Account Security Preferences

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

Classic View: *System Administration > User Security > User Preference Management > Account Security Preferences*

Search Term: *Account Security Preferences*

Account Security Preferences allow 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.

Understanding Account Security Preferences	Student Account Automation	Staff Account Automation
- Password Reset - 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 and Expiration Time - Password Reset Disallowed Time - Minimum Password Characters	- Enable Automatic Creation of Student Accounts - Username (Student Accounts) - Authentication Type (Student Accounts) - Password (Student Accounts) - Homepage (Student Accounts) - Automatically Disable Student Accounts - Additional Information About Generating Student Accounts - Communicating New User Accounts to Students	- Enable Automatic Creation of Staff Accounts - Username (Staff Accounts) - Authentication Type (Staff Accounts) - Password (Staff Accounts) - Rules - Automatically Disable Accounts After Staff Member is No Longer Employed by the District - Help! The Rules Editor is Saying There is an Invalid Configuration - Communicating New User Accounts to Staff Members - Reviewing User Group Calendar/Tool Rights and Associated Rules

Student Account and Staff Account Automation preferences are not available in State Editions of Campus.

Tool Rights

PATH: *System Administration > User Security > Users > Product Security Roles > Student Information System*

New Look of Campus Path: User Management > User Account Information

In order to access and modify Account Security Preferences, you must be granted the **Student Information System** Product Security Role.

Understanding Account Security

Preferences

This section describes how each Account Security Preference works. See the following topics for more information about each option:
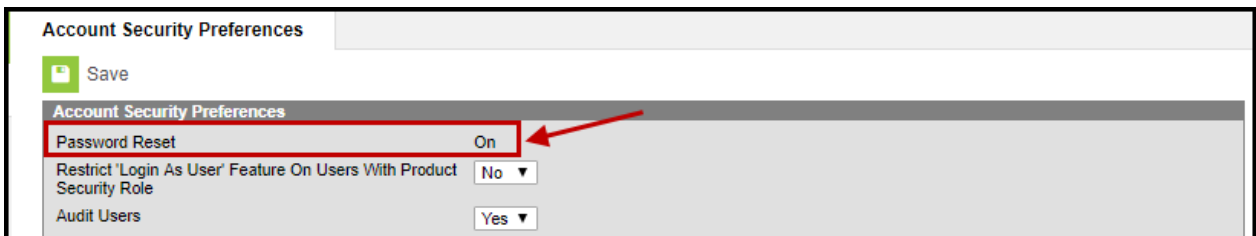
- Password Reset
- Restrict 'Login As User' Feature On Users with Product Security Role
- Audit Users
- Prohibit Passwords That Have Been Previously Disclosed in a Data Breach
- Password History Length and Expiration Time
- Password Reset Disallowed Time
- Minimum Password Characters

BIE USERS: To meet Federal security guidelines, the following default Account Security Preference values have been set for Staff accounts (this does not impact BIE Student or BIE Parent Portal accounts):

Default Value	Description
60-day refreshes for all passwords	This means all users are required to create a new Campus password every 60 days.
12-character minimum for all new passwords	This means all new passwords must be at least 12 characters in length.
1-day minimum lifetime for all passwords	This means a user must wait at least 24 hours between each time they change their password.
No re-use of the last 24 passwords	This means a user cannot reuse the last 24 previous passwords when creating a new password.

Password Reset

A value of 'On' means Password Reset functionality is enabled. This functionality provides Campus users the ability to initiate the reset of their own Campus account password.

This preference is read-only based on whether or not Password Reset functionality has been enabled via the Password Reset Configuration tool. This value cannot be changed once set. See the Managing User Account Passwords article for more information.

# Restrict 'Login As User' Feature On Users with Product Security Role

The **Restrict 'Login As User' Feature On Users With Product Security Role** preference controls whether Product Security users may log in as another user with a Product Security role.

This feature is not available for users only assigned the **Student Information System - Group Assignment** security role.

See this article (Single-Product Environment) or this article (Multi-Product Environment) for more information on how this feature functions for users only assigned the **Student Information System - Login as User** security role.

