Login Security Settings

Last Modified on 10/22/2022 10:10 am CDT

Classic View: *System Administration > User Security > User Preference Management > Login Security Settings*

Search Term: *Login Security Settings*

The Login Security Settings tool allows you to control whether or not Staff users will receive login alert notification emails as well as require two-step verification via an emailed code or authentication application.

For more information about tracking notifications, see the Establishing Trusted Devices for Campus Login section of the Managing User Account Passwords article.

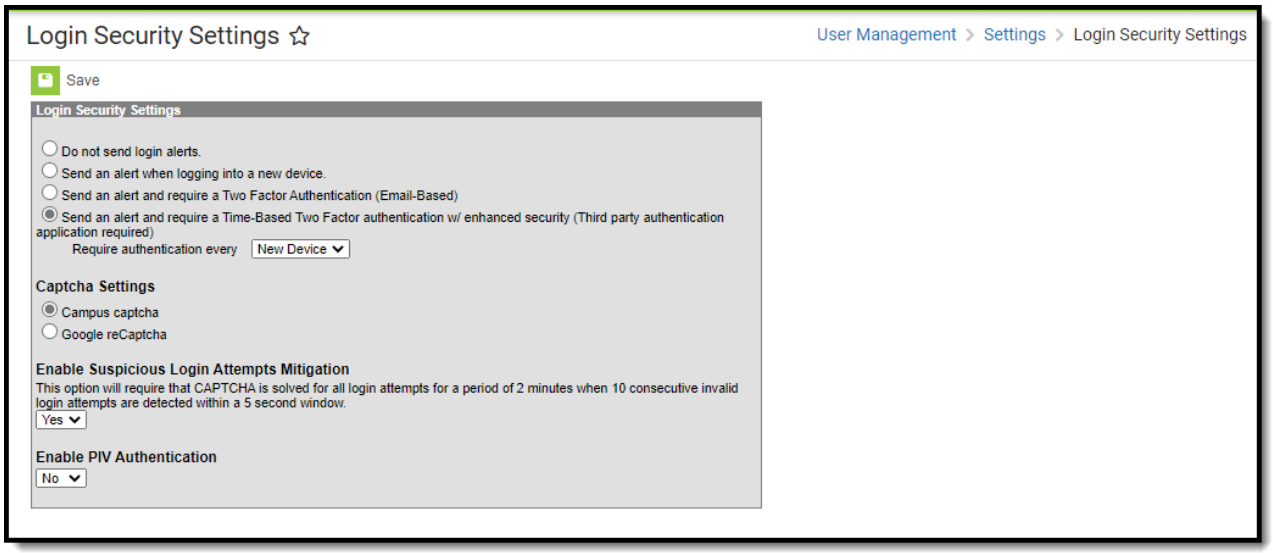


Image 1: Login Security Settings

Tool Rights

Only System Administrators should have access to the Login Security Settings tool.

Only users with a Student Information System (SIS) Product Security role are allowed to access and modify values in the Login Security Settings tool.

Disable Login Alert Notifications

To disable login notification emails, select the **Do not send login alerts** radio button (Image 2) and click the **Save** icon. Users will no longer receive an email each time their Campus account is accessed via a new or unrecognized device/computer.

Infinite Campus highly recommends using at LEAST the 'Send an alert when logging into a new device' setting.

This setting does not apply to Student and Parent Portal accounts.

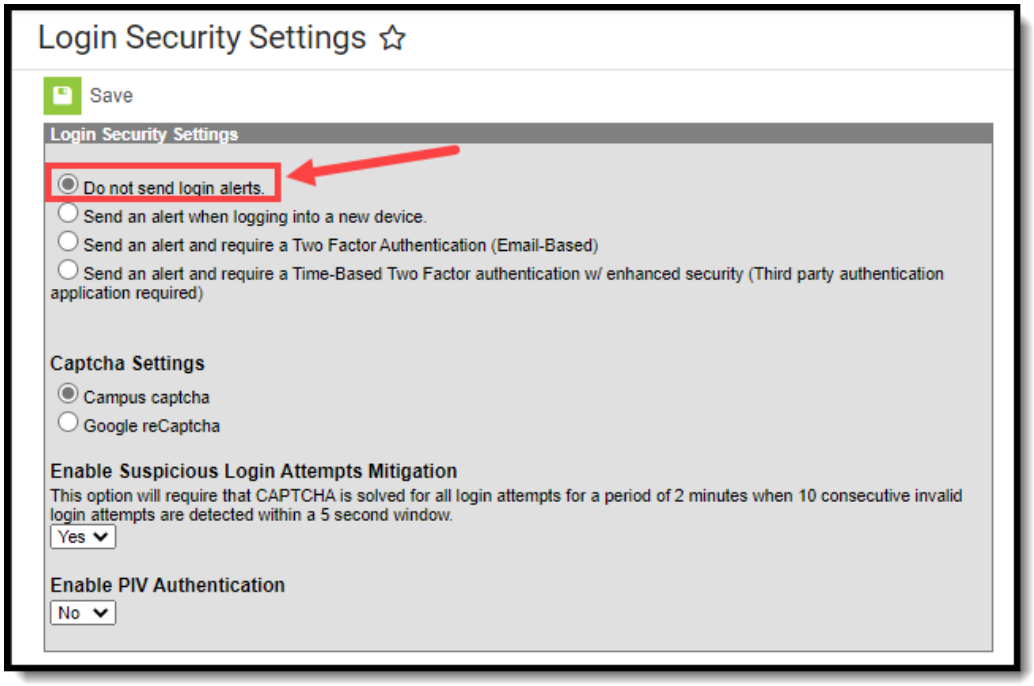


Image 2: Turning Off Login Alert Notification Emails

Enable Login Alert Notifications

To enable login alert notification emails, select the **Send an alert when logging into a new device** radio button (Image 3).

As of Release Pack .2219, this preference is the default setting.

All users who upgrade to Release Pack .2219 or greater and have their setting set to 'Do not send login alerts' will automatically have their Login Security Setting set to a value of 'Send an alert when logging into a new device' in an effort to bolster security across our customers. Users can set this value back to 'Do no send login alerts' at anytime and subsequent updates will not modify this value.

Login notifications will increase email traffic. It is important you have adequate email capacity when enabling and using login alert functionality.

This setting does not apply to Student and Parent Portal accounts.

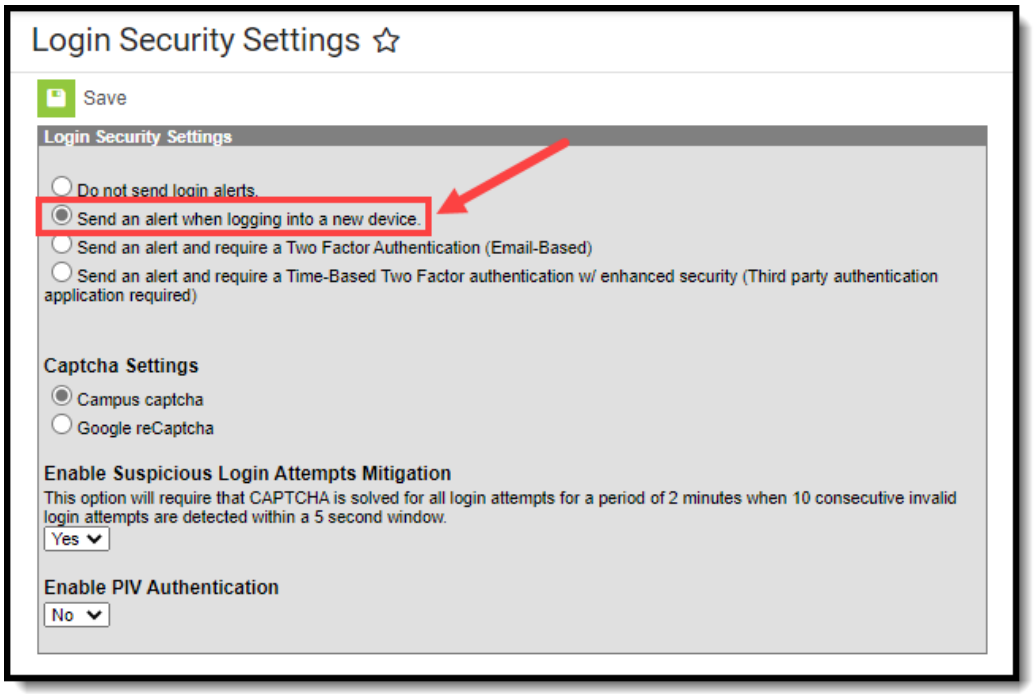


Image 3: Turning On Login Alert Notification Emails

Once notifications are enabled, users will receive an email each time their Campus account is accessed via a new or unrecognized device or computer. The section below describes this process.

What Happens Once Alert Notifications are Enabled

Once the **Send an alert when logging into a new device** radio button is selected, users logging into Infinite Campus for the first time from a device will be required to enter an **Account Security Email** address (if one is not already present within Infinite Campus) and will be asked if they would like the device to be remembered for future logins (Image 4).

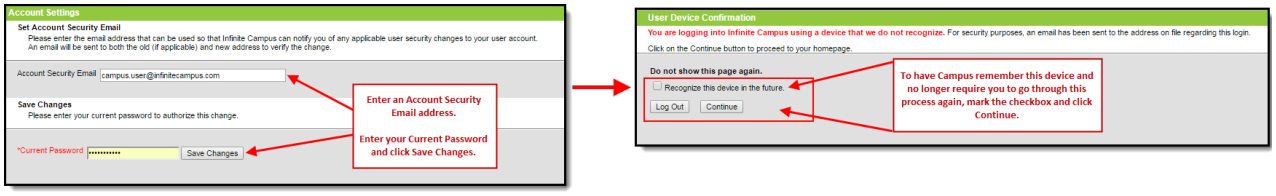


Image 4: Entering an Account Security Email and Remembering the Device

Once an email address is established, any time you log into Infinite Campus using a device that has not been used to login into Infinite Campus before or has not been designated as a device for Infinite Campus to remember will result in an email being sent to your Account Security Email address, alerting you that you (or someone) logged into Infinite Campus. Below is an example of the email you will receive (Image 5).

