Security Best Practices

Last Modified on 07/29/2024 3:57 pm CDT

We know how important data security is for your district, and Infinite Campus works hard to keep your data safe. Compromised email addresses, usernames, and passwords frequently get shared on the dark web. Unfortunately, these are often reused across multiple applications and are not changed until required. This allows potential authenticated access to user accounts in systems like Infinite Campus. To prevent and mitigate these threats, we recommend you follow the best practices listed below.

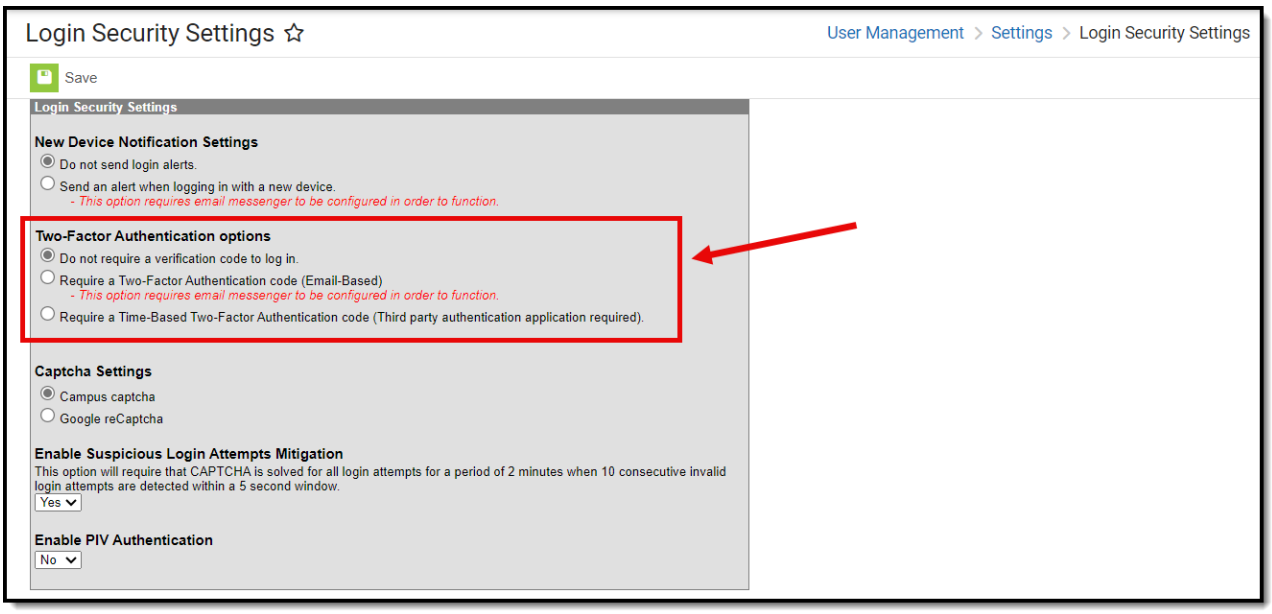
Enable Two-Factor Authentication (2FA) for All Staff Accounts

Enabling two-factor authentication for all user accounts is the most impactful and important security measure your district can enact. For this purpose, it is recommended that you utilize a third-party identity provider integrated with SAML. This provides a wider variety of two-factor options and reuses existing user directories.

Infinite Campus offers built-in 2FA for both local and Active Directory staff accounts. This free feature provides a strong defense against unauthorized access to the system. Authentication can be completed through an emailed verification code or an authentication app like Google Authenticator.

Click the link below for more information about how this feature works and instructions for enabling it.

