Manage User Account Passwords

Last Modified on 09/18/2026 9:56 am CDT

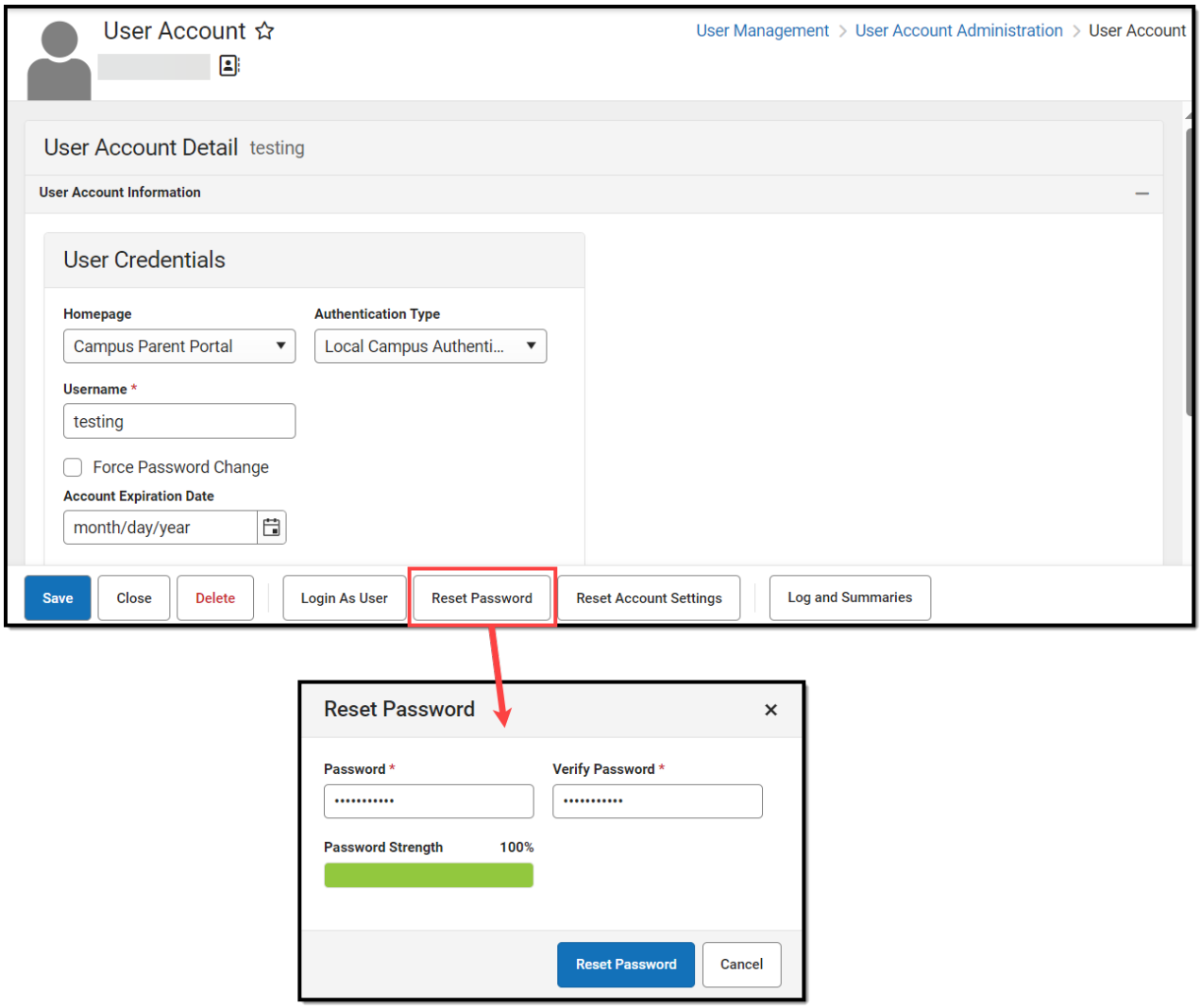
User account passwords can be managed using a number of tools throughout Infinite Campus. This article describes the numerous options and scenarios around account password management.

This article includes the following topics:

Modifying Individual User Passwords

Individual user account passwords can be manually modified by an Administrator within each person's user account.

> Only System Administrators should have access to user accounts.



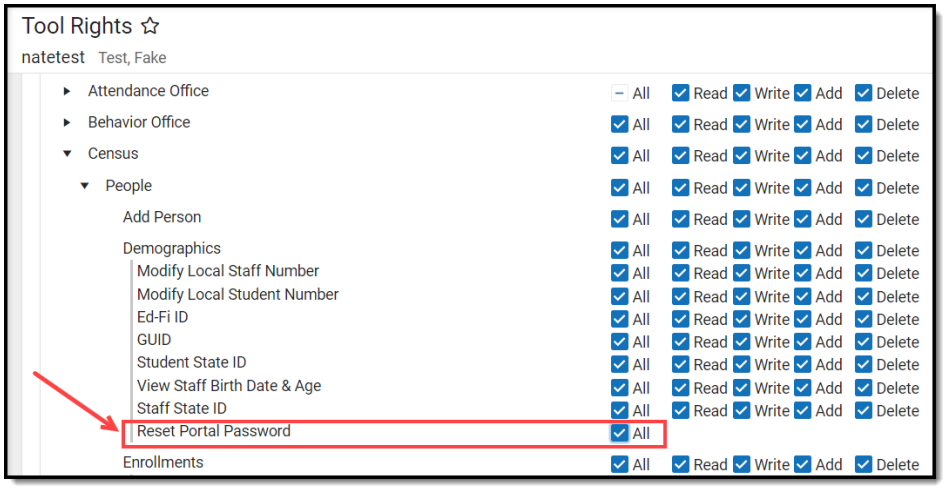
To change your password, select the **Reset Password** button, enter a **New Password** and

Verify the Password. The box beneath the first password field indicates the new password's strength with red meaning weak, yellow meaning medium, and green meaning strong. Users will not be allowed to save weak or medium passwords.

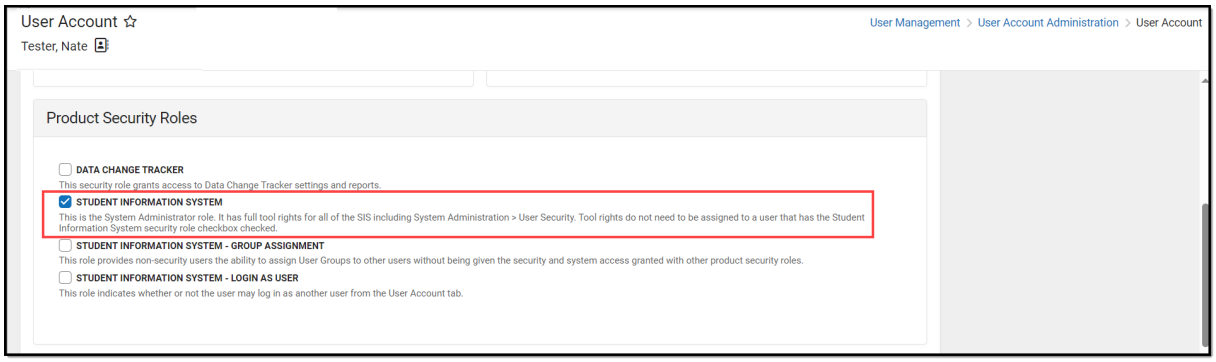
An 8-character password must include at least one letter, one number, and either a special character or a capitalized letter. If the password contains only letters and numbers (no capitals or special characters), it must be at least 9 characters long. The **Minimum Password Character** and **Password History Length and Expiration Time** Account Security Preferences will also impact new passwords after a reset.

