User Account [.2315 - .2411]

Last Modified on 04/08/2024 9:47 am CDT

You are viewing a previous version of this article. See User Account for the most current information.

Creating New Users (User Accounts) | Modifying User Accounts | User Account Tab Fields and Buttons | Understanding Security Role Assignments | Assigning Calendar Rights | Identifying a Person's Campus Portal Username | Related Tools

Tool Search: User Account

In order for a person to be assigned tool rights, be allowed to join user groups, be assigned calendar rights, and other features enabled via the User Accounts category, they must first be added as a user (have a user account created for them). This article will walk you through this process as well as cover the following:

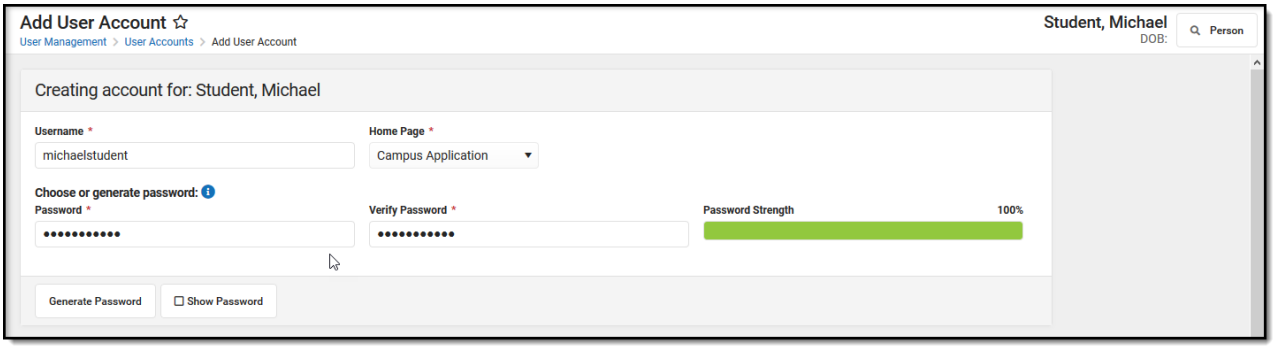
Users are highly advised to create user accounts for students and staff en masse via the User Account Batch Wizard.

If you cannot access Tool Rights, Calendar Rights and/or User Groups you are not assigned a user security role. To gain access, please contact your system administrator as they are responsible for assigning security roles to Campus users.

Creating New Users (User Accounts)

Before a user account can be created, the user must first exist as a person (click here for more information on adding a person to Campus). Once a person exists in Campus, they can then have a user account created.

To create a user account, use the Add User Account tool.



To generate student and staff accounts en masse, please refer to the User Account Batch

Wizard.