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 **Product Security** role (all products) and the **Student Information System - Login As User** role. When logging in as another user, users cannot gain access to tools for which they currently do not have tool rights.
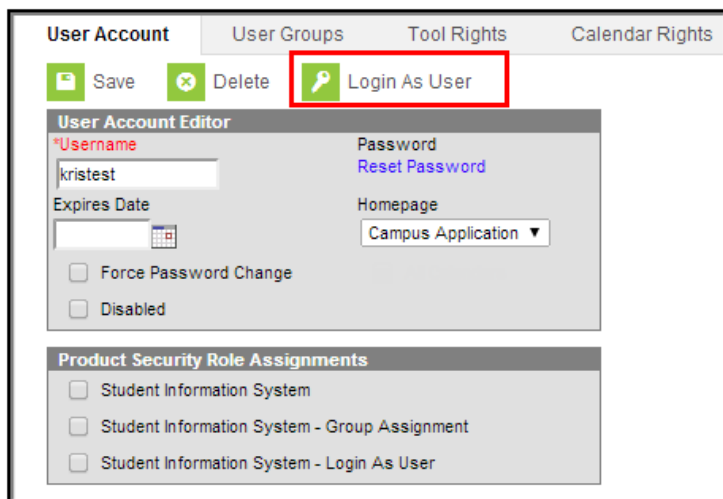
The **Student Information System - Login As User** role is prohibited from logging in as another **Student Information System - Login As User** role regardless of this preference. Users assigned this role are only allowed to log in as another user once per Campus session. This behavior was put in place to ensure users do not jump from one user account to another.

Audit Users

The Audit Users preference allows a district to enable/disable auditing of several user security tools in Campus. This preference controls which data updates (*i.e.*, additions, modifications and deletions of data) are tracked by the View Audit Log tool.

The **Audit Users** preference has two options. This preference may be enabled (set to "Yes") or disabled (set to "No") at any time.

Yes - When this field is set to a value of "Yes," full functionality of the View Audit Log tool is enabled. The View Audit Log tool will track additions, modifications and deletions made to data on the following tools:

- Individual User - User Account tab
- Individual User - User Groups tab
- Individual User - Tool Rights tab
- Individual User - Calendar Rights tab
- User Group - User Group tab
- User Group - Tool Rights tab
- User Group - Calendar Rights tab
- System Preferences

No - When this field is set to a value of "No," the View Audit Log tool will only track changes made to the System Preferences tool. Auditing of the System Preferences tool is ALWAYS enabled.

Prohibit Passwords That Have Been Previously Disclosed in a Data Breach

Infinite Campus is able to read and utilize a global database used to track passwords and accounts affected by data breaches of non-Infinite Campus systems. When this preference is enabled, if Infinite Campus detects a user's password matches a password found in a publicly known data breach, it will automatically notify the user and recommend they update it.

This preference is applicable to Campus and LDAP authenticated accounts.

> **As of Release Pack .2219, this preference is set to a default of 'Yes'.**
>
> All users who upgrade to Release Pack .2219 or greater will have this setting set to 'Yes'. Users can set this value back to 'No' at anytime and subsequent updates will not modify this value however, **Infinite Campus HIGHLY recommends leaving this setting set to Yes.**

Notification of a breached password DOES NOT mean your Infinite Campus account has been breached. It means your password matches a password found in a global database of breached passwords from third-party systems who have had a data breach.

If a user's password is identified as breached, they will receive notification of this issue in the bell 🔔 Messages area (see image below).
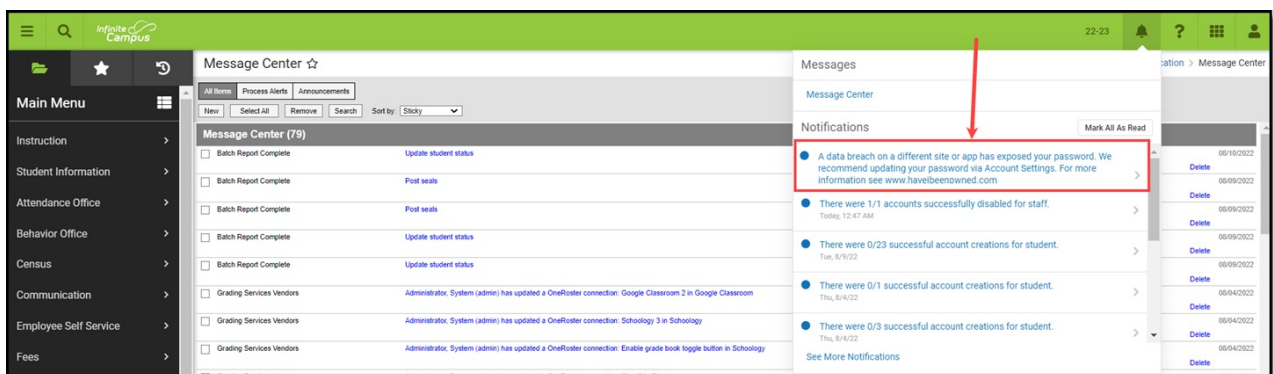
You can create an Ad hoc filter of all identified breached passwords by including the 'usage.pwnedPassword' field (Campus Usage > User Account/Summary > pwnedPassword) within a filter in the Filter Designer tool (see image below).

