

Password Reset Configuration

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

Classic View: System Administration > User Security > User Preference Management > Password Reset Configuration

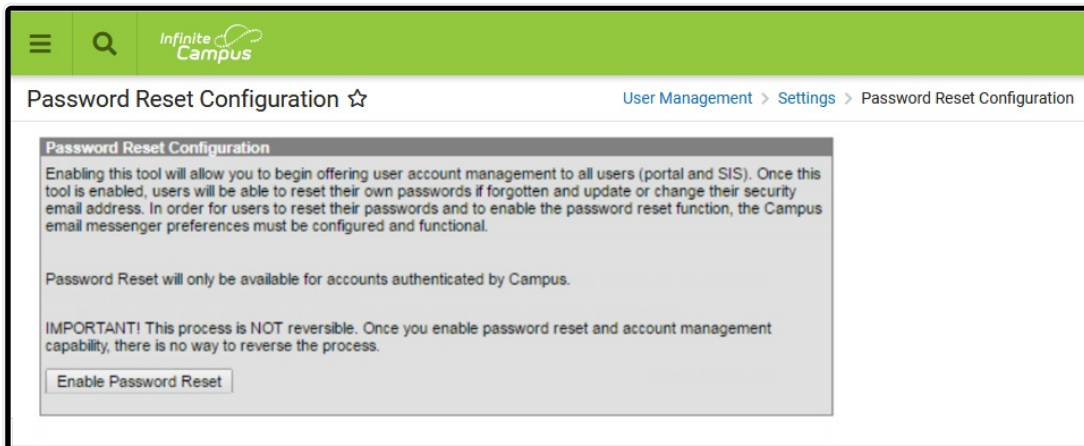
Search Terms: Password Reset Configuration

The Password Reset Configuration tool enables Password Reset functionality for all users. Password Reset allows Campus application and Campus Portal users the ability to reset their account password, as well as the ability to manage their account security email address and security preferences without the need for Administrator intervention.

Only users with a [Student Information System \(SIS\) Product Security](#) role are allowed to access and modify values in the Password Reset Configuration tool.

See the [Managing User Account Passwords](#) page for more information about the Password Reset workflow and related processes.

Once Password Reset functionality is enabled, this tool is hidden in the index and replaced with the [Login Page Preferences](#) tool.



Enable Password Reset

Before enabling Password Reset functionality, consider the following:

- [Messenger Email Settings](#) must be established.
- Once passwords have been enabled, it cannot be disabled or reversed.
- Password Reset functionality is only available for accounts authenticated by Campus (not

SAML). You can have LDAP and Password Reset enabled at the same time, however LDAP enabled accounts are not subject to the Password Reset process.

Enable Password Reset

1. Click **Enable Password Reset**.
2. Click **Save**.

Results

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

- All passwords for all users - school/district personnel, parents/guardians, and students - are hidden from view. No other user has the ability to see any user's passwords, including the System Administrator or other IT staff.
- For parent and student users, the next time they log into the Portal, they are required to configure a User Account Security Email (e.g., an account recovery email), which is sent if they do not remember their login credentials.
- For staff, [login alert notifications](#) can be set that send a verification code or a reset link to users who have forgotten their credentials.
- Passwords are forced to be "strong" passwords, and must include a variety of symbols, lowercase and uppercase letters, numbers, etc. Users who previously did not use strong passwords are required to create a new password that is considered "strong."

Password reset functionality also automatically changes the **Password Reset** preference (viewable on the [Account Security Preferences](#) tool) from Off to On, and cannot be modified.

Account Security Preferences ☆

Save

Account Security Preferences

Password Reset Off

Restrict 'Login As User' Feature On Users With Product Security Role

Audit Users

Prohibit passwords that have been previously disclosed in a data breach.

Password History Length

Number of recent passwords a user cannot choose when forced to change their password. Leave blank to disable.

Password Expiration Time

Number of days before users are required to change their password. Leave blank to disable.

Password Reset Disallowed Time

Number of hours that must elapse before a user is allowed to change their password again after a previous password change. Leave blank to disable.

Minimum Password Characters

Minimum number of characters required for a password. Leave blank to use the default setting of 6 characters.

Password Reset Configuration ☆

Password Reset Configuration

Enabling this tool will allow you to begin offering user account management to all users (portal and SIS). Once this tool is enabled, users will be able to reset their own passwords if forgotten and update or change their security email address. In order for users to reset their passwords and to enable the password reset function, the Campus email messenger preferences must be configured and functional.

Password Reset will only be available for accounts authenticated by Campus.

IMPORTANT! This process is NOT reversible. Once you enable password reset and account management capability, there is no way to reverse the process.

Enable Password Reset

Account Security Preferences ☆

Save

Account Security Preferences

Password Reset On

Restrict 'Login As User' Feature On Users With Product Security Role

Audit Users

Prohibit passwords that have been previously disclosed in a data breach.

Password History Length

Number of recent passwords a user cannot choose when forced to change their password. Leave blank to disable.

Password Expiration Time

Number of days before users are required to change their password. Leave blank to disable.

Password Reset Disallowed Time

Number of hours that must elapse before a user is allowed to change their password again after a previous password change. Leave blank to disable.

Minimum Password Characters

Minimum number of characters required for a password. Leave blank to use the default setting of 6 characters.

Automatic Update to Password Reset Preference

When viewing user account information, the user's password does not display. If that user cannot log in with their existing password, the IT contact can click the Reset Password link, and users are able to reset passwords on their own when logging into the system.

User Account Information ☆ User Management

smeTest A_User

Save Delete Login As User User Rights Summary Reset Account Settings

User Account Editor

*Username Password [Reset Password](#)

Expires Date

Force Password Change

Disabled

Exclude From Multi-Factor

Time-based Two-factor A

Change Password

Change Password

Type in the new password. Warning this will overwrite the existing password!

*New Password *Verify Password

100%

Reset Password

Password Reset Option

See the [User Account Messenger](#) article for additional information on communicating user

account- related emails to staff, parents and students.