In order for a device to be recognized for future logins, your browser MUST be set to allow cookies.

Having your browser set to automatically delete cookies will cause the device to not be recognized and force you to go through this process each time you log into Campus.

See the FAQ section below for more information about reducing the amount of notification emails that may be sent.

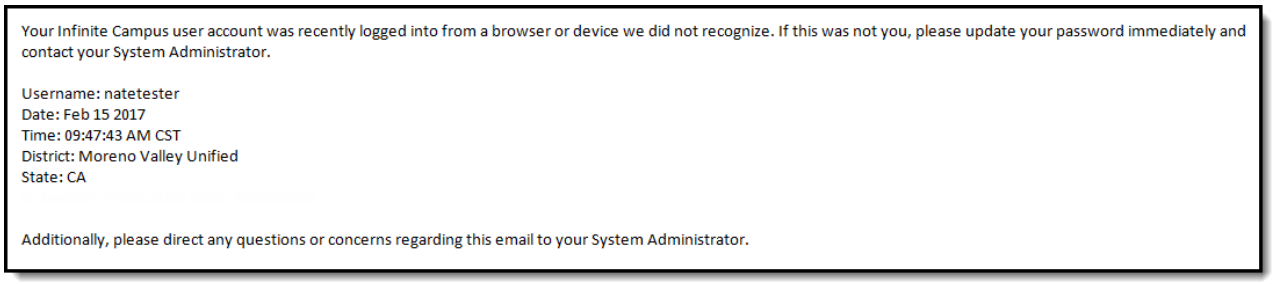


Image 5: Unknown Device Login Email Notification

Enable Email Verification Code Logins

To enable login alert and verification code emails, select the **Send an alert and require a Two Factor Authentication (Email Based)** radio button (Image 6).

Login and verification code notifications will increase email traffic. It is important you have adequate email capacity when enabling and using login alert and verification code functionality.

This setting does not apply to Student and Parent Portal accounts.

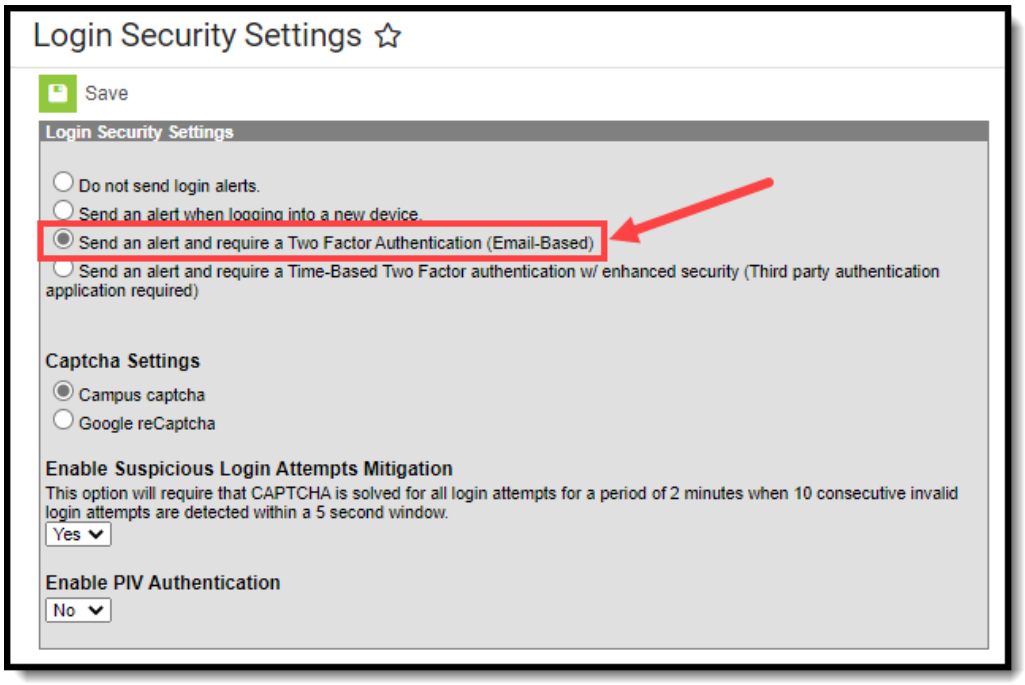


Image 6: Enabling Login Notifications with Verification Codes

Once this setting is selected and saved, users logging into Infinite Campus for the first time from an unrecognized device will be required to enter an **Account Security Email** address (if one is not already present within Infinite Campus) and once saved, they will be directed to a new screen where they will have to enter a verification code (sent in an email to the address entered in the previous step) and decide if they would like the device to be remembered for future logins (Image 7).

In order for a device to be recognized for future logins, your browser MUST be set to allow cookies.

Having your browser set to automatically delete cookies will cause the device to not be recognized and force you to go through this process each time you log into Infinite Campus.

Image 7: Entering an Account Security Email and Entering a Verification Code

Below is an example of the email that will be sent to your account. This email contains the 8-

character verification code that must be entered in the box show above (Image 7).

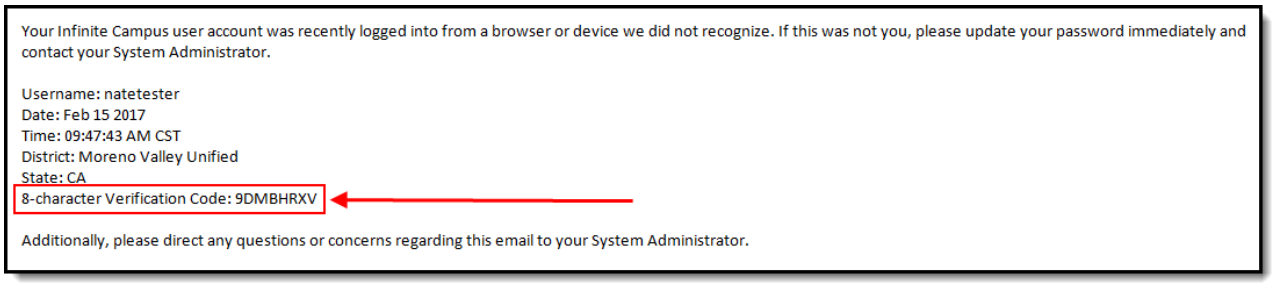


Image 8: Finding the Verification Code

Enter the 8-character verification code into the box shown below, decide if the device should be remembered for future logins by marking the **Recognized this device in the future** checkbox, and click **Continue** (Image 9). The device is now verified and you will no longer receive notification emails when logging into Campus using this device.

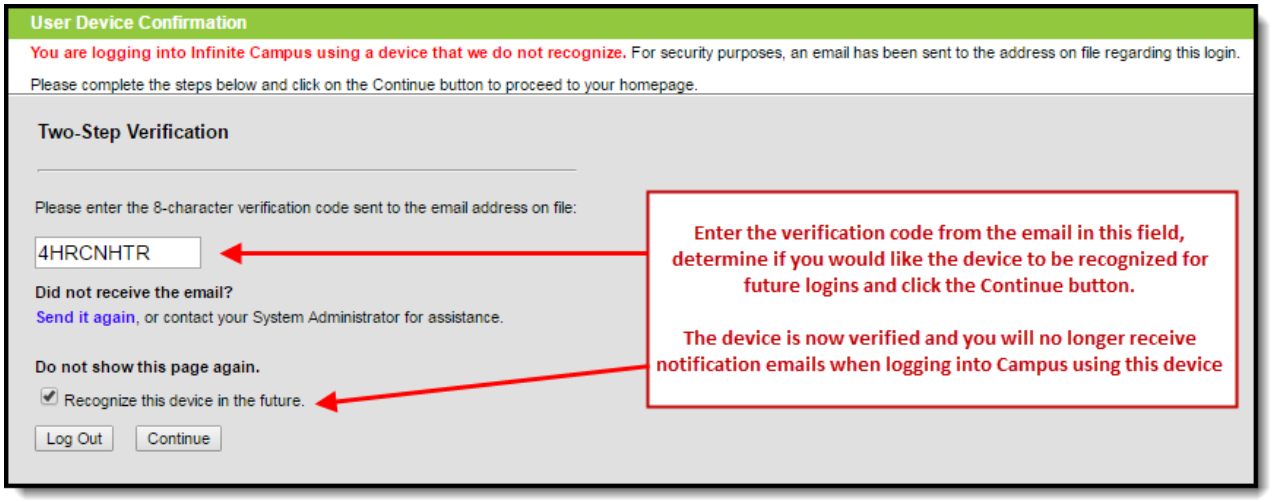


Image 9: Entering a Verification Code

Enable Time-Based Two-Factor Authentication with Enhanced Security

As an increased layer of protection for Infinite Campus accounts, user accounts can be enabled with time-based two-factor authentication functionality with enhanced authenticator security. When enabled, users are provided a unique QR code and Text Code which requires them to authenticate their account using a device and an authenticator application (such as Google Authenticator, Authy, LastPass, etc).

This setting does not apply to Student and Parent Portal accounts.

As of Campus Release Pack .2207 (February 2022), Time-Based Two-Factor Authentication was enabled and is required for all BIE user accounts and cannot be disabled.

If you experience any issues authenticating, know that your device must be in-sync with the actual time in order to authenticate. Compare the time showing on your device to the actual time (https://www.time.gov). If time on your device is out of sync, you can correct this in your device's Date & Time settings. In your device settings, you will likely have the option to enable your device to automatically sync the date and time.

