Security Best Practices

Last Modified on 03/25/2026 11:01 am CDT

We know how important data security is for your district, and Infinite Campus works hard to keep your data safe. Managing accounts and authentication is your responsibility, and is the most significant security risk to your data. Be aware that compromised email addresses, usernames, and passwords frequently get shared on the dark web. These passwords are often reused across multiple applications. This allows potential 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 Multi-Factor Authentication (MFA) for All Staff Accounts

Enabling multi-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 SSO and enable Multi-Factor Authentication within your identity provider whenever possible. This provides a wider variety of multi-factor options and reuses existing user directories.

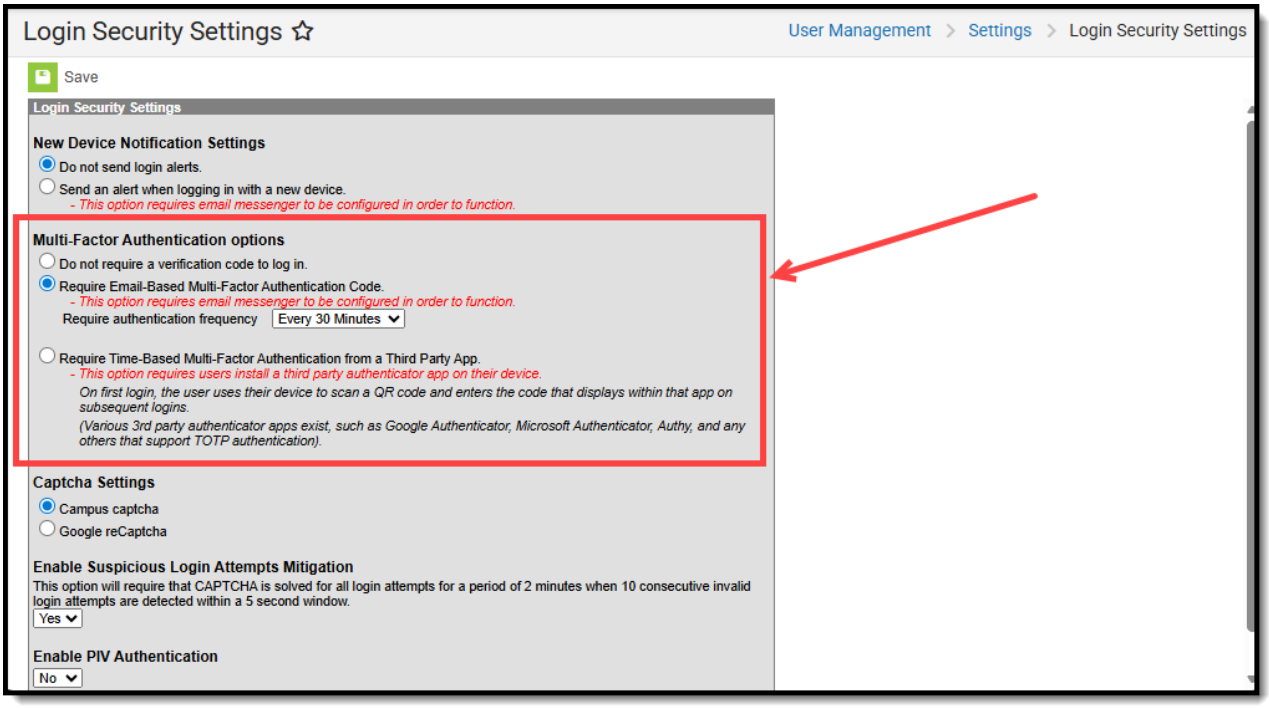
Campus offers built-in MFA for both local and LDAP-authenticated staff accounts. This feature is free and provides a strong defense against unauthorized access to the system. Authentication can be completed via an emailed verification code or an authentication app like Google Authenticator.

