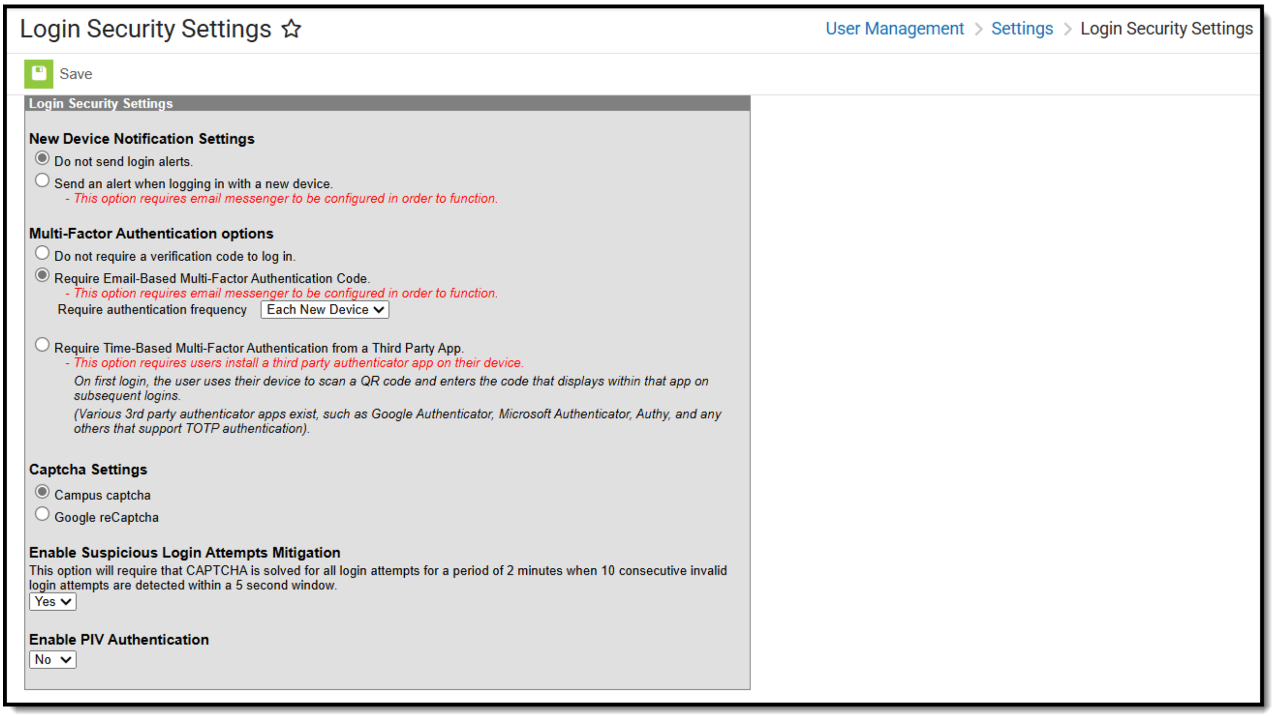
Login Security Settings

Last Modified on 02/13/2026 12:17 pm CST

Tool Search: Login Security Settings

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

For more information about tracking login notifications, see the Enabling Login Alert Notifications Emails of the Managing User Account Passwords article.



Login Security Settings ☆

Login Security Settings

New Device Notification Settings

● Do not send login alerts.
○ Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.
● Require Email-Based Multi-Factor Authentication Code.
- This option requires email messenger to be configured in order to function.
Require authentication frequency: Each New Device

○ Require Time-Based Multi-Factor Authentication from a Third Party App.
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exist, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

● Campus captcha
○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.
Yes

Enable PIV Authentication

No

Image 1: Login Security Settings

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

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

New Device Notification Settings

These settings determine whether or not users will receive an alert when logging into Infinite Campus using a new device (a device that has not been previously used to log into Infinite Campus using their credentials).

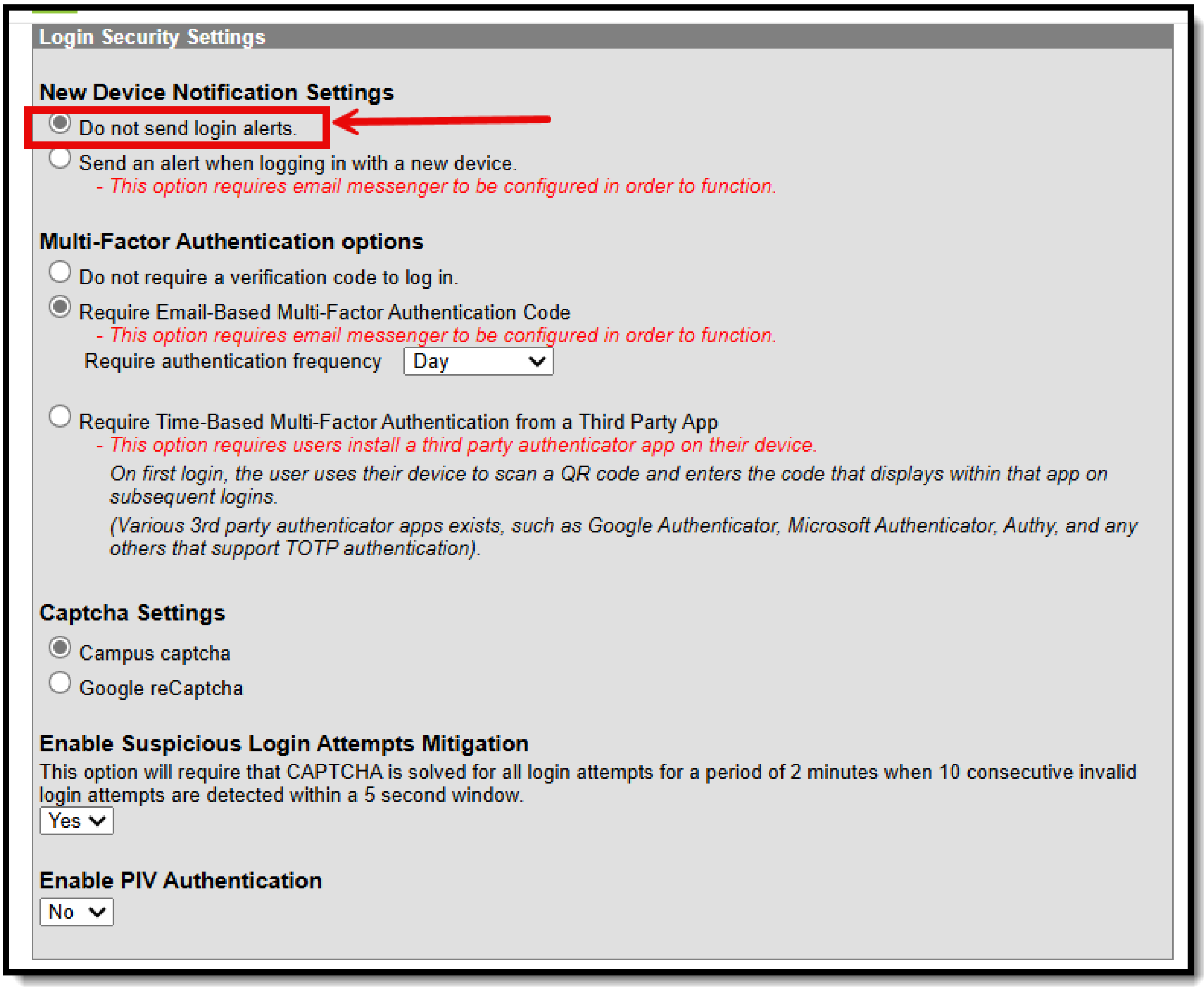
- Do Not Send Login Alerts
- Send an Alert When Logging in with a New Device

Do Not Send Login Alerts

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 in with a new device' setting.

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



Login Security Settings

New Device Notification Settings

● Do not send login alerts.

○ Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.
Require authentication frequency Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.
Yes

Enable PIV Authentication

No

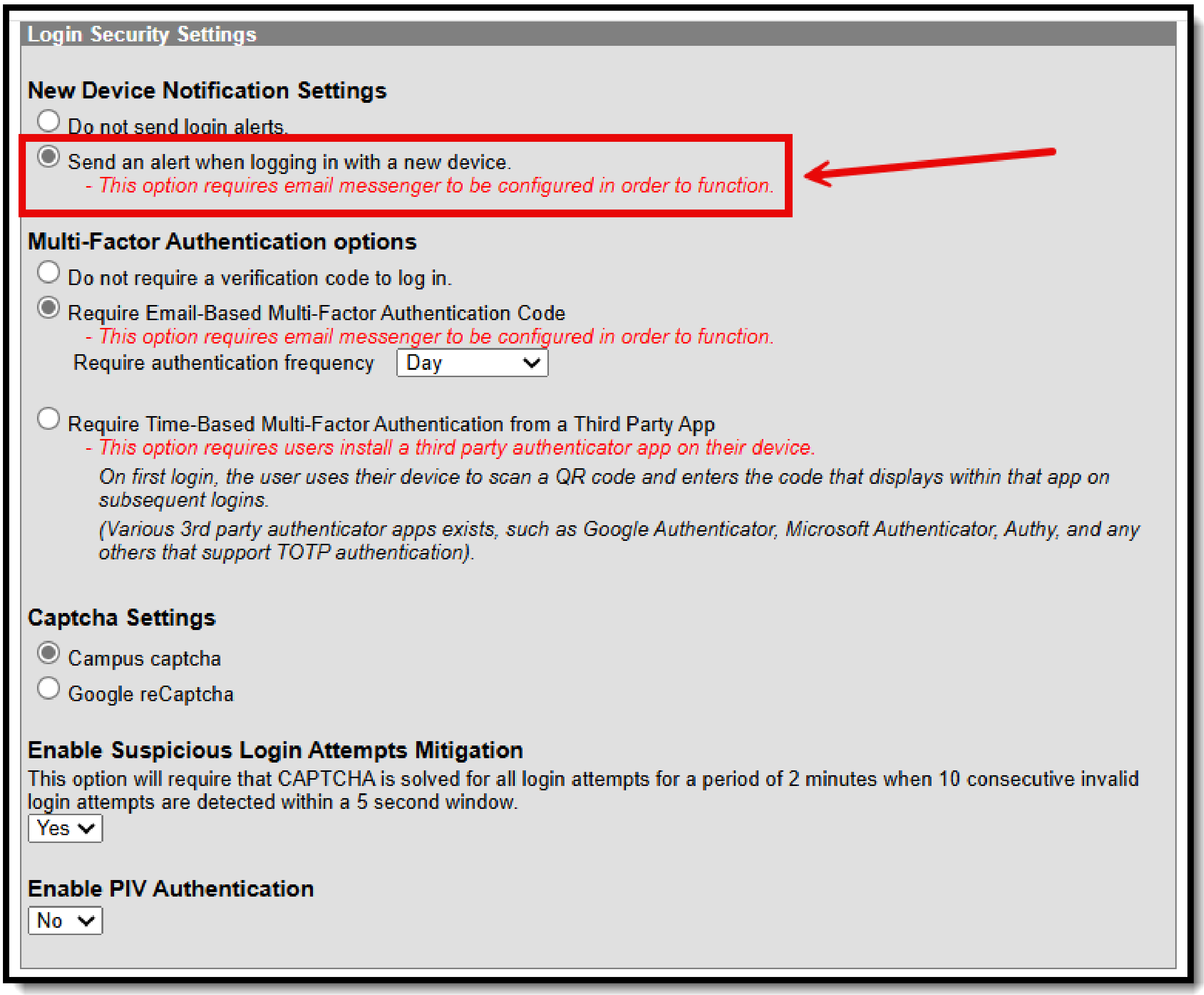
Image 2: Turning Off Login Alert Notification Emails

Send an Alert When Logging in with a New Device

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

Login notifications will increase email traffic. Therefore, it is important to have adequate email capacity when enabling and using login alert functionality.

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



Login Security Settings

New Device Notification Settings

○ Do not send login alerts.

● Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.

Require authentication frequency: Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.

On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.

(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.

Yes

Enable PIV Authentication

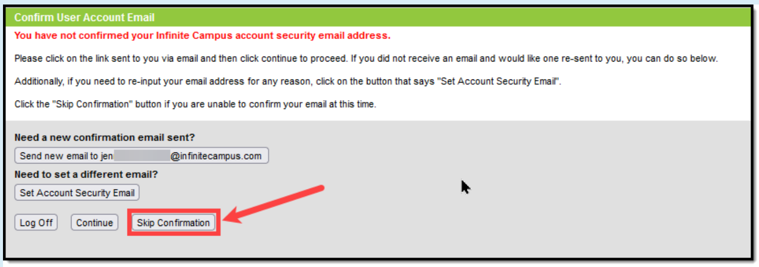
No

Image 3: Turning On Login Alert Notification Emails

Once the **Send an alert when logging into a new device** radio button is enabled, 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).