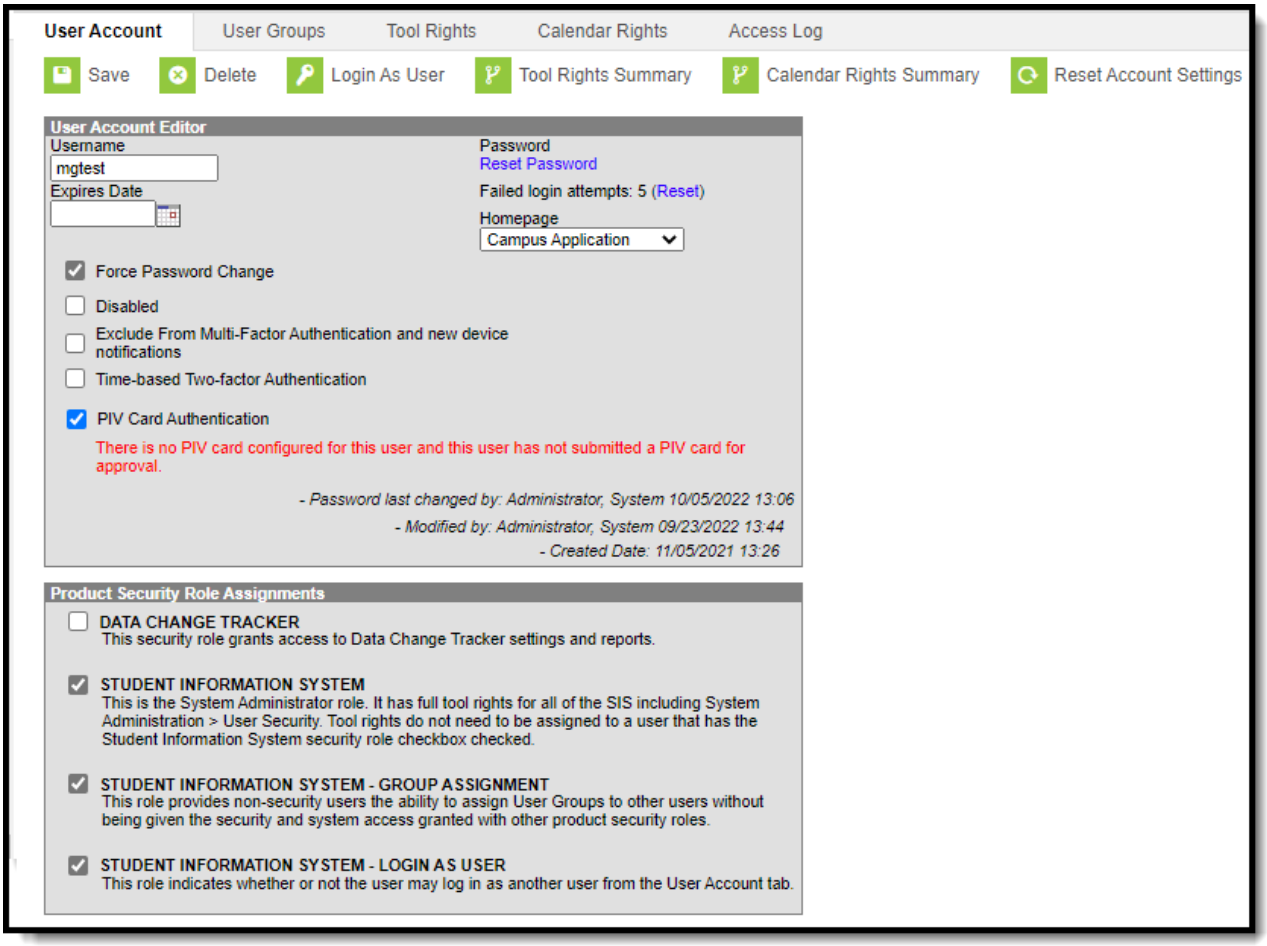
Modifying User Accounts

PATH: *System Administration > User Security > User > User Account*

Search Term: *User Account Information*

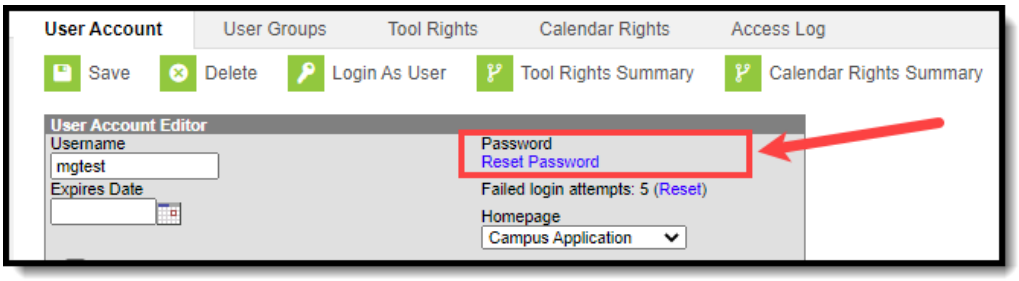
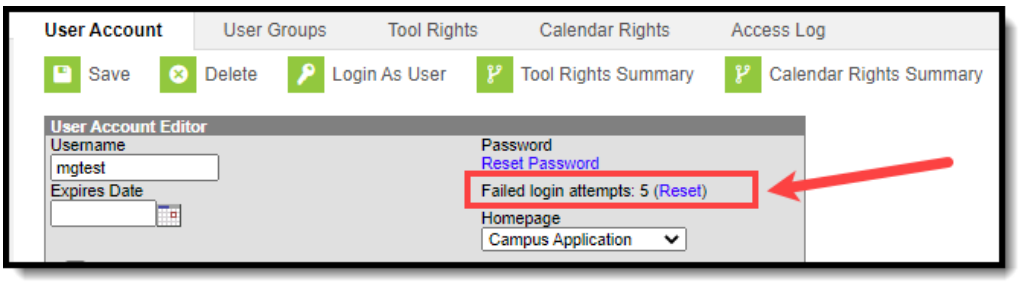
Individual user account information can be viewed and modified on the User Account tab.

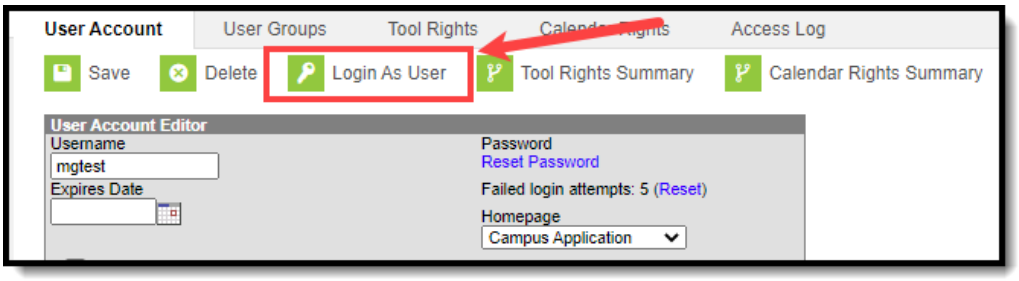
For more information about user account passwords, see the Managing User Account Passwords article.



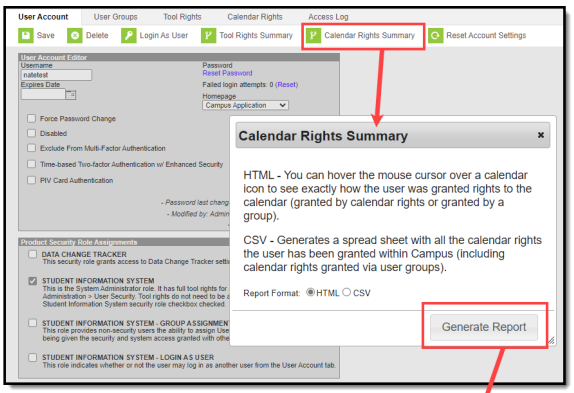
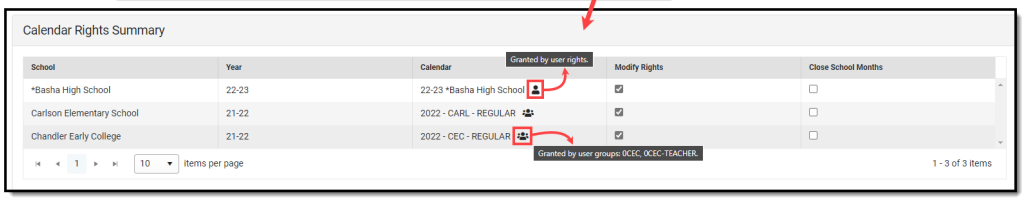
User Account Tab Fields and Buttons

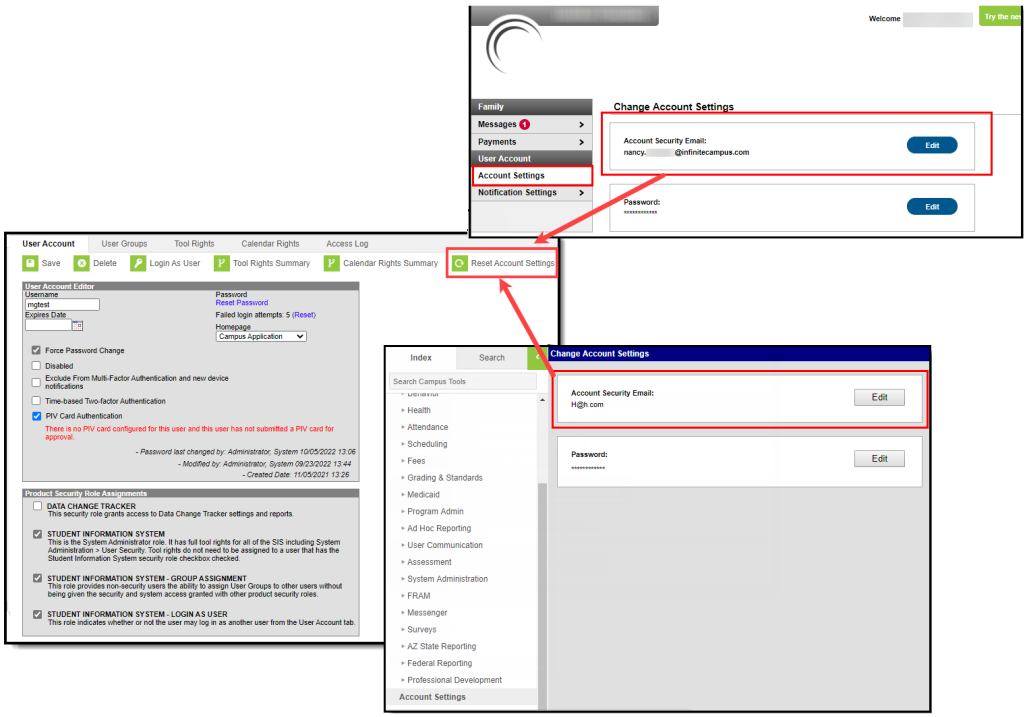
Field	Use and Definition

Field	Use and Definition
Password	To reset the user's password, select the **Reset Password** hyperlink. For more information on establishing, resetting, and managing passwords within Campus, see the Managing User Account Passwords article. 
Failed Login Attempts	This field indicates the number of consecutive times the user has failed to log into Infinite Campus. Administrators can reset this count by clicking the blue Reset button. Resetting this value also resets the need for the user to login via Captcha (which occurs at 5 consecutive failed login attempts). Once a user successfully logs into their account, this count goes back to 0. 

