

# Login Security Settings [.2207 - .2215]

Last Modified on 10/22/2022 10:47 am CDT

You are viewing a previous version of this article. See [Login Security Settings](#) for the most current information.

**Classic View:** [System Administration](#) > [User Security](#) > [User Preference Management](#) > [Login Security Settings](#)

**Search Term:** [Login Security Settings](#)

The Login Security Settings are defaulted as opt-in (Send an alert when logging into a new device) and is ONLY available for staff users.

The Login Security Settings tool allows you to control whether or not Staff users will receive login alert notification emails.

- [Tool Rights](#)
- [Disable Login Alert Notifications](#)
- [Enable Login Alert Notifications](#)
- [Enable Login Alert Notifications with a Verification Code](#)
- [Enable Device-Based Two-Factor Authentication](#)
- [Enable Captcha Settings](#)
- [Enable Suspicious Login Attempts Mitigation](#)
- [Enable PIV Authentication](#)
- [View All Active Sessions and Log Out/Disable User Accounts](#)
- [FAQ](#)

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

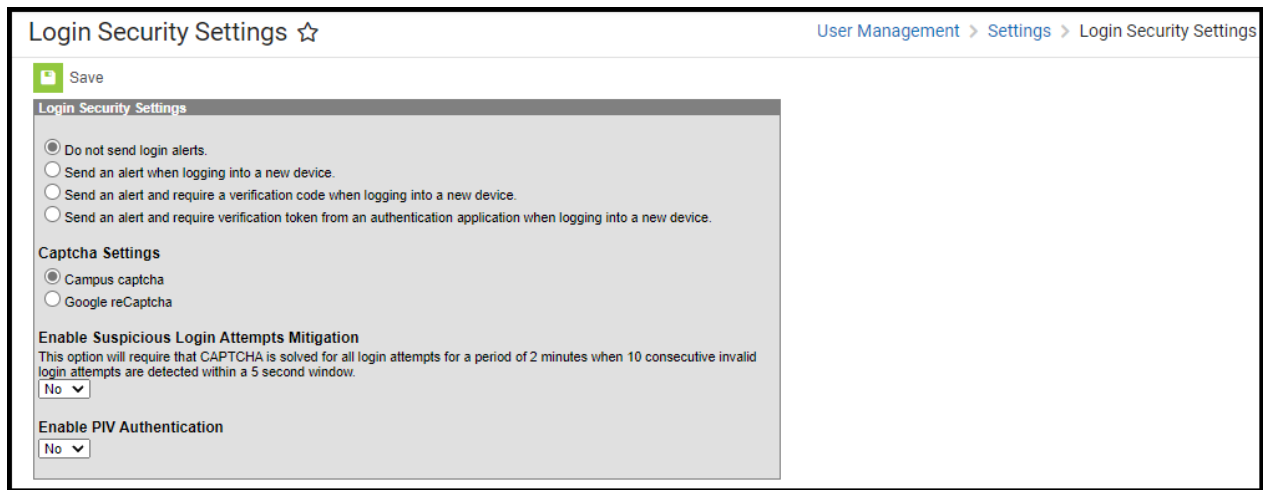


Image 1: Login Security Settings

## 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.

Login Security Settings ☆

Save

Login Security Settings

☒ Do not send login alerts.
☐ Send an alert when logging into a new device.
☐ Send an alert and require a verification code when logging into a new device.
☐ Send an alert and require verification token from an authentication application when logging into a new device.

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.

No

Enable PIV Authentication

No

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).

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

Login Security Settings ☆

Save

Login Security Settings

☐ Do not send login alerts.
☒ Send an alert when logging into a new device.
☐ Send an alert and require a verification code when logging into a new device.
☐ Send an alert and require verification token from an authentication application when logging into a new device.

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.

No

Enable PIV Authentication

No

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 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 Campus) and will be asked if they would like the device to be remembered for future logins (Image 4).