If email is not properly configured for your district, users may skip the Account Security Email verification process to avoid being locked out of Infinite Campus.

In order to properly receive security validation emails, your district needs to have a functional email relay configured within [Email Settings](#).



Confirm User Account Email

You have not confirmed your Infinite Campus account security email address.

Please click on the link sent to you via email and then click continue to proceed. If you did not receive an email and would like one re-sent to you, you can do so below.

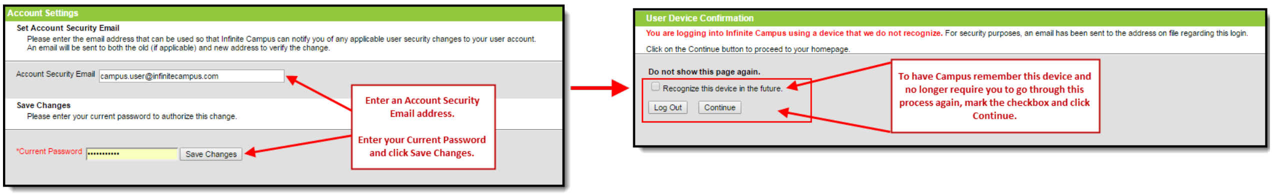
Additionally, if you need to re-input your email address for any reason, click on the button that says "Set Account Security Email".

Click the "Skip Confirmation" button if you are unable to confirm your email at this time.

Need a new confirmation email sent?

Send new email to jen[redacted]@infinitecampus.com

Need to set a different email?



Account Settings

Set Account Security Email

Please enter the email address that can be used so that Infinite Campus can notify you of any applicable user security changes to your user account. An email will be sent to both the old (if applicable) and new address to verify the change.

Account Security Email: campus.user@infinitecampus.com

Save Changes

Please enter your current password to authorize this change.

*Current Password: ••••••••••••

Enter an Account Security Email address.

Enter your Current Password and click Save Changes.

User Device Confirmation

You are logging into Infinite Campus using a device that we do not recognize. For security purposes, an email has been sent to the address on file regarding this login.

Click on the Continue button to proceed to your homepage.

Do not show this page again.

☐ Recognize this device in the future.

To have Campus remember this device and no longer require you to go through this process again, mark the checkbox and click Continue.

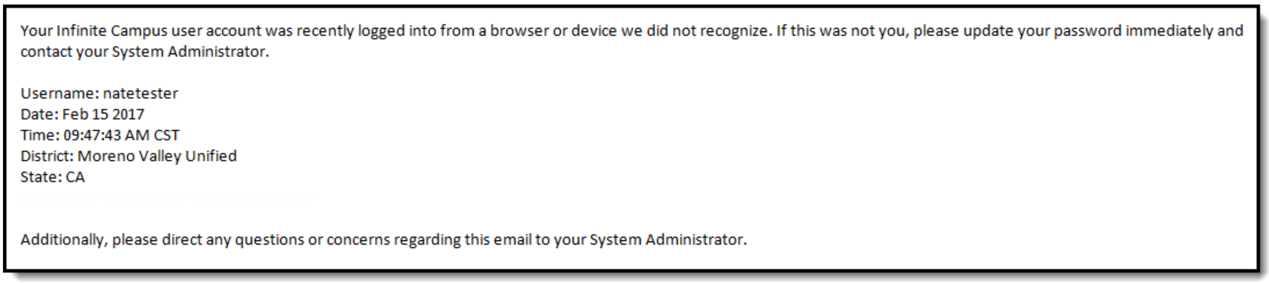
Image 4: Entering an Account Security Email and Remembering the Device

Once an email address is established, any time you log into Infinite Campus using a device that has not been used to log 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 delete cookies automatically will cause the device to be unrecognized, forcing 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.



Your Infinite Campus user account was recently logged into from a browser or device we did not recognize. If this was not you, please update your password immediately and contact your System Administrator.

Username: natetester
Date: Feb 15 2017
Time: 09:47:43 AM CST
District: Moreno Valley Unified
State: CA

Additionally, please direct any questions or concerns regarding this email to your System Administrator.

Image 5: Unknown Device Login Email Notification

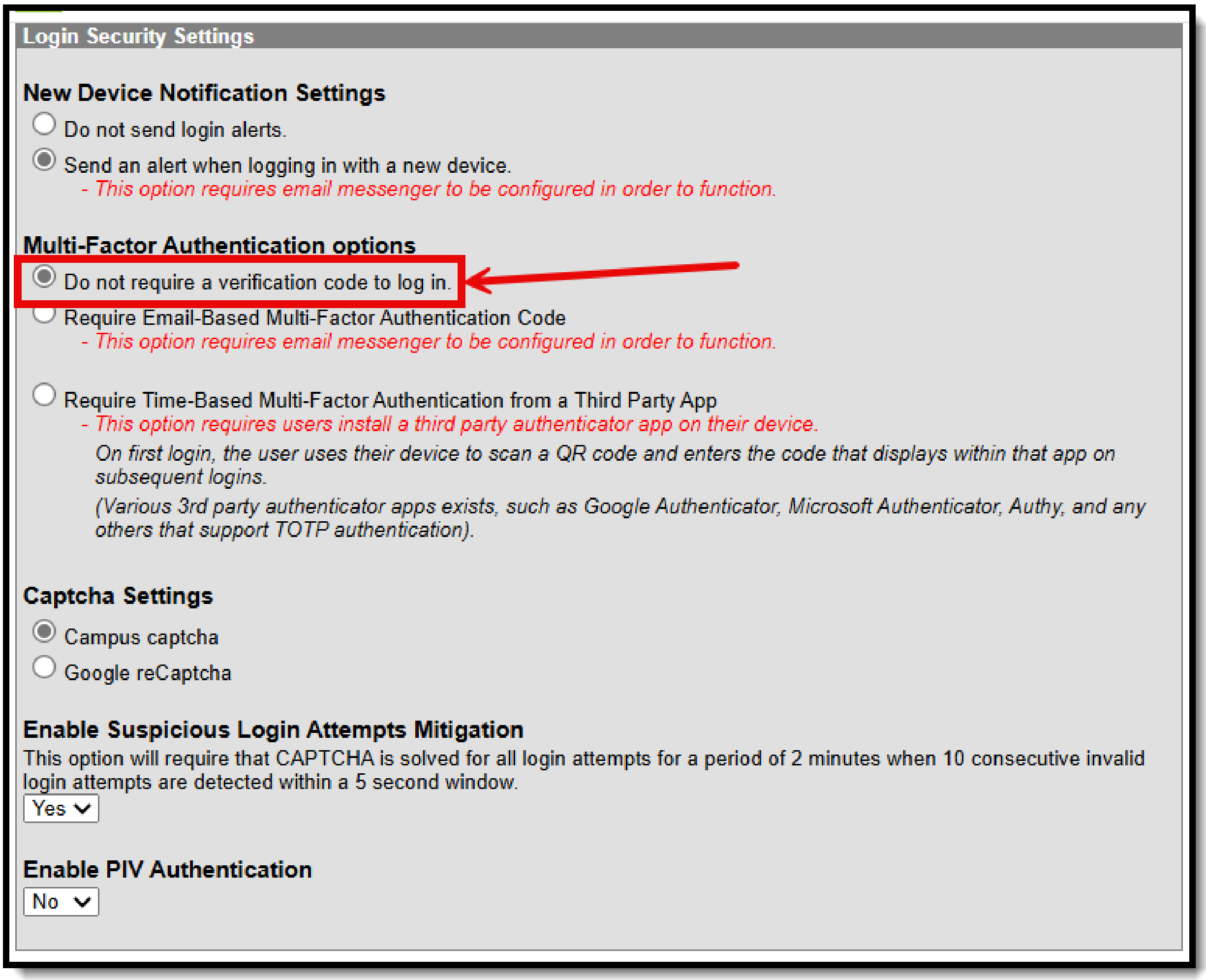
Multi-Factor Authentication Options

These settings are used to enable or disable multi-factor authentication and, if enabled, whether users are authenticated via an email-based code or a third-party authentication app.

- Do Not Require a Verification Code to Log In
- Require Email-Based Multi-Factor Authentication Code
- Require Time-Based Multi-Factor Authentication from a Third Party App

Do Not Require a Verification Code to Log In

Select **Do not require a verification code to log in** to disable and do not require users to use multi-factor authentication when logging into Infinite Campus.



Login Security Settings

New Device Notification Settings

○ Do not send login alerts.

● Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

● Do not require a verification code to log in.

○ Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.

Yes

Enable PIV Authentication

No

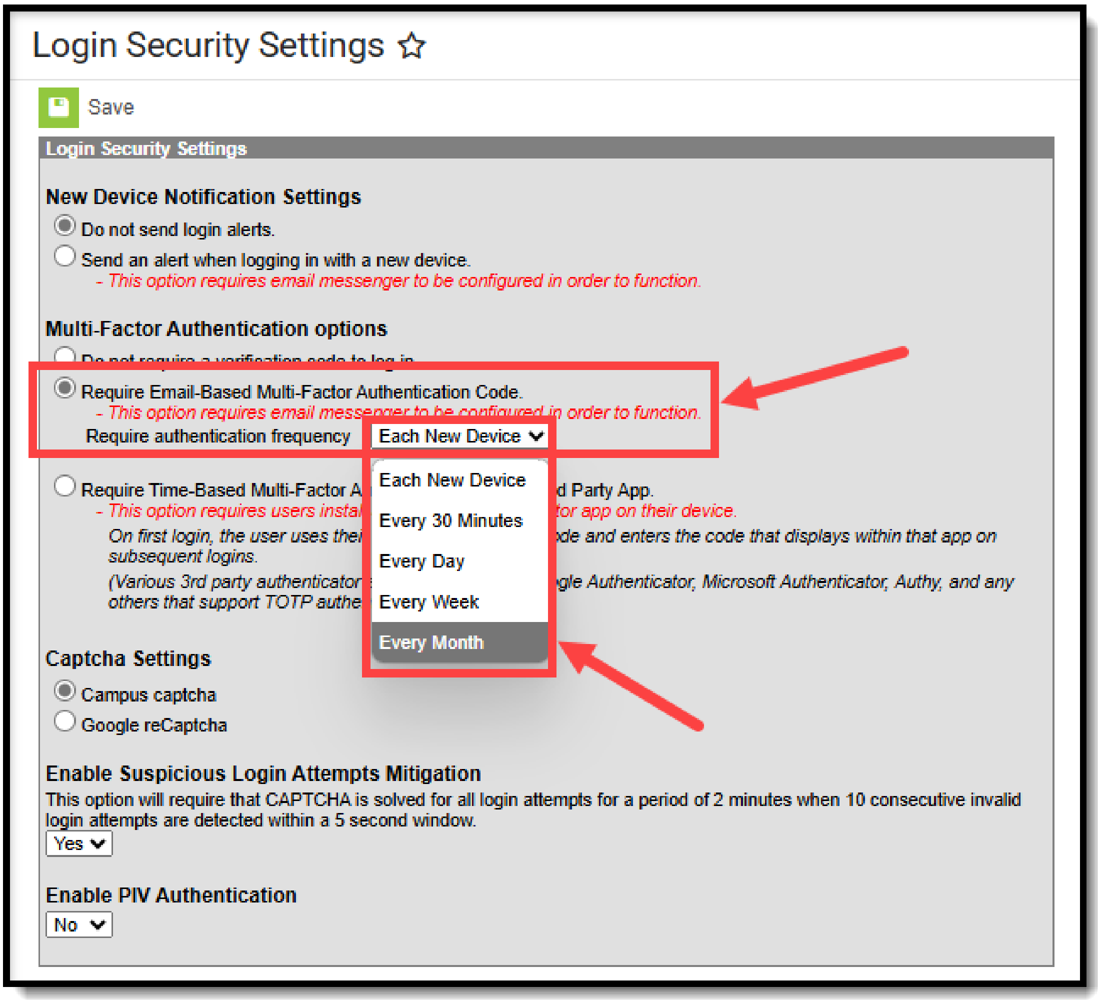
Require Email-Based Multi-Factor Authentication Code

To require users to enter a code emailed to them when logging into Infinite Campus:

1. Click the **Require Email-Based Multi-Factor Authentication Code** radio button
2. Set the frequency at which users must reauthenticate their credentials via email when logging into Infinite Campus.
   - **Each New Device** - Users must reauthenticate each time they log into Infinite Campus using a new, unrecognized device.
   - **Every 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 re-authenticate.
   - **Every 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 re-authenticate.
   - **Every 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 re-authenticate.
   - **Every 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 re-authenticate.
3. Select **Save**.

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.



Login Security Settings ☆

Save

Login Security Settings

New Device Notification Settings

● Do not send login alerts.

○ Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code.
- This option requires email messenger to be configured in order to function.
Require authentication frequency [Each New Device ▾]

- Each New Device
- Every 30 Minutes
- Every Day
- Every Week
- Every Month

○ Require Time-Based Multi-Factor A d Party App.
- This option requires users instal tor app on their device.
On first login, the user uses thei de and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator gle Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authe

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.

Yes ▾

Enable PIV Authentication

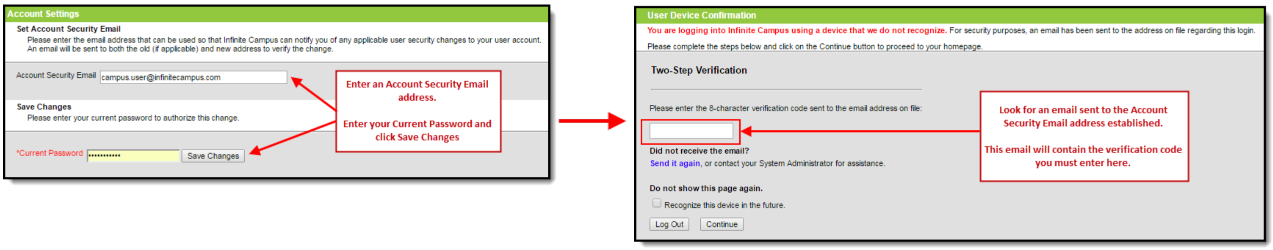
No ▾

Image 7: 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 must enter an **Account Security Email** address (if one is not already present within Infinite Campus). Once saved, they will be directed to a new screen where they must 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 8).

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

Having your browser set to delete cookies automatically will cause the device to be unrecognized and force you to go through this process each time you log into Infinite Campus.



Account Settings

Set Account Security Email

Please enter the email address that can be used so that Infinite Campus can notify you of any applicable user security changes to your user account. An email will be sent to both the old (if applicable) and new address to verify the change.

Account Security Email campus.user@infinitecampus.com

Save Changes

Please enter your current password to authorize this change.

*Current Password ••••••••••• Save Changes

Enter an Account Security Email address.

Enter your Current Password and click Save Changes

User Device Confirmation

You are logging into Infinite Campus using a device that we do not recognize. For security purposes, an email has been sent to the address on file regarding this login.

Please complete the steps below and click on the Continue button to proceed to your homepage.

Two-Step Verification

Please enter the 8-character verification code sent to the email address on file:

Did not receive the email?

Send it again, or contact your System Administrator for assistance.

Do not show this page again.

□ Recognize this device in the future.

Log Out Continue

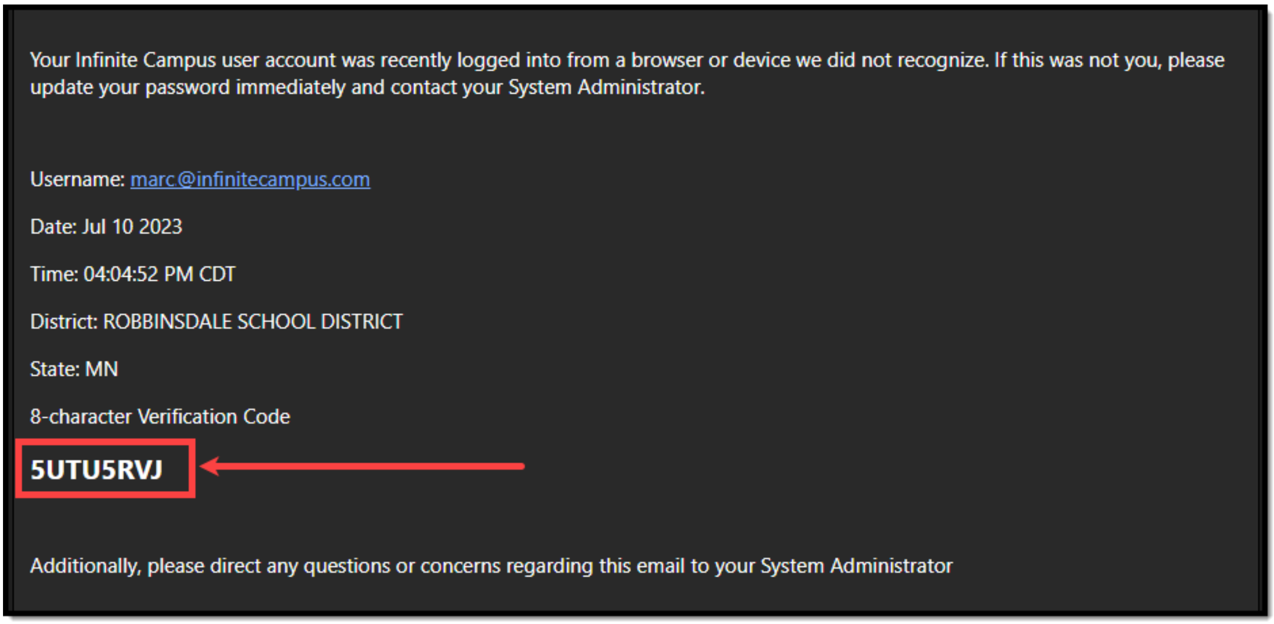
Look for an email sent to the Account Security Email address established.

This email will contain the verification code you must enter here.

Image 8: 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 shown above (Image 8).

This code expires after 20 minutes.



Your Infinite Campus user account was recently logged into from a browser or device we did not recognize. If this was not you, please update your password immediately and contact your System Administrator.

Username: marc@infinitecampus.com

Date: Jul 10 2023

Time: 04:04:52 PM CDT

District: ROBBINSDALE SCHOOL DISTRICT

State: MN

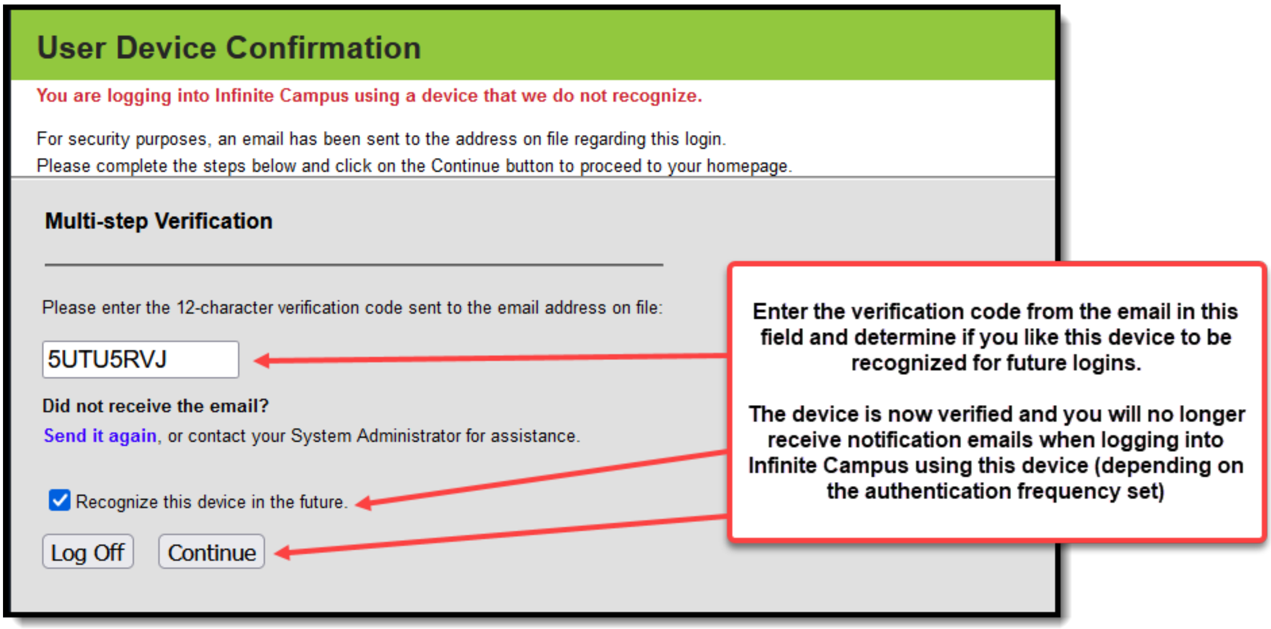
8-character Verification Code

5UTU5RVJ

Additionally, please direct any questions or concerns regarding this email to your System Administrator

Image 9: 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 10). The device is now verified; however, you may be required to reauthenticate depending on the reauthentication frequency set.



User Device Confirmation

You are logging into Infinite Campus using a device that we do not recognize.

For security purposes, an email has been sent to the address on file regarding this login.
Please complete the steps below and click on the Continue button to proceed to your homepage.

Multi-step Verification

Please enter the 12-character verification code sent to the email address on file:

5UTU5RVJ

Did not receive the email?
Send it again, or contact your System Administrator for assistance.

☑ Recognize this device in the future.

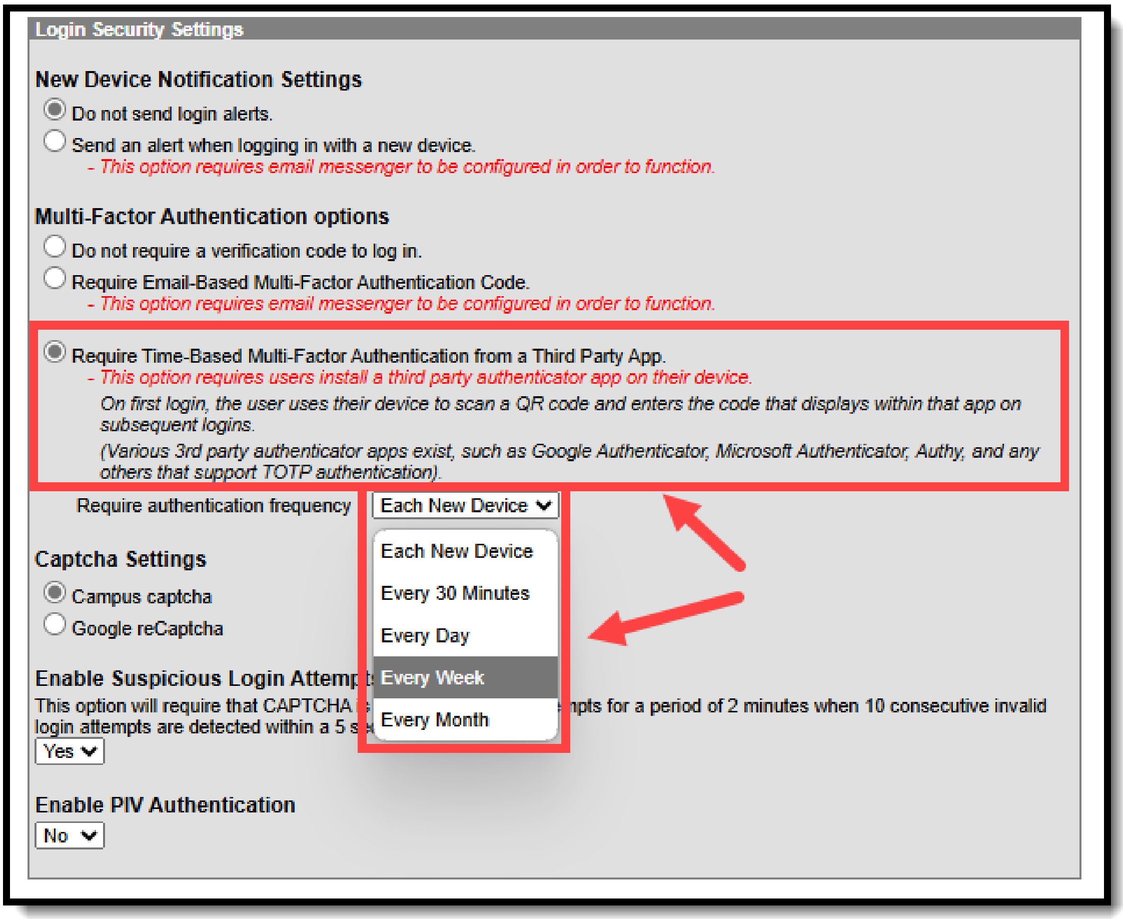
Enter the verification code from the email in this field and determine if you like this device to be recognized for future logins.

The device is now verified and you will no longer receive notification emails when logging into Infinite Campus using this device (depending on the authentication frequency set)

Image 10: Entering a Verification Code

Require Time-Based Multi-Factor Authentication from a Third Party App

User accounts can be enabled with time-based multi-factor authentication functionality as an increased layer of protection for Infinite Campus accounts. 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.).



Login Security Settings

New Device Notification Settings

● Do not send login alerts.

○ Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

○ Require Email-Based Multi-Factor Authentication Code.
- This option requires email messenger to be configured in order to function.

