A BIO-key® Solution.

Addressing the Challenge of User Authentication on Campus

Table of Contents

The Challenge: Cost-Effective Password Security 3

The Solution to Campus Password Security 4

8 Ways to Select the Right Security Solution 6

A Range of Challenges, A Range of Solutions 7

The Challenge: Cost-Effective Password Security

Today's college campuses face enormous challenges with security issues, including integrating front-line software such as the learning management system and student information system, while ensuring the students and faculty have secure but easy-to-use access to those systems and many more.

Basic issues with default password assignment and resets, along with Single Sign-On access, make up some of the most common security hurdles institutions wrestle with. As anyone who has staffed a service center knows, lost and forgotten passwords and account lockouts are unavoidable. Especially at the start of each semester, help desks typically deal with a deluge of calls related to logging into systems. This puts undue strain on IT, which either diverts staff from bigger issues, or must "staff up" temporarily to meet demand.

Making the problem worse, multiple password prompts for different systems -- email, portals, apps, the LMS and the SIS – can mean multiple reset requests from a single student or faculty member. Excess passwords also compound the risk of security breaches, since each password offers a new avenue to hackers, who pick the weak link across multiple systems. Students with many passwords often resort to using the same one over and over. Staff at a service center are exposed to passwords as they help users remember or reset them, creating more security and compliance issues.

In addition, it's challenging to assign and deliver initial passwords to new students in a timely manner – and extremely difficult to ensure participation. One of the primary reasons password reset systems can fail is a simple lack of student participation. To work, the access system needs to be clear, simple and universally enforced. Ideally, different user types will have requirements – for example, full-time, part-time, or online-only students, along with faculty, adjuncts, and staff.

Additional password security steps such as Two-Factor Authentication – requiring a user to prove identity in two separate ways rather than just one – can increase security greatly, but is rare in higher education because such solutions tend to be unaffordable.

With typical enterprise off-the-shelf Single Sign-On solutions, pricing is an issue as well. A Single Sign-On (SSO) security system can simplify many password issues, but unfortunately, many SSO solutions are complex and costly. Although most colleges, especially community colleges and smaller universities, face tight budget constraints, enterprise Single Sign-On solutions generally start at nearly six figures – well outside many education budgets.

Faced with these security challenges, higher education needs an affordable, highly secure solution that zeroes in on the issue that affect campuses most: simple and secure password set and reset tools, and secure Single Sign-On.

The Solution to Campus Password Security

PortalGuard is a user authentication product that specifically addresses the needs of higher education. A web-based solution that is installed in-house or in the cloud, it addresses security and compliance through a multifaceted approach.

PortalGuard provides the following in a single turnkey package (some functions can be purchased separately):

Self-Service Password Reset – This basic PortalGuard function, hugely popular in higher education, allows users to securely reset their own passwords, using previously entered personal information – including, if desired, Two-Factor Authentication.

Single Sign-On – With PortalGuard, independent software systems can be unified under one authentication process, allowing a student or faculty member to enter the same name and password **once** and gain seamless access to multiple systems. Single Sign-On tightens security markedly by creating a single “chokepoint” for authentication and decreasing attack surfaces. It also reduces service calls to the help desk.

Two-Factor Authentication – This security method requires users to present two methods of identifying themselves, such as a password (or answers to personal questions during a password reset), and a mobile phone number. With PortalGuard, personal security questions can be set up, and a mobile phone or personal email address can also be used to verify identity, for example.

Real-time Password Synchronization – PortalGuard helps IT administrators manage passwords, keeping them in sync across user directories. It supports Microsoft Active Directory (including multiple AD domains), Azure Active Directory, and any LDAP v3-compliant directory, plus custom SQL user tables. When a user changes a password, PortalGuard passes the changes down to all linked accounts instantly.

Adaptive Authentication – A cutting-edge approach to security that raises the bar for authentication by weighing context, such as the user’s Geolocation, network, and what device is being used.

PortalGuard also addresses these challenges:

Device-agnostic: PortalGuard is web-based, so it is platform-and browser-agnostic. It works across all devices used by students, faculty, and staff, including Windows and Apple systems, all mobile devices, and Chrome, Firefox, Safari, and Edge browsers.

Password recovery right from Windows: An optional PortalGuard desktop component can be installed directly on Windows workstations to request enrollment of challenge answers, phone or email after a Windows login. It also allows password recovery right from the Windows logon screen, using the same interface as direct browser access which helps reduce training.

Single Sign-On to LMS (e.g. Canvas or Blackboard): One of PortalGuard's most well-known features. A huge win on college campuses is providing Single Sign-On to the LMS. PortalGuard makes Single Sign-On to your LMS possible because it supports standard SSO protocols like SAML, OAuth and OpenID Connect as well as the higher-education-specific CAS SSO protocol.

High initial student participation: Schools can import existing student data into PortalGuard, then ask students to set their own initial passwords by answering a set of questions the first time they use the system. IT administrators control how Self-Service Password Reset is introduced. The first time a student logs in through any standard interface, a popup window can appear asking them to enroll.

Once enrollment is complete, a student who fails at a login is intercepted by PortalGuard, which jumps in with the option to reset their forgotten password. Based on administrative settings, students can also optionally enroll a mobile phone number or personal email address to help prove their identity when resetting their forgotten password.

Separate group policies: Security policies can be applied to single users, groups (faculty vs. students vs. staff), or entire organizational units in the user directory. PortalGuard supports local Active Directory, Azure AD, any LDAP v3 directory, as well as custom SQL-based user repositories.

