Crucial user provisioning
challenges in
K-12 institutions
and how to solve them

Table of Contents

Introduction

The greatest challenge of an IT admin in today's digitally-evolved school system has to be effective user provisioning. Schools now use a variety of cloud applications for teaching. A recent study found that 65%[1] of teachers in K-12 institutions use digital learning tools every day. When manually provisioning student and teachers accounts, IT admins have to create stand-alone accounts in all of these applications individually. IT admins end up spending long, tedious hours provisioning students and teachers at the beginning of every academic year. Another core problem that IT admins face is accurate deprovisioning of user accounts. Accounts that fail to be deprovisioned at the right time become stale accounts and become a security risk to the institution.

Automating user provisioning helps institutions manage student, teacher, and non-teaching user accounts diligently, reducing the chances of data breaches significantly.

User provisioning challenges in K-12 institutions

Loss of IT time in manual operations

K-12 institutions frequently provision and deprovision users. The user data is also highly dynamic, often requiring modification. Manual provisioning procedures lack the capability of synchronizing the user data from HCM solutions to AD and other cloud platforms. IT admins are often forced to spend hundreds of hours manually creating, and updating user accounts. They also frequently have to track and offboard dormant accounts, and manage user permissions for instructional material and cloud apps manually, due to the lack of an effective automated user provisioning solution.

Legacy IAM systems and limited resources

Schools have been rapidly adopting e-learning methods in recent years because of the pandemic. The use of various cloud apps to help student learning has also increased dramatically. The lack of IT budgets and resources for maintenance has forced IT teams to rely on unsustainable methods, such as implementing complex PowerShell scripts that are time-consuming, tedious, and error-prone. Legacy solutions are also not designed to handle rapid changes, and the knowledge of operations is limited to a few IT admins, which becomes disruptive if these IT admins leave the institution. By using legacy solutions and PowerShell scripts, IT admins get caught in the loop of performing routine tasks, and are often distracted from addressing critical issues that require attention.

Learning losses for students

Manually granting group and share folder permissions for students and teachers is a long process that requires teachers or department heads to submit a request to the IT admin. Approval might take up to two to three weeks. The student and teacher do not have access to the instructional material during this time, effectively blocking learning opportunities for students, and prep time with the course materials for teachers.

Security risks from undetected stale accounts

Each year, K-12 institutions experience a high inflow and outflow of students and teachers. Manual deprovisioning of students, teachers, parents and other staff member accounts is a tedious process. Without a proper deprovisioning tool, stale accounts in the database can be unnoticed. In most cases, IT admins do not have an accurate count of the stale accounts, so they might be unaware of many of them. Bad actors can exploit this weakness to infiltrate schools and steal the personal details of students, faculty, and parents.

Contingent workers and ad-hoc requests

Schools employ a variety of contingent workers. They have temporary staff who replace other staff, non-teaching staff, special education instructors, and many others who require just enough access to operate within the institution smoothly. In schools where manual provisioning is the norm, temporary access requests are made through email that can lead to delays and errors in file access. Deprovisioning of these users can also be a challenging task as, in most cases, there is no well-defined process to notify IT admins when the contingent employee leaves. Unmonitored stale contingent user accounts pose a risk of data breaches and are an easy target for cyberattackers.

Ensuring compliance with regulations like FERPA and COPPA

The inability to keep detailed records of manual actions taken by IT technicians and staff makes maintaining compliance difficult. Due to the sensitive nature of the data that schools handle, such as the personal information of children under 13, or the bank account information of faculty and parents, the data are governed by crucial IT regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA). Maintaining audit trails and observing user activity can be difficult for institutions that employ manual user provisioning. Violations of COPPA regulations by schools can cost up to $43,280[2] for each violation.

Automated user provisioning offered by ADManager Plus

With ManageEngine ADManager Plus, schools can replace error-prone and time-consuming manual processes with an automated process that ensures productivity and data security.

Automated lifecycle management

Automate the entire lifecycle management of students, teachers, parents, and other stakeholders like non-teaching staff using ADManager Plus. Implement a simplified automated lifecycle management process with well-defined standardized and prepopulated templates which helps you bulk create users instantly.

Bulk user management: Using ADManager Plus, schools can bulk create, modify, delete users in AD, Office 365, Google Workspace, and Skype for Business while not depending on complex PowerShell scripts. IT admins can import user details through CSV files instantly to create and modify user accounts.

Fig.1 Automation for user provisioning

Templates: ADManager Plus provides user creation and modification templates for users, computers, groups, contacts, mailboxes, and OUs. K-12 institutions can use rule-based user provisioning templates with prefilled attribute values based on the staff department or student class for user creation. For each role, IT admins can use preconfigured templates with specific settings, permissions, and privileges.

Fig.2 User creation templates

Custom naming format: With ADManager Plus, institutions can also utilize custom naming formats in templates to create unique logon names and eliminate name duplication, which is a prevalent issue in bulk user provisioning.

Fig.3 Customizable naming format

Group membership management: IT admins can deploy user modification templates in ADManager Plus to alter AD groups for students and teachers. When students and faculty members transfer from one class or department to another, IT admins can modify their groups seamlessly. This avoids the need to select individual AD users and change their membership with the appropriate AD groups.