● Require Time-Based Multi-Factor Authentication from a Third Party App.
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exist, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Require authentication frequency: Each New Device

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attemp

This option will require that CAPTCHA i ... mpts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 s

Yes

Enable PIV Authentication

No

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

Time-based multi-factor authentication 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 the 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 sync the date and time automatically.

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 multi-factor authentication for all non-Campus Portal accounts:

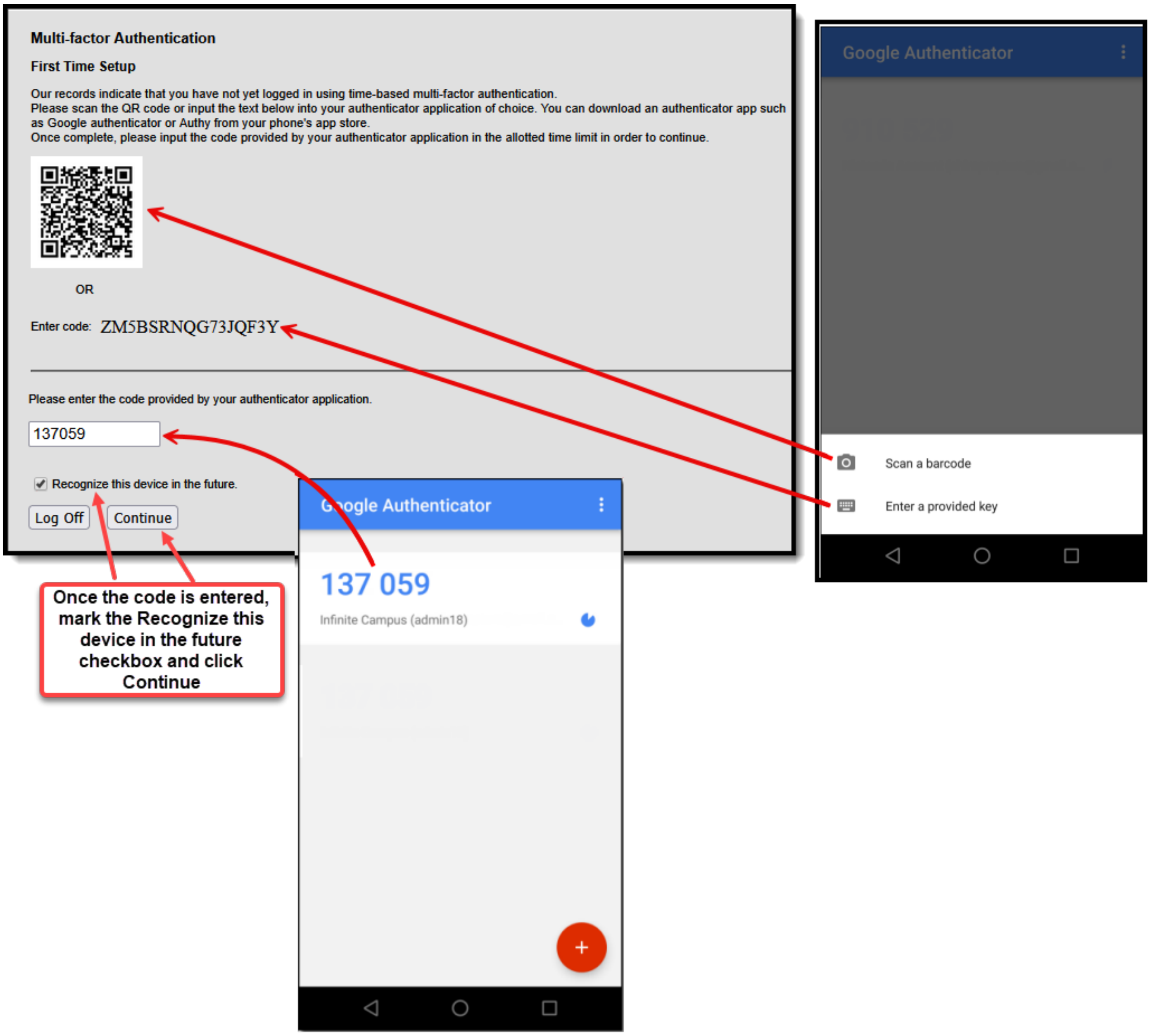
1. Click the **Require Time-Based Multi-Factor Authentication from a Third Party App** radio button

2. Set the frequency at which users must reauthenticate their credentials when logging into Infinite Campus.
   - **Every New Device** - Users must reauthenticate using an authentication application each time they log into Infinite Campus using a new, unrecognized device.
   - **Every 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.
   - **Every 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.
   - **Every 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.
   - **Every 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**.

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 a cell phone), users must download an authenticator app (such as Google Authenticator, Authy, LastPass, etc) and use the app to 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 future** checkbox, and click **Continue** (see image below). The user will be logged into Campus.



Multi-factor Authentication

First Time Setup

Our records indicate that you have not yet logged in using time-based multi-factor authentication.
Please scan the QR code or input the text below into your authentication application of choice. You can download an authenticator app such as Google authenticator or Authy from your phone's app store.
Once complete, please input the code provided by your authenticator application in the allotted time limit in order to continue.

OR

Enter code: ZM5BSRNQG73JQF3Y

Please enter the code provided by your authenticator application.

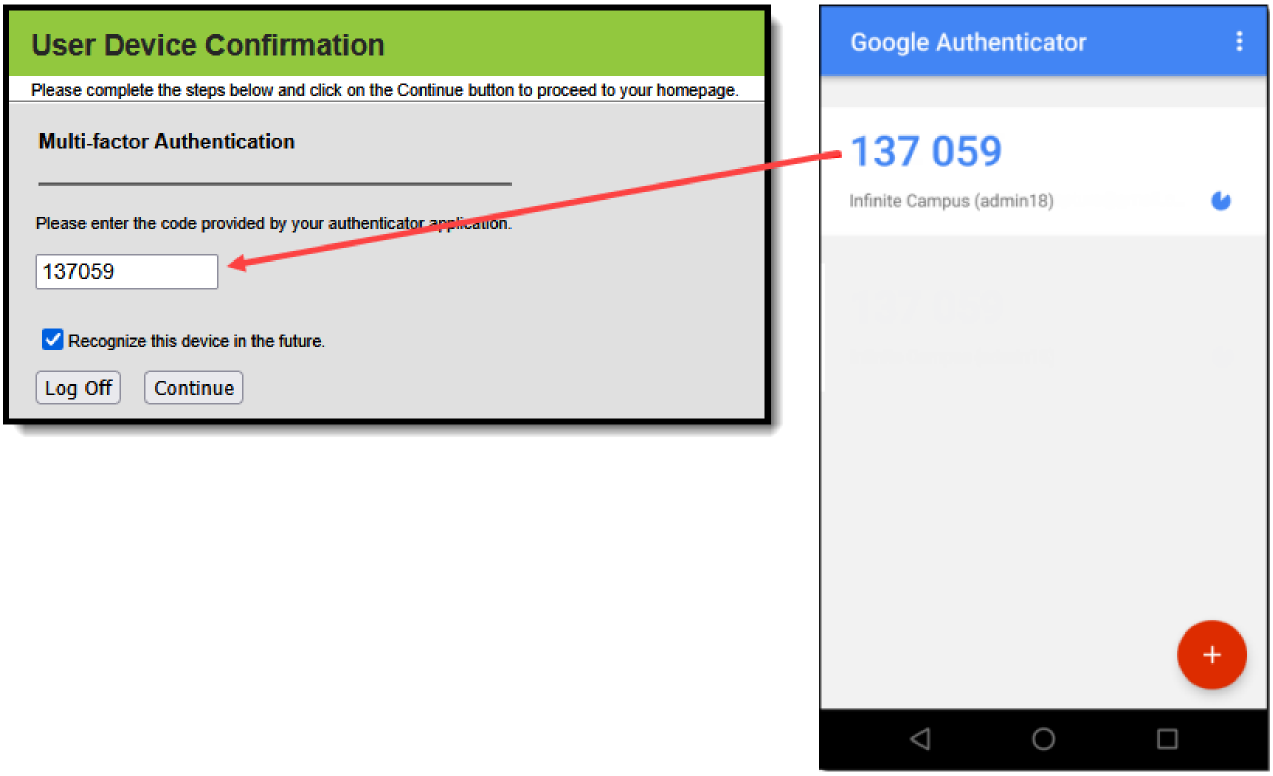
137059

☑ Recognize this device in the future.

Once the code is entered, mark the Recognize this device in the future checkbox and click Continue

Image 12: 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 the 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.



User Device Confirmation

Please complete the steps below and click on the Continue button to proceed to your homepage.

Multi-factor Authentication

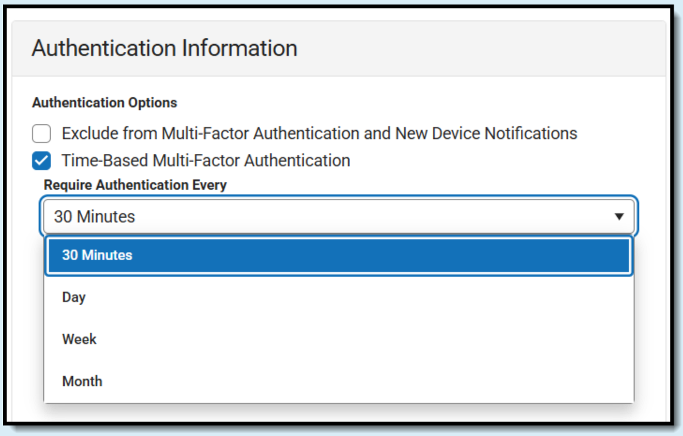
Please enter the code provided by your authenticator application.

137059

☑ Recognize this device in the future.

Image 13: 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.



Authentication Information

Authentication Options

□ Exclude from Multi-Factor Authentication and New Device Notifications

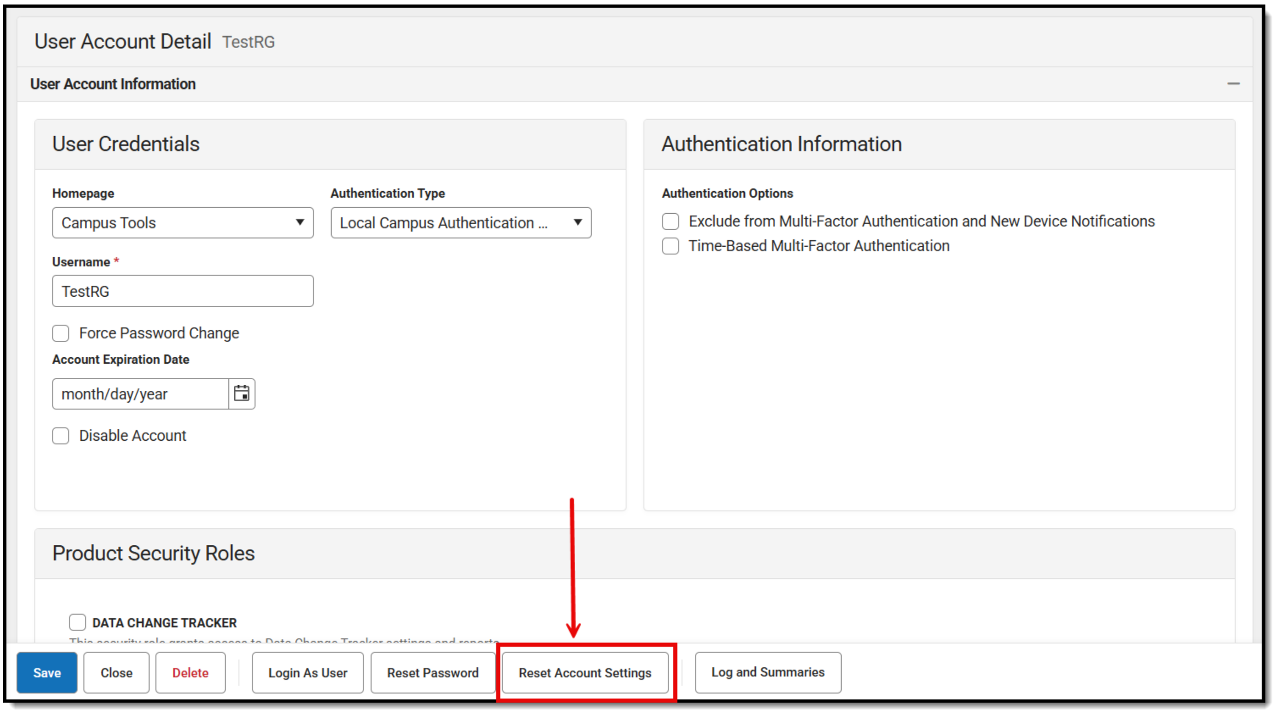
☑ Time-Based Multi-Factor Authentication

Require Authentication Every: 30 Minutes

Resetting a User's Multi-Factor Authentication Credentials

Tool Search: User Account Information

For districts using multi-factor authentication, selecting the **Reset Account Settings** button on their User Account will reset the user's multi-factor authentication configuration, requiring them to establish a new trusted device and log in using an Authentication app. See the Login Security Settings article for information about multi-factor authentication.



