Security Best Practices

Last Modified on 10/19/2026 1:19 pm 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 it 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 configurations, settings, and best practices listed below.

Configurations and settings

The table below outlines configurations and settings you should apply to bolster your application's security.

Enable Multi-Factor Authentication 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 use a third-party identity provider that supports 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 email verification code or an authentication app such as 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
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 in real time, so staff should be trained to report it. • Instructions for enabling New Device Notifications

Enable breached password detection	Infinite Campus can read and use a global database that tracks passwords and accounts affected by data breaches involving non-Infinite Campus systems. When password breach detection is enabled, if Infinite Campus detects that a user's password matches one from a publicly known data breach, it will automatically notify the user and recommend updating it. This preference applies to Campus and LDAP authenticated accounts. • Instructions for enabling 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
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
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

Securely manage user accounts and data

Once your Infinite Campus instance is properly configured, it is important to securely manage your day-to-day usage by implementing the user accounts and data items listed below.

Manage tool rights using user groups	Individual user tool rights should be managed through user groups rather than granting rights to every user. By setting up user groups for the various roles and job duties throughout a school, you can tailor tool and data access for each user group, assuring staff have uniform and appropriate access to the tools pertaining to their job(s), denied access to tools and data not pertaining to their job(s), and an easy way to remove or add access to tools or data for each subset of people, as needs or situations dictate. It is also a simple way to remove a person's access to tools and data by merely removing them from the user group. • Understanding and assigning User Group tool rights. • Suggested User Groups and associated tool rights
Limit the number of Product Security Roles	Product Security Roles grant system administrative-level access to Infinite Campus, as well as access to specific premium products and functionality, such as the ability to log in as other users. Because of their advanced access to tools, data, and user accounts, you should greatly limit the number of people in your district who hold one of these roles. • Understand and assign Product Security Roles in a single-product environment • Understand and assign Product Security Roles in a multi-product or premium product environment Use the Product Security Role Report to audit which users have been granted these rights.
Deactivate unneeded administrative accounts	When users, especially those with administrative rights, no longer need access to Infinite Campus, their accounts should be disabled via the **Disable Account** checkbox on their user account. • Instructions for disabling an account. If a user with administrative rights, such as a Product Security Role, no longer requires these elevated rights, you should remove their Product Security Role(s) and assign them to the appropriate user group(s). • Information on Product Security Roles

Run the SSN Purge Tool	If your district does not 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 to hide core Social Security Number fields from the interface, so that no new data can be added. • Instructions on purging SSN data 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.
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 a group of tools. You can audit tool and calendar rights via the Tool & Calendar Right Access Report.
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.

Version History

Click here to expand...

Version	What Changed?	Date
1.0	Initial creation of the document	9-21-26