Alternatively, if you use Google Authenticator for Android, you can also try the Time Sync (https://support.google.com/accounts/answer/2653433) feature.

To enable device-based two-factor authentication for all non-Campus Portal account:

1. Click the **Send an alert and require a Time-Based Two Factor authentication w/enhanced security (Third party authentication application required)** radio button
2. Set the frequency in which users will be required to reauthenticate their credentials when logging into Infinite Campus.
    - **New Device** - Users will need to reauthenticate using an authentication application each time they log into Infinite Campus using a new, unrecognized device.
    - **30 Minutes** - Users who log out of Infinite Campus and attempt to log back in 30 minutes or later after the last time they logged in will be required to reauthenticate using the authentication application.
    - **Day** - Users who log out of Infinite Campus and attempt to log back in 24 hours or later after the last time they logged in will be required to reauthenticate using the authentication application.
    - **Week** - Users who log out of Infinite Campus and attempt to log back in 7 days or later after the last time they logged in will be required to reauthenticate using the authentication application.
    - **Month** - Users who log out of Infinite Campus and attempt to log back in 1 month or later after the last time they logged in will be required to reauthenticate using the authentication application.
3. Select **Save**.

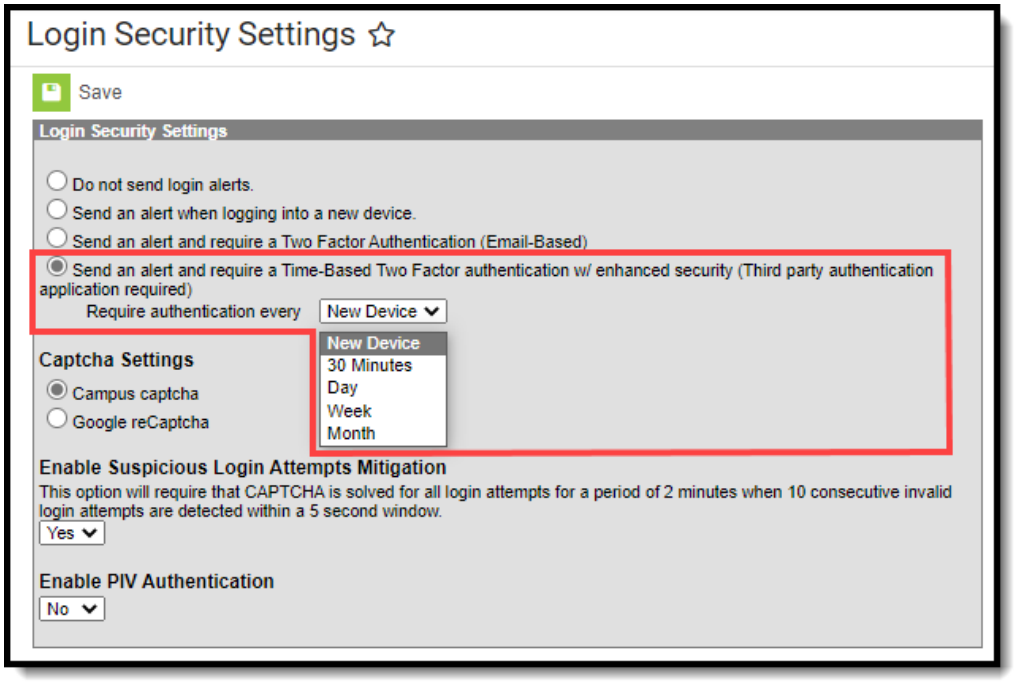


Image 10: Enabling Device-Based Two-Factor Authentication for All Non-Portal Accounts

Once enabled, the next time users attempt to log into Infinite Campus they will see a screen displaying a unique QR Code and Text Code.

Using a device (such as cell phone), users must download an authenticator app (such as Google Authenticator, Authy, LastPass, etc) and use the app the scan the **QR Code** or enter the **Text Code**. This will register the device and tie it to their Infinite Campus account.

Once they have scanned the QR Code or entered the Text Code in the authenticator app, the app will display a code. Enter the code from the authenticator app into the field on the Campus login screen, mark the **Recognize this device in the the future** checkbox, and click **Continue** (see image below). The user will be logged into Campus.

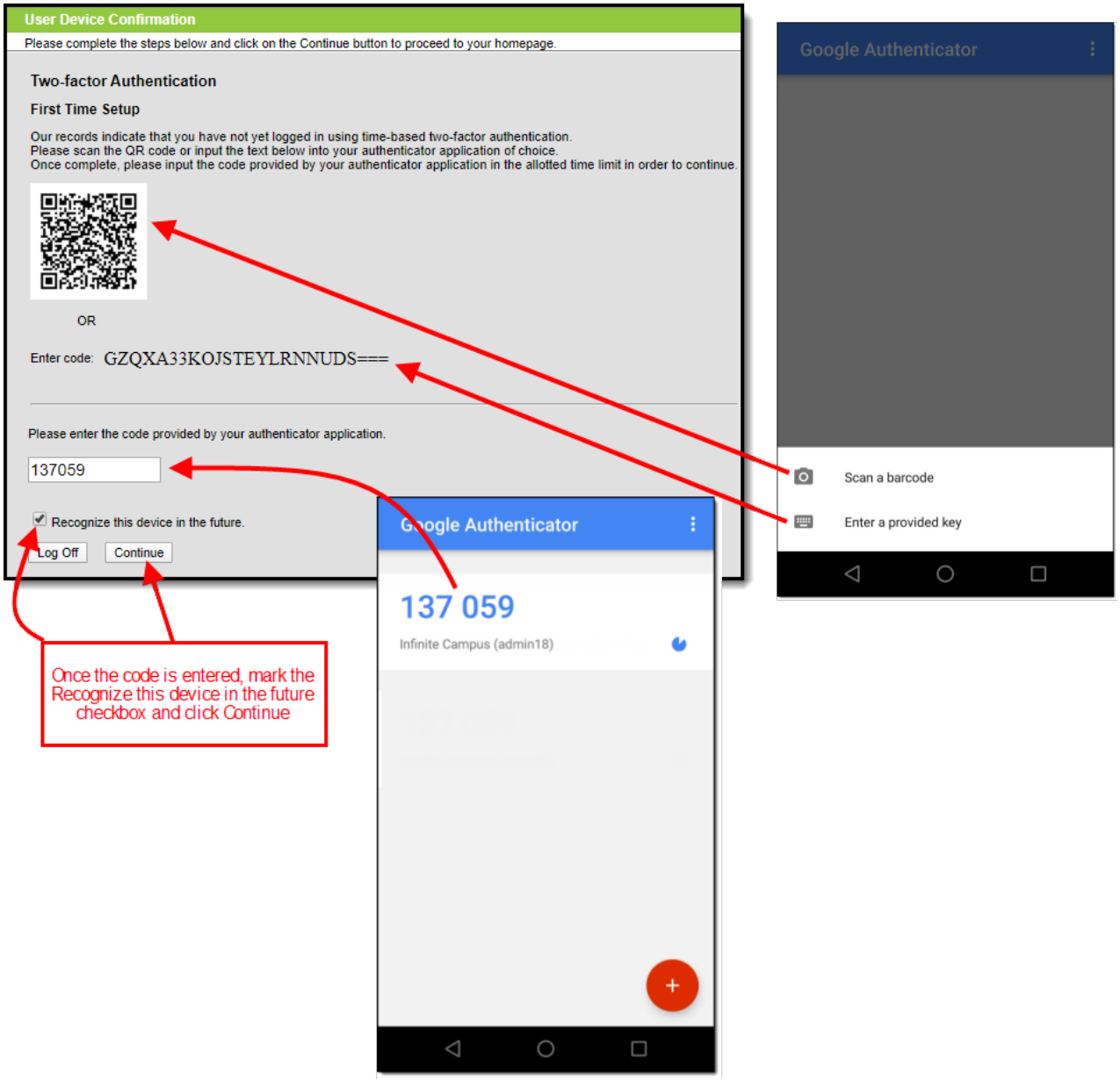


Image 11: Registering a Device and Logging into Infinite Campus

In the future when logging into Infinite Campus, depending on the reauthentication frequency set by the administrator, users will need to access their authenticator app on their registered device and enter the code displayed in the authenticator app into field on the Infinite Campus login screen. Users should mark the **Recognize this device in the future** checkbox and click **Continue**. If the code they entered is correct, they will be logged into Campus.