Staff members who have proper calendar rights and one of the following:

- Assigned the 'Reset Portal Password' sub-right



- Assigned the Student Information System (SIS) product security role



- Assigned proper User Account tool rights



have the ability to reset a parent or student's account password by selecting a Reset Password hyperlink found to the right of the Portal Username in the Person Identifiers section of the Demographics tab (see image below).



Suggestions for Creating a Strong Password

Complex, tricky passwords are not always strong passwords and can be difficult to remember. For example, TheBr0wnC@t is a stronger password than !@#$%&() because TheBr0wnC@t uses a combination of character types and is long, whereas !@#$%&() uses only symbols and is short. A computer program can crack !@#$%^&() easier than it can crack TheBr0wnC@t.

When creating a password, consider the following:

- **Content** - Use a short two or three-word sentence as your password.
- **Length** - Make your passwords long (8-10 characters).
- **Combination** - Include letters, punctuation, symbols, and numbers.

- **Uniqueness** - Do not use your username or words found in the dictionary.

After a password is reset, creating a new 8-character password must include at least one letter, one number, and either a special character or a capitalized letter. If the password contains only letters and numbers (no capitals or special characters), it must be at least 9 characters long. The Minimum Password Character, Password History Length, and Expiration Time Account Security Preferences will also impact new passwords after a reset.

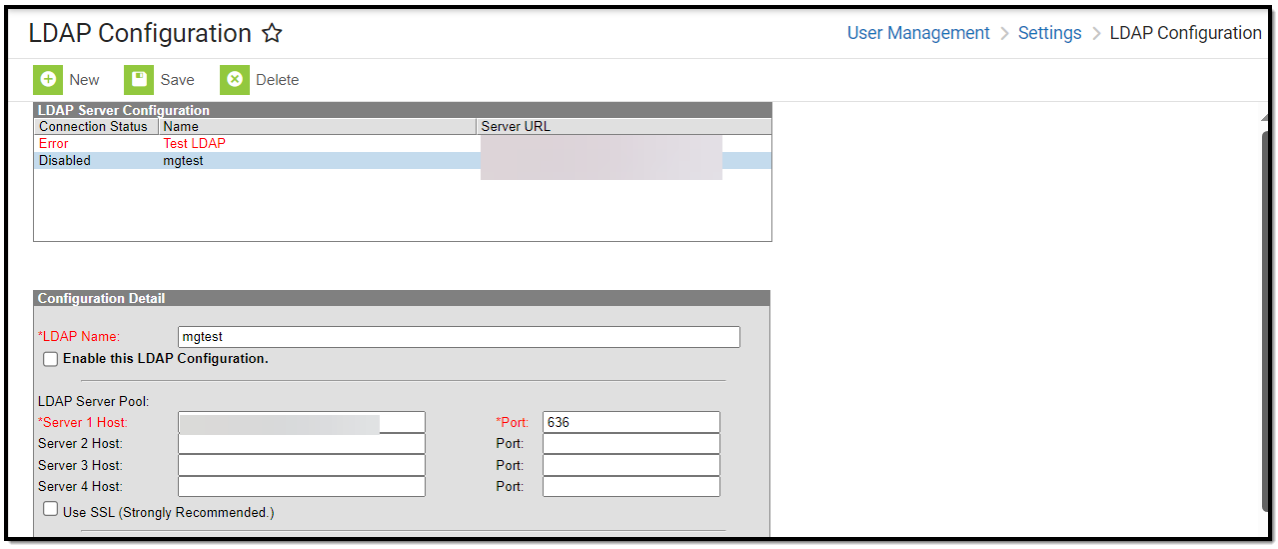
Managing Passwords via LDAP Authentication

Tool Search: LDAP Authentication

User account passwords can also be linked to a district's Active Directory using the LDAP Authentication tool. Schools and districts using LDAP Authentication need to manage and update all user account passwords within their Active Directory.

Districts can enable Password Reset and E-signature if they have LDAP to begin using the Online Meal Benefits Application. LDAP environments will not be affected by enabling Password Reset functionality.

A change to a Campus password is ignored if the account is linked to an LDAP server. The only way to change the login password for an LDAP-managed account is to change it on the LDAP server.

