

Universidad de La Rioja manages AD more efficiently

Systems administrators deliver more value now that routine tasks can be securely delegated to help desk staff with Active Roles from One Identity

Key Facts

Company

Universidad de La Rioja

Industry

Education

Country

Spain

Employees

7,600 students, 700 employees

Website

www.unirioja.es

Challenges

Systems administrators at Universidad de La Rioja were spending too much time on routine administration of Active Directory. Native tools could not secure, granular delegation of these tasks to help desk staff and resource owners. Moreover, provisioning of accounts was time-consuming and error-prone, and a lack of detailed auditing introduced security risks.

Results

- Saved valuable IT time by enabling secure, granular delegation of routine administrative tasks
- Increased productivity of help desk operators by delivering an easy-to-use web interface
- Enhanced security with role-based access and detailed auditing

Products

Active Roles

The Universidad de La Rioja was founded in the academic year 1992-1993 and today is the only higher education and scientific research center in the Rioja region of Spain. The institution has 7,600 students, 450 professors and researchers, and 250 staff members.

Managing Active Directory is difficult with native tools

IT staff at the Universidad de La Rioja were trying to manage Active Directory (AD) using native tools, but found those tools to be insufficient. Staff found the tools to be too complex and not sufficiently flexible or intuitive. In particular, they were unable to provision accounts efficiently, to create forms with specific values to facilitate basic administrative tasks, or to provide closed forms for standard processes.



“Thanks to Active Roles, systems administrators no longer have to perform routine administrative tasks without any **technical value.**”

Jesús M^a Álvarez Ruiz, Systems Engineer, Universidad de la Rioja

In addition, the university was finding that systems administrators were spending too much time on routine administrative tasks. It wanted to be able to delegate those tasks to support engineers, help desk operators and advanced users—but without giving them broad administrative rights, and while being able to audit their individual actions. The university also wanted to offer self-service capabilities to users—and, of course, it wanted all of this functionality through an easy-to-use web interface.

“Native AD management was not as comprehensive as we wanted. We sought to administer identities, improve administration monitoring, allow end-user self service, and enhance security in a centralized way, all with extended delegation and auditing capacities,” comments Jesús M^a Álvarez Ruiz, Systems Engineer, Universidad de la Rioja. “We also needed a customizable AD management web console—functionality that was missing in the native environment.”

Active Roles simplifies comprehensive AD management

The Universidad de la Rioja began looking for a comprehensive AD management tool. IT staff were already using several One Identity tools, including Quest Toad for Oracle. It therefore decided to evaluate One Identity’s AD management solution, Active Roles, as well as Microsoft Forefront Identity Manager (FIM).

After carefully reviewing both products, the university selected the One Identity solution. Active Roles enables easy administration of user and group accounts, strictly enforced role-based security, day-to-day identity administration, and built-in auditing and reporting. The Universidad de la Rioja was particularly impressed with the tool’s ease of use, power and speed of deployment.

“Active Roles has enabled us to deliver important functionalities to network administration, without the user being affected or the need for additional

technical knowledge. The quality of the product and functionalities in terms of deployment time and ease of use are clear differentiating factors over other solutions in the market,” notes Álvarez.

Give control over resource access to the resource owners, not IT

Using Active Roles, the university has been able to delegate appropriate administrative authority to help desk operators and heads of service throughout the organization, enabling those staff members to act as delegated administrators of the resources assigned to their services. And because the solution’s web-based interface is easy to use, the delegated administrators do not need extensive technical skills or training, which enhances productivity. And delegating administration of resources to the resource owners—who understand better than IT who needs access—makes systems function more effectively.

An easy-to-use web interface means no technical training is required

“Before deployment of Active Roles, all assignment of members to groups and all assignment of permissions in AD had to go through us, the Microcomputing and User Service,” explains Álvarez. “Now, once the solution is deployed via a webpage, the delegated administrators can keep users updated and assign permissions independently, without needing technical knowledge. We can also create groups based on user attributes, which was not possible previously.”

Granular delegation of administrative rights frees up highly skilled IT staff

Delegating specific administrative rights to help desk operators and others has freed more highly skilled system administrators to work on more difficult projects important to the university. “Thanks to Active Roles, systems administrators no longer have to perform routine administrative tasks without any technical value,” explains Álvarez. “That enables them to focus on tasks

that deliver greater value to the organization.”

Detailed auditing enhances security and ensures accountability

Moreover, with Active Roles, the university can audit in detail 100 percent all the tasks performed on Active Directory, enhancing security by ensuring accountability for all administrators. Finally, the university credits the automation provided by Active Roles with reducing human errors, which has also helped enhance system performance for users.

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.

Learn more: OneIdentity.com