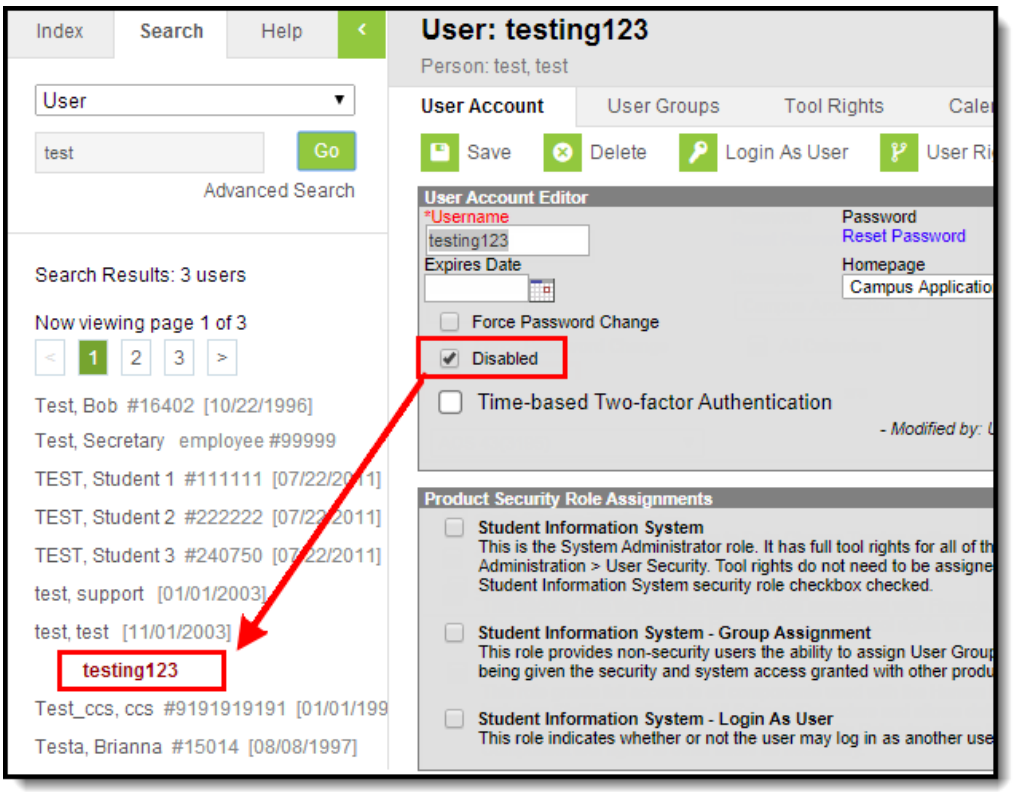
Field	Use and Definition
Login As User	The **Login As User** button allows a user log in as another user for the purpose of troubleshooting, testing and/or verifying properly assigned user rights. The Login As User button only appears for users who have equivalent or greater tool rights than the user they want to log in as and is only available with the **Student Information System** or **Student Information System - Login as User** security roles.  For more information about this feature, see the Login as User Feature article section. Users are only allowed to login as another user once per Campus session. Users with a **Student Information System** Product Security role are allowed to log in as a user with a **Student Information System - Login as User** Product Security Role but once they have logged in as that user, they cannot use that user account to then log into another Campus user account via the Login as User button on the User Account tab. Users with a **Student Information System - Login As User** role are prohibited from logging in as another user with the **Student Information System - Login As User** role. This behavior was put in place to ensure users do not jump from one user account to another. The Administrator selecting this button MUST have calendar rights for the school listed on the other user's (person being logged into) District Assignment page.

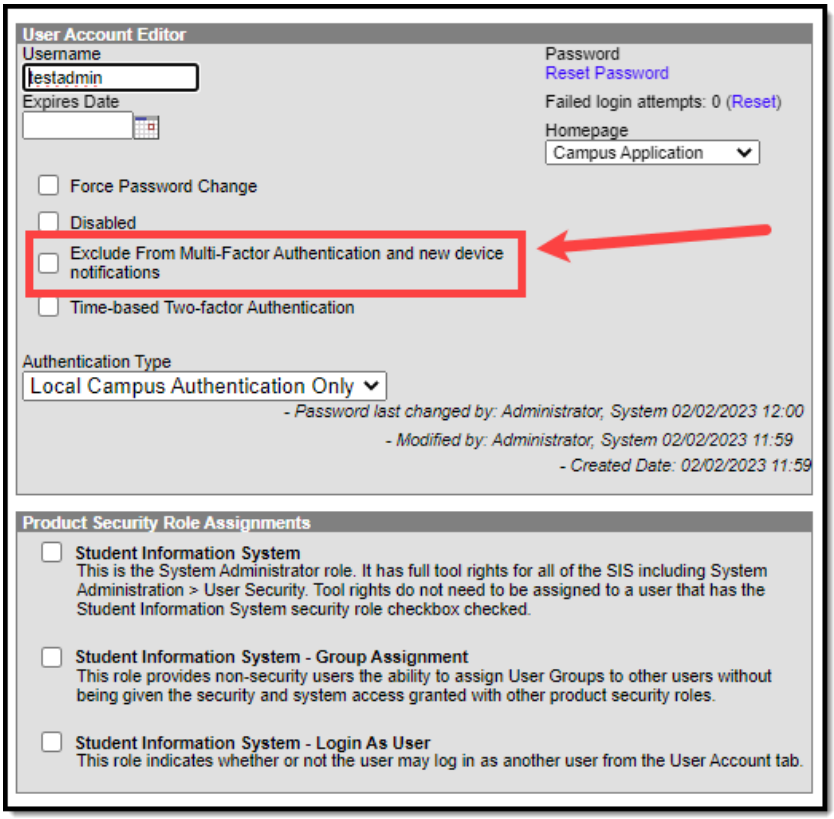
Field	Use and Definition
Tool Rights Summary	To access a comprehensive view of all tool rights the user has been granted within Campus (including tool rights granted via User Groups), click the **Tool Rights Summary** button. A window will appear, asking you to generate the summary in HTML or CSV format. Select a format and click the **Generate Report** button. The Tool Rights Summary will appear in a separate window (see image below). You can expand tools to view additional tool rights and sub-rights. You can also hover the mouse cursor over a tool to see exactly how the user was granted rights to the tool (granted by tool rights or granted by a group). You will only see tools for which the user has been granted access within Campus. 

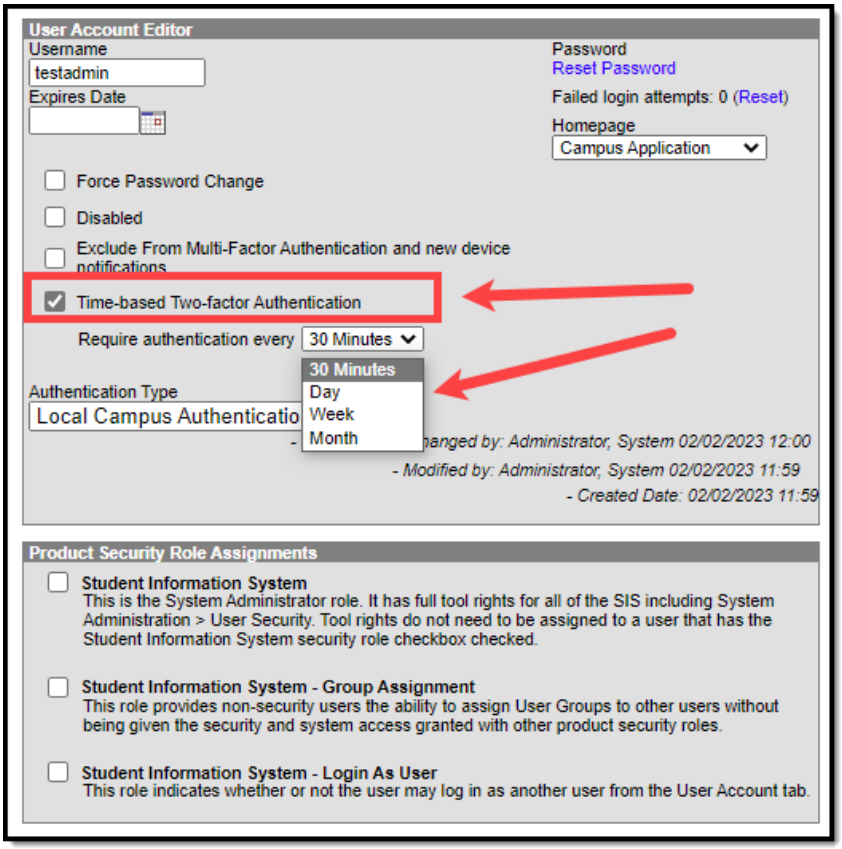
Field	Use and Definition
Calendar Rights Summary	The Calendar Rights Summary details which calendars in which years a specific user has rights to access and how this access was granted. A single person icon indicates access to that calendar was granted via individual user Calendar Rights (via the Calendar Rights tab). A group icon indicates calendar access was granted by the user being a part of a specific user group. Hovering your cursor over the group icon will indicate which user group(s) granted the user rights to the calendar.  