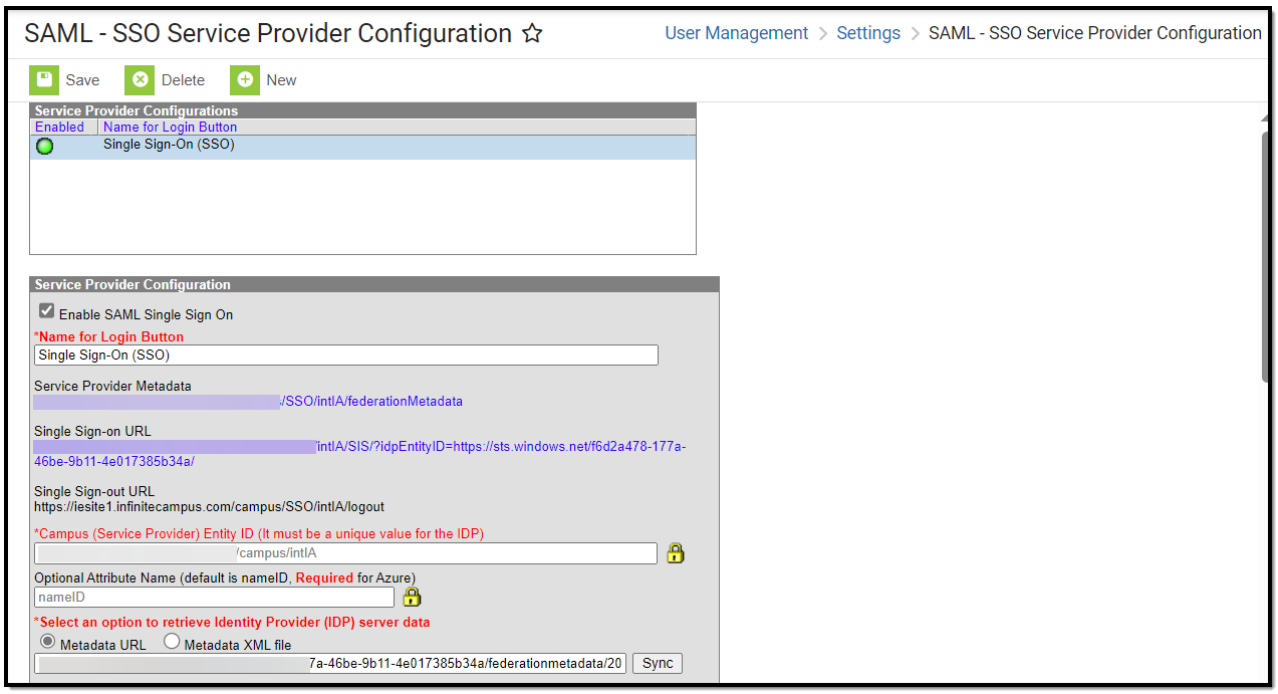


Managing Passwords via SAML SSO Authentication

Tool Search: SAML SSO Service Provider Configuration

User accounts can be authenticated via a SAML SSO IDP (such as Active Directory Federated Services (ADFS)). SAML SSO functionality is enabled and configured in the SSO Service Provider Configuration tool, and Campus accounts are tied to SAML SSO authentication via the User Account Type Wizard.

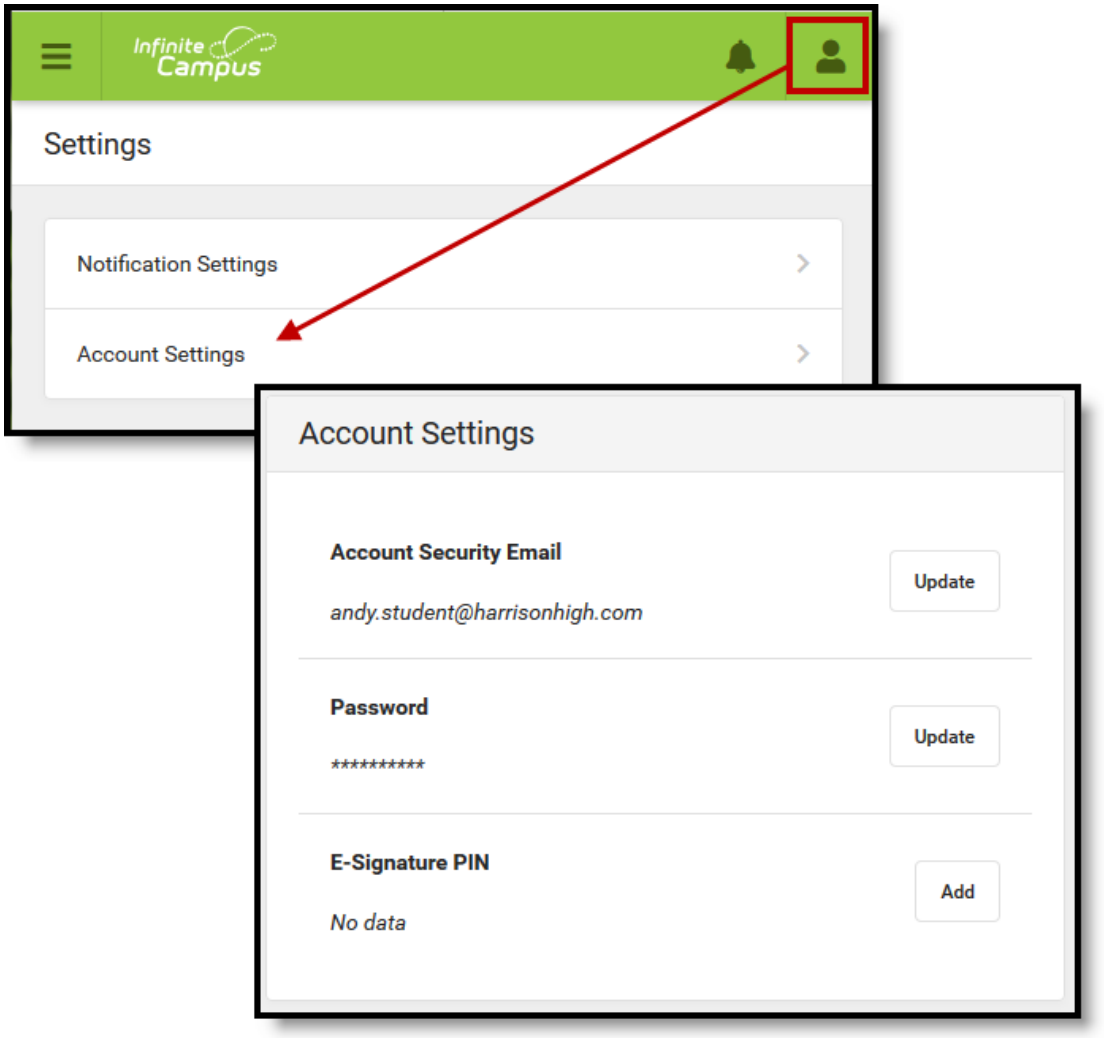
All account passwords and credentials are managed outside of the Infinite Campus product by a district's Network Administrator and the IDP.



Managing Password Preferences within the Student and Parent Portal

Account settings allow users to update their security email on record or to change their Password and E-Signature PIN. From the User Menu, select Settings, then Account Settings.

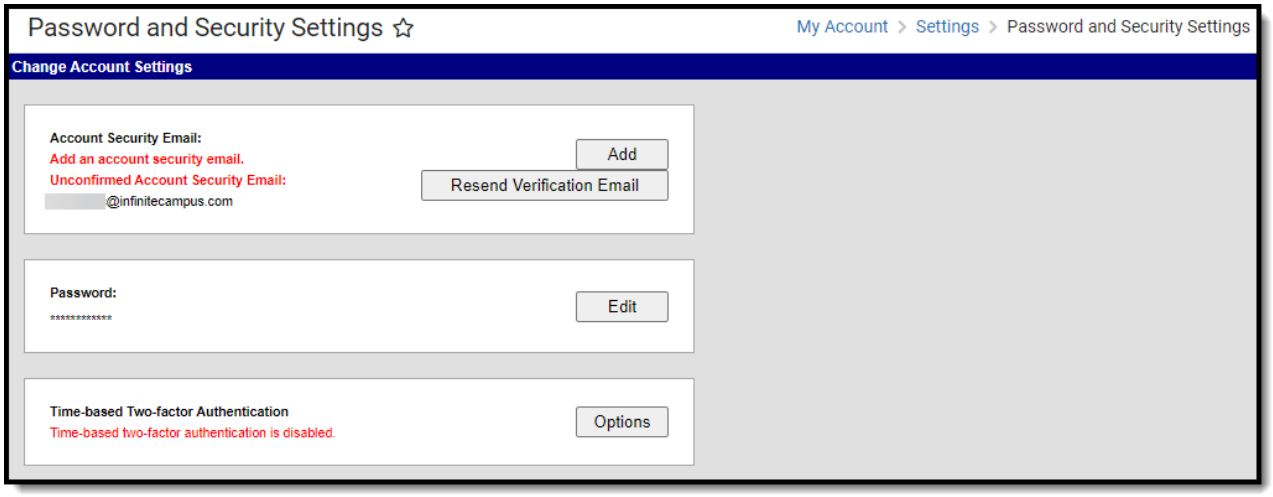
- The Account Security Email is the email used if a user forgets their username or password.
- Strong passwords are required, meaning they should include a mix of letters, numbers, and other characters to make them more secure.
- E-Signature PINs are used to electronically verify and sign Meal Benefit Applications. This field is only available if enabled by the district.



