ManageEngine
AD360

9 IAM challenges in education and how to solve them

Table of Contents

Introduction

Identity and access management (IAM) is the security discipline that enables the correct individuals to access the right resources at the right times for the right reasons. IAM capabilities such as identity life cycle management, user authentication methods, policy and role management, and approval-based workflows are used to protect and manage user identities, which is critical for the organisation and individuals to maintain appropriate security. IAM has become an essential element of security plans for many organizations.

Why IAM is important for the educational sector

Educational institutions contain sensitive data of students, staff, faculty, research materials, and so on, and they are often overlooked when talking about cybersecurity. They must secure their user identities and prevent unauthorized access to sensitive user information such as contact details, academic records, financial information, and health data, while offering systems that are easy to use and reliable with consistent uptime.

Recently, identity management for education has witnessed a dramatic change. There is a notable increase in e-learning, where classes are conducted remotely and on digital platforms. Now that's a massive amount of data to keep up with. Many educational institutions are already facing security crises and trying their best to respond to them. Providing a secure learning environment has become a high priority, as technology and cloud resources continue to play a growing role on educational premises.

Schools and universities not only have to consider employees using their systems, resources, and information, but external users like students as well. Aside from students, teachers, and other staff, depending on the age of the student, parents will also be given access to these resources. Adding to this, users are becoming more and more technically savvy with each year—they expect intuitive interfaces and modern functionality. Therefore, one of the major technology challenges that educational institutions face is providing an optimal user experience while securing access to their systems.

IAM challenges in the education industry

Outdated, homegrown, legacy IT systems and multiple data sources

Initially, colleges and universities have been using outdated, homegrown, legacy, open-source software for years due to limited IT budgets. These systems are often challenging to maintain, costly to fix, and provide poor customer service. Both users and IT security teams may experience frustrating user interfaces due to older IT infrastructures and identity management solutions. With legacy and homegrown IAM systems, many identity-related tasks such as de-provisioning are labour incentive, repetitive, and time consuming. As a result, these systems are putting the college or university at risk since they weren't built to be secure.

It's common for users to have multiple roles in the higher education sector. Faculty may take classes, students may work as staff, and graduates may become alumni. IAM systems treat each of these users as a separate ID, therefore a user who has multiple roles must handle multiple user credentials to perform their activities. It is important to maintain and protect information about the university's faculty and other affiliated groups. This data must be combined and made accessible.

Ever-changing user life cycle

In the education industry, the problem of having users with multiple roles comes up frequently. Each semester, IT departments must deal with thousands of new users being onboarded and offboarded.

For new students, the admin team is tasked with creating an account in the university portal; creating an email account; and granting access to applications, course materials, the library, and Wi-Fi. The student should be able to get access before arriving on campus so they can go through orientation.

For a student who finishes a semester and gets promoted to the next level of classes, they need access related to the course work. That access should continue until a certain amount of time until the student is promoted to enable them to move emails or files off the system.

For graduating students, admins are tasked with disabling user accounts and removing access from all applications and services.

For a staff member, access to sensitive data such as personal information and training on responsibilities related to it is provided. This employee continues to have access until he or she leaves. Then the access should be revoked immediately upon termination.

Manual provisioning and de-provisioning

Educational institutions handle a tremendous amount of sensitive data that includes personal information and financial and credit data pertaining to students, staff, and faculty. Universities tend to have a concentrated periods throughout the year where thousands of user accounts are created, managed, updated, and deleted—generally at the start of a new semester. This can lead to delays in both onboarding, which creates poor user experience, and offboarding, which could pose a risk to security.

If IT teams are manually managing user access for each requirement, the cost and time incurred doing it will be significantly high. Manual identity management increases costs due to help desk overload, security threats, and excessive license usage. Another problem is the lack of auditing of user accounts. For educational institutions, this makes it difficult to prove that they are following the rules established by external auditors.

Lack of privileged access management

The majority of educational institutions lack a proper privileged access management system. One of the biggest security risks in the cyber landscape is the potential misuse of privileged accounts. Privileged accounts are constantly targeted by malicious actors as they look to infiltrate valuable information or cause damage to an organisation.

Schools and universities are not only tasked with providing secure access to applications and resources, but also face the responsibility of correctly managing access rights. This can be further complicated when students receive new subjects and courses each quarter, resulting in necessary adjustments. Teachers and employees will also need access to new applications and data regularly.

One of the most unnoticed security risks your school or university can face stems from employees acquiring too many access rights because of role or responsibility changes. Applications and service accounts frequently possess excessive privileged access rights by default and also suffer from other serious security deficiencies.

Managing temporary access for transient, contingent users

Education institutions, especially community colleges, must deal with transient users on a massive scale. Students and teachers flow in and out of the system. Sometimes they take several semesters off or might never return at all. When students have to wait for access to critical resources, such as online course materials and homework assignments, it negatively impacts the end-user experience.

Colleges and universities also often hire contingent faculty rather than full-time, salaried professors. While this move might save money, it creates a number of challenges for the IT departments that must manage the identities of these contingent workers. Most IAM systems don't have an easy way to manage external users who don't exist in authoritative HR databases and student information systems. When workers leave, there isn't a process in place to notify IT, and frequently, no one does due diligence. The institution is left with orphaned accounts to which the former contingent workers still have access. That's a security risk, especially if the people have access to sensitive data.

Manual workflows to authorize access

Faculty and students need to access resources used in their courses. If a user's job changes or they leave the school system, there might not be enough time to ensure that access permissions are updated or deleted.