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

- Instructions for Enabling Multi-Factor Authentication for local and LDAP authenticated accounts

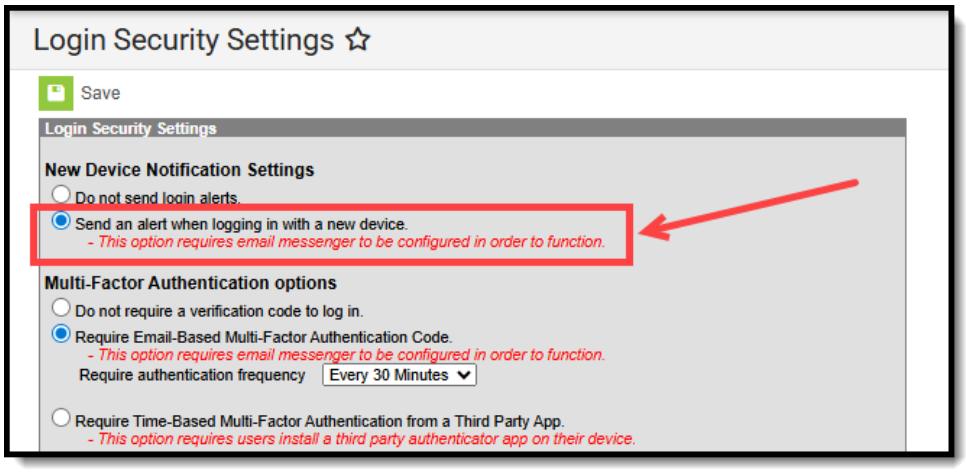
See the articles below for more information on enabling and configuring SAML SSO and/or LDAP within Campus:

- Enabling an SSO Service Provider
- Enabling LDAP



Additional Best Practices

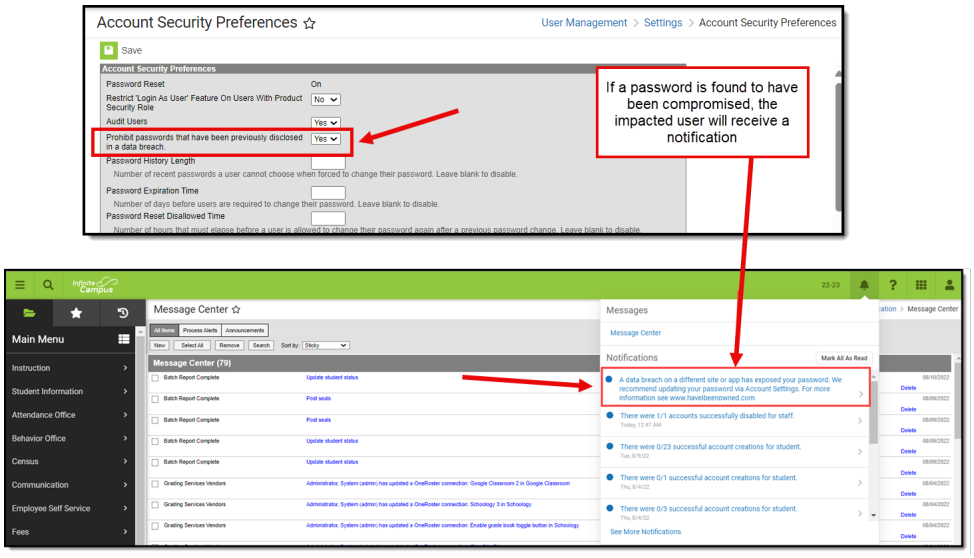
The table below details additional security best practices that all districts should implement and follow.