For more information, see the Campus Student Portal and Campus Parent Portal articles.

Managing Your Own Password within Infinite Campus

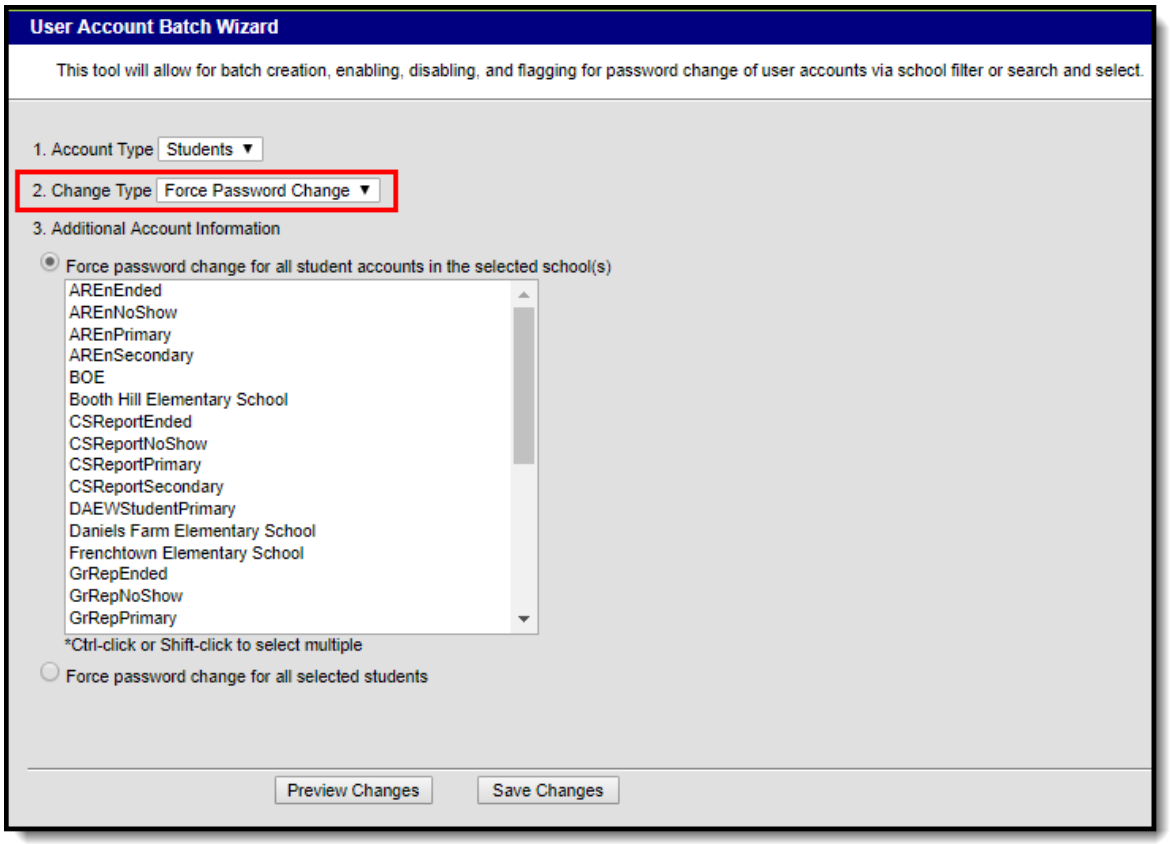
Non-Portal users can manage their account security preferences via Password and Security Settings. This tool behaves differently depending on whether your district has enabled Password Reset.



Forcing a Password Change for all Student Accounts

Tool Search: User Account Batch Wizard

You can force a password change for all students in a school or for a specific set of students using the User Account Batch Wizard.

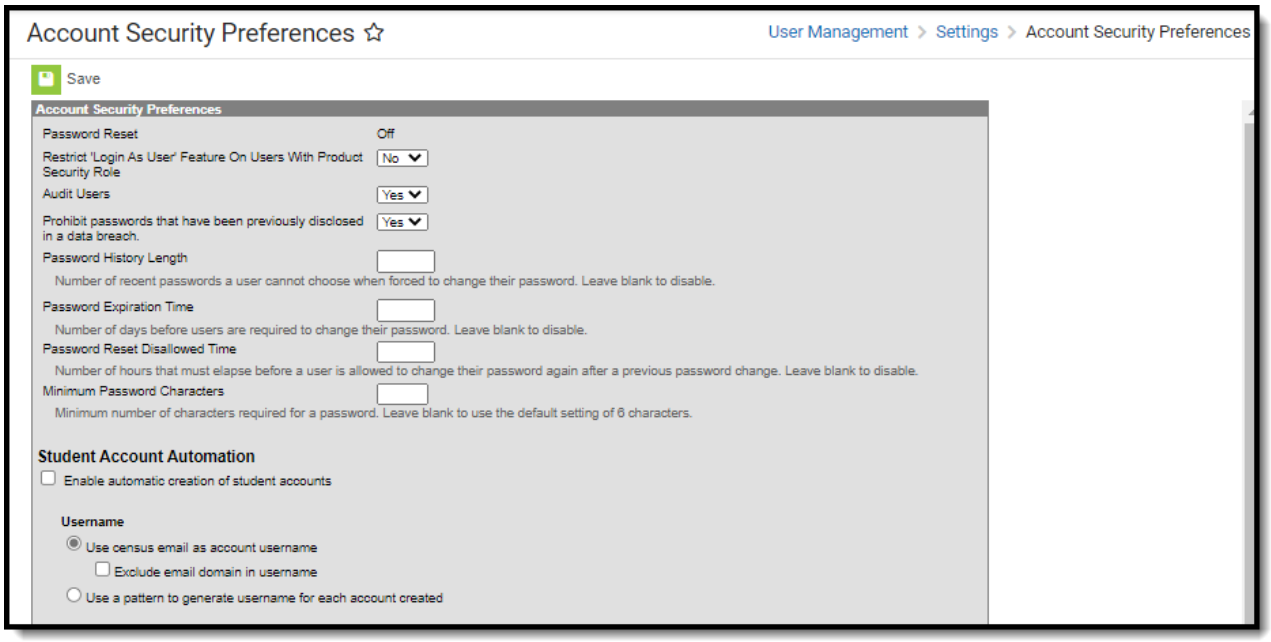


Password-Related System Preferences

Tool Search: Account Security Preferences

The Password Reset preference indicates whether you have Password Reset enabled. A value of Yes means Password Reset functionality is enabled. This preference cannot be changed once set. This value is established in the Password Reset Configuration tool.