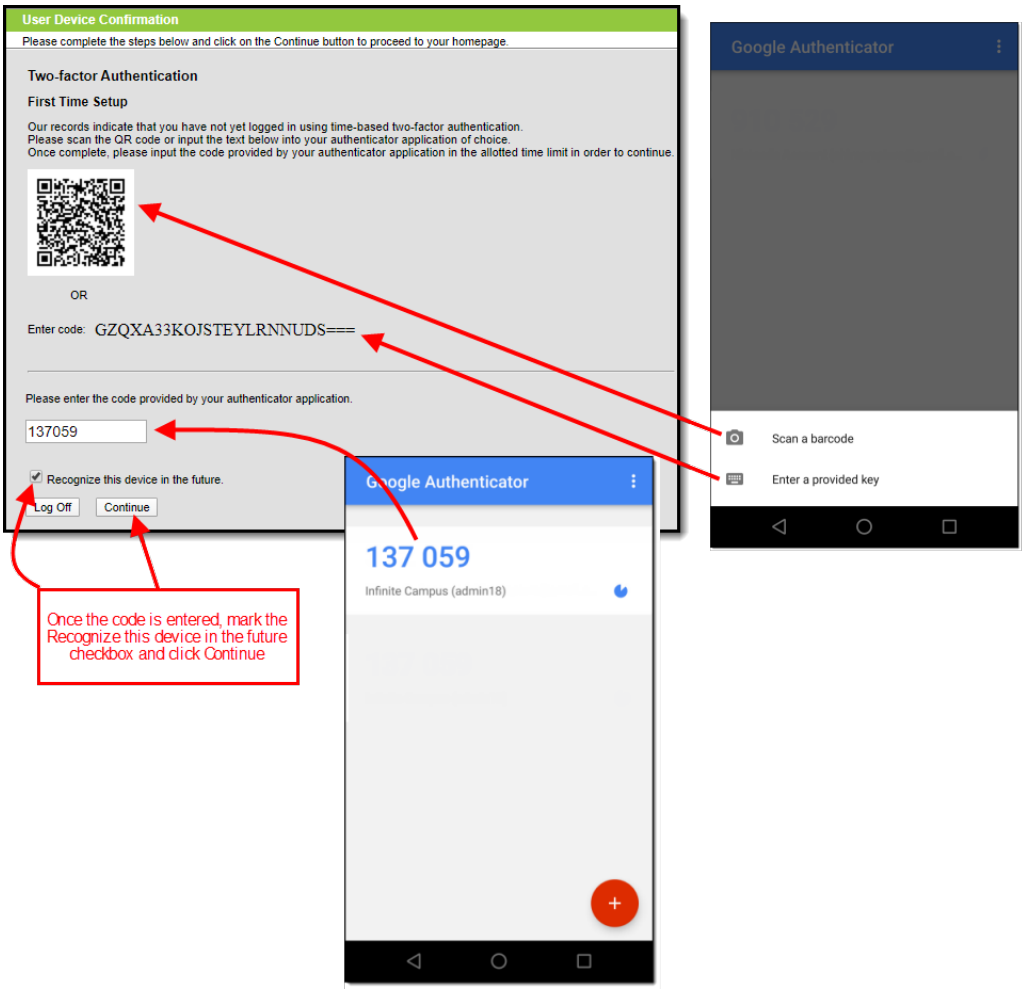
Field	Use and Definition
Reset Account Settings	Selecting the **Reset Account Settings** button will clear all trusted devices tied to the person's account, requiring the user to reestablish each device as a trusted device when logging into Campus. For districts using two factor authentication, selecting this button will reset the user's two 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 two facto authentication. This button will also reset the user's account recovery email address, requiring them to enter a new recovery email address the first time they log into Campus after this button has been selected. This button will only appear for user accounts which have an Account Security Email address established in Campus and/or the Parent Portal. A person's Account Security Email is used to recover a forgotten username or reset a Campus password when the Forgot your password? or Forgot your username? options are selected on the Campus login screen. The Account Security Email is set in the Account Settings tool (found in both Campus and the Parent Portal). 
Username	The user name the individual uses to log in to the Campus system.
Password	The password the individual uses to log into the Campus system. See the Managing User Account Passwords article for more information.

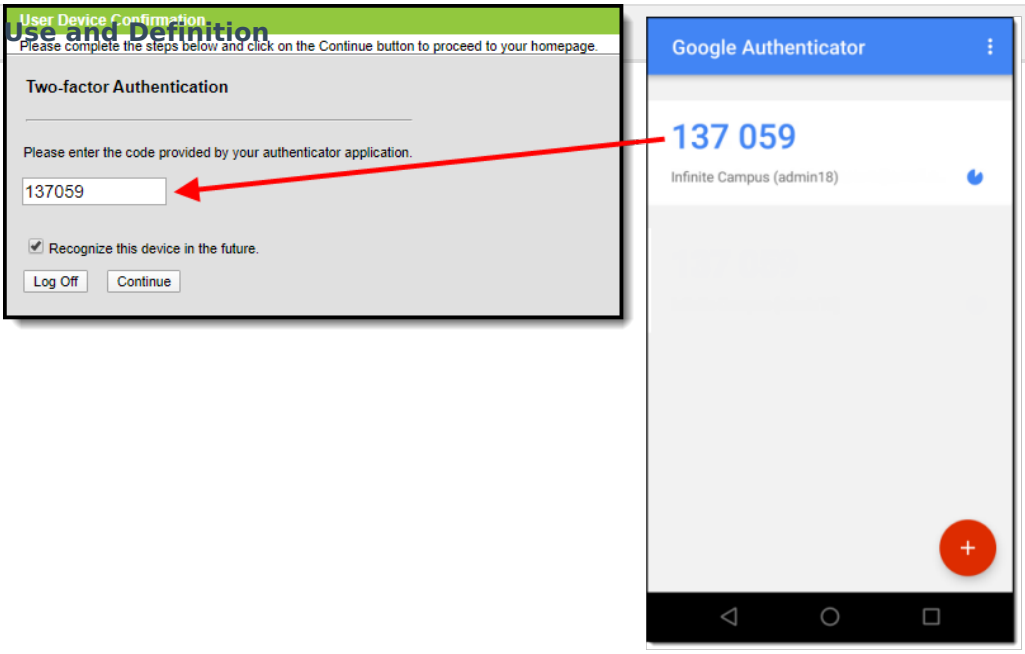
Field	Use and Definition
Force Change	If flagged, this checkbox indicates the user will be required to update his/her password at the next login. Once the password is updated, the system will uncheck this box automatically.
Expires Date	If a date is entered in this field, the user's account will expire on 11:59 PM of this date. This tool is often used to automate account management for temporary staff.
Homepage	This field indicates which interface the user name and password allow access to: • ***Campus Application*** - for district employees • ***Campus Parent Portal*** - for parents • ***Campus Instruction*** - for teachers and staff • ***Campus Student Portal*** - for students (enhanced features and optimized for mobile devices and tablets) • ***Public Store*** - for Public Store customers who are **not** district employees, students, or staff. Campus does not recommend manually creating this type of account. When someone creates an account on the Public Store, their name and email address are saved in Campus in the Demographics tool and Campus creates and assigns the *Public Store* Homepage to their user account.