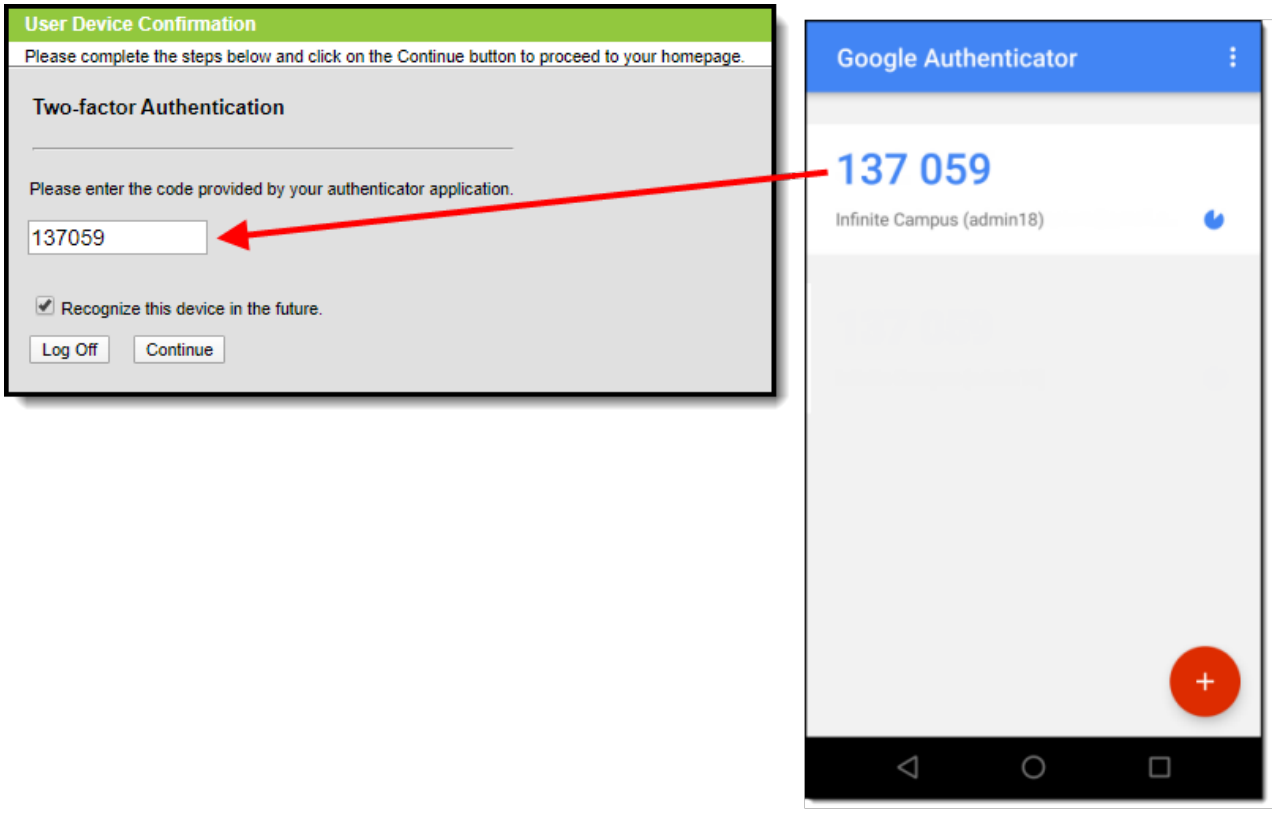
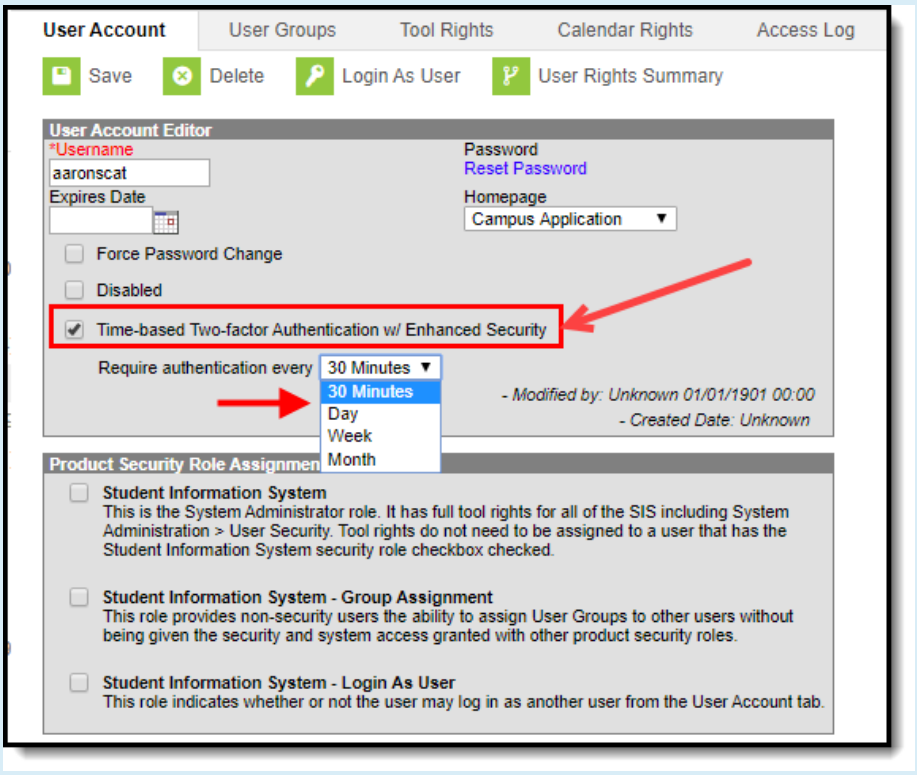


Image 12: Logging into Infinite Campus Using an Authentication Code

You can change the reauthentication frequency on a per-user basis by navigating to their **User Account**, changing the value and selecting Save.



Enable Captcha Settings

Captcha Settings determine which captcha is used on the Infinite Campus login screen for users who have failed to properly log into Infinite Campus several times in a row. This feature prevents users from being locked out of their account after several failed login attempts and protects accounts from malicious bots and scripts.

> These settings apply to Staff, Student, and Parent Portal accounts but do NOT apply to LDAP and SSO-authenticated user accounts.

The following captcha options are available:

- Campus Captcha
- Google reCaptcha

Campus Captcha

Campus captcha displays a captcha with a randomly generated set of letters and numbers the user must enter in order to log into Infinite Campus.

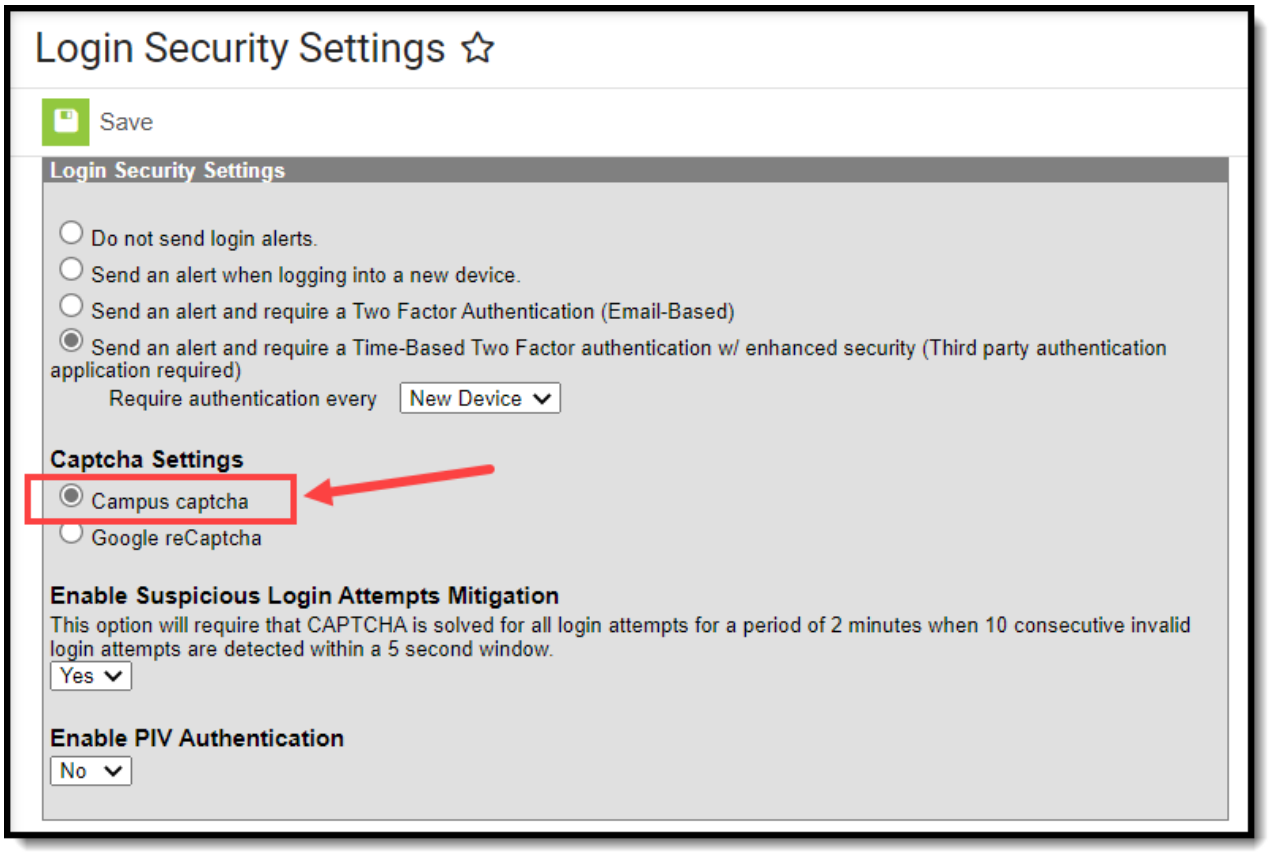


Image 13: Enabling Campus Captcha

The image below is an example of the Campus captcha (Image 14).