The other preferences in the Account Security Preferences tool are important and should be set according to your needs, but they do not directly relate to passwords within Campus.



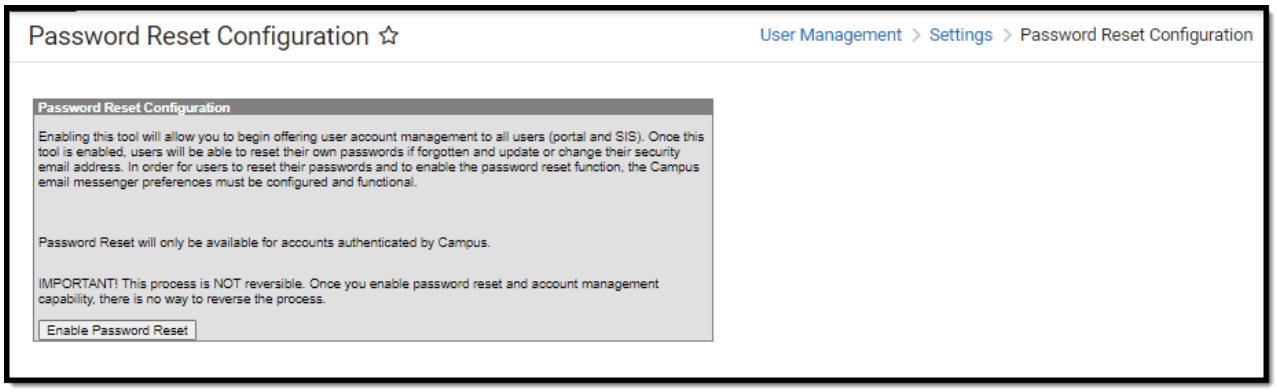
Enabling Password Reset Functionality

Tool Search: Password Reset Configuration

Password Reset functionality is enabled in the Password Reset Configuration tool. This functionality allows Campus application and Portal users to reset their account passwords without Administrator intervention.

Before enabling Password Reset functionality, consider the following:

- Once enabled, it cannot be disabled or reversed.
- Password Reset functionality is only available for accounts authenticated by Campus (not LDAP).
- E-Mail Messenger must be enabled prior to enabling Password Reset functionality.
- Ensure parents are given their own Portal accounts to view and manage Portal information. Because each individual Portal account will need to have new security information established once Password Reset functionality is enabled, providing parents with their own account prevents them from having to set up each student's Portal account they may log into.



To enable Password Reset functionality, click the **Enable Password Reset** button. Users will encounter a pop-up message, requiring them to confirm this action. Select OK to enable password reset functionality.

Once the Enable Password Reset button is selected and the action is confirmed, the following will occur:

- All passwords will appear hidden throughout Infinite Campus.
- All passwords must be strong. This means all users who do not have a strong password will be required to change it to a strong one the next time they change their password or use the password reset function.

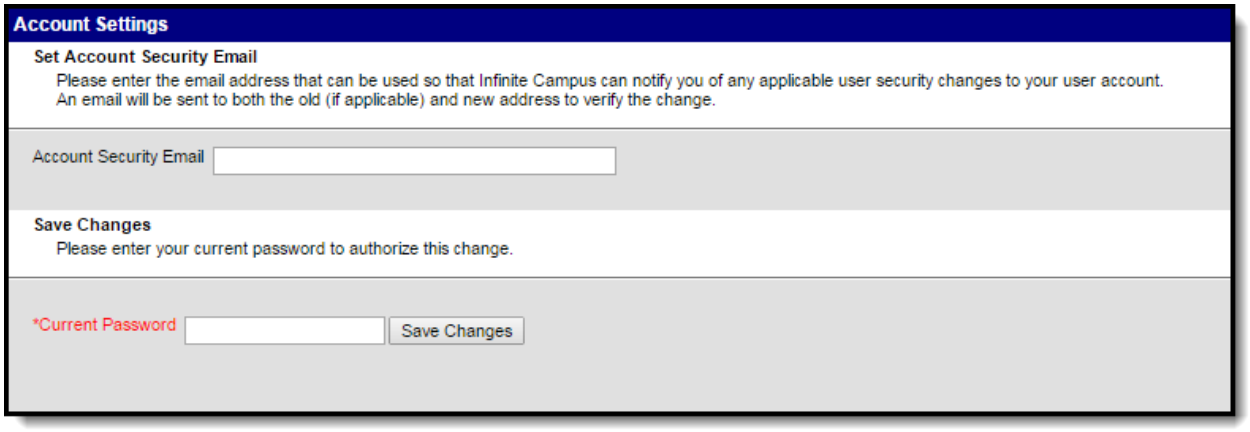
  An 8-character password must include at least one letter, one number, and either a special character or a capitalized letter. If the password contains only letters and numbers (no capitals or special characters), it must be at least 9 characters long. The Minimum Password Character, Password History Length, and Expiration Time Account Security Preferences will also impact new passwords after a reset.

- Password reset functionality also automatically makes the Password Reset System Preference/Account Security.

To create text to display to users on the login page, see the Login Page Preferences article.

Existing Users Logging into Campus After Password Reset is Enabled

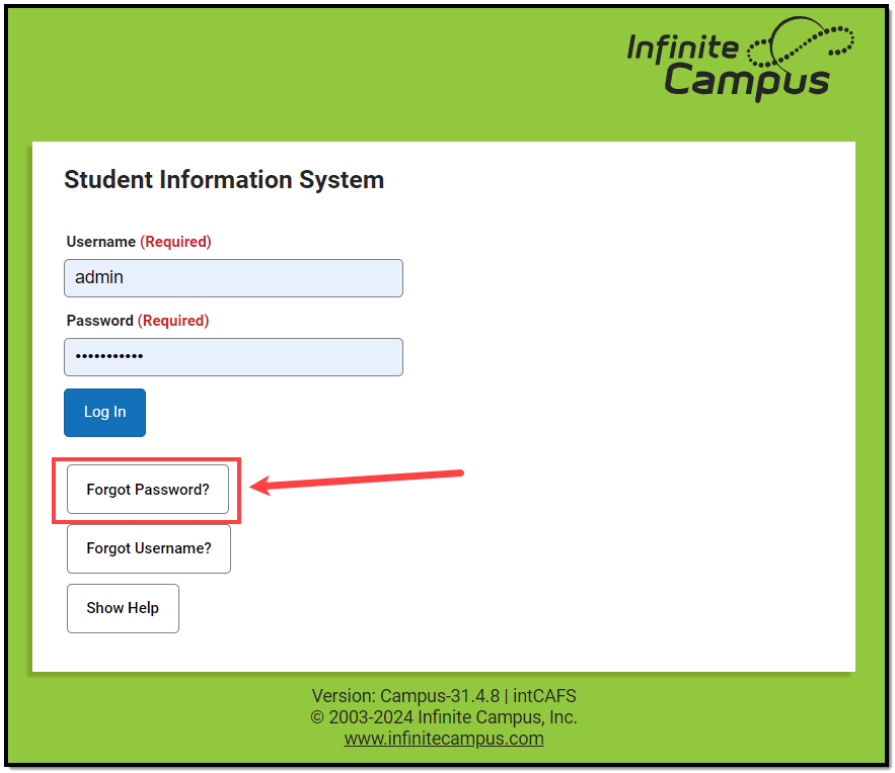
All users logging in to Campus for the first time after Password Reset functionality is enabled must enter an **Account Security Email** address. This ensures that the password/username recovery process, as well as the account notification process, has a valid email address to use.