Pricing Tailored for Higher Ed: PortalGuard offers a Student Full-Time Equivalent (FTE)-based licensing that eliminates the overhead associated with monitoring active user counts, and can drop the per-user price dramatically. PortalGuard Self-Service Password Reset is available as a standalone product, or as part of the complete authentication solution set.

8 Ways to Select the Right Security Solution

Selecting a solid, affordable solution for addressing Single Sign-On and password reset issues in higher education isn't easy. As with any security solution, it requires ample research to make sure the solution fits. Here are eight general issues to consider:

1. Solutions based on industry standards and protocols are nearly always more desirable, since they are more easily extensible and can help prevent vendor lock-in. For Single Sign-On, look for a solution that can work with security standards such as SAML, Shibboleth, CAS and OAuth.
2. Look for a mature product, with functionality that meets current needs yet offers advanced functions and features you can grow into. Future-proofing yourself will save money in the long term. On the other hand, don't get caught up in considering too many opinions and trying to peer too far into the future – that can lead to inaction and excessive scope-creep. Set reasonable parameters for what you need and stick with them.
3. No matter who you choose to work with, adopt a methodical approach to the evaluation process. First, group users by their different needs and use patterns – perhaps faculty, staff, alumni and students, with further divisions for students such as new, existing, graduate, and so forth.
4. It's important to determine how each group's needs will differ. Map out usage scenarios for each – this will help you understand how a solution can integrate with your environment.
5. Work with your IT staff and with potential vendors to understand how users and hackers can misuse or subvert the system. It is a truism on college campuses that not everyone follows the rules.
6. Weigh how difficult the solution will be to deploy and implement. Consider whether you'll need additional staff or consulting expertise. Be sure to ask potential vendors what sort of support they offer during installation – and avoid excessive complexity. Implementing any security solution is not trivial. Look for a vendor who will partner with you to fully understand your requirements before recommending anything.
7. To be seriously considered, any reputable solution should include ample logging and auditing, clearly showing user activity at any point in time, along with return on investment over time, break-even points, and even reporting based around risk.
8. Finally, any solution should be independently tested and certified on a regular basis.

A Range of Challenges, A Range of Solutions

Different solutions are good fits for various institutions based on their needs and issues; password security challenges differ widely by school size, budget and focus. Here are three examples of PortalGuard solutions in action at three very different institutions..

Self-Service Password Reset

This institution, a midsize college in the Northeast, had purchased a third-party Self-Service Password Reset product two years ago, but the system never got off the ground. Issues centered on an inability to get students to enroll, and a cumbersome user-licensing model.

User participation is a common problem Self-Service Password Reset tools -- simply getting students to enroll initially so that passwords can be securely reset later if needed.

With PortalGuard Sidecar in place, the school asked students to enter passwords and set up personal challenge answers during their first attempt to log in to Office 365 Outlook Web App. That ensured password reset was in place immediately. PortalGuard won points with students for its flexibility during a reset, allowing a choice between answering any three previously answered questions, or having a One-Time Password sent to their mobile phone.

With Sidecar mode, participation can be requested from any existing HTML login form. That means that PortalGuard can prompt for enrollments nearly anywhere, without making users change their current behavior or learn a new system – leading to much higher participation.

Password Expiration Notifications

At this midsize college in the Southeast, expired passwords weren’t adequately conveyed on the Outlook Web App login screen, leading to confusion since the “correct” password was supplied but did not result in successful login. Students and faculty contacted IT with questions, leading to increased staff time on inconsequential issues.

Once PortalGuard was installed, it was configured to send students clear, multiple, pre-emptive “expiration reminder” emails that included a link for updating passwords immediately. PortalGuard was also configured to ask users to enter challenge answers at that point, thus enabling Self-Service Password Reset later.

Single Sign-On

This small community college in the Midwest had separate logins for Google Apps, Moodle and Blackboard, costing IT staff time and effort in maintenance. Because budget is such a factor at most institutions -- even more so for state and community colleges -- a cost-effective Single Sign-On solution can mean huge savings.

At this college, PortalGuard introduced SAML-based Single Sign-On, thus reducing manual logins from three separate screens and processes, to a single unified portal login – also branded with the college logo and color theme. The solution also allowed IT to selectively enforce Two-Factor Authentication.

A Good Security Solution Pays for Itself

With data breaches an all-too-common occurrence in the news these days, colleges and universities clearly need better security solutions in order to lock down access to data and systems. The challenge is compounded by the funding constraints common in higher education.

In fact, colleges and universities can get the most value for their security dollars by addressing some of the most basic issues first. For example, security breaches are made easier by systems that make passwords the main determining factor in authenticating the user. Tools that focus on tightening user access -- such as Multi-Factor Authentication, Self-Service Password Reset, Password Synchronization, and Single Sign-On -- all help to tighten common areas of security breaches.

The right security solution can cost-effectively allow students, faculty and staff easy and unencumbered access to systems, while reducing support issues, ensuring more secure and compliant systems – and avoiding embarrassing security breaches. A product that maintains a balance among security, user participation and ease of use, pays for itself very quickly.

A BIO-key® Solution.

About Us

BIO-key's PortalGuard offers both a cloud-based and on-premises turnkey user authentication solution-set for campuses with external-facing web applications for their students, staff, and faculty. This all-in-one integrated design includes Two-Factor methods, Single Sign-On, Centralized Self-Service Password reset/unlock, Password Synchronization, plus transparent barriers to confirm user identities by validating their context.