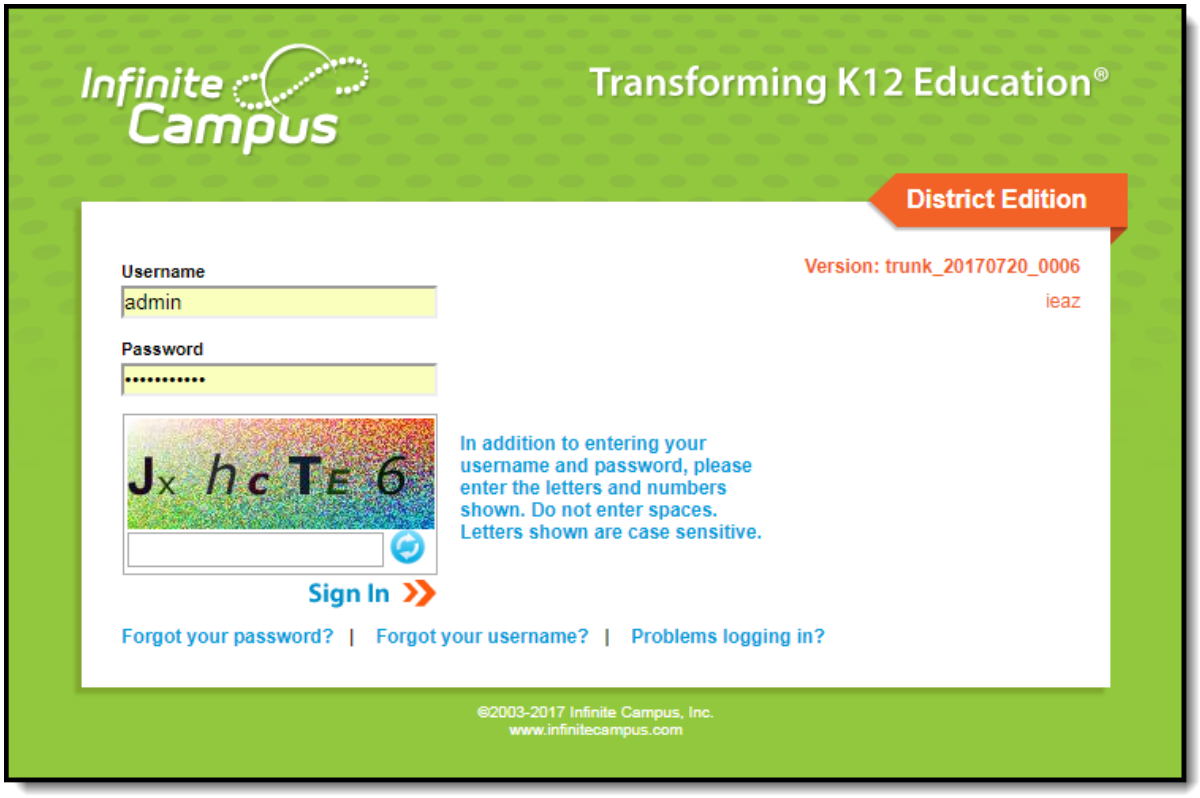


Image 14: Example of the Campus Captcha

Google reCaptcha

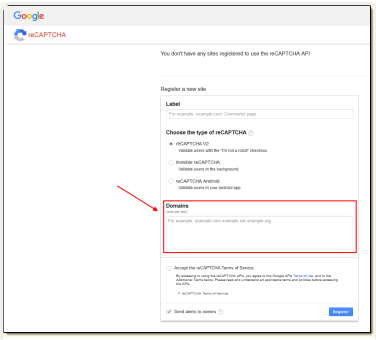
The Google reCaptcha displays a checkbox the user must click and a series of pictures the user must select to prove they are human and not a bot.

Before you can enable Google reCaptcha, you must first go through a registration process with Google to acquire the **Site Key** and **Secret Key** and enter this data within Campus (Image 15).

See the Google reCaptcha website for more information about registration.

Campus only supports reCaptcha V2. You must use this option when connecting Campus to reCaptcha functionality.

When registering for Google reCaptcha, enter the **Domain** by removing the http:// from the Campus site URL (for example, infinitecampus.org instead of http://infinitecampus.org). Do NOT enter the full URL. **Failure to remove the http:// or https:// from the beginning of the URL will result in errors.**



Click to see image

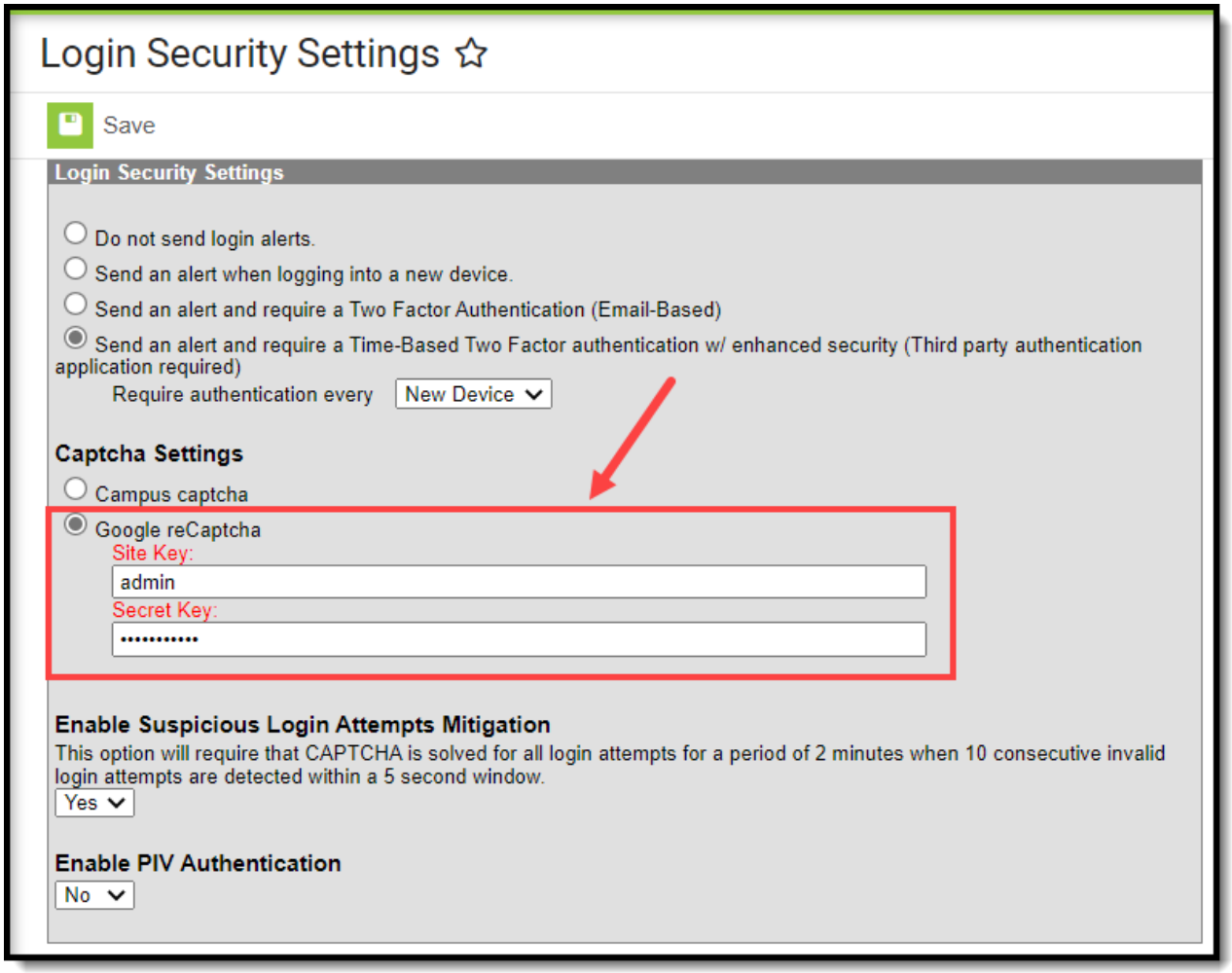


Image 15: Setting Google reCaptcha Settings

Once Google reCaptcha is enabled, a user who has unsuccessfully attempted to log into Campus several times in a row will be required to first mark a checkbox (Image 16).

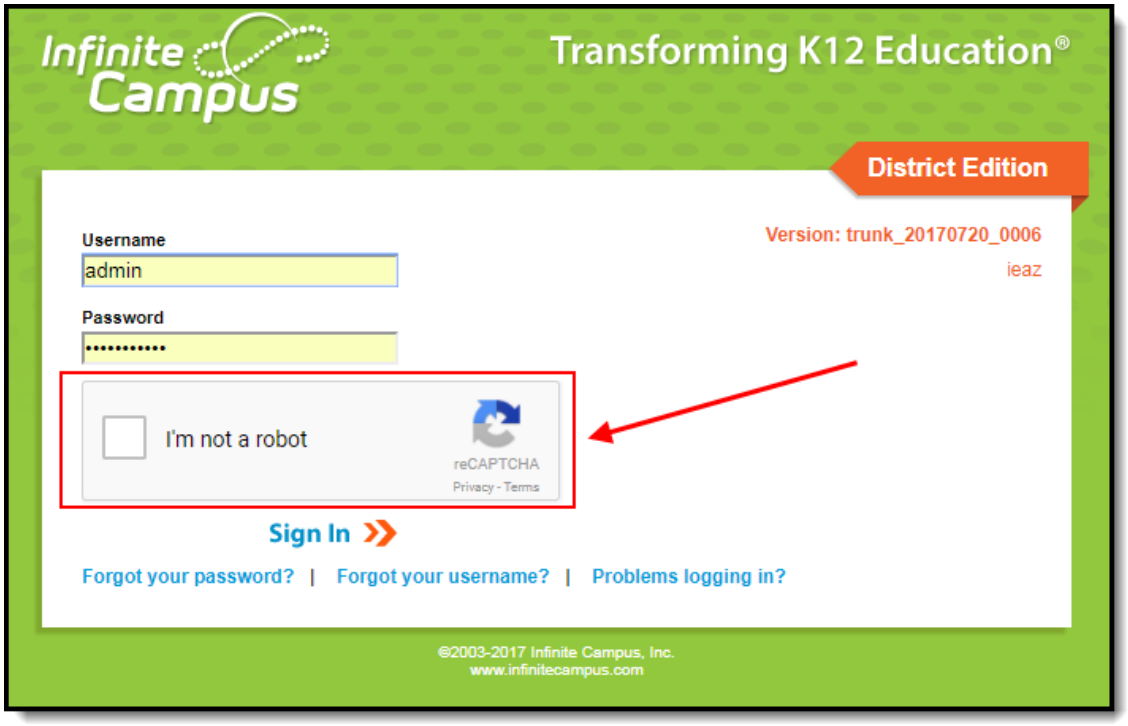
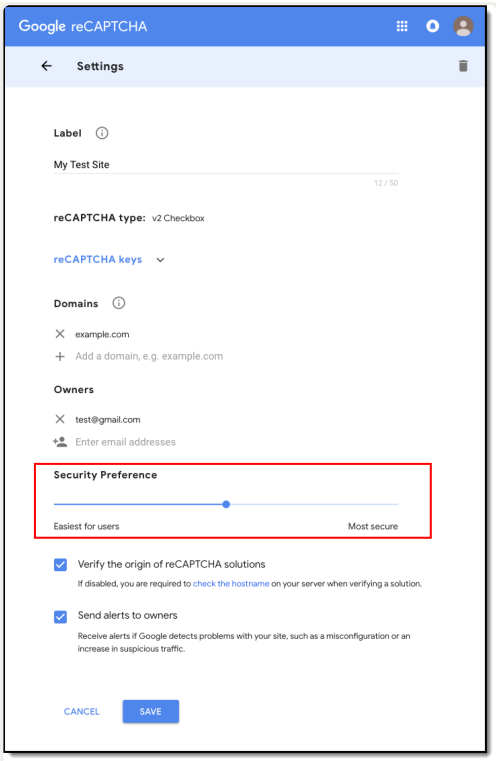


Image 16: Confirming You are Not a Robot

Once the user has marked the checkbox, reCaptcha will validate the user's behavior and return success if it believes that the user is not a robot.