Recovering Passwords via the Forgot Your Password Link

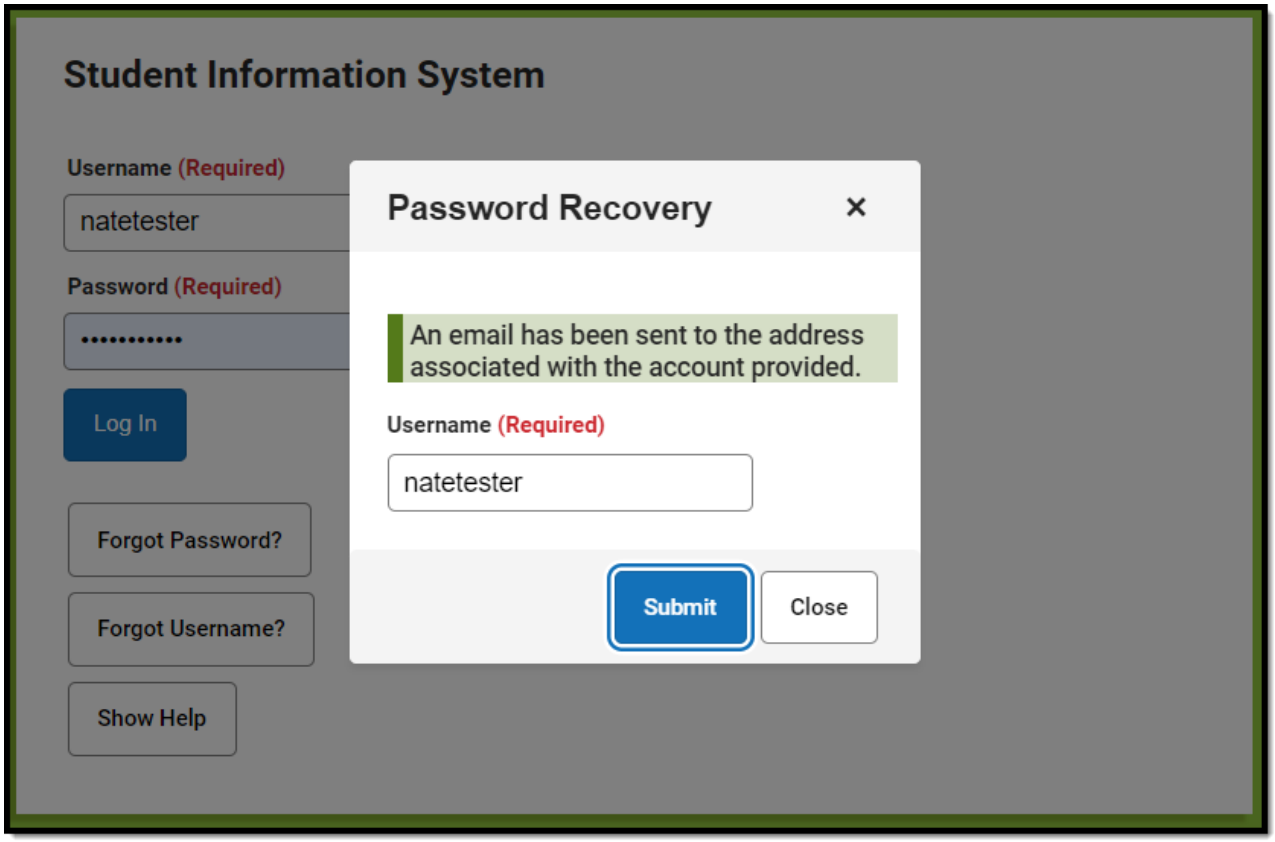
If a user is part of a school or district with Password Reset enabled, they may recover their password using the "Forgot Password?" link.

If the school or district does not have Password Reset functionality enabled, a message will appear informing users of the steps they must take to recover their password (often this means calling the school or district to correct the issue).

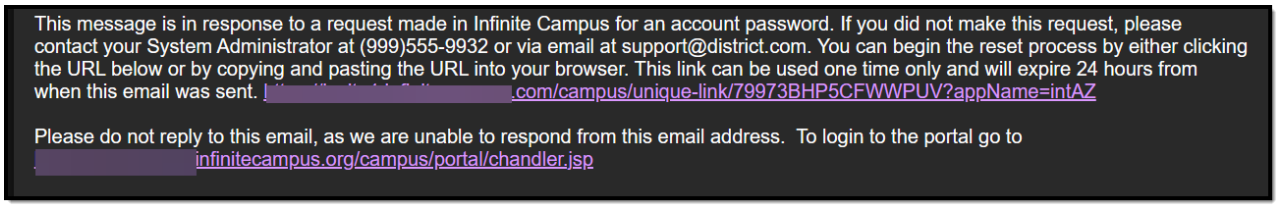


Once the **Forgot Your Password?** link is selected, enter your Campus username in the field below and click **Continue**. A message will appear, informing you to check your email (sent to your recovery email address).