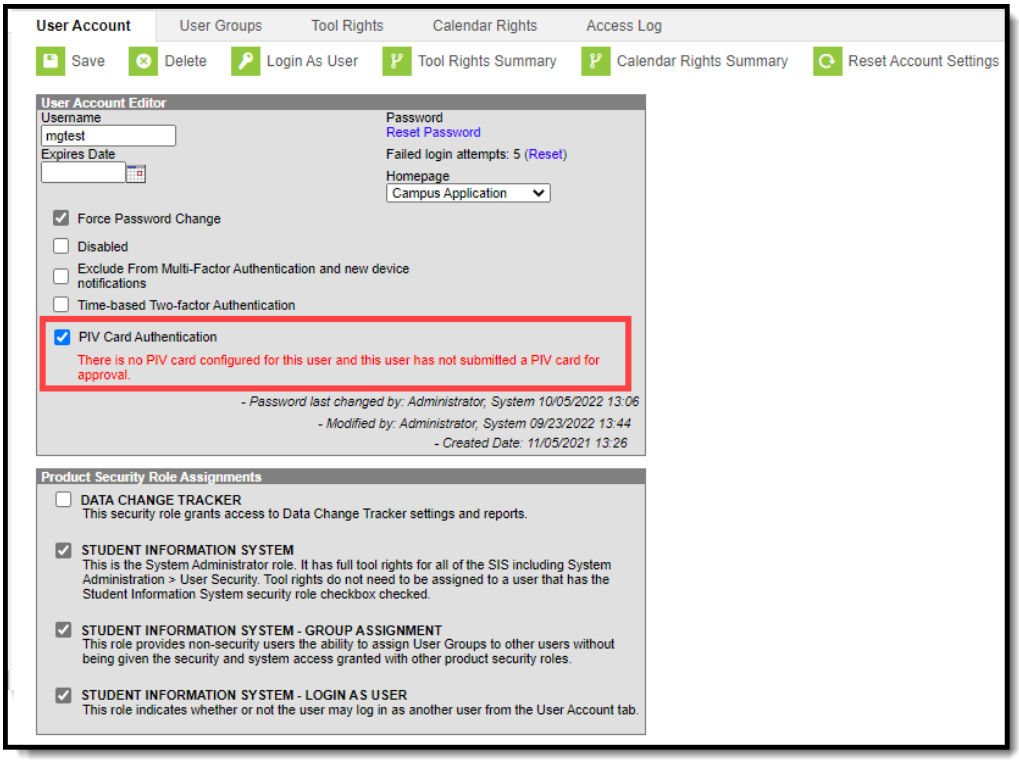
Field	Use and Definition
Disabled	If flagged, this checkbox indicates the user will not be able to access his/her account, even if the proper credentials are entered. When disabled, a notification message appears to the user.  In addition, disabled users appear in red font on the Search tab and on the Membership Summary tab of any groups to which they are assigned.  

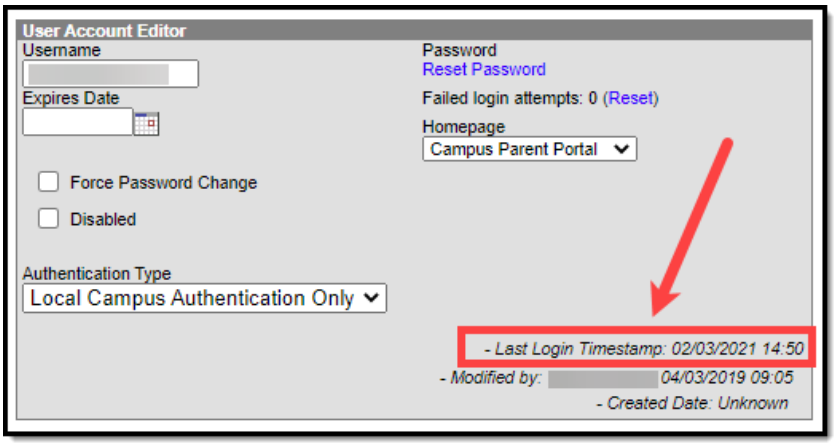
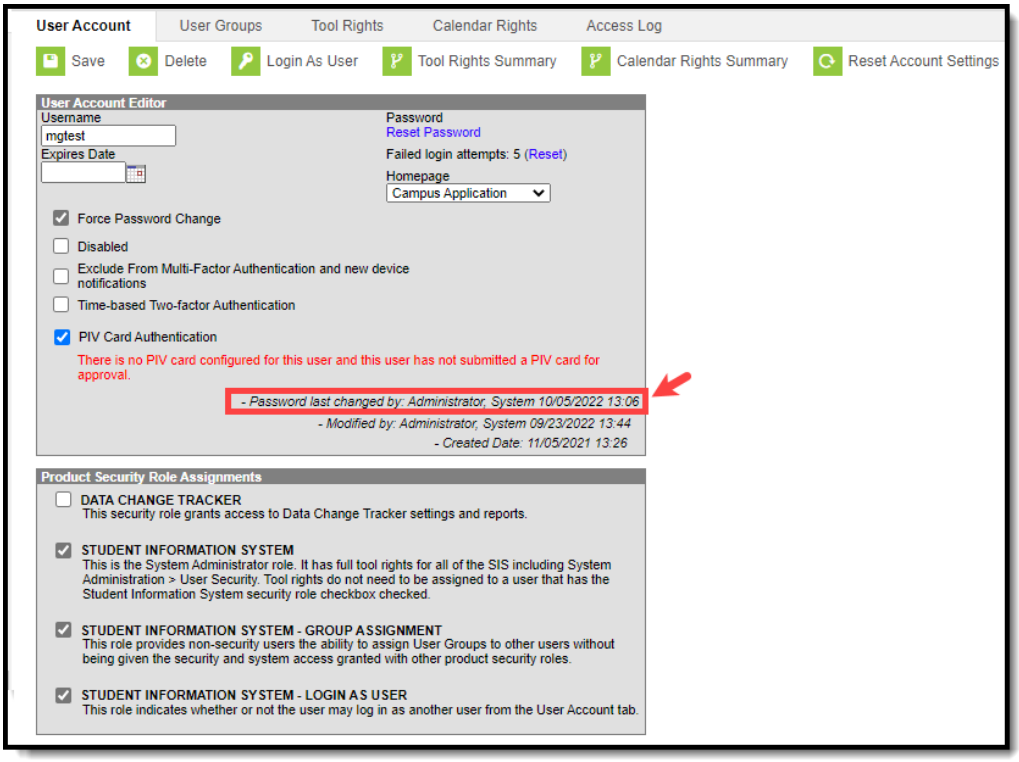
Field	Use and Definition
Exclude from Multi-Factor Authentication and new device notifications	This preference allows you exclude individual user accounts from requiring Time-based Two Factor Authentication (when enabled) as well as preventing users from receiving notifications when logging in using a new device. This option should only be used when absolutely necessary and only applied to the least amount of accounts necessary. This setting is not available for user accounts set with a Homepage of Campus Parent Portal, Campus Student Portal, or School Store as it does not apply to these types of accounts. 
Time-based Two-Factor Authentication	As an increased layer of protection for Infinite Campus accounts, all non-Campus Portal 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 authenticate their account using a device and an authenticator application (such as Google Authenticator, Authy, LastPass, etc). This setting is not available for user accounts set with a Homepage of Campus Parent Portal, Campus Student Portal, or School Store as it does not apply to these types of accounts.