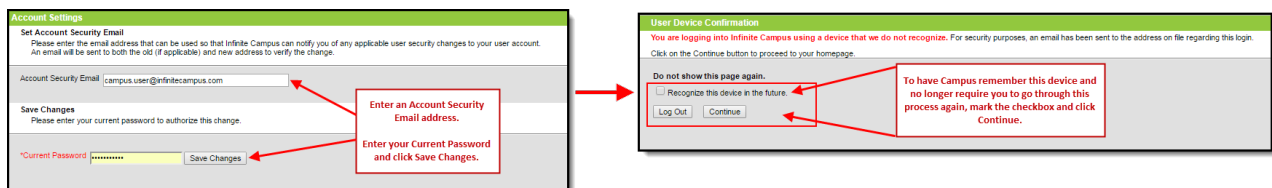


Image 4: Entering an Account Security Email and Remembering the Device

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

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

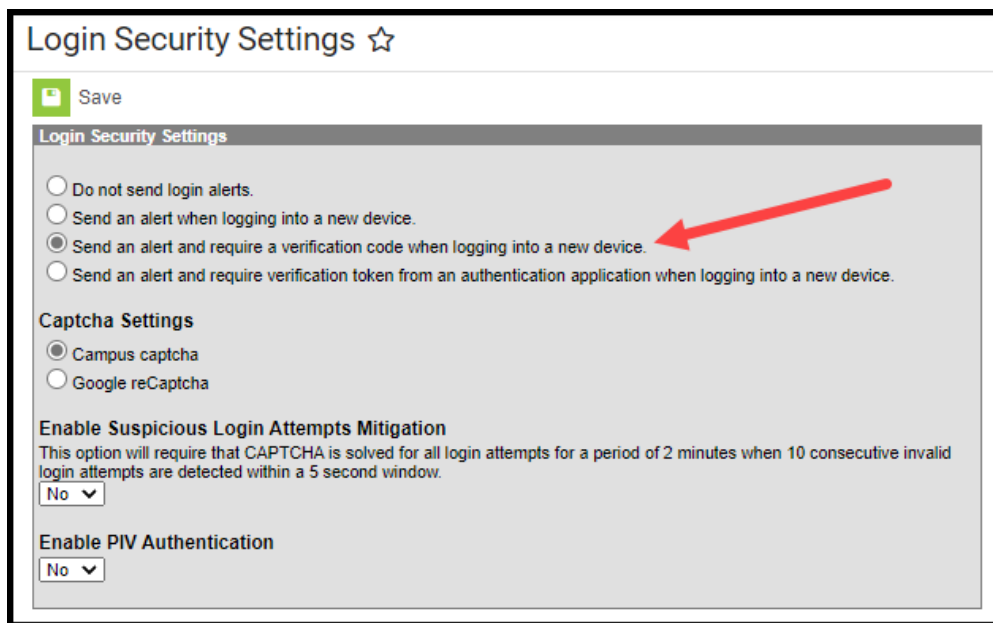
Additionally, please direct any questions or concerns regarding this email to your System Administrator.

Image 5: Unknown Device Login Email Notification

# Enable Login Alert Notifications with a Verification Code

To enable login alert notification emails, select the **Send an alert and require a verification code when logging into a new device** 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.



Save

**Login Security Settings**

- ☐ Do not send login alerts.
- ☐ Send an alert when logging into a new device.
- ☒ Send an alert and require a verification code when logging into a new device.
- ☐ Send an alert and require verification token from an authentication application when logging into a new device.

**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.

No ▾

**Enable PIV Authentication**

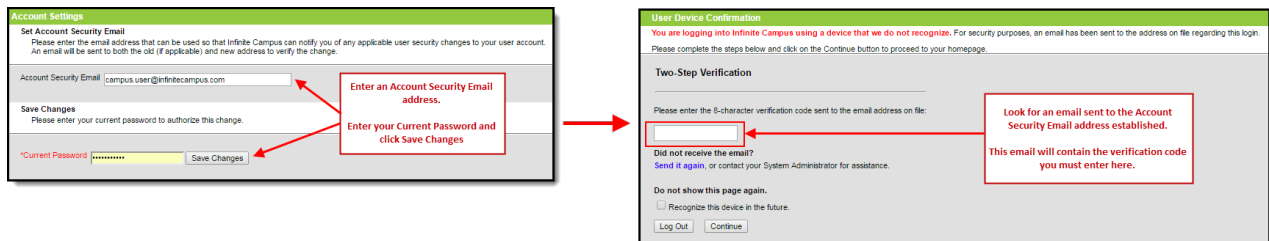
No ▾

Image 6: Enabling Login Notifications with Verification Codes

Once the **Send an alert and require a verification code when logging into a new device** radio button is selected, users logging into 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 Campus) and will be directed to a new screen where they will have to enter a verification code 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.**

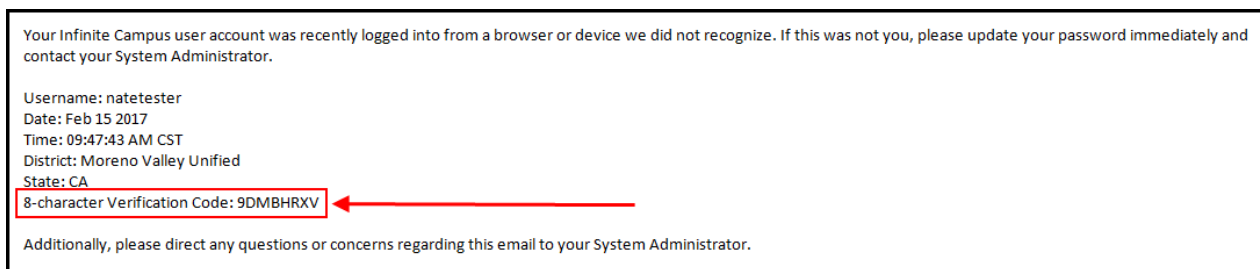
Having your browser set to automatically delete cookies will cause the device to not be recognized and force you to go through this process each time you log into Campus.



The image shows two screenshots from the Infinite Campus interface. The left screenshot is the 'Account Settings' page, specifically the 'Set Account Security Email' section. It has a text input field for 'Account Security Email' (containing 'campus.user@infinitecampus.com'), a 'Save Changes' button, and a 'Current Password' field with a masked password. Red arrows point from the 'Account Security Email' field to a red box containing the text 'Enter an Account Security Email address.' and from the 'Current Password' field to a red box containing the text 'Enter your Current Password and click Save Changes'. The right screenshot is the 'User Device Confirmation' page. It has a heading 'Two-Step Verification' and a text input field for the verification code. Red arrows point from the verification code field to a red box containing the text 'Look for an email sent to the Account Security Email address established. This email will contain the verification code you must enter here.' and from the 'Continue' button to a red box containing the text 'Enter the verification code from the email in this field, determine if you would like the device to be recognized for future logins and click the Continue button.'