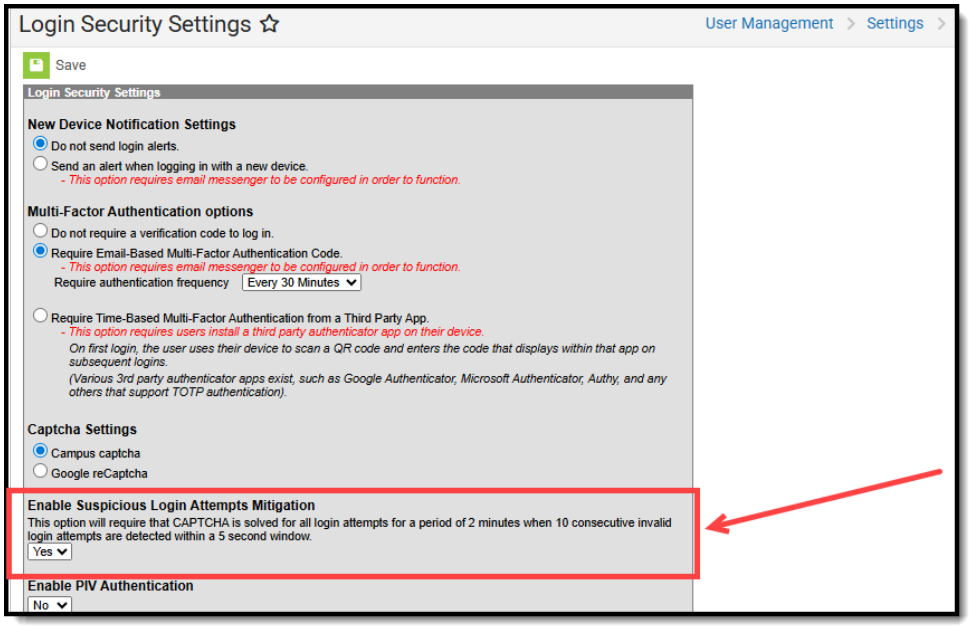
Turn on Login Alert Notifications	Enable Login Alert Notifications so users are notified when a new device logs in. This security measure can be an effective tool for catching unauthorized access as it occurs, so staff should be trained to report it. • Instructions for Enabling New Device Notifications 

Enable Breached Password Detection

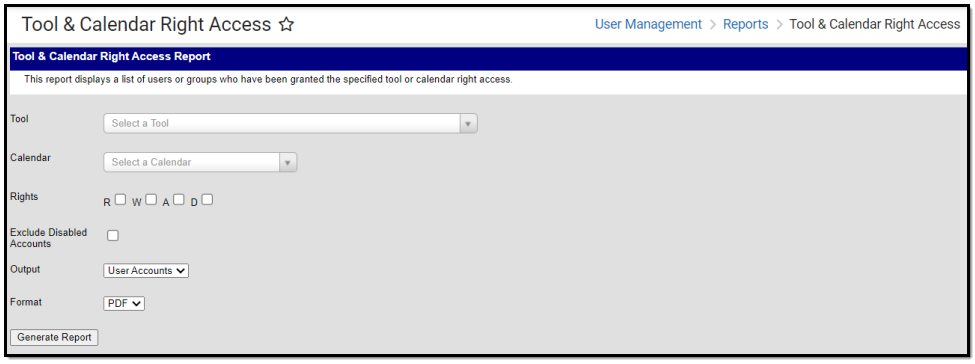
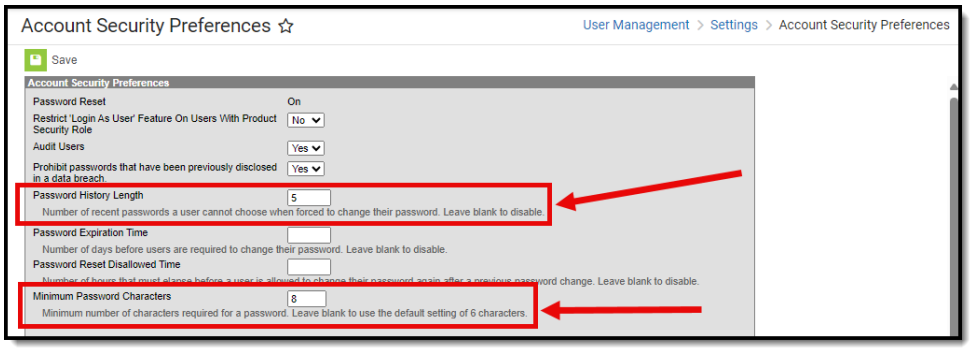
Infinite Campus can read and utilize a global database used to track passwords and accounts affected by data breaches of non-Infinite Campus systems. When password breach detection is enabled, whenever Infinite Campus detects that a user's password matches a password found in a publicly known data breach,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