User Account Detail TestRG

User Account Information

User Credentials

Homepage: Campus Tools

Authentication Type: Local Campus Authentication ...

Username *: TestRG

□ Force Password Change

Account Expiration Date: month/day/year

□ Disable Account

Authentication Information

Authentication Options

□ Exclude from Multi-Factor Authentication and New Device Notifications

□ Time-Based Multi-Factor Authentication

Product Security Roles

□ DATA CHANGE TRACKER

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.

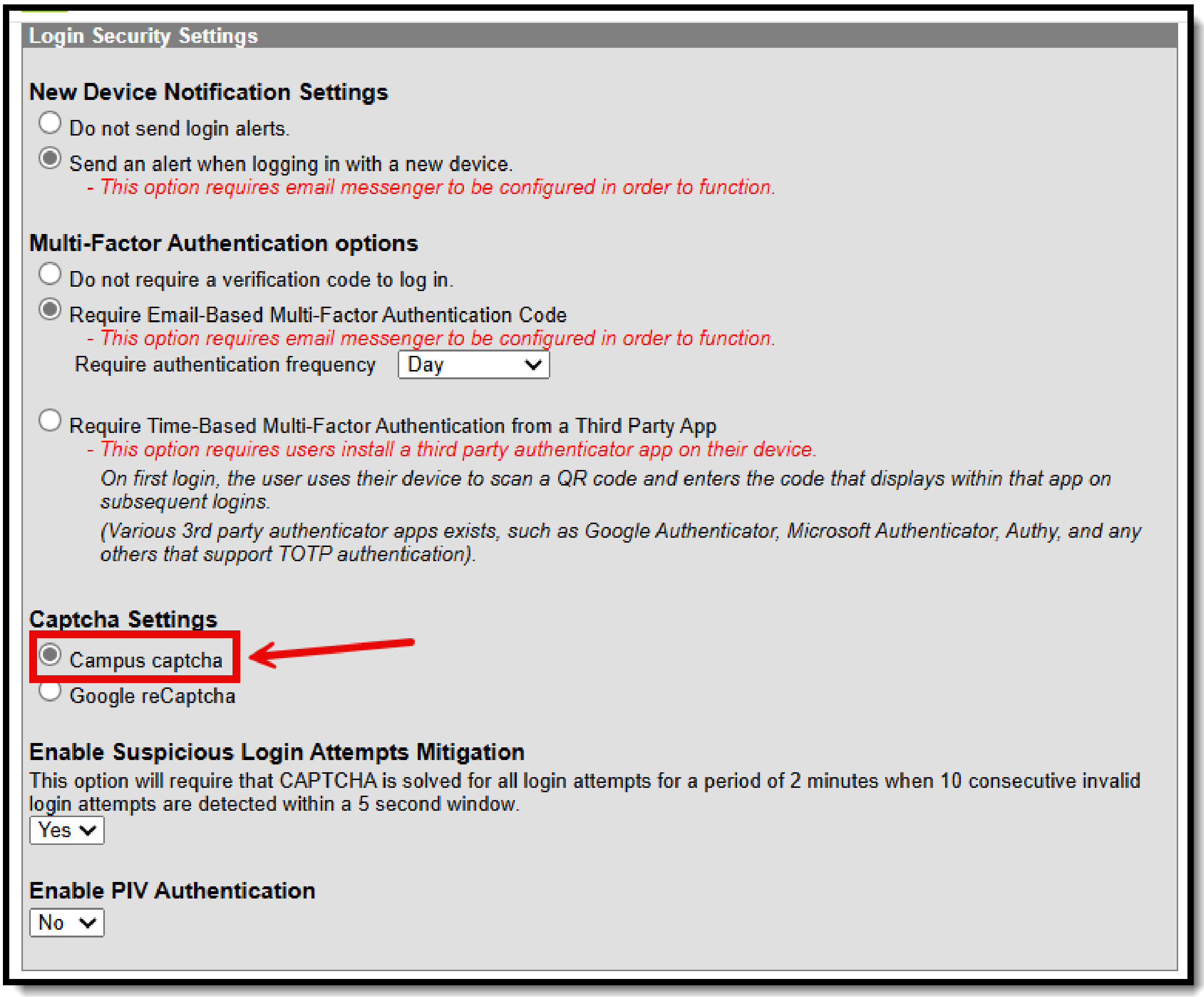
> These settings apply to Staff, Student, and Parent Portal accounts but do NOT apply to LDAP and SSO-authenticated user accounts.

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.



Login Security Settings

New Device Notification Settings

○ Do not send login alerts.

● Send an alert when logging in with a new device.

- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code

- This option requires email messenger to be configured in order to function.

Require authentication frequency: Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App

- This option requires users install a third party authenticator app on their device.

On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.

(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.

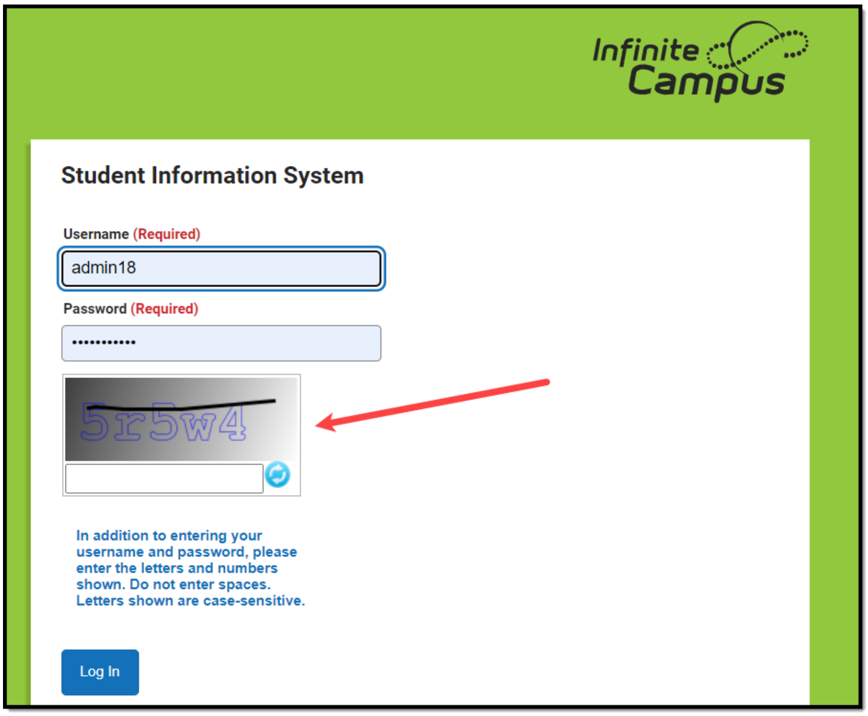
Yes

Enable PIV Authentication

No

Image 14: Enabling Campus Captcha

The image below is an example of the Campus captcha (Image 15).



Student Information System

Username (Required)

admin18

Password (Required)

•••••••••••

In addition to entering your username and password, please enter the letters and numbers shown. Do not enter spaces. Letters shown are case-sensitive.

Image 15: Example of the Campus Captcha

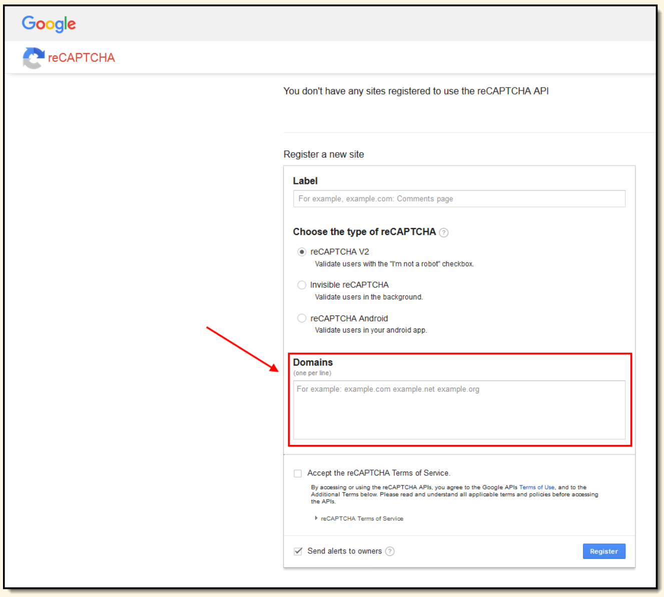
Google reCaptcha

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 enabling Google reCaptcha, you must register with Google to acquire the **Site Key** and **Secret Key** and enter this data within Campus (Image 16).

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.



Google

reCAPTCHA

You don't have any sites registered to use the reCAPTCHA API

Register a new site

Label

For example, example.com: Comments page

Choose the type of reCAPTCHA ?

● reCAPTCHA V2
Validate users with the "I'm not a robot" checkbox.

○ Invisible reCAPTCHA
Validate users in the background.

○ reCAPTCHA Android
Validate users in your android app.

Domains
(one per line)

For example: example.com example.net example.org

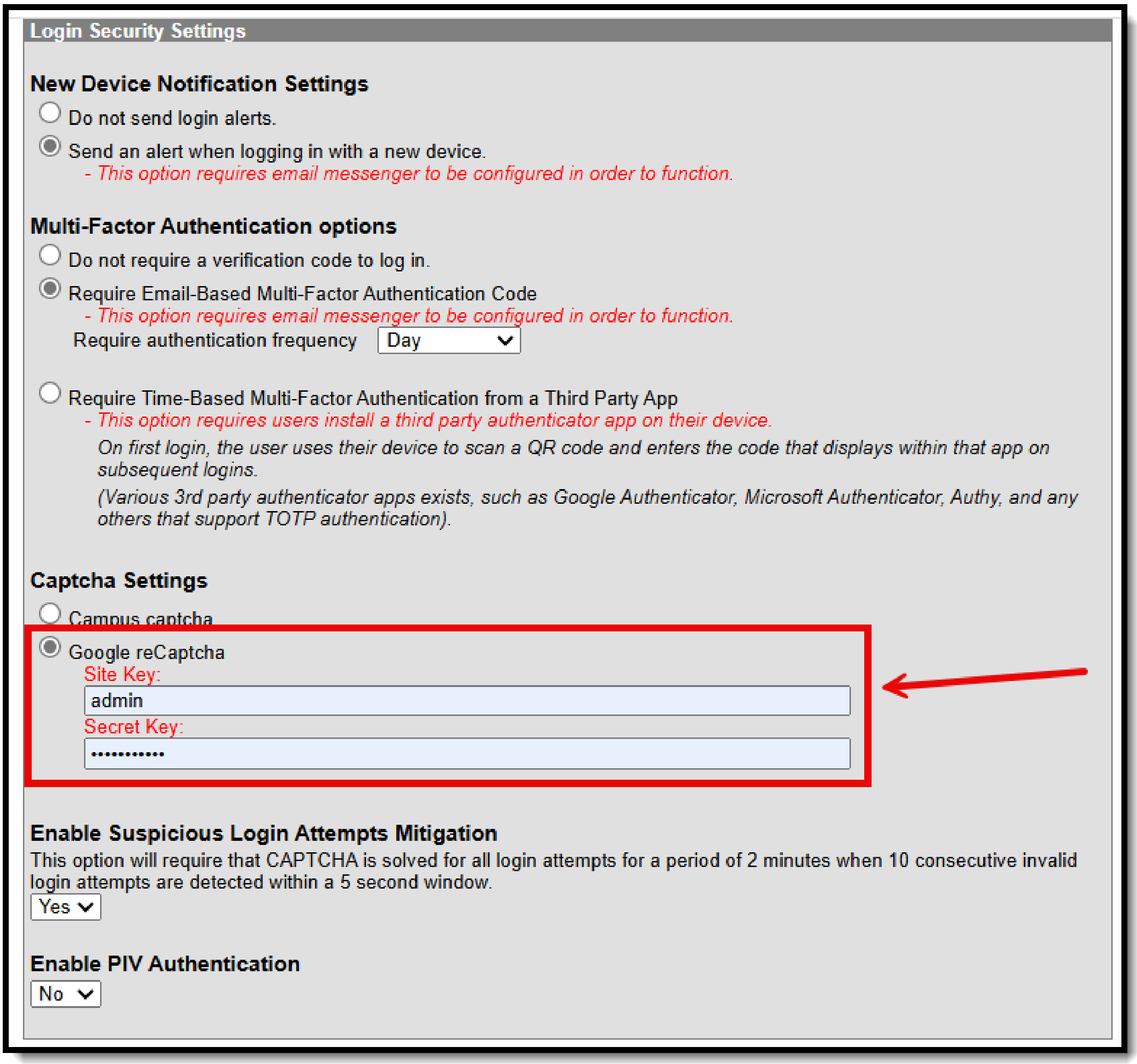
□ Accept the reCAPTCHA Terms of Service.