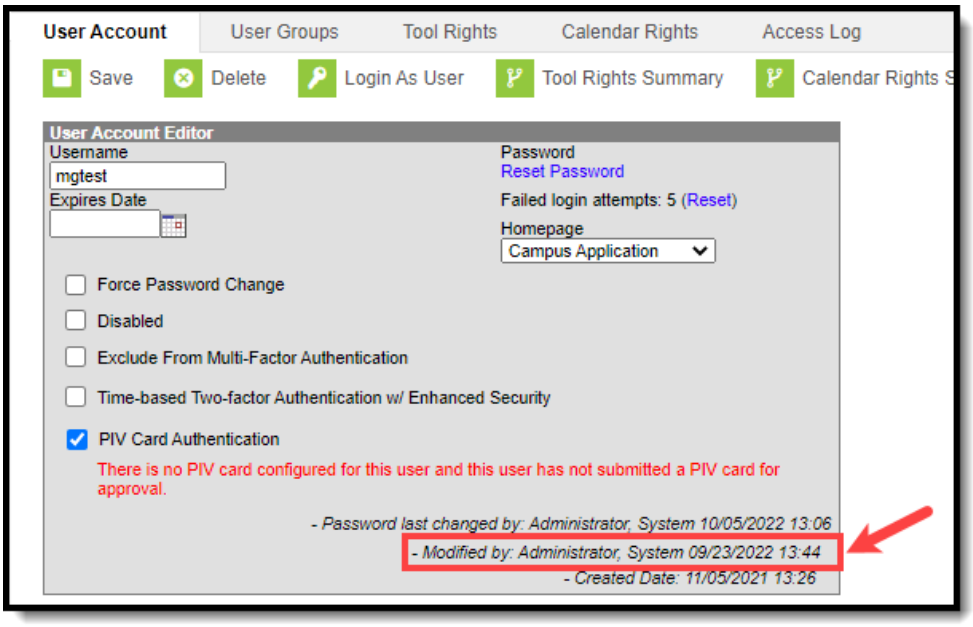
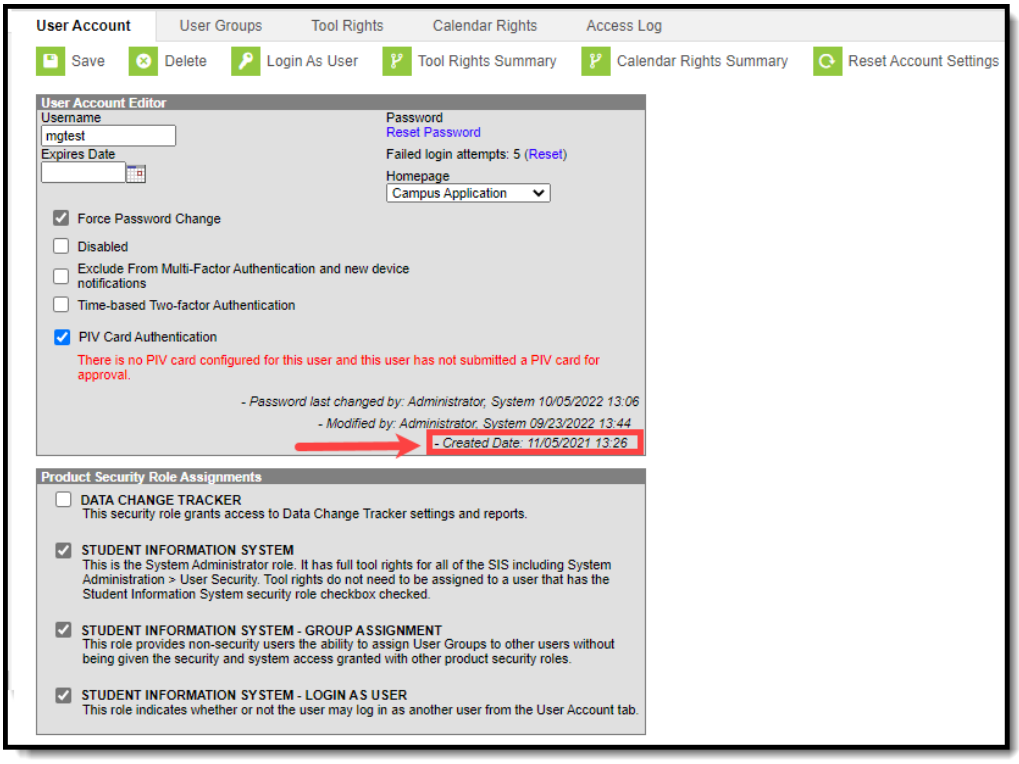
Field	Use and Definition
	If you experience any issues authenticating, know that your device must be in-sync with the actual time in order to authenticate. Compare the time showing on your device to the actual time (https://www.time.gov). If time on your device is out of sync, you can correct this in 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 this feature: 1. Mark the **Time-based Two-factor Authentication** checkbox 2. Select the frequency in which the user must use an authenticator app when logging into Infinite Campus (30 minutes, Day, Week, Month). For example, if a user logs in using an authenticator and this field is set to 30 minutes, after 30 minutes has passed, the next time the user attempts to log into Infinite Campus they will be required to go through the authenticator process. 3. Click **Save** Device-based two-factor authentication is now enabled for this user account.  Once enabled, the next time the user attempts to log into Infinite Campus they will see a screen displaying a unique QR Code and Text Code.

