CASE STUDY

UK university cuts IT burden with Unix/Linux single sign-on

University of East Anglia achieves 100 percent ROI in just nine months with Authentication Services

Key Facts

Company
University of East Anglia

Industry
Higher education

Country
England

Employees
3,000 plus 16,500 students

Website
www.uea.ac.uk

Challenges

The university needed to enable single sign-on to Windows and Unix applications for more than 40,000 user accounts in order to cut help desk costs, reduce administrative overhead and improve security.

Results

- Delivered 100 percent ROI in just nine months
- Enabled single sign-on, reducing help desk workload and improving the user experience
- Enabled centralised control and auditing of access to all systems, saving IT time and enhancing security
- Enabled security policy compliance through stronger password security

Products

Authentication Services

Founded in the 1960s, the University of East Anglia (UEA) is one of the most popular universities in the UK, with more than 300 different subjects available for study. UEA's IT department supports a community of approximately 13,000 undergraduate students, 3,500 postgraduate students and 3,000 staff members. The Active Directory (AD) and authentication team used One Identity Authentication Services to improve access to the university's Unix and Windows applications.

Lack of centralised authentication means extra work for IT and frustrations for users

The AD and authentication team at UEA is responsible for providing users with secure access to the university's various IT systems, including email, desktop applications and UEA's portal. However, separate authentication processes were required for UEA's Unix and Windows applications. Users were assigned the same username and password on each platform,

> "The benefits we've realised mean that Authentication Services has already paid for itself. Over time, the ROI will continue to rise as **Authentication Services** continues to add value."
>
> *Jon Woodley, Head of Systems, UEA*

but there was no automatic password synchronisation. Users were encouraged but not required to keep their passwords the same across systems. But because this was a tedious, manual process, passwords often got out of sync, resulting in a high volume of support calls to the help desk.

The lack of centralised access control also taxed IT staff resources significantly. Each of the 250 Unix servers and 1,750 Unix workstations had to be configured individually to ensure the systems were not subject to unauthorised access, so each of the 50 IT support staff was spending one to five days per week just on Unix maintenance.

Microsoft's Services for Unix unified identities but led to recurring unplanned downtime and security risks

To address these issues, UEA implemented Microsoft's Services for Unix to combine the two authentication processes by supplying AD with information from Unix's directory services, NIS. This resulted in a single database of users and an automated synchronisation of passwords.

However, the solution was short-lived; the numerous systems at UEA put Services for Unix under strain, causing delays and occasional crashes. If a crash occurred during the day, downtime was limited to about five minutes. But if a crash happened after normal working hours, email, other critical applications and user data were unavailable for a much longer period. With students working at all times of the day and night, this downtime was not acceptable to the university. Furthermore, at certain key times in the year—for example, during exams, at the start of new academic year, or during clearing (the process to offer university places)—unplanned system downtime meant risks to UEA revenues.

In addition, the AD and authentication team also discovered limitations in the password security of Services for Unix that left the program open to security abuses and phishing attacks.

Authentication Services extends AD security to Unix and Linux

One year after implementing Services for Unix, UEA began to search for an alternative solution. Following a thorough proof of concept project, the university selected Authentication Services from One Identity.

Authentication Services seamlessly extends the security and compliance of the existing Active Directory infrastructure to Unix and Linux platforms and applications. This approach simplifies identity management and enables cross-platform access control, reducing IT workload while enhancing security and compliance. And it improves the user experience by enabling centralised authentication and single sign-on.

UEA was impressed that Authentication Services integrated with the Services for Unix information already in its

AD; this enabled the university to make use of its existing AD-based user provisioning with a phased migration. UEA was also pleased that the One Identity team took time to understand the university's requirements. In addition, the university saw Authentication Services as good value for the money because it contained all of the functionality UEA required, eliminating the need to purchase any additional modules.

Centralised access control enhances security

Security concerns have diminished for UEA thanks to the new, centralised approach to access control. "Authentication Services provides single sign-on authentication for access to all of our systems, enabling us to centrally configure, control and verify access to each of them," explains Jon Woodley, Head of Systems at UEA. "This gives us peace of mind—for example, we have considerably more confidence that a student is unable to gain unauthorised access to sensitive systems such as the university's finance system—and Authentication Services also simplifies the auditing process."

Single sign-on eliminates manual password synchronisation—and associated help desk calls

Authentication Services has also dramatically reduced the number of help desk and support calls at UEA. "I would estimate that each year, around 25 percent of our 4,000 new students needed help with a password synchronisation problem—which equates to a lot of calls," says Woodley. "Authentication Services has eliminated these problems, freeing up the help desk to focus on other issues."

UEA's IT support staff have seen similar time savings. "These people now have more time to focus on other tasks, instead of being bogged down with system access issues," notes Woodley.

Eliminating unplanned downtime reduces risk of lost revenue

The risk of lost income due to authentication issues has been considerably reduced at UEA because Authentication Services has eliminated unplanned system downtime at critical times. "Authentication Services provides us with greater confidence in our systems and ensures that our users experience reliable system availability," explains Woodley.

Compliance with password policy means enhanced security

Password security is much stronger with Authentication Services as well. "Our previous issue with limited password security has been resolved," states Woodley. "We now fully comply with the standards set in our security policy."

Full ROI in less than a year

In fact, Authentication Services has provided UEA with a full return on its investment in only nine months. "The benefits we've realised mean that Authentication Services has already paid for itself," adds Woodley. "Over time, the ROI will continue to rise as Authentication Services continues to add value."

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