- Instructions for Enabling Two-Factor Authentication for local and Active Directory accounts



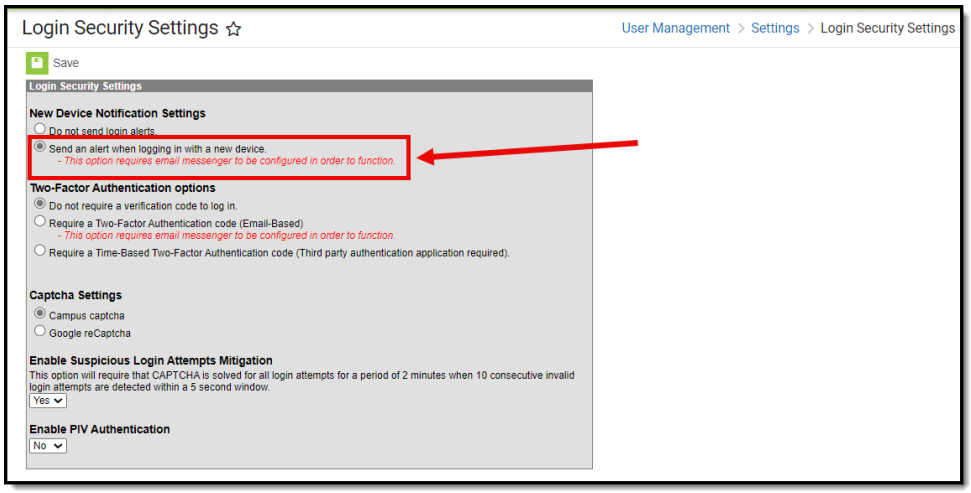
You can also configure LDAP and SSO authentication options to manage and control user login

credentials.

- Enabling an SSO Service Provider
- Enabling LDAP

Additional Best Practices

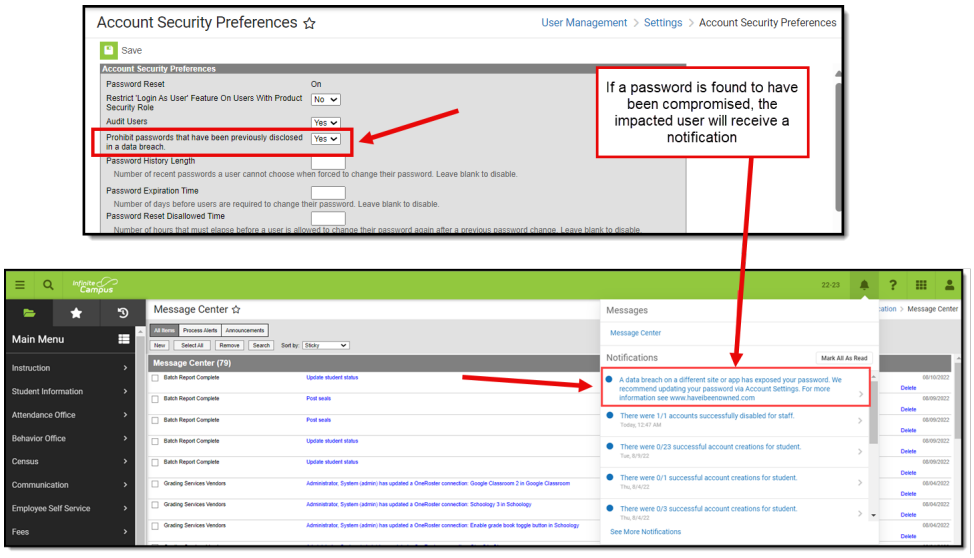
The table below details additional security best practices all districts should implement and follow.