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

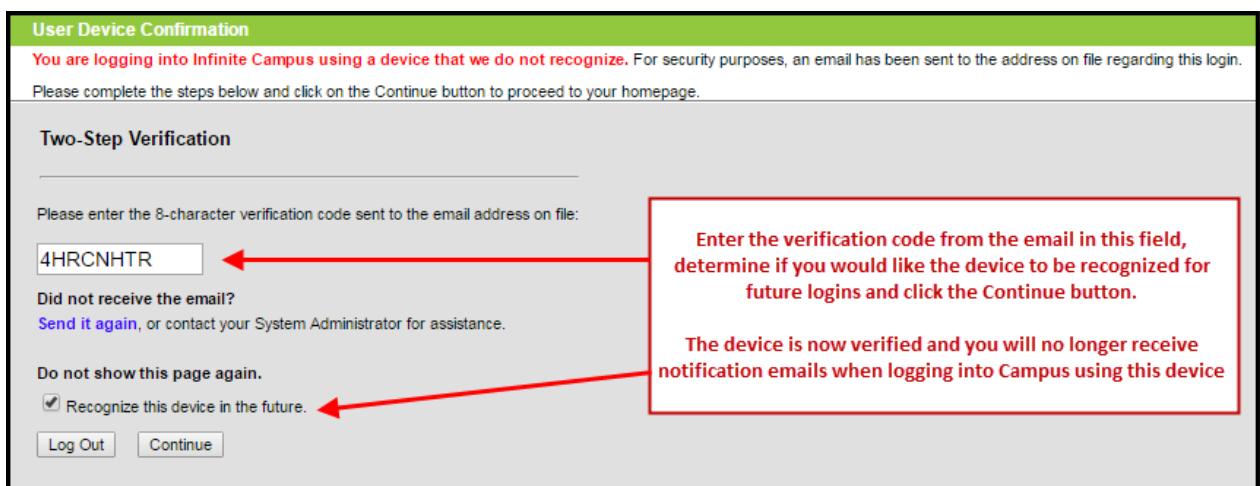
Below is an example of the email that will be sent to your account. This email contains the 8-character verification code that must be entered in the box show above (Image 7).



The image shows an email notification from Infinite Campus. The text reads: '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.' Below this, the user's details are listed: 'Username: natetester', 'Date: Feb 15 2017', 'Time: 09:47:43 AM CST', 'District: Moreno Valley Unified', and 'State: CA'. A red box highlights the '8-character Verification Code: 9DMBHRXV' with a red arrow pointing to it. At the bottom, it says 'Additionally, please direct any questions or concerns regarding this email to your System Administrator.'

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.



The image shows the 'User Device Confirmation' page. It has a heading 'Two-Step Verification' and a text input field for the verification code. Red arrows point from the verification code field to a red box containing the text 'Enter the verification code from the email in this field, determine if you would like the device to be recognized for future logins and click the Continue button.' and from the 'Continue' button to a red box containing the text '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 Device-Based Two-Factor Authentication

As an increased layer of protection for Infinite Campus accounts, user accounts can be enabled with

device-based two-factor authentication functionality. 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).

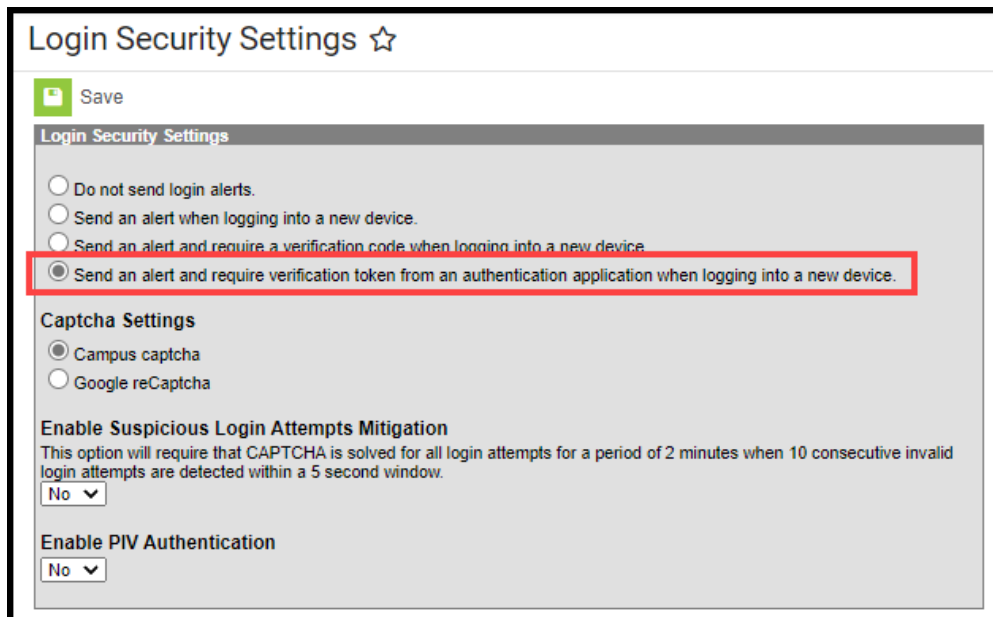
This functionality does not apply to Portal accounts.

**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 accounts, click the **Send an alert and require verification token from an authentication application when logging into a new device** radio button and select **Save** (Image 10).



Login Security Settings ☆

Save

**Login Security Settings**

- ☐ Do not send login alerts.
- ☐ Send an alert when logging into a new device.
- ☐ Send an alert and require a verification code when logging into a new device.
- ☒ Send an alert and require verification token from an authentication application when logging into a new device.

**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.

No ▾

**Enable PIV Authentication**

No ▾

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 to scan the **QR Code** or enter the **Text Code**. This will register the device and tie it to their 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.