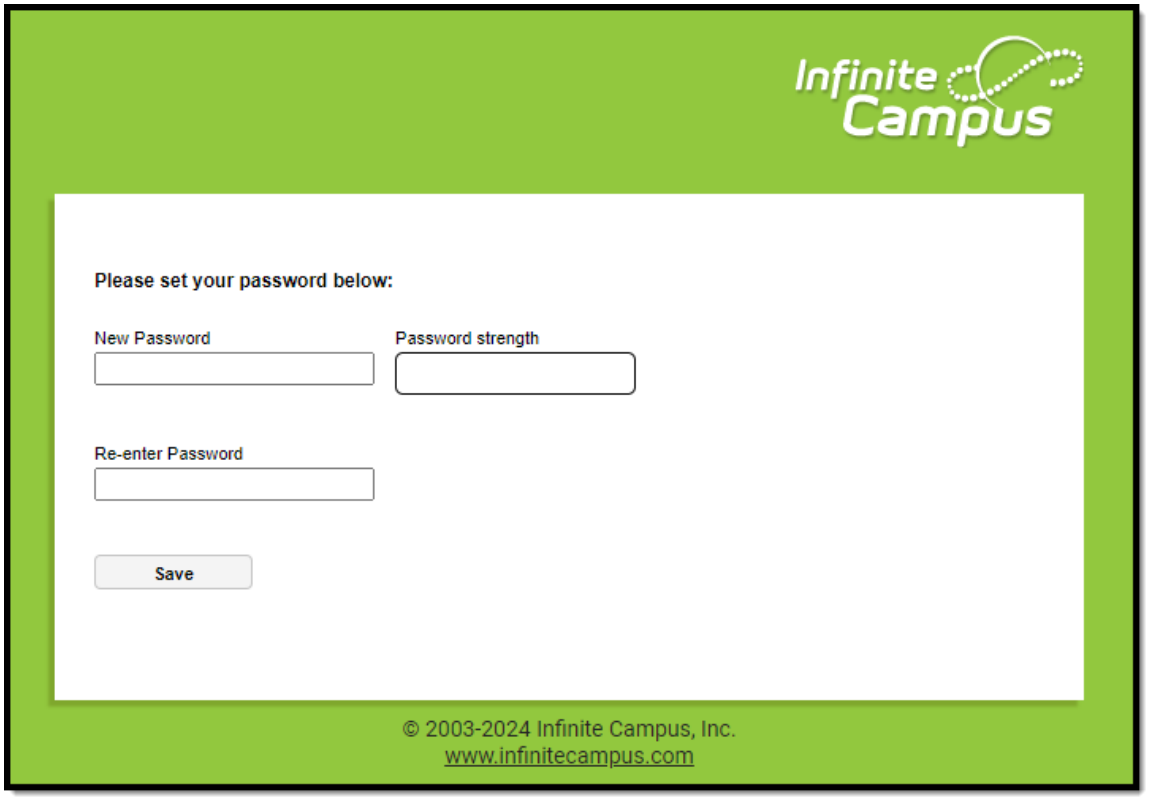
It is critical that the Recovery Email address established in the Account Settings tool is valid. Users with an invalid email address will be unable to finish the password recovery process. The recovery email address is established during the initial setting of preferences, as well as managed on the Account Settings tool (for Campus users) or Campus Parent Portal.



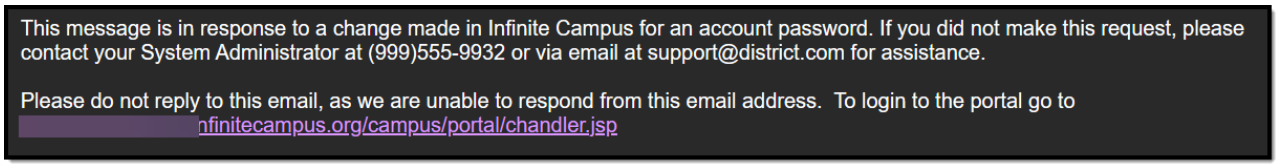
Open the email and select the unique URL provided. This will direct you to an editor where you can enter and save a new Campus account password.



Enter a **New Password** (ensuring the password is considered strong), **Re-enter the Password**, and click the **Save** button.



Once a new password has been entered and saved, you will receive an email confirming the change. This email is a safety precaution to ensure you are made aware that your password has been changed in case it was changed without your knowledge or consent.



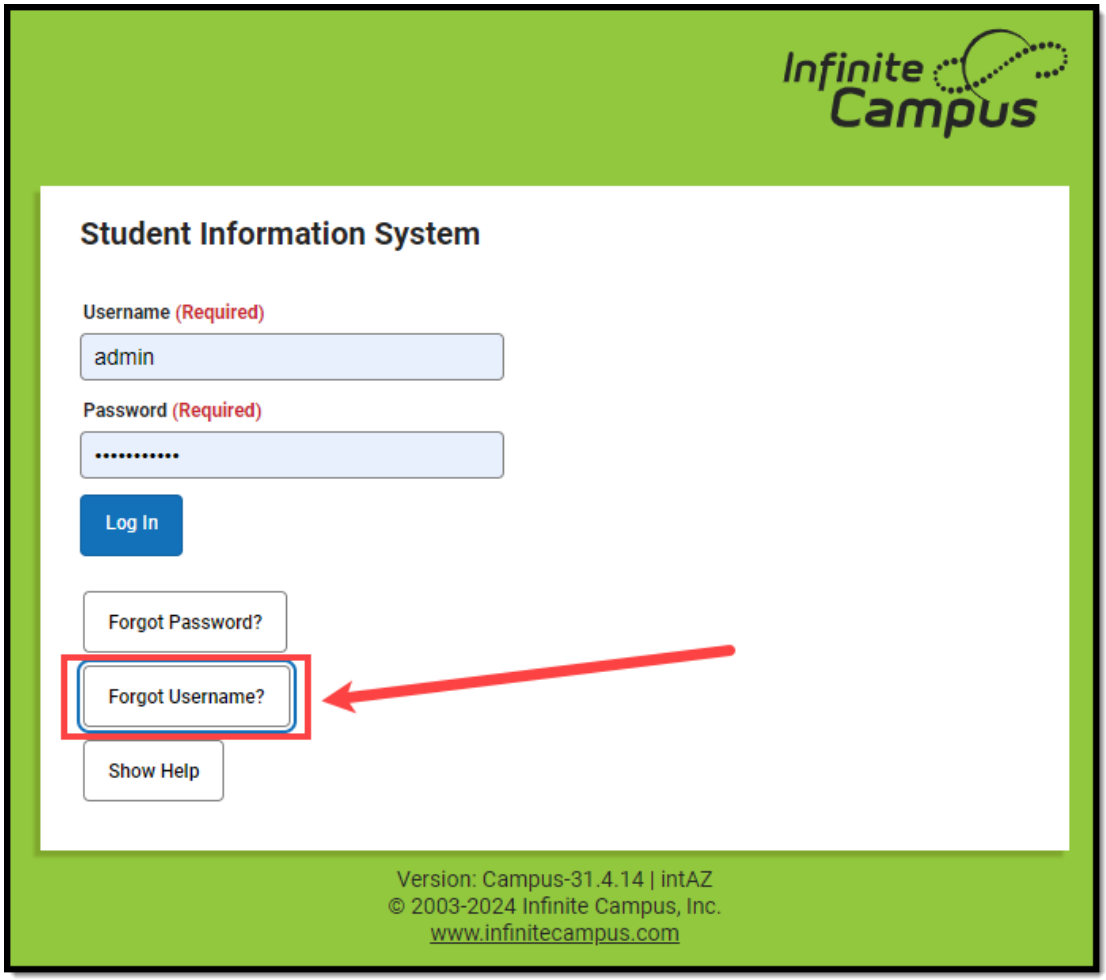
Recovering Usernames via the Forgot Your Username Link

If a user is part of a school or district that has Password Reset functionality enabled, they may recover their username using the **Forgot Username?** button.

Staff members with proper tool rights to the Demographics tab can also look up a user's Campus Portal username on their Demographics record.