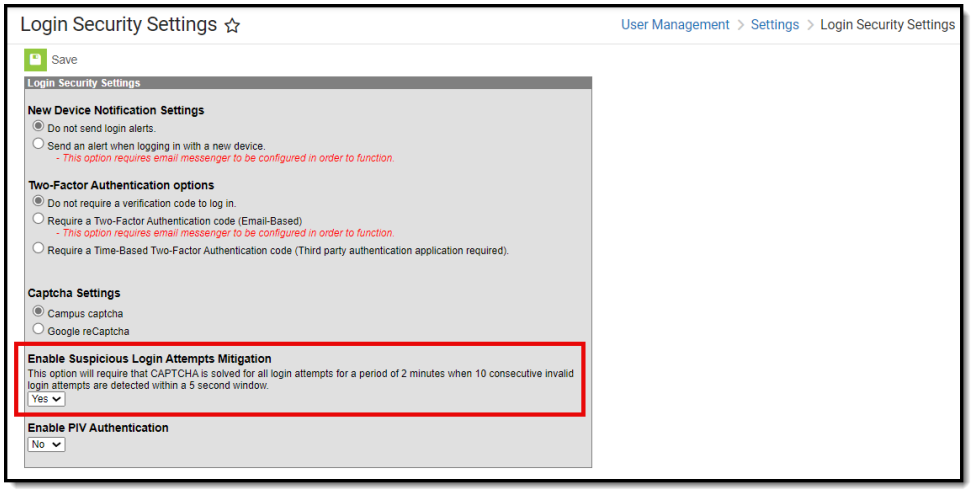
Turn on Login Alert Notifications	Turn on Login Alert Notifications so users can be notified when a new device logs in for the first time. This security measure can be an effective tool for catching unauthorized access as it occurs, so staff should be trained to report it. • Instructions for Enabling New Device Notifications 

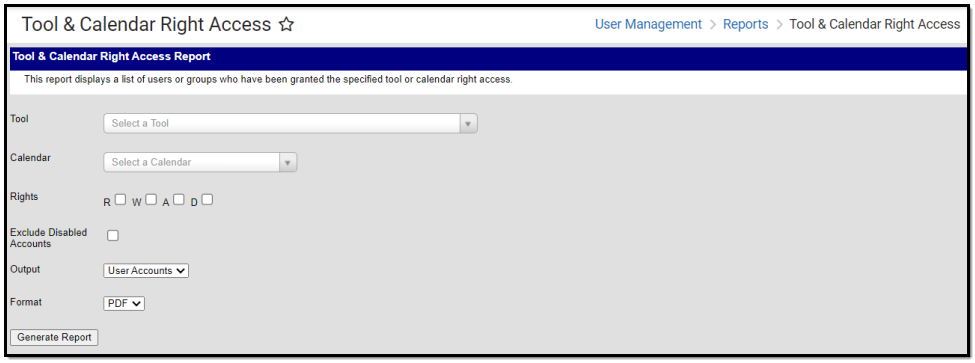
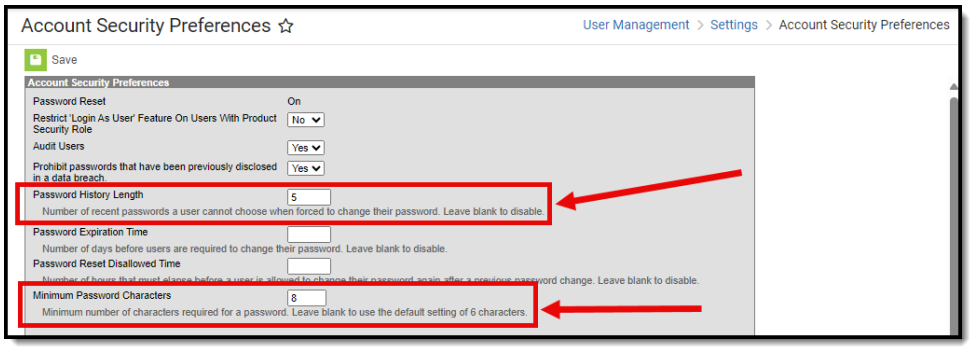
Enable Breached Password Detection

Infinite Campus can read and utilize a global database used to track passwords and accounts affected by data breaches of non-Infinite Campus systems. When breached password detection is enabled, anytime Infinite Campus detects a user's password matches a password found in a publicly known data breach, it will automatically notify the user and recommend they update it. This preference applies to Campus and LDAP authenticated accounts.