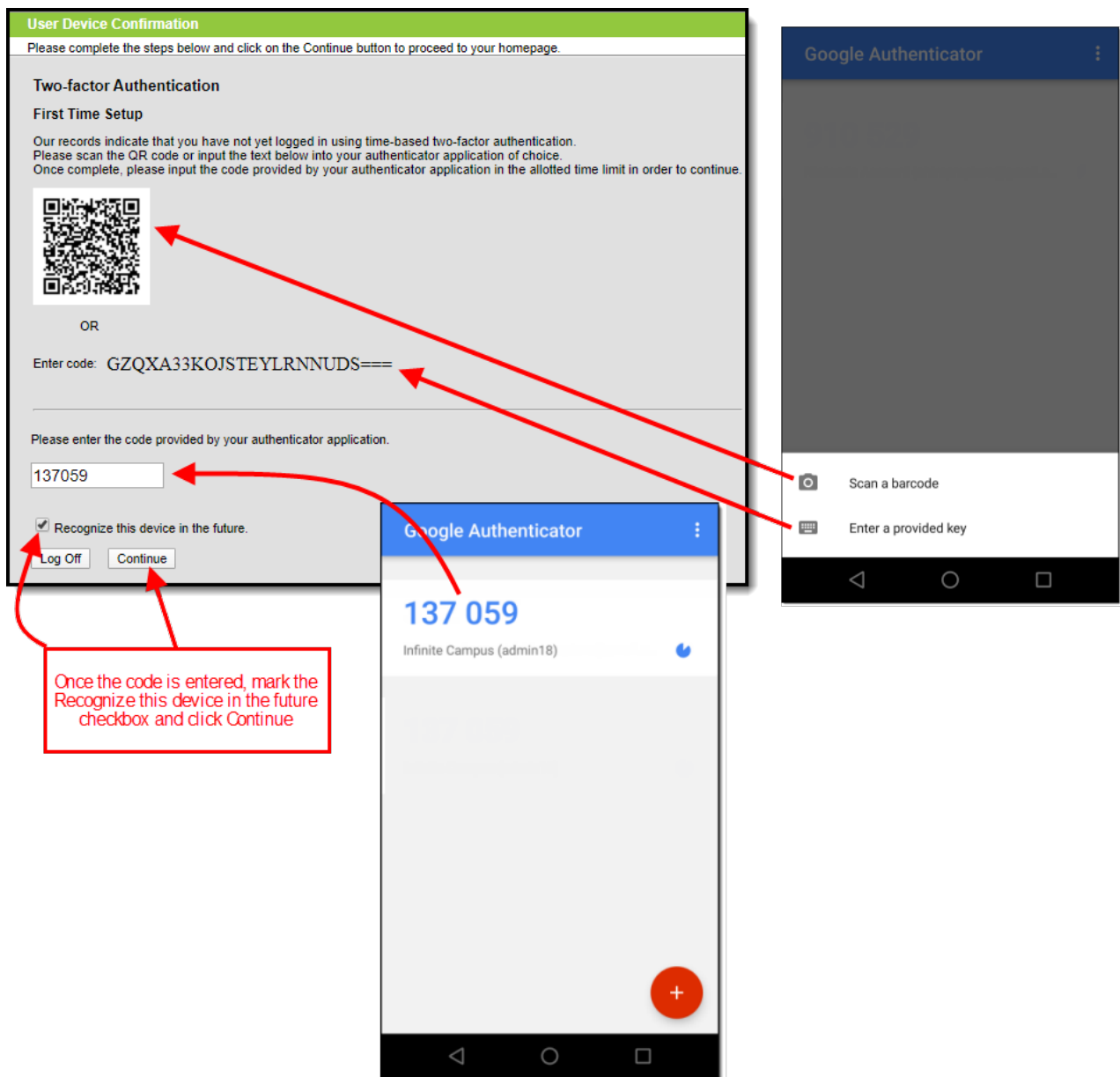


Image 11: Registering a Device and Logging into Infinite Campus

In the future when logging into Campus on a new device, 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.