By accessing or using the reCAPTCHA APIs, you agree to the Google APIs Terms of Use, and to the Additional Terms below. Please read and understand all applicable terms and policies before accessing the APIs.

▸ reCAPTCHA Terms of Service

☑ Send alerts to owners ?

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.**



Login Security Settings

New Device Notification Settings

○ Do not send login alerts.

● Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.
Require authentication frequency: Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

○ Campus captcha

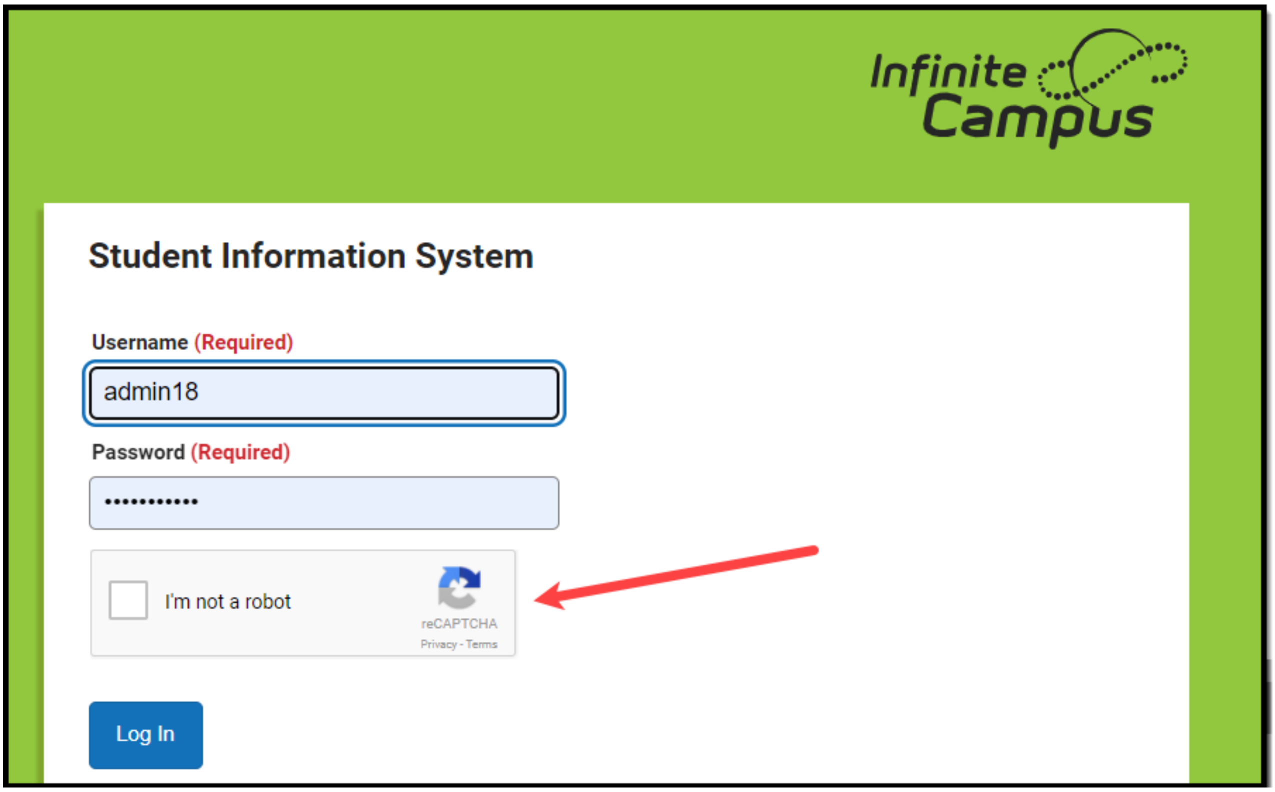
● Google reCaptcha
Site Key: admin
Secret Key: •••••••••••

Enable Suspicious Login Attempts Mitigation
This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.
Yes

Enable PIV Authentication
No

Image 16: 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 first to mark a checkbox (Image 17).



Student Information System

Username (Required)

admin18

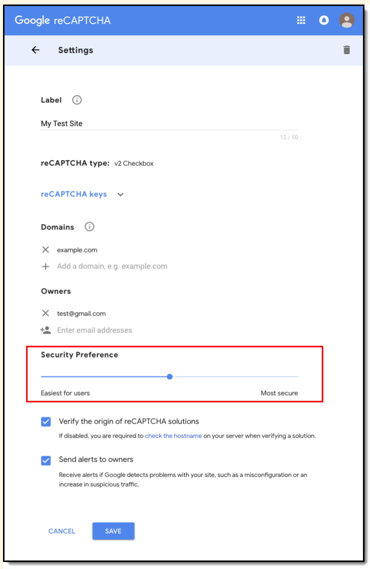
Password (Required)

•••••••••••

□ I'm not a robot

Image 17: 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 the user is not a robot.



Label

My Test Site

12 / 50

reCAPTCHA type: v2 Checkbox

Domains

example.com

Add a domain, e.g. example.com

Owners

test@gmail.com

Enter email addresses

Security Preference

Easiest for users — Most secure

☑ Verify the origin of reCAPTCHA solutions

If disabled, you are required to check the hostname on your server when verifying a solution.

☑ Send alerts to owners

Receive alerts if Google detects problems with your site, such as a misconfiguration or an increase in suspicious traffic.

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).

Depending on the reCaptcha security preference level, a popup may appear, asking the user to select a series of squares or pictures based on a specific question (Image 18) or listen to an audio challenge.

The audio challenge option for Google reCaptcha does NOT work properly within the Microsoft Edge web browser.

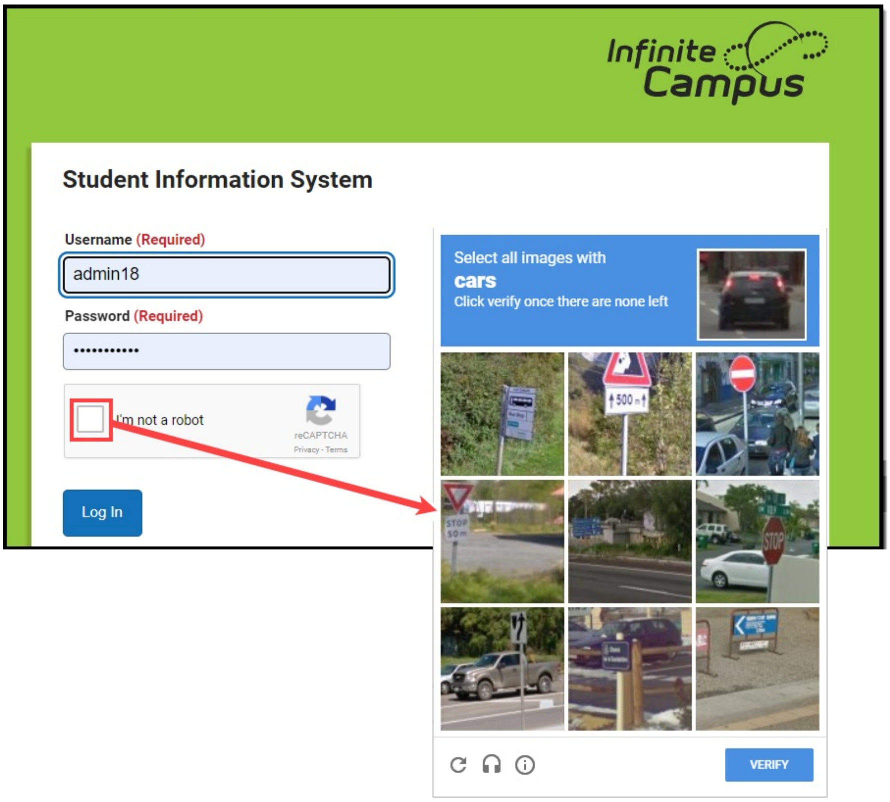


Image 18: Selecting Verification Images

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 its 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

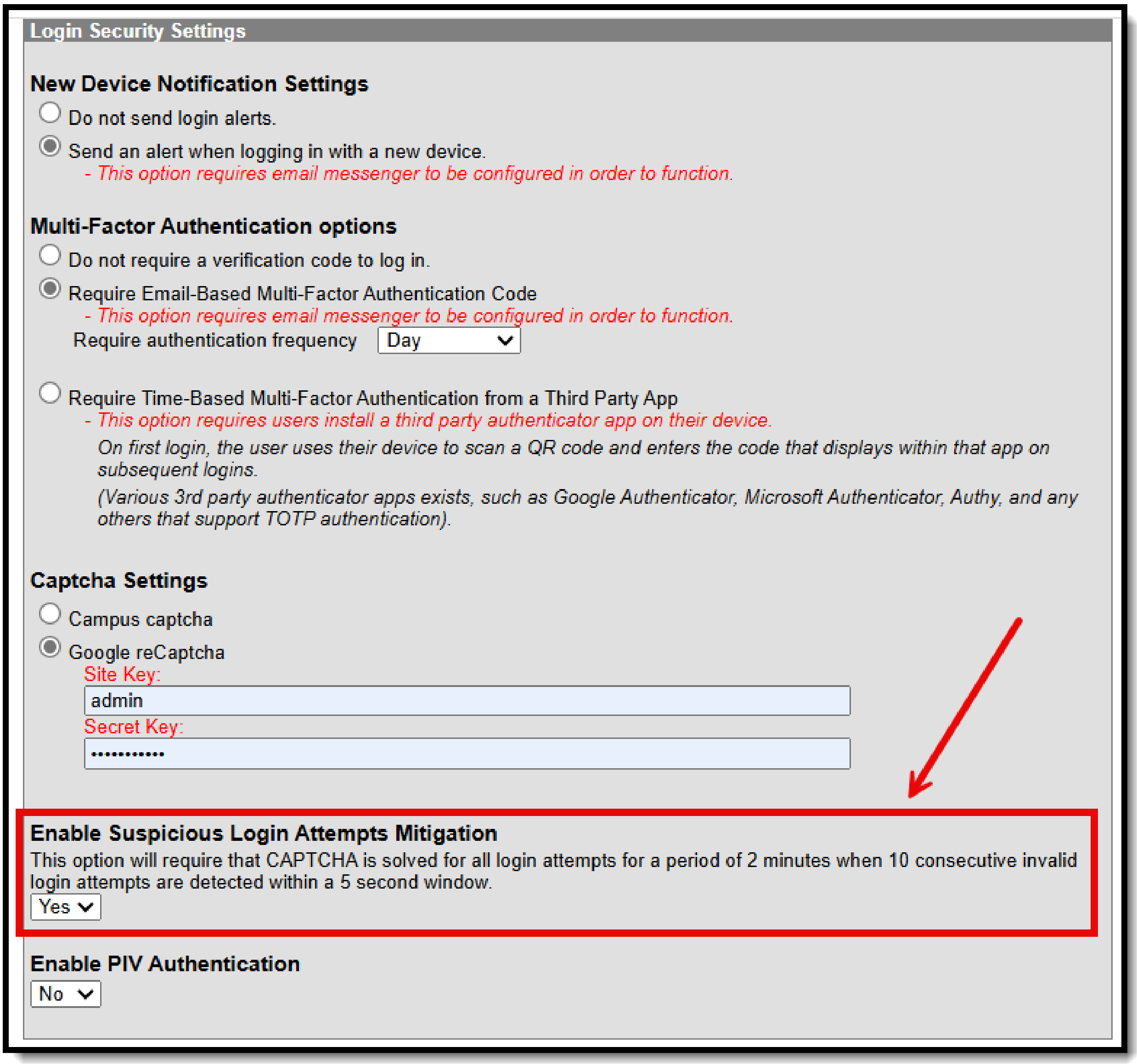
For more information on troubleshooting other reCaptcha-related issues, see the Troubleshooting Google ReCaptcha article.

Enable Suspicious Login Attempts Mitigation

When the **Enable Suspicious Login Attempts Mitigation** setting is set to 'Yes', anytime there are 10 consecutive failed logins 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.

Infinite Campus HIGHLY recommends leaving this setting set to Yes as it provides a line of defense against automated attacks on your system.



Login Security Settings

New Device Notification Settings

○ Do not send login alerts.

● Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.
Require authentication frequency: Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

○ Campus captcha

● Google reCaptcha
Site Key: admin
Secret Key: •••••••••••

Enable Suspicious Login Attempts Mitigation
This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.
Yes

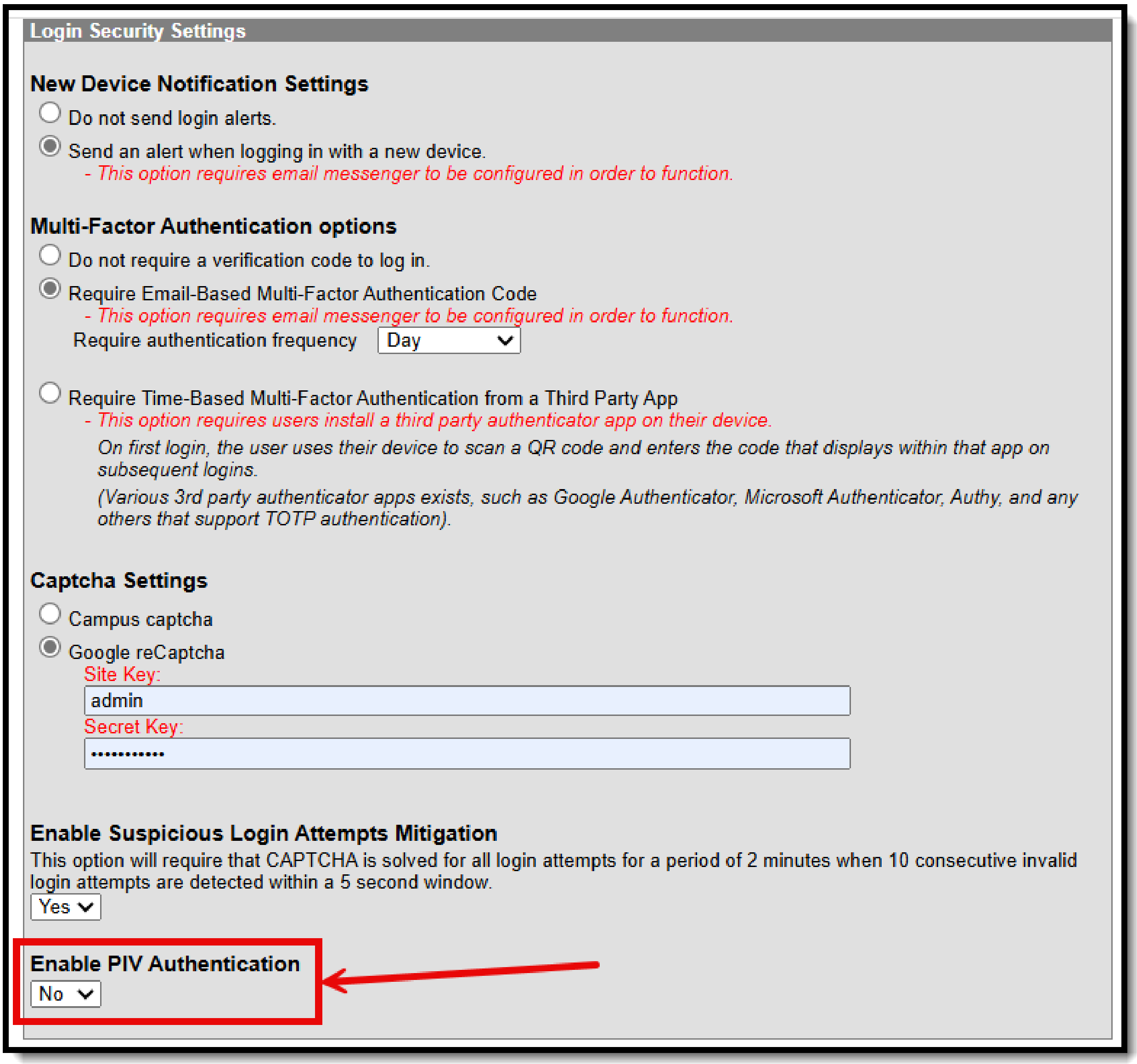
Enable PIV Authentication
No

Enable PIV Authentication

The **Enable PIV Authentication** setting enables 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



Login Security Settings

New Device Notification Settings

○ Do not send login alerts.

● Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.
Require authentication frequency: Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

○ Campus captcha

● Google reCaptcha
Site Key: admin
Secret Key: •••••••••••

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.

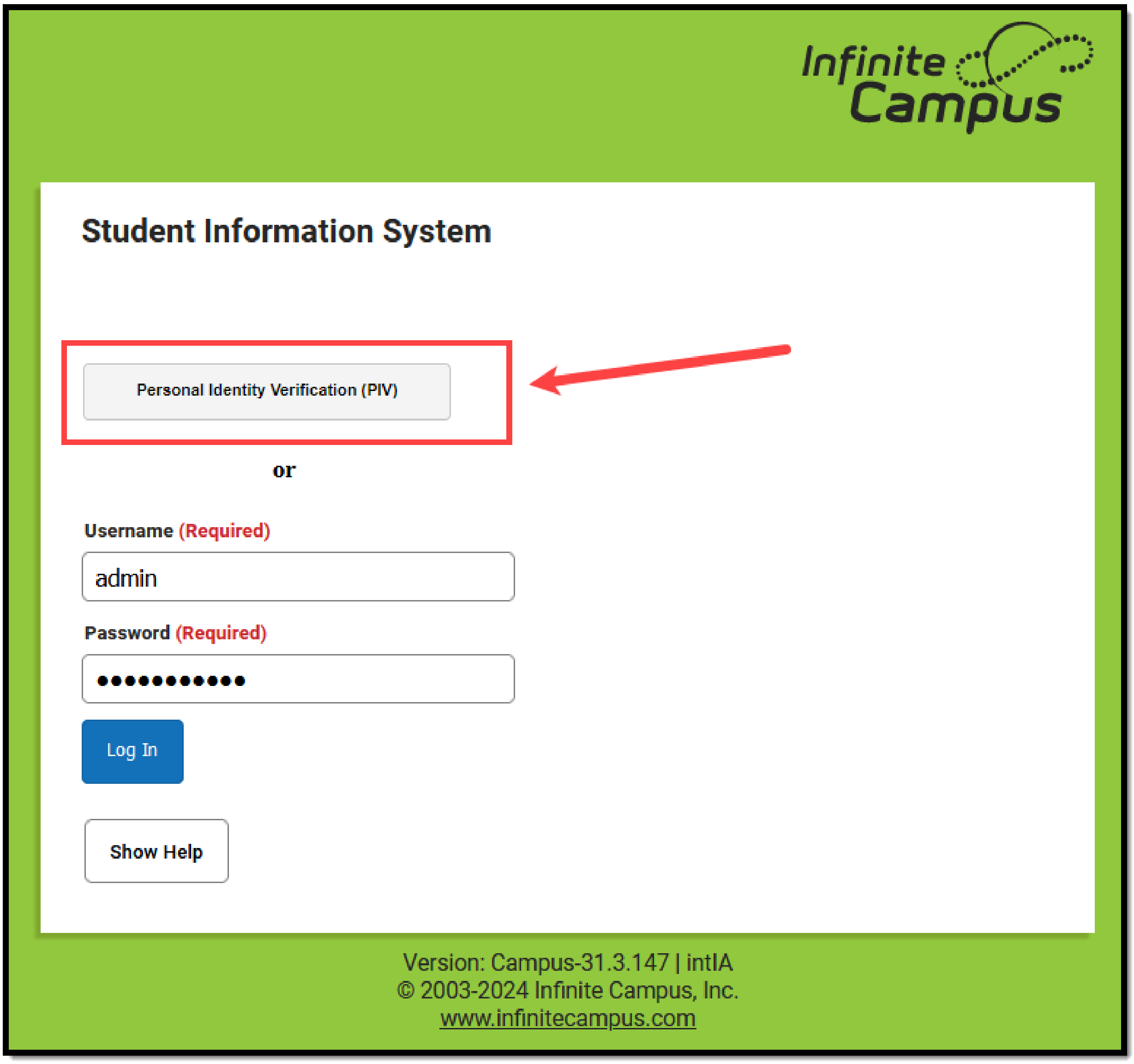
Yes

Enable PIV Authentication

No

When set to ‘Yes’, a PIV Card Authentication field is 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. This button allows users to register their PIV card, and once approved, they can insert their PIV card into a card reader and select this button to log into Infinite Campus instantly.



Student Information System

Personal Identity Verification (PIV)

or

Username (Required)

admin

Password (Required)

●●●●●●●●●●●

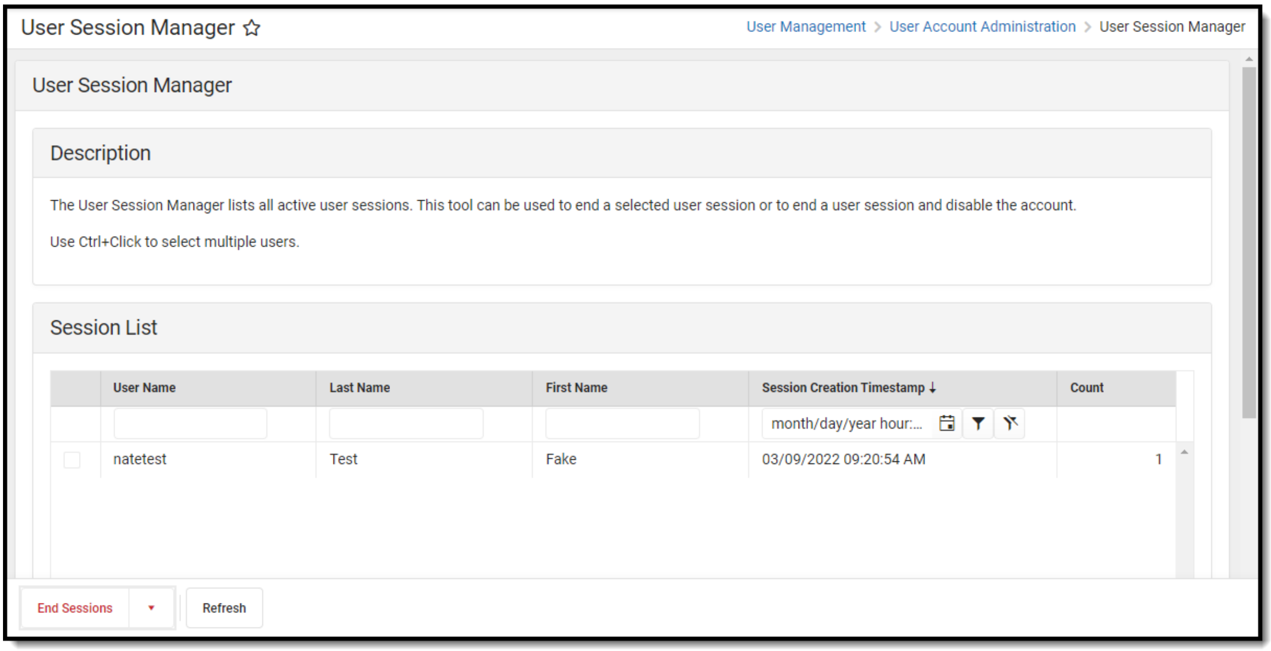
Log In

Show Help

Version: Campus-31.3.147 | intIA
© 2003-2024 Infinite Campus, Inc.
www.infinitecampus.com

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.


User Session Manager ☆

User Management > User Account Administration > User Session Manager

User Session Manager

Description

The User Session Manager lists all active user sessions. This tool can be used to end a selected user session or to end a user session and disable the account.

Use Ctrl+Click to select multiple users.

Session List

	User Name	Last Name	First Name	Session Creation Timestamp ↓	Count
				month/day/year hour:...	
□	natetest	Test	Fake	03/09/2022 09:20:54 AM	1

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?
- What if I Clear My Cookies Each Time I Close My Browser?
- How Do I Minimize the Amount of Notification Emails?
- Will the Login as User Feature Result in a Notification Email?
- How Do I Reset a User's Account Security Email Address?
- Why Can't I Get reCaptcha to Work?
- Do Login Security Settings Apply to Both Staff and Student/Parent Accounts?

How Does Campus Remember a Device?

Once you log in to Campus, a unique ID is generated and stored as a cookie in 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.
>
> For help in troubleshooting why your cookies keep being cleared, see the Troubleshooting Cookie Deletion article.

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 enter an email and set up the device as a remembered device each and every time you log into Campus.