A Security Preference slider on the reCaptcha Settings screen allows for adjusting the security preference of the reCAPTCHA from 'Easiest for users' to 'Most secure'. This will determine the types of challenges generated by the captcha (i.e., easiest only requiring the I'm Not a Robot checkbox to be checked).



Click to see image

Depending on the reCaptcha security preference level, a popup may appear, asking the user to either select a series of squares or pictures based on specific question (Image 17) or listen to an audio challenge.

The audio challenge option for Google reCaptcha does NOT work properly within Microsoft Explorer and Edge web browsers.

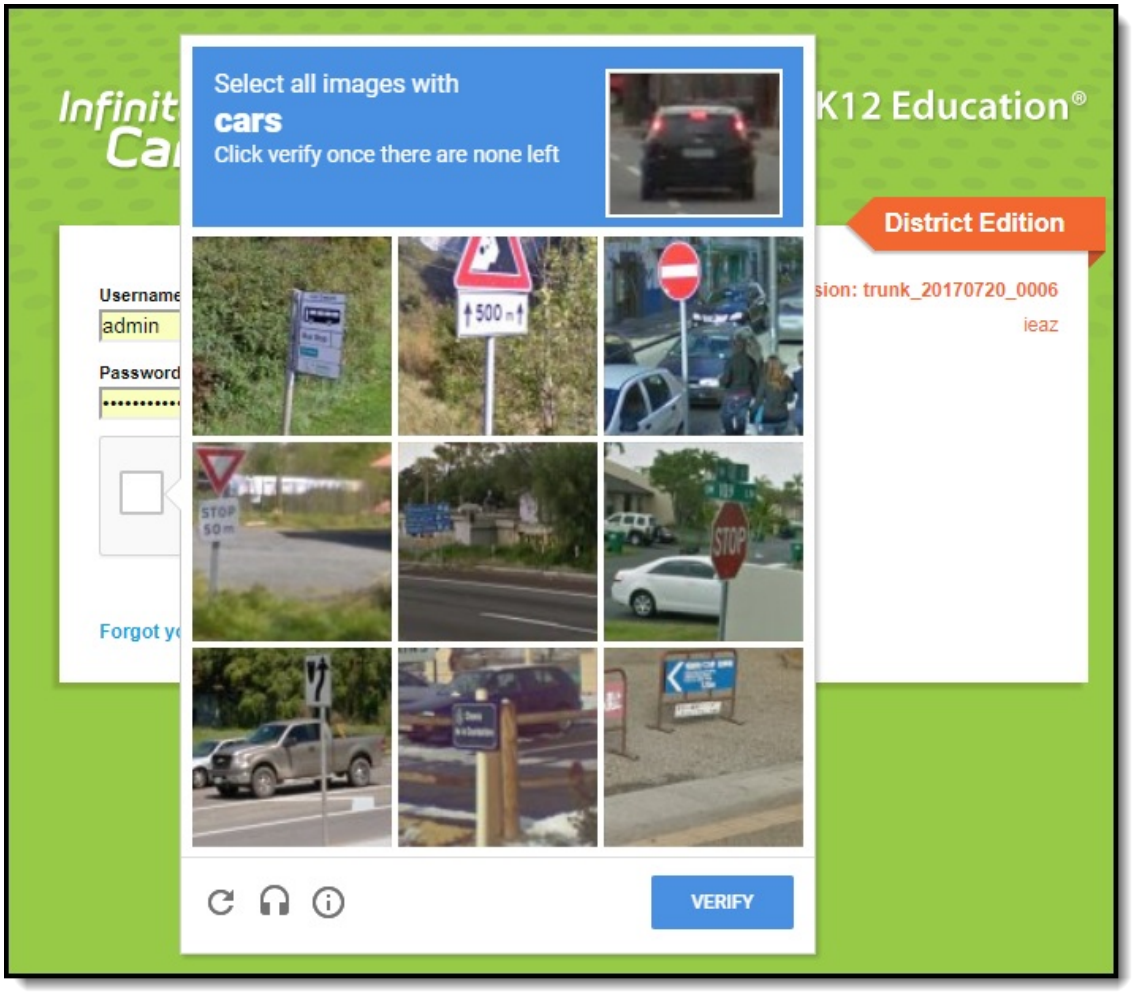


Image 17: Selecting Verification Images

Once the user has successfully selected the proper images, they will be redirected to the Campus login screen where they can proceed to log into Campus.

If you experience any issues after setup, ensure the IP addresses that Google requires for reCAPTCHA functionality have been AllowListed. Google maintains their list of IP addresses that must be AllowListed in order for reCAPTCHA functionality to work here:

https://code.google.com/archive/p/recaptcha/wikis/FirewallsAndRecaptcha.wiki

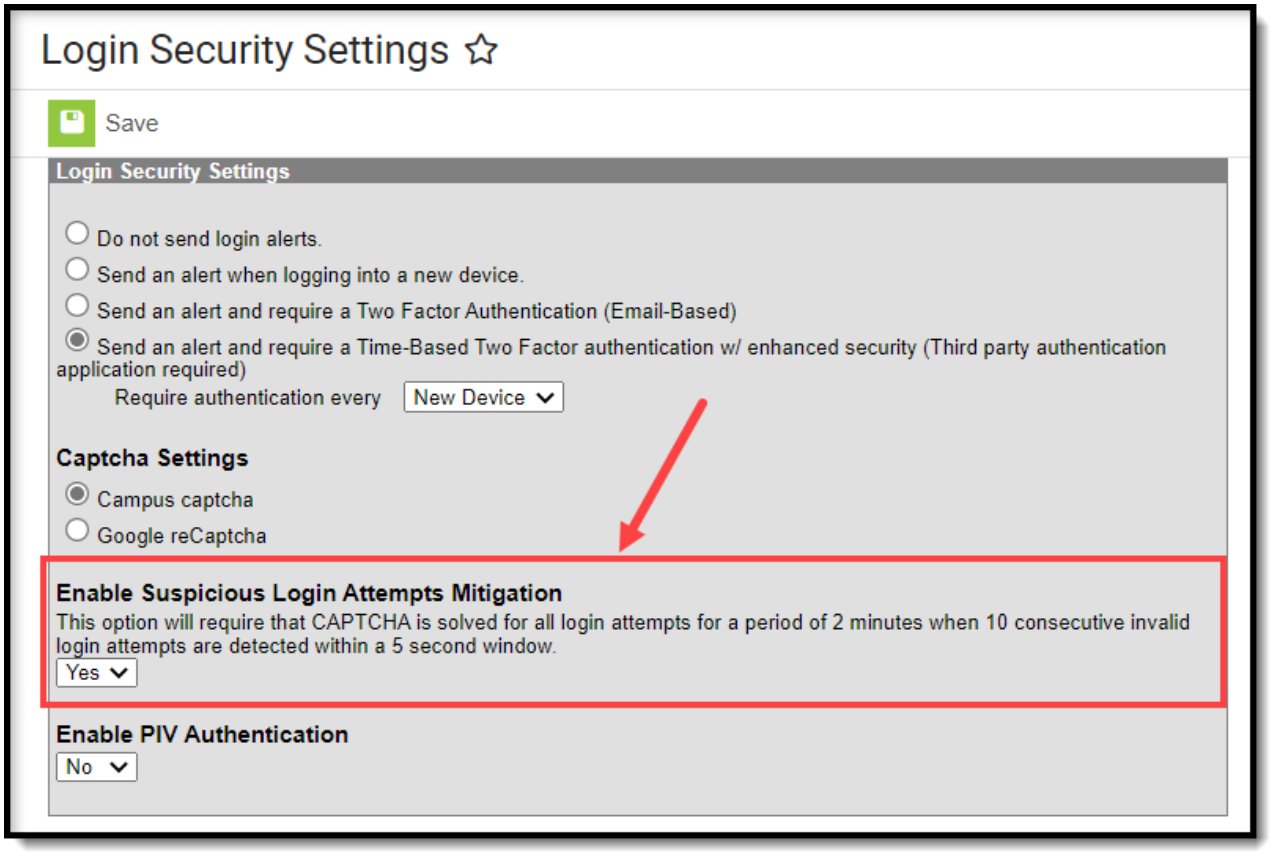
Enable Suspicious Login Attempts Mitigation

When the **Enable Suspicious Login Attempts Mitigation** setting is set to 'Yes', anytime there is 10 consecutive failed login within a 5 second window, all users attempting to log into Infinite Campus for the next two minutes are required to solve a CAPTCHA.