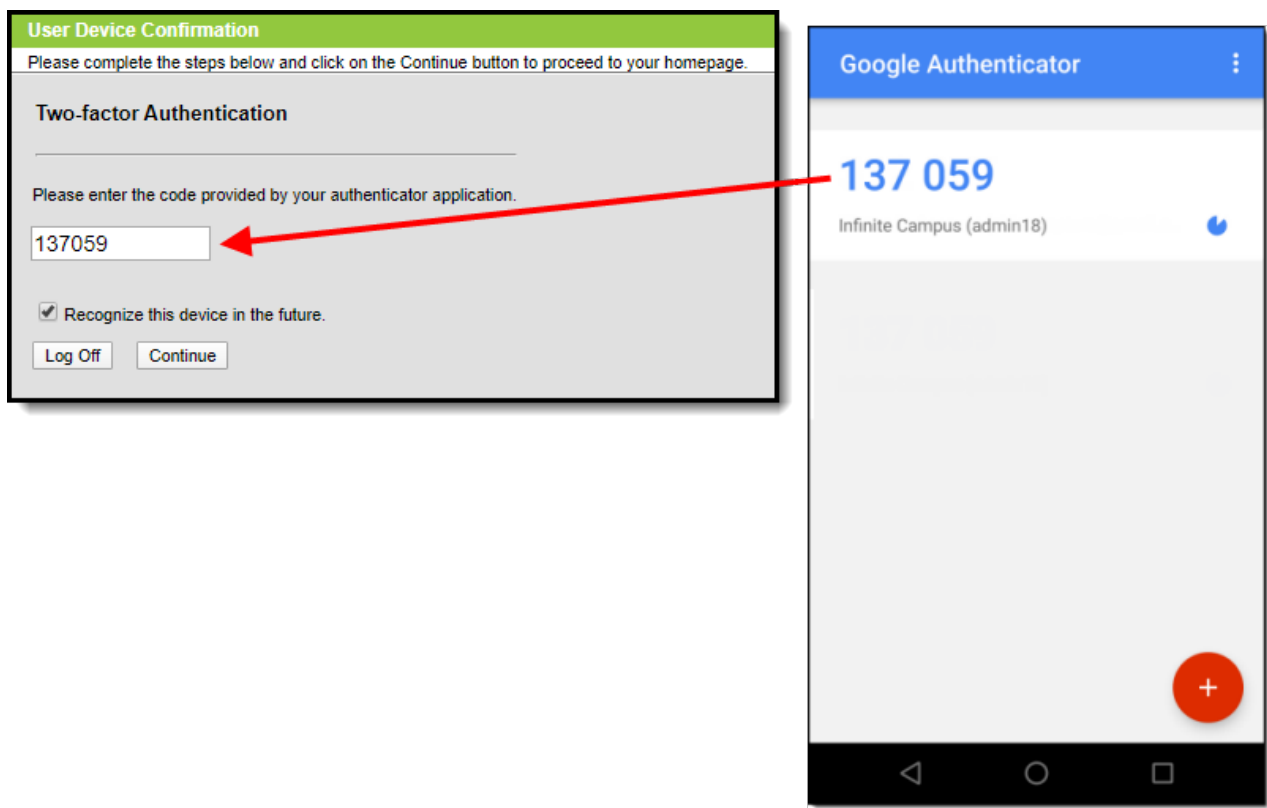


Image 12: Logging into Infinite Campus Using an Authentication Code

This preference is not time-based and triggers whenever it detects the login as coming from a new device. If an additional time-based trigger is desired for specific users, this can be configured user-by-user by enabling the '**Time-based Two-Factor Authentication w/Enhanced Security**' preference on each specific [User Account](#).

**User Account** | User Groups | Tool Rights | Calendar Rights | Access Log

Save | Delete | Login As User | User Rights Summary

**User Account Editor**

\*Username: aaronscat | Password: | Reset Password

Expires Date: | Homepage: Campus Application

☐ Force Password Change

☐ Disabled

☒ Time-based Two-factor Authentication w/ Enhanced Security

Require authentication every: 30 Minutes (selected)

- Modified by: Unknown 01/01/1901 00:00  
- Created Date: Unknown

**Product Security Role Assignment**

- ☐ 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.
- ☐ Student Information System - Group Assignment  
This role provides non-security users the ability to assign User Groups to other users without being given the security and system access granted with other product security roles.
- ☐ Student Information System - Login As User  
This role indicates whether or not the user may log in as another user from the User Account tab.

## Enable Captcha Settings

Captcha Settings determine which captcha is used on the Campus login screen for users who have failed to properly log into 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.

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 Campus.

Login Security Settings ☆

Save

**Login Security Settings**

☐ Do not send login alerts.  
☐ Send an alert when logging into a new device.  
☐ Send an alert and require a verification code when logging into a new device.  
☒ Send an alert and require verification token from an authentication application when logging into a new device.

**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.  
 No ▼

**Enable PIV Authentication**  
 No ▼

Image 13: Enabling Campus Captcha

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

Infinite Campus Transforming K12 Education®

District Edition

Version: trunk\_20170720\_0006  
leaz

Username  
admin

Password  
.....

Jx hc TE 6

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

Sign In >>

Forgot your password? | Forgot your username? | Problems logging in?

©2003-2017 Infinite Campus, Inc.  
www.infinitecampus.com

Image 14: Example of the Campus Captcha

## Google reCaptcha

The Google reCaptcha displays a checkbox the user must select and a series of pictures the user

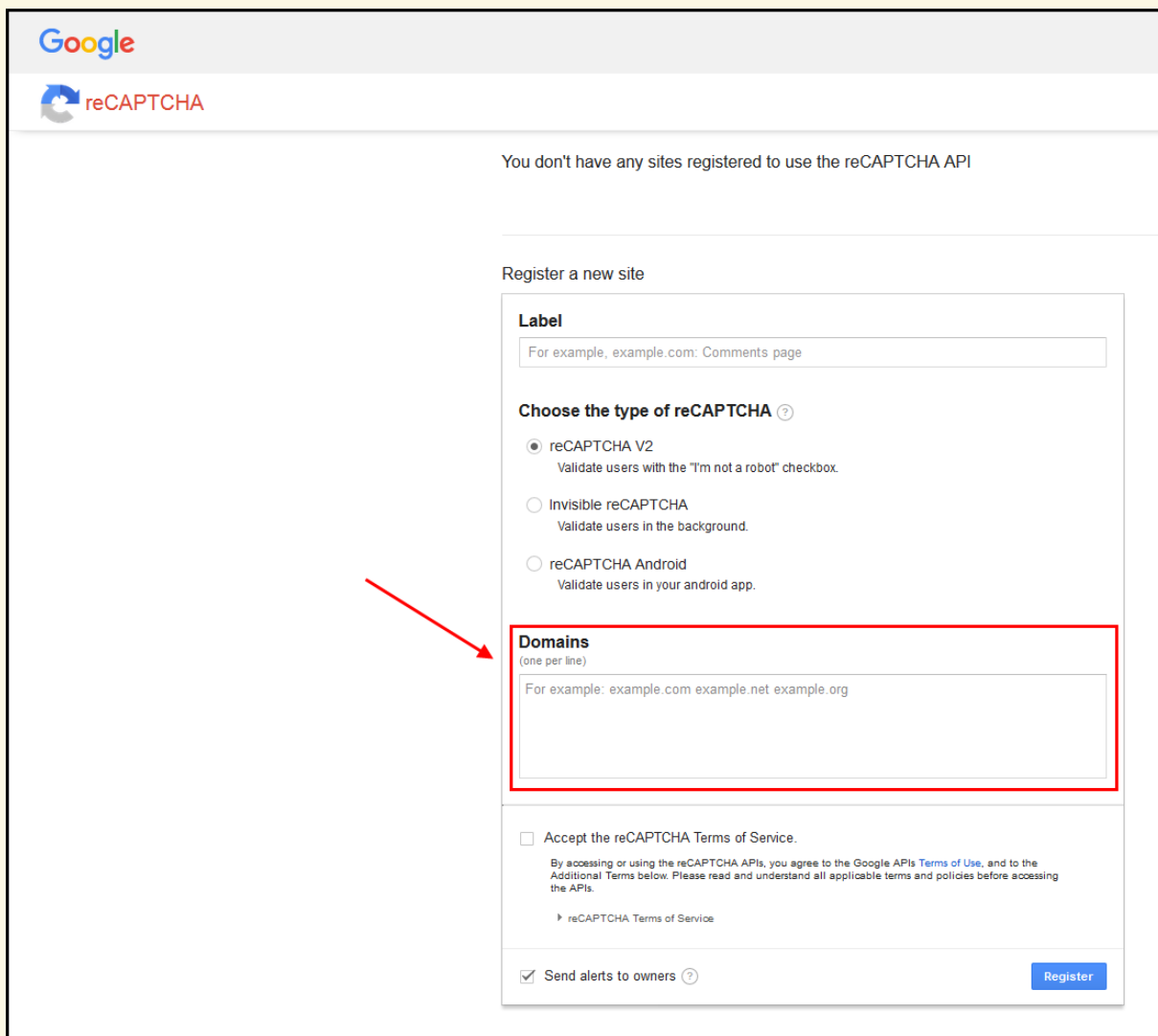
must select to prove it is a human and not a bot.