Manage NTFS and Share permissions: Schools can manage access permissions to NTFS and share folders by automating permissions based on factors like the OU or the group of a student or teacher. Permissions to the resources can be granted for a specific duration as required by the role, like a school year for a student and teacher.

Fig.4 Automate group permissions

Enterprise-ready integrations

ADManager Plus enables administrators to integrate with HCM solutions such as UKG Pro, WorkDay, BambooHR and others with API support. With ADManager Plus, IT admins can also utilize databases such as MS SQL or Oracle, to automatically create, remove, and manage accounts in AD and other cloud platforms.

Custom HCM integrations: K-12 institutions can use ADManager Plus to set up custom HCM integrations to acquire user data from their preferred HCM product for user provisioning.

Fig.5 Custom HCM integration

Webhooks: Schools can use ADManager Plus to configure webhook integration with applications used by schools and automate the creation or removal of users in the application whenever the webhook posts to a specific URL.

Fig.6 Configuring webhooks for access to the school's app

REST APIs: ADManager Plus can be integrated with REST API-supported applications used by schools. With this integration, AD user management actions like user creation, password reset, account unlock, user deletion, etc., can be performed from the application by accessing ADManager Plus through the API.

Manage student accounts and passwords in bulk from reports

IT admins can perform routine management actions for students from ADManager Plus reports, such as resetting forgotten and expired passwords, unlocking accounts following the return from a school break, and identifying and disabling inactive user accounts.

Role-based access control

ADManager Plus gives IT admins the ability to provision users by applying the least privilege principle. This ensures that teachers, students, parents, consultants, contractors, and even temporary users can only access resources within the scope of their role. ADManager Plus enables IT admins to limit the scope of file access of students and teachers within their OUs and groups.

Delegated administration

Using ADManager Plus, IT admins can create technician roles for delegating user management actions to teachers and department heads for changing passwords, modifying user attributes, disabling user accounts, enabling accounts of student joining after a break, and more. The technician role is created in ADManager Plus and not in AD. These teachers and department heads have access only to the tasks that have been delegated to them and cannot make any further modifications. IT admins are freed from routine tasks, and can concentrate on crucial tasks that demand their attention. The waiting period for students and teachers to obtain access to educational material is also reduced significantly.

Fig.7 Help Desk Role creation

Just-in-time access

Using ADManager Plus, temporary employees, special educators, and others can be granted limited access to files and permissions for a specified duration. This is especially useful when schools are legally bound to grant consultants and contractors temporary access to sensitive resources.

Fig.8 Automation policy

Enhanced security and compliance

Using ADManager Plus' workflow capability, schools can ensure that all AD user management activities are supervised and verified. The workflow feature helps define a hierarchy of approvals required to complete an automation.The supervision breaks eliminates errors and comply with IT regulations. The workflow process not only reduces the margins for errors, but also helps create a ticket-based method for managing tasks. For compliance purposes ADManager Plus also maintains a repository of all requests and tickets created. Audit trails can be used to monitor changes made by teachers and department heads as well. This enables the school to protect the data of its students and faculty, and be complaint with FERPA and COPPA regulations.
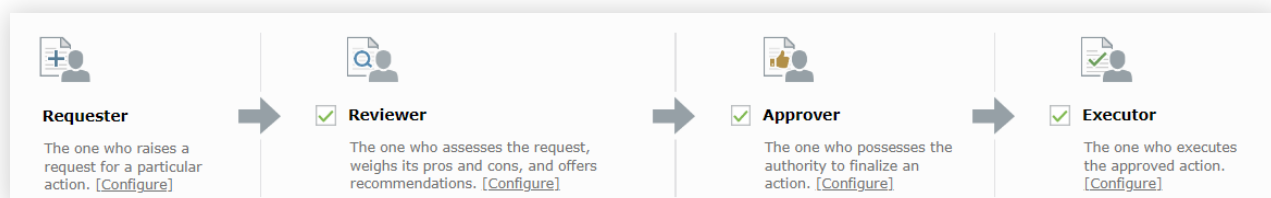

Fig.9 Review Approval workflow

Audit trails: ADManager Plus also provides audit trail of actions performed by delegated non IT users like teachers, HODs, HR etc... The audit trail records who performed the task, when it occurred, and what was accomplished. This enables the school to protect the data of its students and faculty and be complaint with FERPA and COPPA regulations.

ManageEngine
ADManager Plus

About ADManager Plus

ManageEngine ADManager Plus is a web-based Windows AD management and reporting solution that helps AD administrators and help desk technicians efficiently accomplish their day-to-day activities. With an intuitive, easy-to-use interface, ADManager Plus handles a variety of complex tasks and generates a comprehensive list of AD reports, some of which are essential requirements to satisfy compliance audits. The solution also helps administrators manage and report on their Exchange Server, Microsoft 365, and Google Workspace environments, all from a single console.

$ **Get Quote**   ⬇ **Download**

[1] Education Technology Use in Schools, Gallup   [2] Children's Online Privacy Protection Act