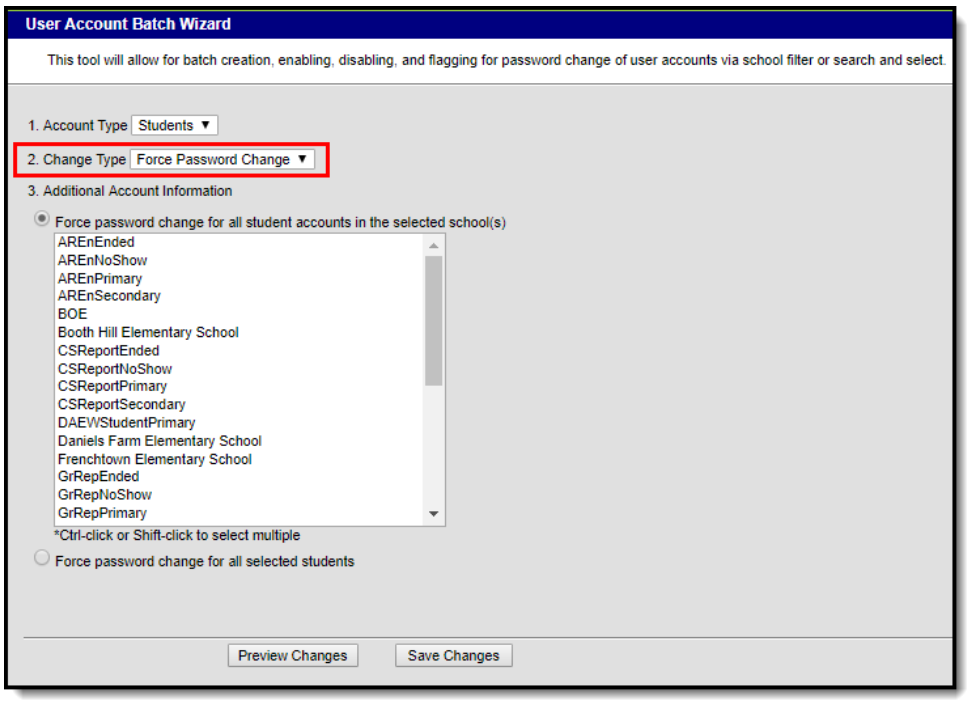
- Instructions for Enable Breached Password Detection



Enable Suspicious Login Attempts Mitigation	Enabling this setting prevents scripted and automated login attempts. When set, whenever an account has 10 consecutive failed login attempts within a 5-second window, all users attempting to log in to Infinite Campus for the next 2 minutes must solve a CAPTCHA. • Instructions for Enabling Suspicious Login Attempts Mitigation 

Run the SSN Purge Tool	If your district does not need or require Social Security Numbers for reporting purposes, we highly recommend running the SSN Purge Tool to permanently delete Social Security Number values across the district and hide core Social Security Number fields from the interface so that no new data can be added. What the tool does: • Permanently deletes SSN data from the database for 6 database fields at the district • Hides SSN fields from the UI at the district, preventing new SSN data entry through the UI • Removes all SSN tool rights for all users • **Irreversible: Once executed, SSN fields will remain hidden and cannot be restored** Deleted database fields: • RecordsTransfer.studentSSN • PlanStudent.ssn • IdentityHistory.ssn • StaffMemberSync.ssn • Identity.ssn • EvalStudent.ssn This tool will not remove SSN data stored outside of the identified fields. If districts have created and stored SSN data in other fields, the SSN Purge tool *will not* alter those records. Districts will remain responsible for managing any SSN data stored in any other fields. The following states are excluded from this tool for reporting reasons: VA, KY, GA, IN, MO, and TX.
Upgrade to Google reCaptcha	Infinite Campus has a built-in CAPTCHA system to deter repeated automated login attempts. This can be upgraded to use Google's reCAPTCHA v2 for greater effectiveness and configurability. This will require registration with Google. • Configure Google reCaptcha
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

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 reusing old passwords when changing their passwords, and set the **Minimum Password Characters** preference to require longer passwords. 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, use the User Account Batch Wizard to force a password change for all user accounts or a select set. This setting only applies to Local Campus Authenticated user accounts. • Forcing a Password Change via the User Account Batch Wizard 
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.