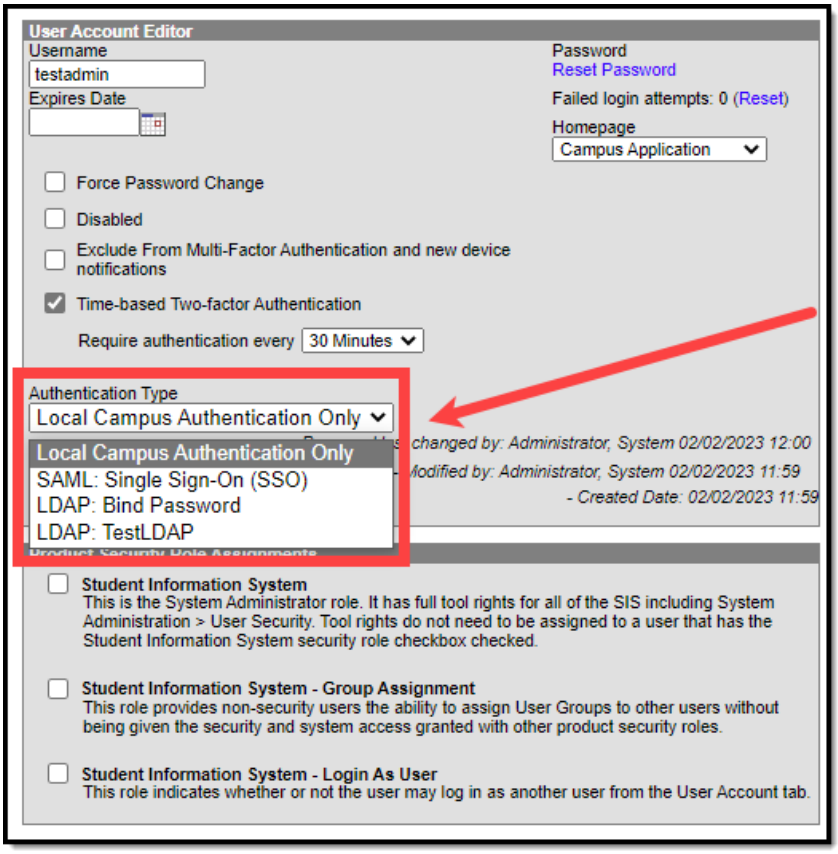
Field	Use and Definition
	Using a device (such as cell phone), the user must download an authenticator app (such as Google Authenticator, Authy, LastPass, etc) and use the app to scan the **QR Code** or enter the **Text Code**. This will register the device and tie it to their Campus account. Once they 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.  Based on the frequency of when they need to authenticate (30 minutes, Day, Week, Month), the user 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.

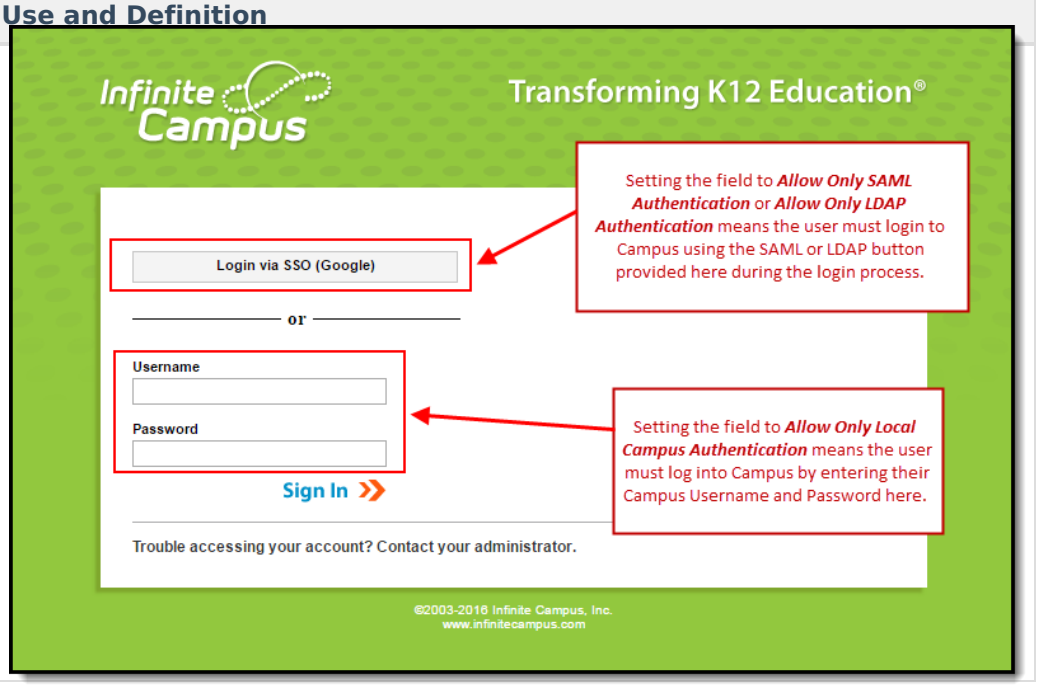
Field	Use and Definition
	

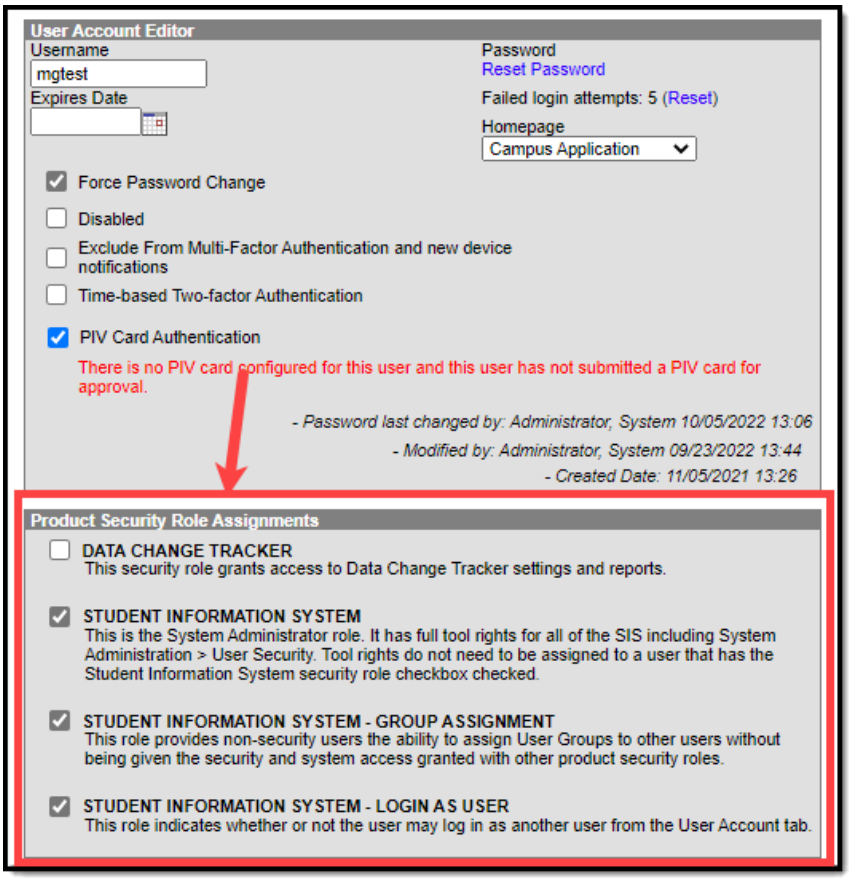
Field	Use and Definition
PIV Card Authentication	The Enable PIV Authentication field enables or disables the ability for the user to register and use a PIV card to log into Infinite Campus. This setting is not available for user accounts set with a Homepage of Campus Parent Portal, Campus Student Portal, or School Store as it does not apply to these types of accounts.  Note: This field is only available if the **Enable PIV Authentication** field in Login Security Settings is set to *Yes*. 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

Field	Use and Definition
Last Login Timestamp	This field indicates the exact date and time the user last logged into Infinite Campus. This field is not impacted by Login as User functionality. It only registers when the user themselves log into Infinite Campus. 
Password last changed by	This field indicates who was the last user to change this user's password and exact date and time in which the password change occurred. 