This setting applies to Staff, Student, and Parent Portal accounts but does NOT apply to LDAP and SSO-authenticated user accounts.

As of Release Pack .2219, this preference is set to a default of 'Yes'.

All users who upgrade to Release Pack .2219 or greater will have this setting set to 'Yes'. Users can set this value back to 'No' at anytime and subsequent updates will not modify this value however, **Infinite Campus HIGHLY recommends leaving this setting set to Yes** as it provides a line of defense against automated attacks on your system.



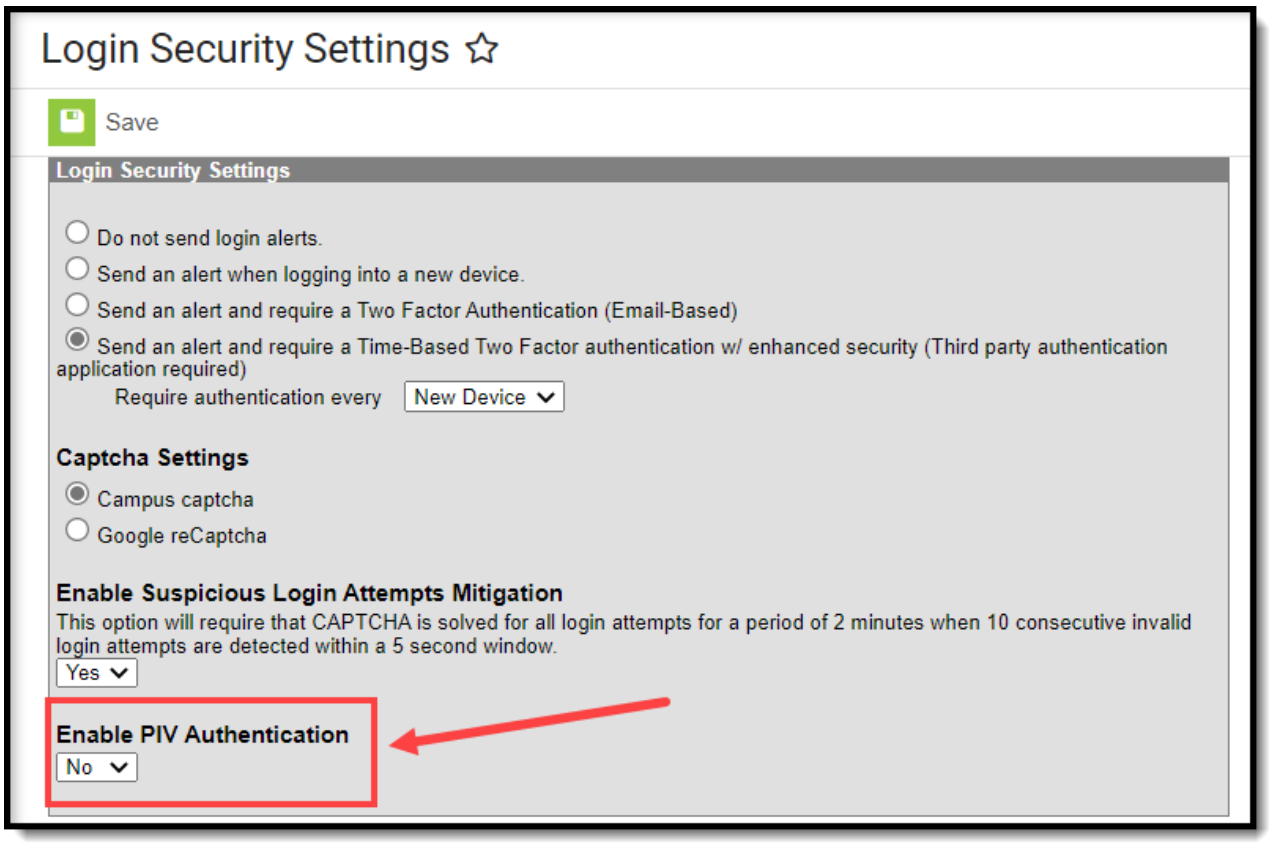
Enable PIV Authentication

The **Enable PIV Authentication** setting enables the ability for users to authenticate and log into Infinite Campus using a Personal Identity Verification (PIV) card.

PIV authentication only applies to Staff user accounts. This functionality does not affect Campus Student/Parent Portal accounts.

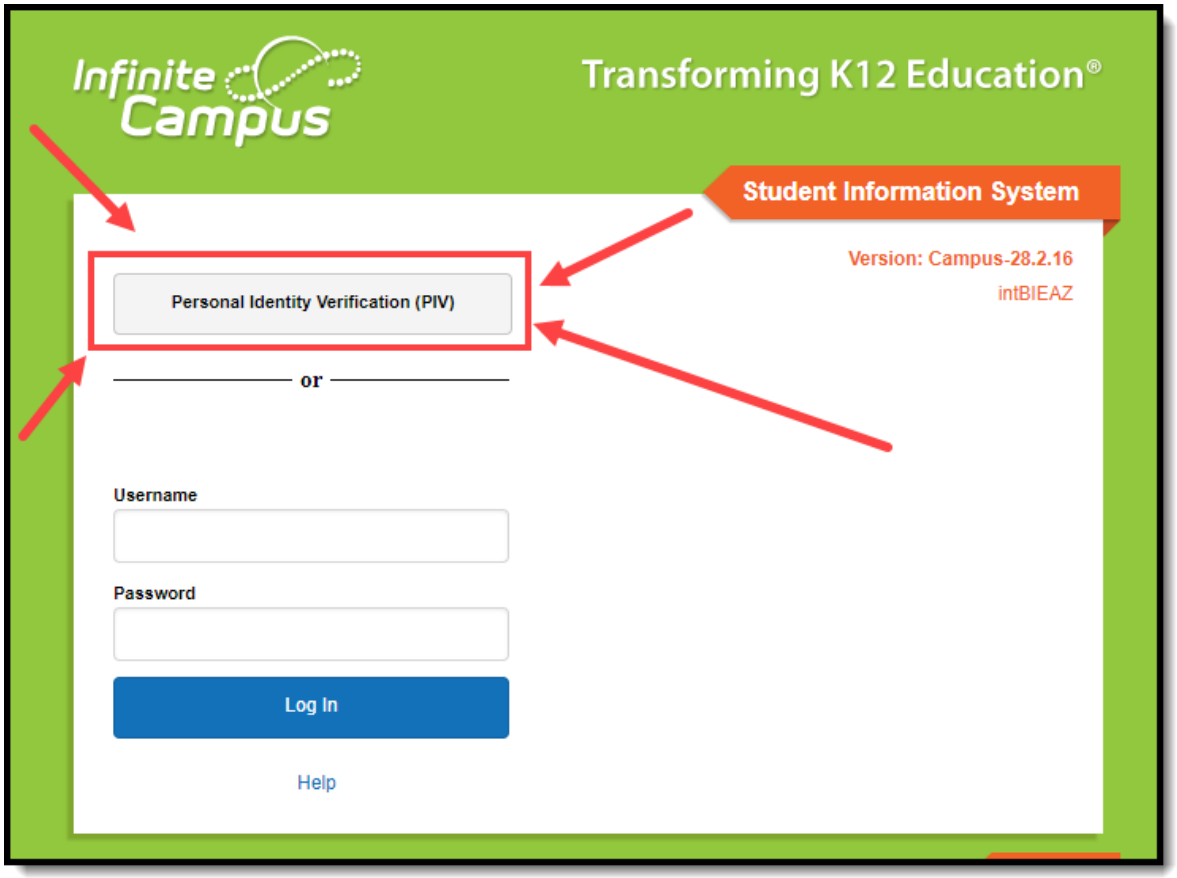
For a walkthrough of the PIV Authentication registration process, see the following articles:

- Administrators: PIV Card Registration Process for Administrators
- Staff Members: PIV Card Registration Process for Staff Members



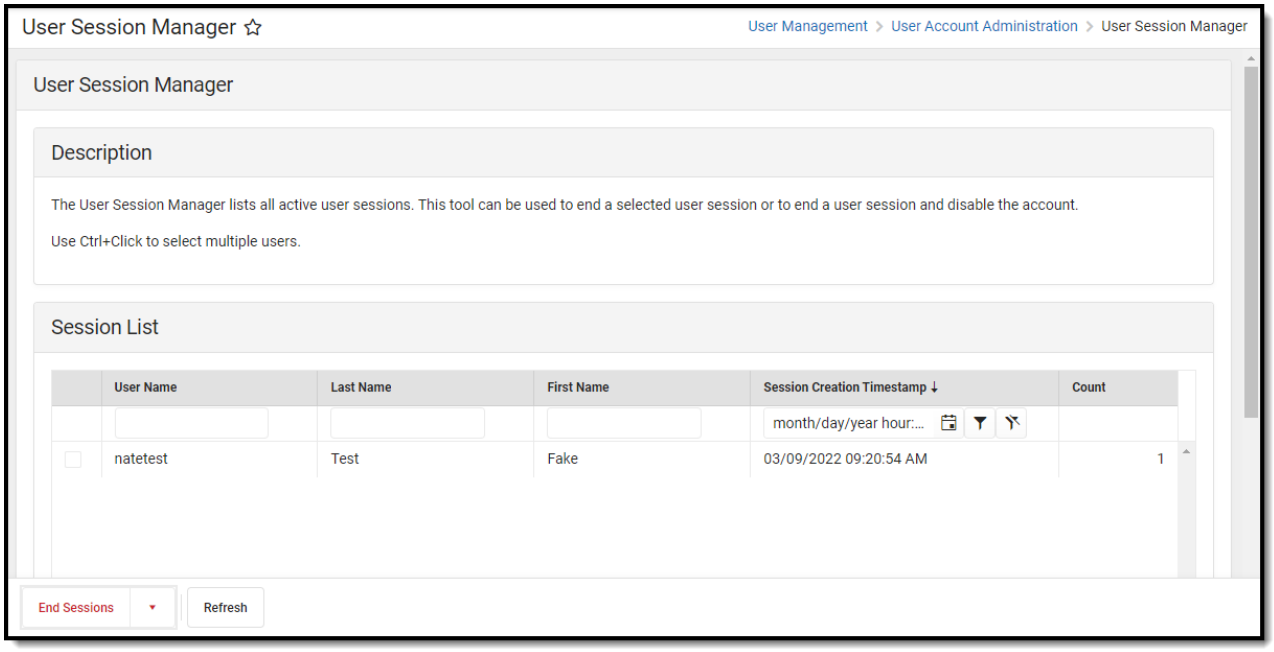
When set to 'Yes', a PIV Card Authentication field is made available on a person's User Account tab.

