Case Study

Clermont Northeastern Schools

About Clermont Northeastern Schools

Clermont Northeastern Schools uses PortalGuard to fully integrate Google Apps and Moodle with Active Directory for Single Sign-On and Self-service Password Reset.

Specific Pain Point

Students and Faculty at Clermont Northeastern Schools required a method to reduce login prompts for Google Apps and Moodle while relying on a single set of credentials established by the local active directory.

Administrators also required a solution that provided flexible options for password reset to increase end-user adoption rates.

Customer Profile

Industry:

K-12 Education

5,000 Users

Location:

Ohio

Top Applications Used:

Google Apps and Moodle

Existing Challenge

Like many K-12 educational institutions, Clermont Northeastern provides students with access to multiple applications such as Google Apps for Education and Moodle. Due to this scenario, user accounts need to be created in a minimum of three locations during each specific enrollment – in the local Active Directory, within Google Apps and within Moodle. Oftentimes, this lead to difficulty remembering usernames and passwords, as they are not always created with the same format.

One of the major challenges facing Clermont Northeastern Schools was the discrepancy between usernames on each application platform. On top of that, requiring a separate login form for each application led to both an increased sense of frustration for end-users and a decrease in the ability to properly login

Clermont Northeastern Schools needed a solution that would resolve issues with username differences and remove various authentication prompts from blocking end-user access to necessary applications.

The PortalGuard Resolution

Tackling the Single Sign-On Issue

A PortalGuard server was installed as an on-premise Identity Provider (IdP) for Clermont Northeastern Schools. With PortalGuard in place, unauthenticated requests to either Moodle or Google Apps are redirected to the PortalGuard IdP for initial authentication.

Once PortalGuard authenticates the user, the PortalGuard IdP creates a SAML response and the browser redirects the end-user to the originally requested server and URL with this SAML response. This redirect happens independently of the user without any additional action being required.

Google Apps natively supports SSO via the SAML v2.0 protocol. Moodle v1.9 does not have native support for SAML SSO, so integration with the AUTHSAML plug-in was used to add this support.

Account Creation Resolution

Before PortalGuard, usernames within the local Clermont Northeastern Schools Active Directory differed from the usernames for the same users within Moodle and Google Apps (i.e. a jsmith faculty member in AD has the name smith_j in Moodle and Google Apps). With the use of the Google Apps Directory Sync (GADS) utility, newly created users (students, faculty, or staff) will have the same usernames across AD, Moodle and Google Apps.

Additionally, the AUTHSAML plug-in for Moodle automatically creates new users on the fly. The first time users attempt to access Moodle, a SAML Token is created in relation to the specific AD account. The attributes in the SAML token are then used to create and/ or update the user's account in Moodle.

The Google Apps Password Synch (GAPS) utility was also configured alongside the Clermont Northeastern Schools AD Domain Controller. GAPS is fully developed and supported by Google, and is used to keep users' Google Apps and Active Directory passwords in sync to accommodate password resets and changes.

The Password Reset Problem

During a local survey of the Clermont Northeastern Schools student body, 60% of those who responded admitted to forgetting their passwords. In order to alleviate the associated strain on the Help Desk, Clermont Northeastern introduced the PortalGuard Password reset tool with Knowledge Based Authentication (KBA) to enable web-based password reset.

Alongside the introduction of the PortalGuard IdP and integration with GAPS and GADS, these changes are updated automatically within the local directory, and take effect immediately upon successful completion of the password reset process. This functionality effectively reduced the amount of help desk calls being fielded by the local Help Desk, and empowered uses to be more proactive in their password management

Potential Future

Despite integration with KBA for Self-service Password Reset, Clermont Northeastern is also looking to integrate some of the additional features in the PortalGuard solution to further increase user adoption for password reset. Located in a veritable mobile dead-zone, typical SMS OTP delivery for password reset verification is unavailable. With out-of-the-box support for over a dozen OTP Delivery methods, PortalGuard has multiple options that users can choose from in order to make password reset even more simple to undergo.

The top choice for secure integration and adoption of Self-service Password Reset is the use of the Google Authenticator for OTP generation. The Google Authenticator is compatible with the PortalGuard server and will continuously produce a unique code that is recognized by the PortalGuard server to validate an authentic password reset attempt. Due to the nature of the Google Authenticator, and the fact that it does not rely on a mobile network connection, this solution directly addresses a newer pain point for Clermont Northeastern, without requiring the installation of any additional solutions.

Additional Resources

Centralized Self-Service Password Reset Tech Brief

SAML Single Sign On Tech Brief

Overcoming 2FA Hurdles Tech Brief

One Time Password Pros and Cons - 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.