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.**



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 ?

Register

## Login Security Settings ☆

 Save

### Login Security Settings

☐ Do not send login alerts.  
☐ Send an alert when logging into a new device.  
☐ Send an alert and require a verification code when logging into a new device.  
☒ Send an alert and require verification token from an authentication application when logging into a new device.

### Captcha Settings

☐ Campus captcha  
☒ Google reCaptcha


Site Key:  
  
 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.

**Enable PIV Authentication**

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).




# Transforming K12 Education®

**District Edition**

Version: trunk\_20170720\_0006  
ieaz

**Username**

**Password**

☐ I'm not a robot
 

reCAPTCHA  
Privacy - Terms

**Sign In >>**

[Forgot your password?](#) | 
 [Forgot your username?](#) | 
 [Problems logging in?](#)

©2003-2017 Infinite Campus, Inc.  
www.infinitecampus.com

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).

Google reCAPTCHA

←

Settings

Label ⓘ

My Test Site

12 / 50

reCAPTCHA type: v2 Checkbox

reCAPTCHA keys ▾

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.

CANCEL

SAVE

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.**

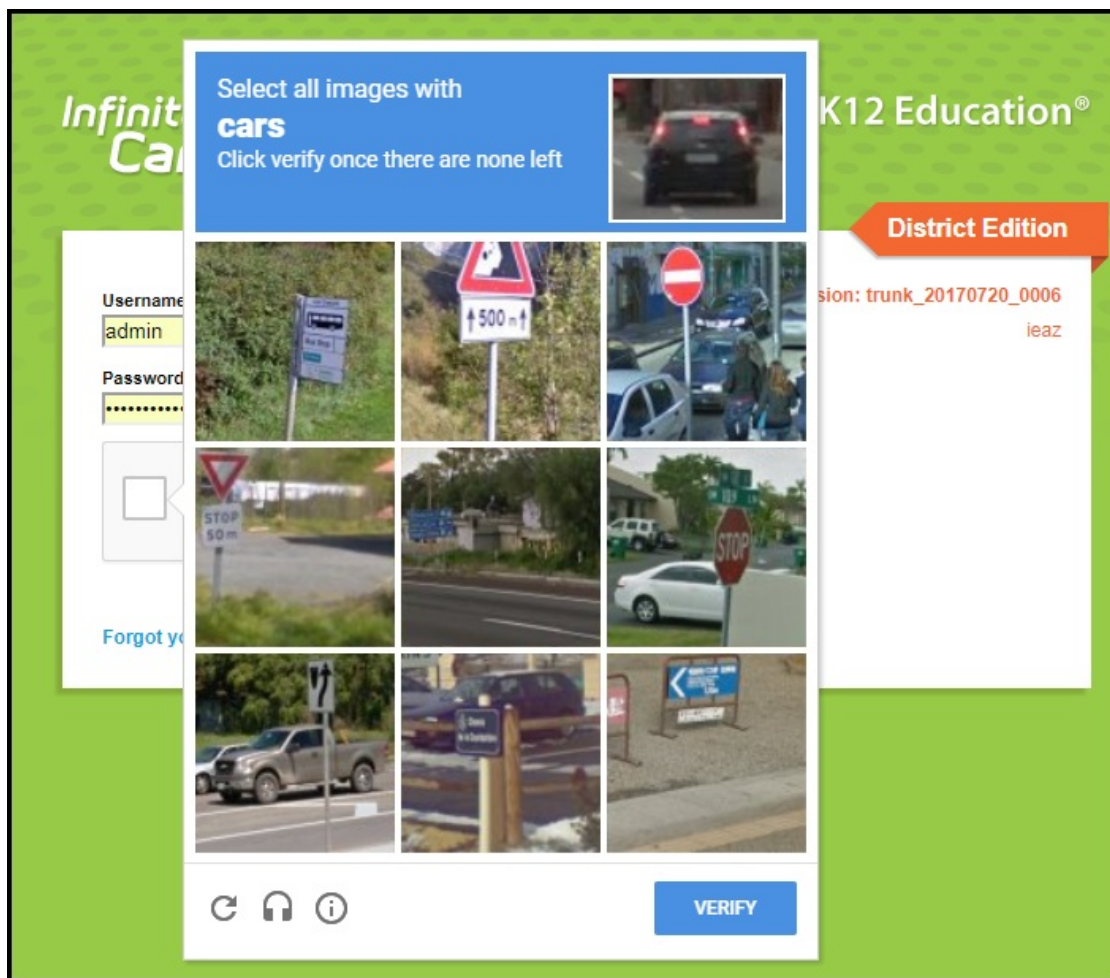


Image 17: Selecting Verification Images

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.