IT staff are responsible for frequently authorizing access. Moreover, these requests are sent in person, via email, or on paper forms. As a result, when students switch positions or classes, get new privileges, or even become alumni, there may be delays, mistakes, and potential compliance and security concerns. If done manually, managing user access for each demand is difficult and prone to mistakes.

Lack of integration with cloud-based platforms

In a world where most industries are moving from on-premises software to cloud-based services, the education industry is also shifting to and using some cloud-based platforms, including Microsoft 365 and Google Workspace, which are offered and controlled by an outside vendor outside the school system's network.

Identity management can be difficult in such applications. Institutions deploying cloud software must ensure it integrates with existing identities to maximize the value of its investments and keep on-premises systems secure and accessible. Therefore, it is a huge burden on the IT team to ensure identities are extended to cloud applications.

Help desk cost for password and account unlock requests

A common problem faced by educational institutions is the absence of dedicated IT help desk teams, possibly due to a lack of funds to invest. It is common for users to forget their passwords, have their passwords expire, or have their accounts locked. They contact the IT team to reset their passwords or unlock their accounts.

Help desk calls and frequent calls aren't difficult for the IT staff to resolve, but they take up time that could be used for other tasks. The number of calls to resolve password issues is particularly high at the beginning of the school year or semester. because many users forget their passwords after a long break. As a result, the help desk is backlogged, and the end user cannot do anything that they need to do.

Security and compliance requirements

All educational institutions deal with large amounts of personal and sensitive information, making them prime targets for data breaches. Following a successful attack on an educational institution, cyber attackers will have access to personal information, including birthdates, full names, addresses, payment information through weak passwords, outside hackers, etc. Maintaining the security of this data is essential for creating trust in an institution and preventing data breaches or leaks.

How AD360 meets IAM needs of your institution

AD360 is a unified solution for identity and access management (IAM). This solution helps administrators manage user life cycles, protect privileged accounts, govern access, and implement advanced adaptive Multi-factor authentication (MFA).

The key capabilities of AD360 are:

User life cycle management

AD360 lets admins create, modify, and retire accounts when users change roles or leave the organization. They can modify users in bulk by applying customized templates or by importing data from a CSV file. To deprovision users, they can bulk disable or delete accounts based on your organization's policy.

Access management

AD360 helps admins make sure each user has the right amount of privileges and access. Maintain an audit trail of every user's access to resources while managing permissions and rights granted to users.

Single sign-on (SSO)

AD360 provides enterprise SSO capabilities with OU- and group-based security policies, which makes it easy for users to access all of their cloud applications.

MFA

AD360 supports authenticators such as YubiKey, Duo Security, RSA SecureID, etc. You can also selectively configure MFA for users based on domains, OUs, and group memberships.

Role-based help desk delegation

AD360 lets admins delegate administrative tasks to non-administrative users through an established workflow for completely secure delegation. They can delegate tasks with a scope limited to a specific OU or group.

1. Automate user life cycles of students and teachers

- Auto-create user accounts in AD, Microsoft 365, and Google workspace using data from CSV files, HCM solutions, and Microsoft SQL and Oracle databases.
- Modify existing students' records in bulk using grade-based and year-based templates.
- Automatically modify the accounts of existing students (e.g. their folder permissions and group memberships) using rule-based templates based on the year or course change.
- Automate workflow processes to remove access to groups, educational apps and folders from students who have graduated or dropped out, disable their accounts and mailboxes, archive them for a specific number of days, and then remove the account after the retention period.

2. Create a better user experience with SSO and self-service password management

- Enable students and teachers to reset passwords and unlock accounts for AD, Microsoft 365, and other enterprise applications without IT assistance.
- Provide users one-click access using SAML, OpenID Connect, and OAuth to enabled education apps.

3. Provide users access to learning resources from day one

- Grant relevant group memberships right at the time of user creation using user creation templates, which give students access to relevant resources.
- Automatically assign and modify share folder access of new and existing users for course materials.
- Create automated templates using orchestration to provide access to learning apps.
- Create a Microsoft 365 or Google Workspace account for new students at the time of user provisioning itself.

4. Just-in-time access to external users

- Grant select individuals access to sensitive resources for a limited time.
- Authorized duration of access can be specified while creating just-in-time (JIT) access policies.

5. Give users just enough access to the resources they need

- View detailed reports on which users have access to confidential student folders and resources.
- Grant users (students, teachers, non-teaching staff) the least required access for only the required duration of time to prevent unwanted usages.

6. Delegation and approval workflows

- Implement approval workflows to ensure all access, create, and modify requests are supervised before approval and prevent any unwanted changes.
- Delegate repetitive requests from students like password resets, account unlocks, and user modifications, and grant group memberships or folder access to teachers and staff.

7. Enhance security and compliance

- Get real-time alerts on file and folder changes, user creation, and user modifications to see who changed which file or folder, when, and from where.
- Back up and restore all AD objects, Azure AD, Microsoft 365, Google Workspace, and Exchange to protect data against disasters.
- Detect ransomware attacks by setting real-time alerts and threat responses for suspicious user activities, like malicious logins and attempts to delete data, and shut down infected machines.

8. Simplify authentication methods while ensuring security

- Configure custom password policies for OUs and groups.
- Provide simplified MFA based on user capability.
- Configure MFA for students' and teachers' machine, cloud app, Microsoft Exchange, and VPN logins.

About ManageEngine AD360

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps you perform all your IAM tasks with a simple, easy-to-use interface.

With AD360, you can just choose the components you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from within a single console.

$ Get Quote Download