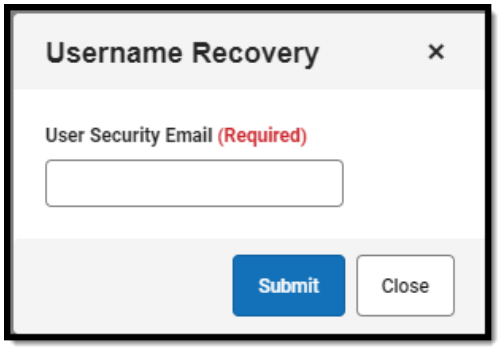
Users can request their forgotten username up to five times per day. On the sixth try, the user

will be locked out of their account and will need to wait until the next day to try again.

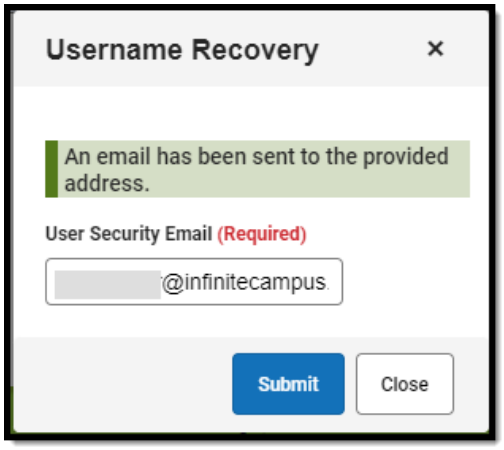


Once the **Forgot Username?** link is selected, enter your **User Security Email** address, and click the **Submit** button.

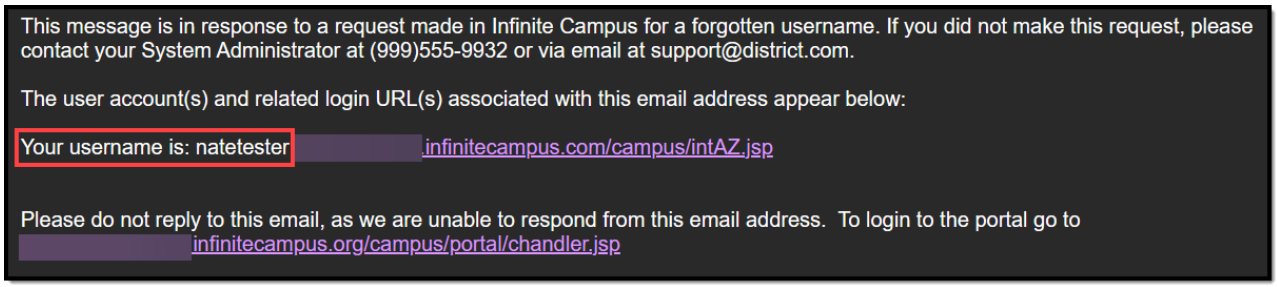
The recovery email address is established during the initial setting of preferences and is managed on the Account Settings tool (for Campus users) or Campus Parent Portal.



A message will appear, informing you to check your email.



You will receive an email with your current Infinite Campus username.



User Incorrectly Attempts to Log Into Campus Multiple Times

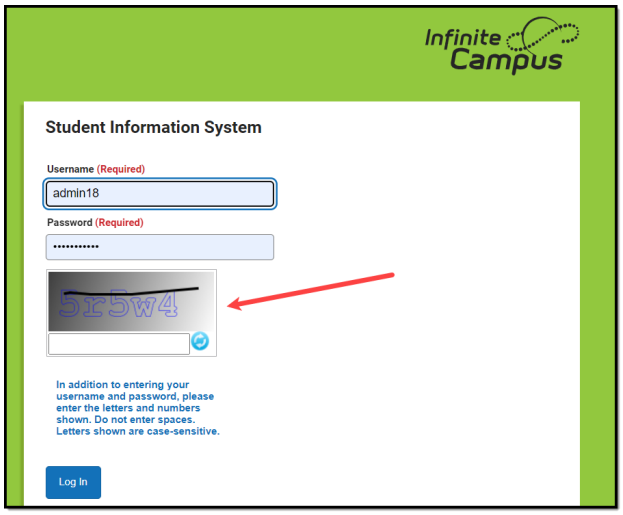
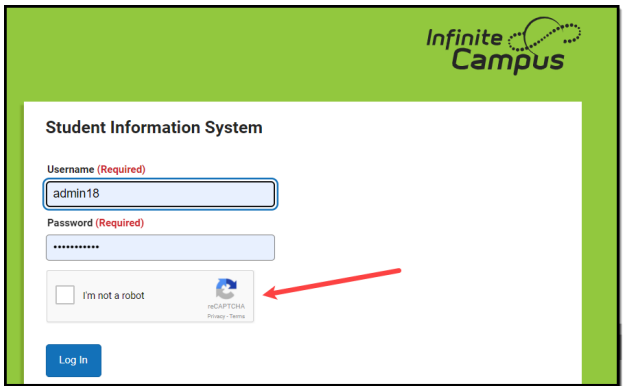
Users who incorrectly log into their account multiple times will be required to enter a CAPTCHA each time they attempt to log in. This feature prevents users from being locked out of their account after several failed login attempts and protects accounts from malicious bots and scripts.

The type of CAPTCHA displayed is dictated by the settings established in the Login Security Settings tool.

CAPTCHA functionality enforces case sensitivity for all letters other than C, O, P, S, U, V, W, X, and Z.

The audio challenge option for Google reCAPTCHA does NOT work properly in Microsoft Edge.

Below is an example of each available CAPTCHA:

Campus Captcha	Google reCaptcha
	

Enabling Login Alert Notification Emails

In an effort to increase security and Campus account awareness, the Login Security Settings tool allows users to enable login notification and verification code emails to alert users when someone logs into Campus using their account from an unknown device.

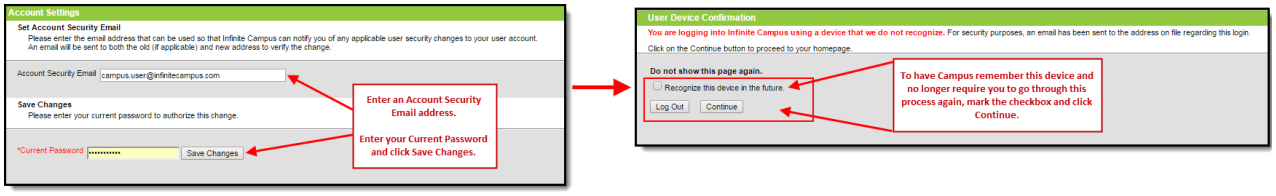
For more information about this functionality, please see the following:

- Enable Login Alert Notifications
- Enable Login Alert Notifications with a Verification Code

The image below shows a user setting up their Account Security Email and deciding whether Campus should remember the device for future logins.

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 Campus.



Below is an example of the email users will receive if someone logs in to their account from an unknown device.

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.

Identifying a Person's Campus Portal Username

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

