, and privileged management.

View all One Identity case studies at OneIdentity.com/casestudies