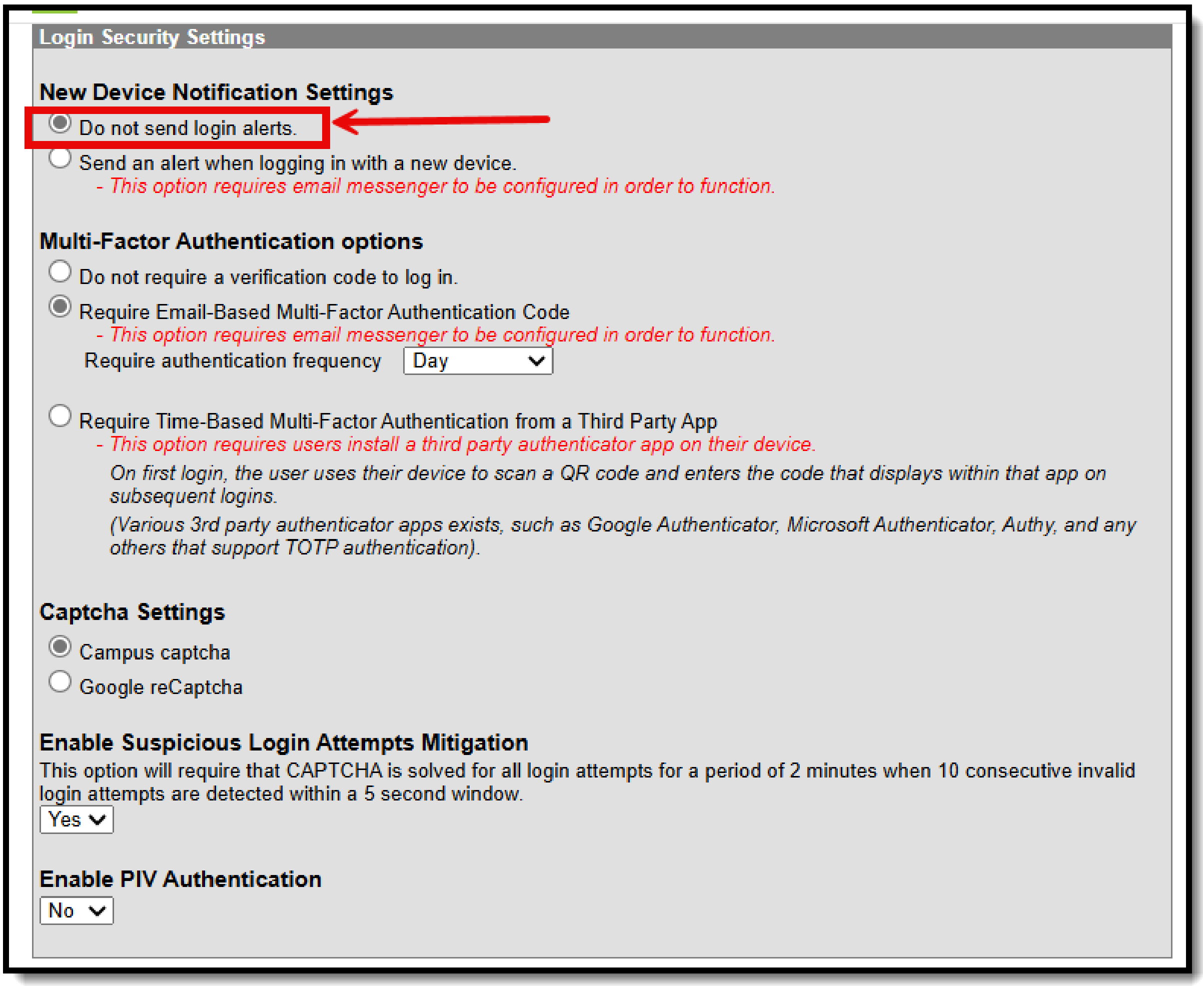
It is highly recommended that you do not set your browser to delete cookies automatically to prevent the notification process from repeating each time you log into Campus.

For help in troubleshooting why your cookies keep being cleared, see the Troubleshooting Cookie Deletion article.

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 number 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



Login Security Settings

New Device Notification Settings

● Do not send login alerts.

○ Send an alert when logging in with a new device.
- This option requires email messenger to be configured in order to function.

Multi-Factor Authentication options

○ Do not require a verification code to log in.

● Require Email-Based Multi-Factor Authentication Code
- This option requires email messenger to be configured in order to function.
Require authentication frequency: Day

○ Require Time-Based Multi-Factor Authentication from a Third Party App
- This option requires users install a third party authenticator app on their device.
On first login, the user uses their device to scan a QR code and enters the code that displays within that app on subsequent logins.
(Various 3rd party authenticator apps exists, such as Google Authenticator, Microsoft Authenticator, Authy, and any others that support TOTP authentication).

Captcha Settings

● Campus captcha

○ Google reCaptcha

Enable Suspicious Login Attempts Mitigation

This option will require that CAPTCHA is solved for all login attempts for a period of 2 minutes when 10 consecutive invalid login attempts are detected within a 5 second window.

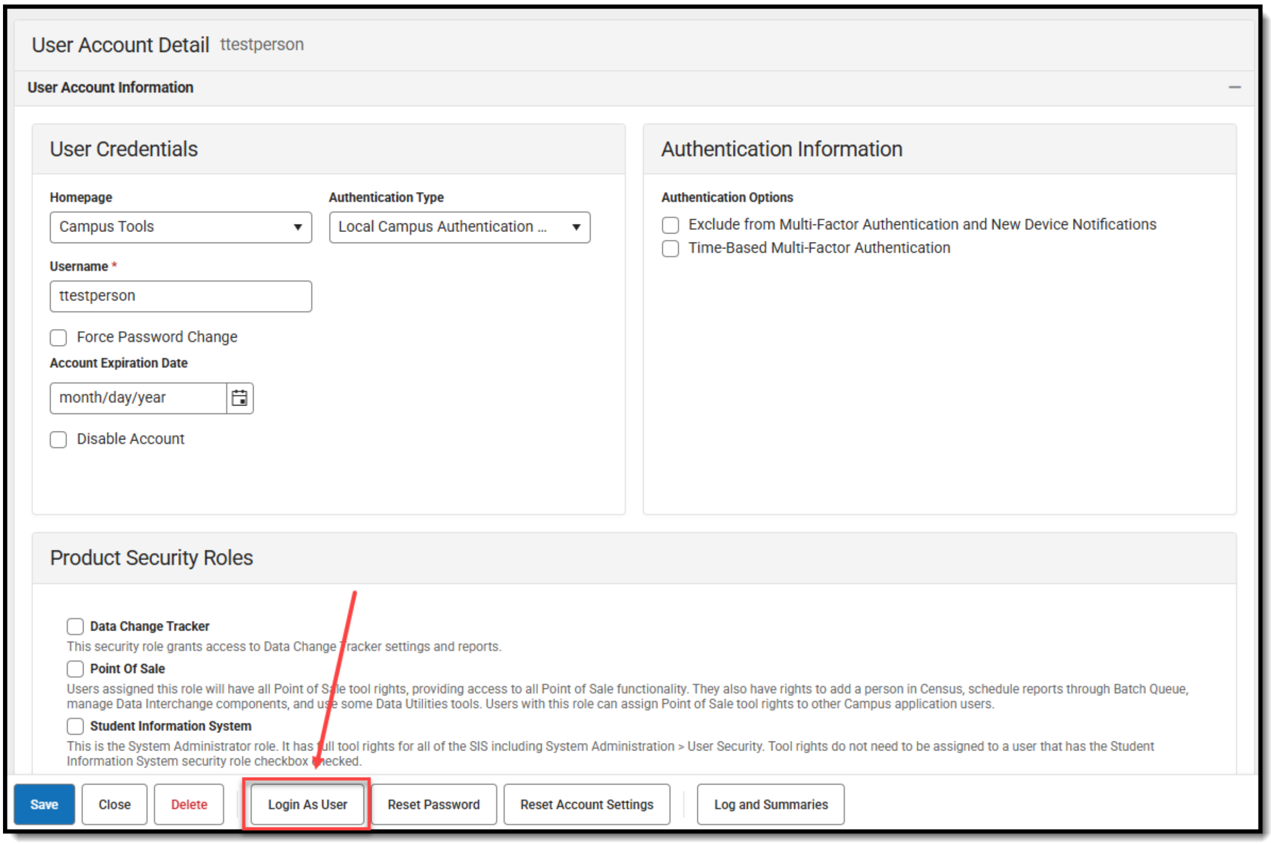
Yes

Enable PIV Authentication

No

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 a notification to the person you are logging in as. Login notifications only occur upon login via the Campus login screen.



User Account Detail ttestperson

User Account Information

User Credentials

Homepage: Campus Tools

Authentication Type: Local Campus Authentication ...

Username *: ttestperson

□ Force Password Change

Account Expiration Date: month/day/year

□ Disable Account

Authentication Information

Authentication Options

□ Exclude from Multi-Factor Authentication and New Device Notifications

□ Time-Based Multi-Factor Authentication

Product Security Roles

□ Data Change Tracker

This security role grants access to Data Change Tracker settings and reports.

□ Point Of Sale

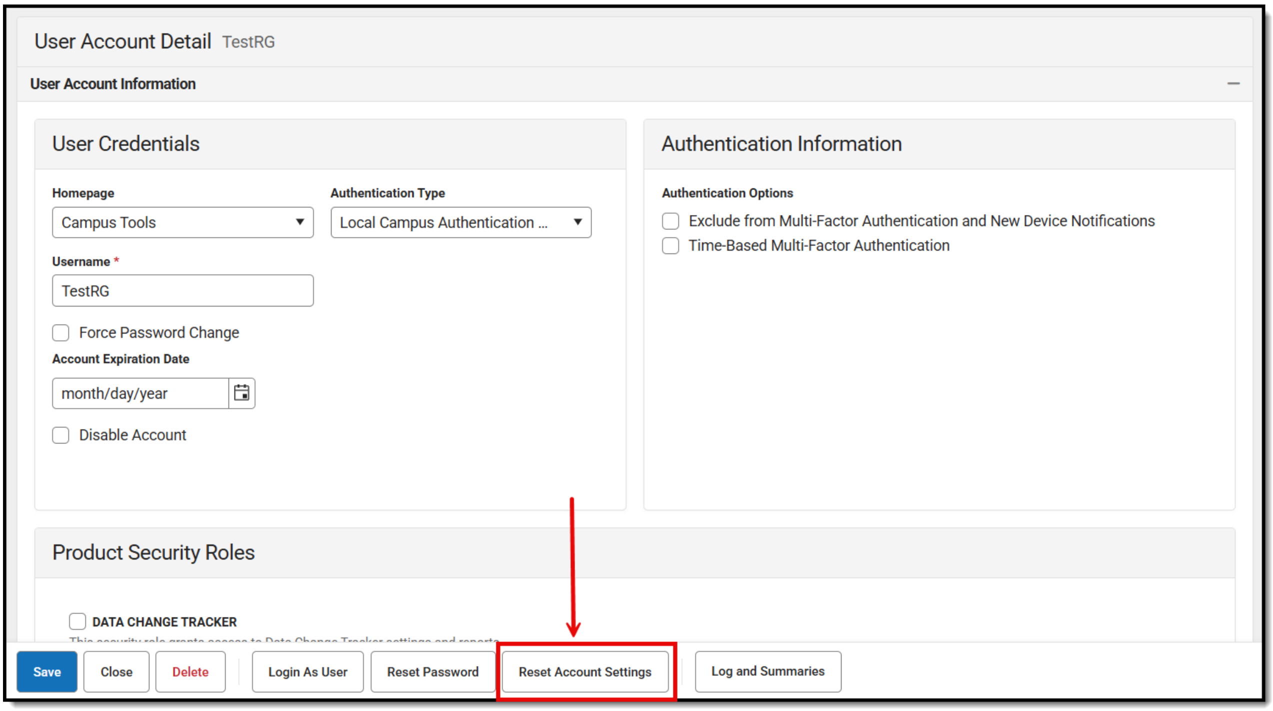
Users assigned this role will have all Point of Sale tool rights, providing access to all Point of Sale functionality. They also have rights to add a person in Census, schedule reports through Batch Queue, manage Data Interchange components, and use some Data Utilities tools. Users with this role can assign Point of Sale tool rights to other Campus application users.

□ Student Information System

This is the System Administrator role. It has full tool rights for all of the SIS including System Administration > User Security. Tool rights do not need to be assigned to a user that has the Student Information System security role checkbox checked.

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.



User Account Detail TestRG

User Account Information

User Credentials

Homepage: Campus Tools

Authentication Type: Local Campus Authentication ...

Username *: TestRG

□ Force Password Change

Account Expiration Date: month/day/year

□ Disable Account

Authentication Information

Authentication Options

□ Exclude from Multi-Factor Authentication and New Device Notifications

□ Time-Based Multi-Factor Authentication

Product Security Roles

□ DATA CHANGE TRACKER

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 its 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
- Do not require a verification code to log in
- Require Email-Based Multi-Factor Authentication Code
- RequireTime-Based Multi-Factor Authentication from a Third Party App
- Enable PIV Authentication

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