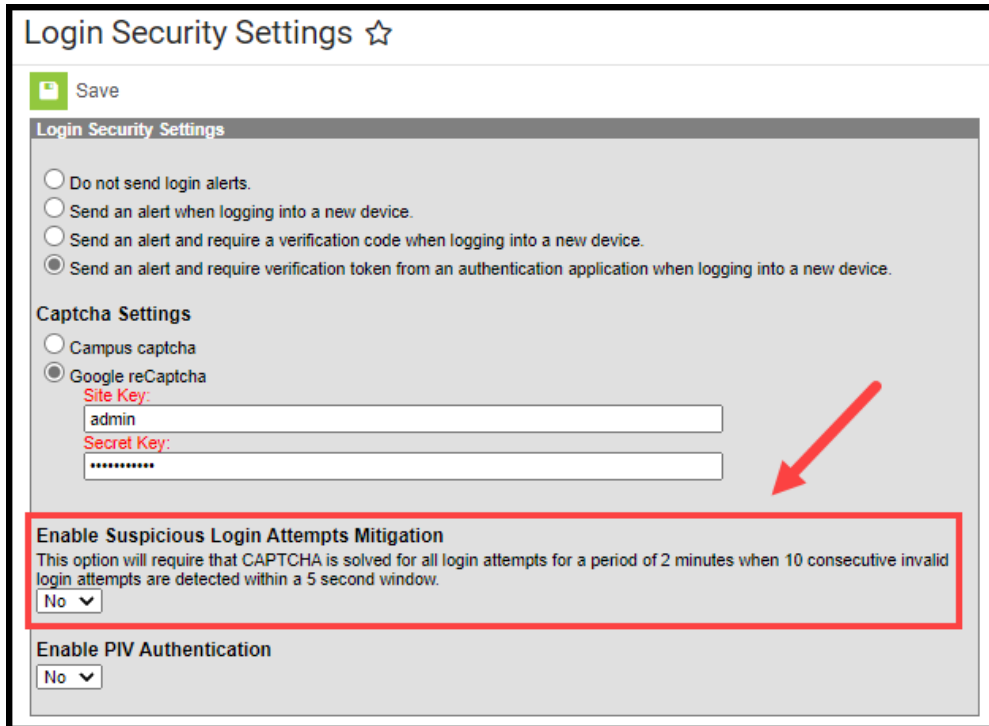
If you experience any issues after setup, ensure the IP addresses that Google requires for reCAPTCHA functionality have been AllowListed. Google maintains their list of IP addresses that must be AllowListed in order for reCAPTCHA functionality to work here:

<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.



Save

**Login Security Settings**

☐ Do not send login alerts.  
☐ Send an alert when logging into a new device.  
☐ Send an alert and require a verification code when logging into a new device.  
☒ Send an alert and require verification token from an authentication application when logging into a new device.

**Captcha Settings**

☐ Campus captcha  
☒ Google reCaptcha  
 Site Key:  
  
 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.  
 No ▾

**Enable PIV Authentication**  
 No ▾

## 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.

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 ☆

Save

Login Security Settings

☐ Do not send login alerts.  
☐ Send an alert when logging into a new device.  
☐ Send an alert and require a verification code when logging into a new device.  
☒ Send an alert and require verification token from an authentication application when logging into a new device.

**Captcha Settings**  
☐ Campus captcha  
☒ Google reCaptcha  

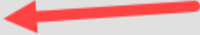
Site Key:

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.  

No ▼

**Enable PIV Authentication**  
No ▼



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 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.

The screenshot shows the Infinite Campus login interface. At the top left is the Infinite Campus logo. At the top right is the text 'Transforming K12 Education®'. Below the logo, there is a white login box. Inside this box, at the top left, is a button labeled 'Personal Identity Verification (PIV)'. To the right of this button is a red banner that says 'Student Information System'. Below the banner, the text 'Version: Campus-28.2.16' and 'intBIEAZ' is displayed. Below the PIV button is a horizontal line with the word 'or' in the center. Below this line are two input fields: 'Username' and 'Password'. Below these fields is a blue 'Log In' button. At the bottom of the login box is a 'Help' link. Three red arrows are overlaid on the image: one points to the 'Personal Identity Verification (PIV)' button, one points to the 'or' separator, and one points to the 'Username' input field.