If enabled on the User Account, the Personal Identity Verification (PIV) button is made available on the Infinite Campus login screen, allowing users to register their PIV card and once approved, have the ability to insert their PIV card into a card reader and select this button to instantly log into Infinite Campus.



View All Active Sessions and Log Out/Disable User Accounts

Administrators can view a list of all active sessions within their instance of Infinite Campus and instantly log out or even disable specific user accounts via the User Session Manager. See the User Session Manager article for more information.



FAQ

Below is a list of answers to questions that may arise when enabling account notifications and verification codes.

How Does Campus Remember a Device?

Once you login to Campus, a unique ID is generated and stored as a cookie within your browser.

If you clear your browser cookies or do not mark the **Have Infinite Campus remember this device/browser in the future** checkbox, you will have to go through the Notification process each time you log into Campus.

What if I Clear My Cookies Each Time I Close My Browser?

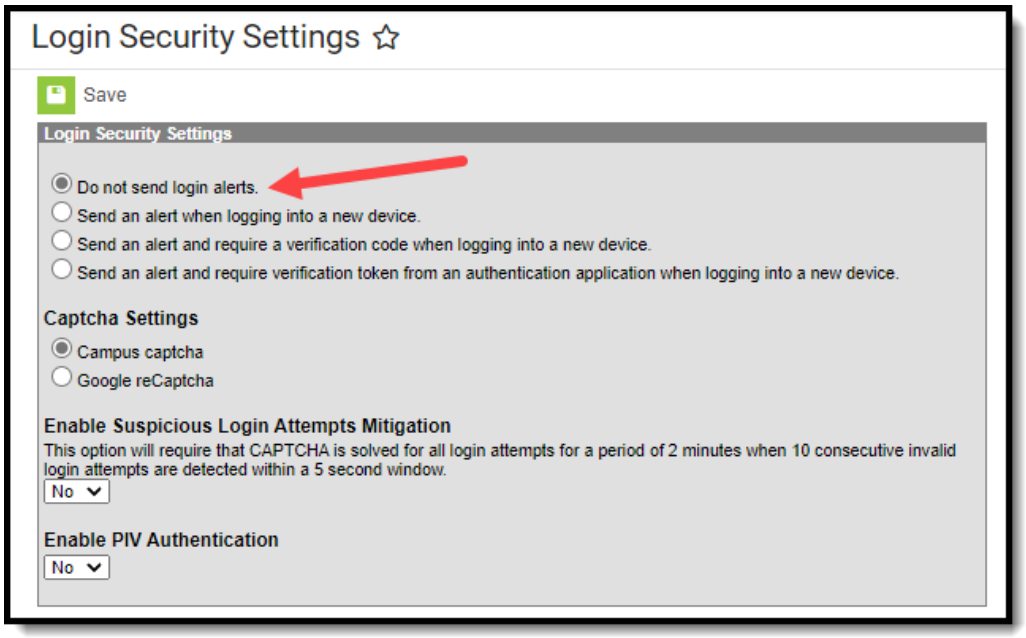
Clearing your browser cookies will remove the device from being remembered by the Campus notification process and will require you to go through the entering an email and setting up the device as a remembered device each and every time you log into Campus.

To prevent having to repeat the notification process each time you log into Campus, it is highly recommended you do not set your browser to automatically delete cookies.

How Do I Minimize the Amount of Notification Emails?

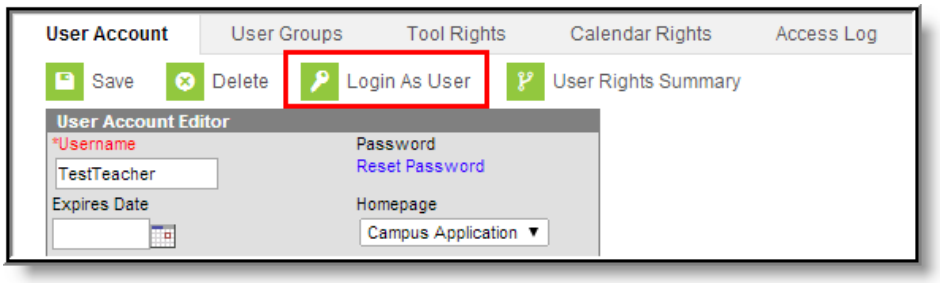
You can minimize the amount of notification emails you receive by:

- Marking the **Have Infinite Campus remember this device/browser in the future** checkbox when logging in with a device.
- Ensuring your browser does not automatically delete cookies.
- Reducing the amount of times you log into Campus using a public computer (since you would NOT want to mark the device as a remembered device).
- Turning off all Campus account login notifications by selecting the **Do not send login alerts** radio button.



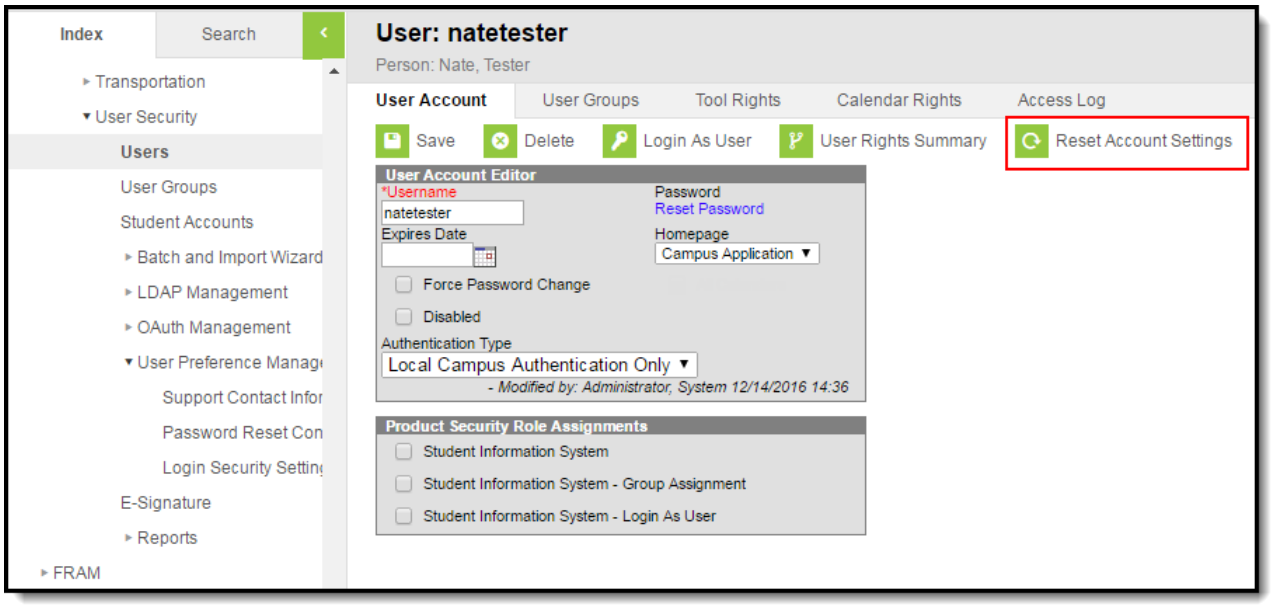
Will the Login as User Feature Result in a Notification Email?

Using the Login as User feature on the User Account tab will not send notification to the person you are logging in as. Login notifications only occur upon login via the Campus login screen.



How Do I Reset a User's Account Security Email Address?

If a user has accidentally entered an incorrect Account Security Email and thus cannot access the verification code email, you can reset the user's email address by going to System Administration > User Security > Users > User Account and clicking the **Reset Account Settings** button (see image below). Once selected. the user will be forced to go through the initial Account Security Email login process again.



Why Can't I Get reCaptcha to Work?

If you experience any issues after connecting Campus to reCaptcha, ensure the IP addresses that Google requires for reCAPTCHA functionality have been AllowListed. Google maintains their list of IP addresses that must be AllowListed in order for reCAPTCHA functionality to work here:

- https://code.google.com/archive/p/recaptcha/wikis/FirewallsAndRecaptcha.wiki

Do Login Security Settings Apply to Both Staff and Student/Parent Accounts?

The following Login Security Settings *only apply to Staff user accounts:*

> These settings apply to LDAP and SSO-authenticated user accounts.

- Do not send login alerts
- Send an alert when logging into a new device
- Send an alert and require a Two Factor Authentication (Email-Based)
- Send an alert and require a Time-Based Two Factor Authentication w/ enhanced security (Third party authentication application required)

The following settings apply to Staff, Student, and Parent accounts:

> These settings do NOT apply to LDAP and SSO-authenticated user accounts.

- Campus captcha
- Google reCaptcha
- Enable Suspicious Login Attempts Mitigation

Previous Versions

- Login Security Setting [.2207 - .2215]
- Login Security Setting [.2116 - .2203]