

Case Study

Husson University

About Husson University

Husson University uses PortalGuard to provide automatic batch importing of account data as well as to increase initial login security with mandatory security questions.

Specific Pain Point

Husson University needed a secure method to enroll new users to the local directory. Administrators require a way to update user accounts in a batch on-demand or automatically so that account details are always accurate and up to date.

Existing Challenge

New user accounts at Husson University were initially created with generic passwords that followed a formulaic makeup – reducing the inherent security of the password until it was reset to something more complex. No password expiration was set, and end-users would often opt to use the initial password for some time. Additionally, each end-user account was created with a series of fields full of personal information. This information did not update automatically when a change was made – requiring manual updates to be handled by IT. Husson University populated and updated users via CAMS on a set schedule – they required a solution that could integrate with this setup while still providing the ability to automate the process.

The PortalGuard Resolution

Increasing Security of User Accounts

With the installation of the PortalGuard server on premises at Husson University, PortalGuard was able to fully integrate with the local directory for account updating and synchronization. In order to increase account security for users that were assigned potentially weak initial passwords, Husson University configured Mandatory Knowledge Based Authentication (KBA) during forced enrollment. Forced enrollment requires an end-user to login through PortalGuard and setup the specifics of their account before it is fully activated.



Customer Profile

Industry:

Higher Education

700 - 1000 Users

Location:

Maine

Top Applications Used:

Active Directory, CAMS, Google Apps

Mandatory KBA prompts the user to answer various security questions based on the unique personal information associated with their local active directory account. This adds an extra layer of security to the account, as it cannot be fully utilized without completing forced enrollment, which requires intimate knowledge of personal information related to the user. This system also prompts the user to create a new, updated password that meets a customizable password policy that can be set by an IT administrator – effectively eliminating the possibility of an end-user continuing to use a weak password for day-to-day authentication.

Automating Batch Functionality

Before PortalGuard, Husson was experiencing issues with one of their user repositories; these difficulties made it unlikely that they would be able to integrate with a password-reset solution. Within this repository, user-specific personal information – such as address and phone number – was stored and associated with a specific account. The issues arose due to the inability of this information to update automatically with the authentication credentials that were tied to the user. PortalGuard was able to solve this problem by using automated batch updating. In order for it to work, Husson was required to upload a .csv document that contained all the pertinent information of a given user. As long as this information was formatted correctly within the .csv, it was possible for Husson to upload and update user information within PortalGuard's system for a seamless integration. In addition, PortalGuard can be scheduled to run at set intervals to make sure that all the user information is up to date. This feature overcame scheduled update challenges that Husson was experiencing, without necessitating the development of a new strategy.

Additional Resources

[Centralized Self-Service Password Reset Tech Brief](#)

[Configurable Password Management Tech Brief](#)

[Knowledge Based Authentication and the Grid - Blog](#)

PortalGuard is a cybersecurity authentication package that delivers a full set of features in a single, fully customizable solution. PortalGuard provides single sign-on (SSO), self-service password reset (SSPR), two-factor authentication (2FA), and over 130 other features to ensure that each campus is equipped with the tools needed to face any authentication challenge.