Field	Use and Definition
Modified by	This indicates the last person to modify the user's account and the date and time in which the change occurred. 
Created Date	This indicates when the user account was created. This date is populated by any method used to create the user account (e.g., student/staff automation, imported new user, Quartz job, etc). This field is also available within Ad Hoc Reporting. 
Authentication	

Field	Use and Definition
Authentication Type	This field determines how the user is required to authenticate and log into Campus. Users are forced to either log in using: • Their Campus ID and password (**Allow Only Local Campus Authentication**) • Their SSO username and password (**Allow Only SAML Authentication**) • Or their LDAP username and password (**Allow Only LDAP Authentication**) The default value in this field is set via the Authentication Type Droplist Default preference found in System Preferences. This field is only available if SAML SSO authentication and/or LDAP is enabled for your district. Please note that when setting a User Account to "Allow Only SAML Authentication", Cafeteria Serve only authenticates with a local Campus or LDAP account and the Schedule Wizard will authenticate with a SSO enabled account but requires a re-login to open a saved trial. For more information about SAML SSO functionality, see the SAML Management article. For more information about LDAP, see the LDAP Authentication article.  The value set in this field determines the method the user users to log into Campus (click image below).

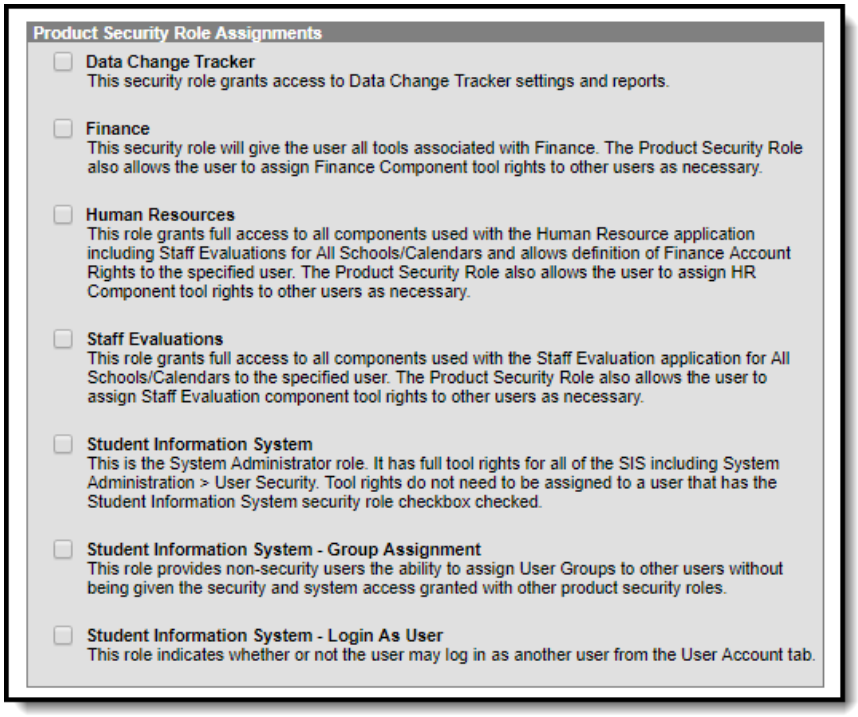
Field	Use and Definition
	

Field	Use and Definition
Product Security Role Assignments	Product Security Roles determine whether a user may assign Tool Rights to other Campus Application users. Product Security Roles are assigned to users on each person's User Account tab.  This section only displays when "Campus Application" is selected in the **Homepage** dropdown list. Users assigned the Product Security Role automatically inherit all tool rights associated with the specific product. For more information about Product Security Role Assignments, see the Understanding Security Role Assignments section below.

Understanding Security Role Assignments

Product Security Roles determine whether a user may assign Tool Rights to other Campus Application users. Product Security Roles are assigned to users on each person's User Account tab. For a detailed explanation of each role, see the following articles.

- Single-Product Environment (Campus SIS Only)
- Multi-Product or Premium Product Environment



Assigning Calendar Rights

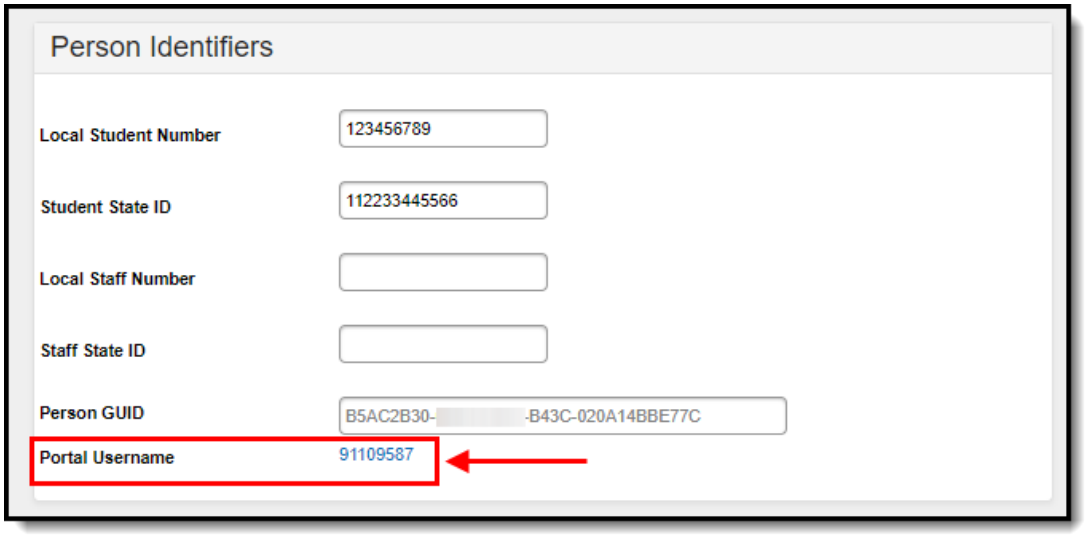
Calendar rights are assigned and managed via the Calendar Rights tab per user and/or user group.

To grant calendar access which mirrors the access granted via the previous **All Calendars** checkbox (access to view and modify all data within all calendars in the district), provide the user with Calendar Rights where **School** is set to 'All Schools', **Calendar** is set to 'All Calendars', **Year** is set to 'All Years', and the **Modify Rights** checkbox is marked (see image below).

> See the Calendar Rights tab article for more information.

Identifying a Person's Campus Portal Username

You can look up a person's Campus Portal username by going to Census > Person > Demographics > Person Identifiers > Portal Username. This may help when troubleshooting issues such as assisting a person who forgot their username .



Related Tools

Tool	Description
Account Security Preferences	This tool allows you to control various functionality such as resetting of passwords, restricting the ability for Product Security Users to log in as other people, auditing of users, and the automatic creation/disabling of student and staff accounts.
User Account Batch Wizard	This tool allows you to batch create student and staff user accounts using the census email address or a username patterns, enable student and staff user accounts, disable student and staff user accounts, or force a password reset for student and staff user accounts.
User Account Automation Log	This tool allows you to view detailed information about user account username modifications, user account creation failures, and accounts automatically disabled via preferences set in the Account Security Preferences tool.
User Group Report	This tool provides high-level and detailed information about which user groups exist, all tool rights and calendar rights assigned to each user group, and which user groups are assigned to which Staff Account Automation rules.
Product Security Role Report	The Product Security Role Report provides a list of all users who have been granted specific Product Security Roles.