

ATU

The Atlantic Technological University (ATU) is the learning place of over 22,000 students, offering almost 600 academic programmes from pre-degree to doctoral level. Their mission is to advance economic, social, and environmental sustainability through education and engagement, producing graduates who are innovative, confident, and capable of leading the development of the region and beyond.

Industry:

Tertiary Education

Number of Employees:

Ca. 2700

Number of Sites:

9 in West and Northwest Ireland

Endpoints Running ABR:

4000 (Windows and macOS)



The Challenge

The challenge faced by ATU stemmed from their vast number of users with varying needs. This, combined with security concerns over users having around-the-clock administrative access, led to the search for a solution that would give the organization visibility, allowing them to gain a better understanding of what programs their users required on their endpoints; and control, providing the tools for users to gain elevated access in a safe and secure manner.

The solution needed to adhere to compliance regulations such as the GDPR, and, with the move to a mobile workforce (accelerated by COVID-19), the university required a solution that would work across Azure AD and domain-joined devices.

The Solution

ATU chose Admin By Request Privileged Access Management as the solution due to the range of features available which would allow for granular access control across IT systems (Settings and Sub-Settings for user groups), as well as the Pre-Approval and Run as Admin features - both of which negate the need to provide full admin access to users at any point by allowing only approved applications to gain elevated privileges when they're needed.

These features, in addition to extensive logging capabilities and Azure AD and Intune integration, made Admin By Request an Ideal solution for ATU to invest in.

The solution was deployed to all staff and student-loaned laptops using Intune, with installation taking a few hours. Configuration was a simple process through extensive use of the Admin By Request Pre-Approval feature, and Azure AD and SCIM integration.

The Impact

Since deploying the solution, ATU is able to apply least privilege principles with 'surgical precision', providing different levels of access to staff and users.

"This allows us to keep our attack surface to the absolute minimum while still providing the end user access to the software they require. It has been a crucial piece in our endpoint security management and adoption of a zero-trust security model."

They have added Power BI to their Admin By Request integrations, have been able to replace Microsoft LAPS on Azure AD-joined devices with the Admin By Request Break Glass feature, and administrative sessions are no longer needed for users to install the software they require.

Compliance requirements have been met, desktop-related support issues have decreased, and Administrators are more than satisfied with the solution, "It is an invaluable tool".

Moving Forward

In future, ATU is looking to deploy Admin By Request on all endpoints, in conjunction with moving the organization to Azure AD-joined devices only. They have ensured all new devices have the PAM solution installed through Autopilot, and are interested in further Admin By Request integrations with the Microsoft Power Platform, in particular, Power Automate.

“

Admin By Request has been fundamental to adopting a secure least privilege model. Our users can install software without being administrators, and technical staff can support users with administrative privileges using the Support Assist feature when needed. Admin By Request has enabled us to substantially reduce the attack surface previously present when users had constant administrative privileges.

”