## 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
<input type="checkbox"/>	natetest	Test	Fake	03/09/2022 09:20:54 AM	1

End Sessions ▼

Refresh

## 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?](#)

## 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?

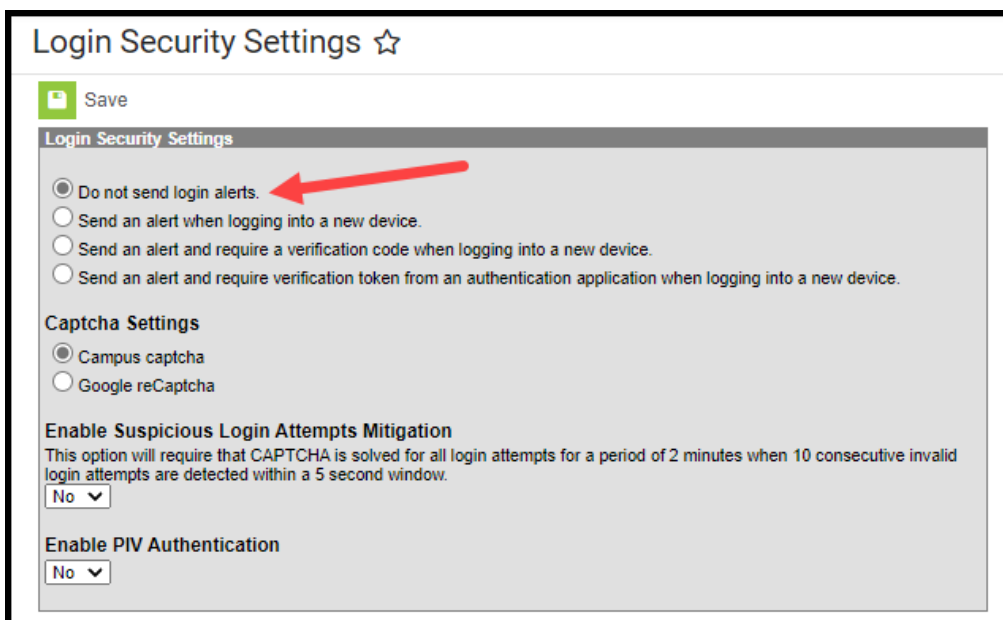
Clearing your browser cookies will remove the device from being remembered by the Campus notification process and will require you to go through the entering an email and setting up the device as a remembered device each and every time you log into Campus.

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.



**Login Security Settings** ☆

Save

**Login Security Settings**

☒ Do not send login alerts.
   
☐ Send an alert when logging into a new device.
   
☐ Send an alert and require a verification code when logging into a new device.
   
☐ Send an alert and require verification token from an authentication application when logging into a new device.

**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.

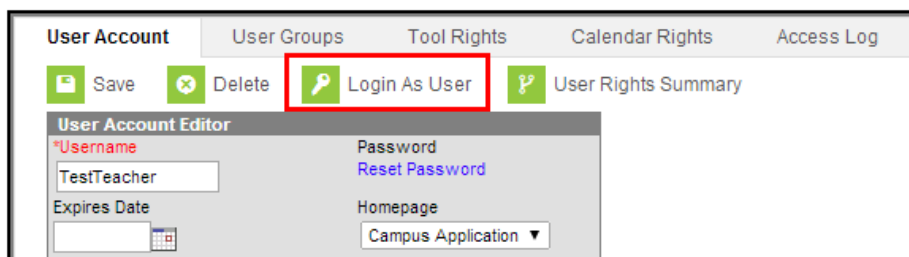
No ▾

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



**User Account** | User Groups | Tool Rights | Calendar Rights | Access Log

Save | Delete | **Login As User** | User Rights Summary

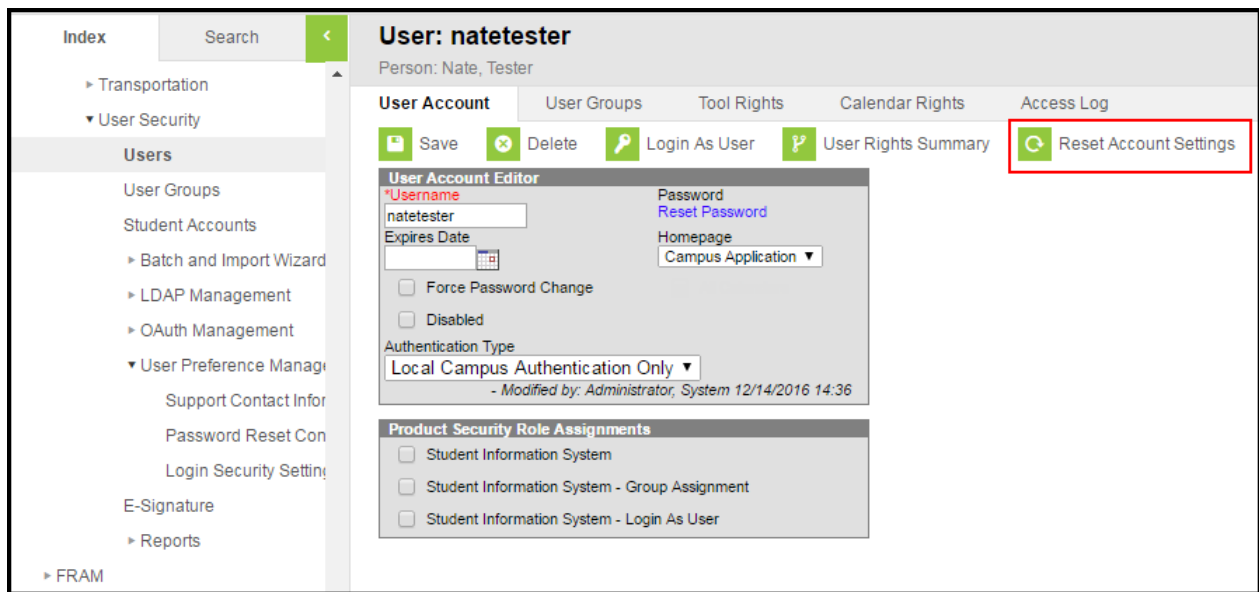
**User Account Editor**

\*Username: TestTeacher | Password: Reset Password

Expires Date: | Homepage: Campus Application ▾

## 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>