- Instructions for Enable Breached Password Detection



Enable Suspicious Login Attempts Mitigation	Enabling this setting prevents scripted and automated login attempts. When set, anytime an account has 10 consecutive failed login attempts within a 5-second window, all users attempting to log into Infinite Campus for the next two minutes are required to solve a CAPTCHA. • Instructions for Enabling Suspicious Login Attempts Mitigation 

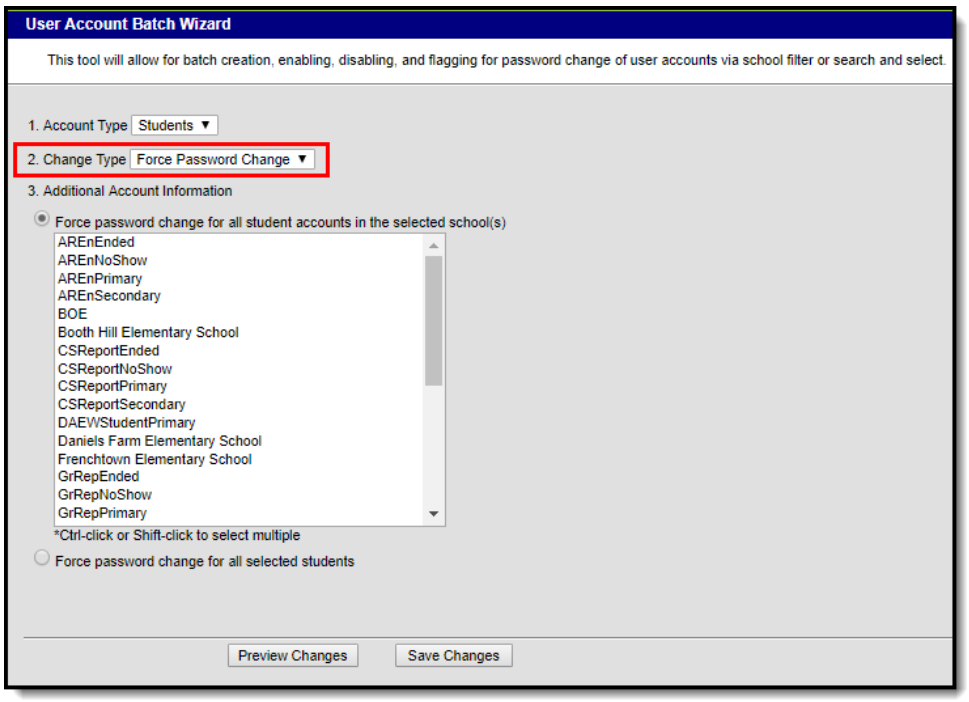
Perform Tool Rights Audits	You should routinely perform tool right audits and ensure users are granted access to tools via User Groups, not individual user account tool rights. User groups allow administrators to quickly and easily add or remove permissions for a user, a group of users, and/or group of tools. You can audit tool and calendar rights via Tool & Calendar Right Access Report. 
Strengthen Password Policies	Set the **Password History Length** preference to prevent users from being able to reuse old passwords when changing or updating their passwords and establish a **Minimum Password Characters** amount to require longer passwords to be created. This setting only applies to Local Campus Authenticated user accounts. • Setting the Password History Length • Set the Minimum Password Characters 

Force a Password Change for All or Select Users

When appropriate, you should use the User Account Batch Wizard to force a password change for all user accounts or a select set of user accounts.

> This setting only applies to Local Campus Authenticated user accounts.

- Forcing a Password Change via the User Account Batch Wizard



Take the Latest Infinite Campus Update	We recommend you always take the latest Campus Release Pack to ensure you have the latest security features and improvements. Authorized Support and Technical Contacts can request the latest Campus Release Pack within the Campus Support Portal. • Request a Campus Version Update
Enforce and Regularly Review Your Security Protocols	Review your security protocols, particularly about phishing, with staff regularly. Keep a close watch for reports of phishing attempts, and don't hesitate to contact Campus Support if you have any concerns.