Ad Hoc Query Wizard - Field Selection

For more information on how this functionality works and how we discover breached passwords, see this page.

Campus **DOES NOT** send any credentials to a third-party for use of this functionality.

Password History Length and Expiration Time

The **Password History Length** field determines the number of previous passwords a user cannot use when changing their password.

The **Password Expiration Time** field allows administrators to determine how long a password is valid before the user is required to change it.

Password History Length	5
Number of recent passwords a user cannot choose when forced to change their password. Leave blank to disable.	
Password Expiration Time	365
Number of days before users are required to change their password. Leave blank to disable.	

Password Reset Disallowed Time

The **Password Reset Disallowed Time** field allows you to set the minimum amount of hours that must pass between password reset requests for a user. If left blank, this preference is disabled.

Password Reset Disallowed Time	24
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

The Minimum Password Characters preference allows districts to set the minimum number of characters required for Infinite Campus account passwords. If the preference is left blank, a default value of 6 characters is used.

> Administrators can create user account passwords with less than the minimum amount of required characters however, upon initial login, all user accounts with a password less than the minimum amount of characters will be forced to change their password to one that adheres to the minimum value set in this preference.

Minimum Password Characters	10
Minimum number of characters required for a password. Leave blank to use the default setting of 6 characters.	

Student Account Automation

Student Account Automation allows you to enable the automatic creation of student accounts and control how usernames, passwords, and the default homepage is established for each account created.

See the following sections below for more information about setting up this preference:

- Enable Automatic Creation of Student Accounts
- Username (Student Accounts)
- Authentication Type (Student Accounts)
- Password (Student Accounts)
- Homepage (Student Accounts)
- Automatically Disable Student Accounts
- Additional Information About Generating Student Accounts
- Communicating New User Accounts to Students

Enable Automatic Creation of Student Accounts

Marking the **Enable automatic creation of student accounts** checkbox will turn on student account automation functionality within Campus.

This preference will automatically create a student account for students who are given an enrollment record (active or future) and do not currently have a student account within Campus. Students who already have enrollment records but no student account will automatically have student accounts created 24 hours after the the preference is enabled (a nightly job is run to generate these accounts).

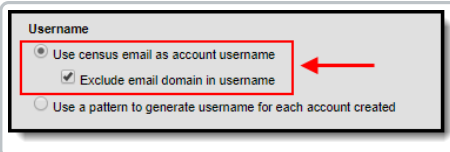
Please consider the following:

- You must opt-in to this preference. It is not automatically turned on by default.
- A student account username and password are generated for each student missing an existing student account.
- This preference is district-wide. It cannot be enabled at the school level.
- Each night a job is run to identify any students who have active or future enrollment records without student accounts and automatically generates an account for each of these students.
- A notification is generated if any conflicts or failures occurred during the creation of accounts. This notification does not generate if accounts were created successfully.
- Once this preference is enabled, at the time an enrollment record is created for a student who does not have a student account, a student account is automatically generated for them.

Automatically created student accounts will indicate they were Created By the person who initially created the student within Campus.

Username (Student Accounts)

Usernames are generated based on two available options: the email address of the student or a pattern used to create usernames for each account. The table below describes each option.

Field	Description
Use census email as account username	Selecting this option means usernames will be generated to match the email address listed in the **Email** field on the student's Demographics tab (see below). If you would like to remove the domain from usernames generated from a student's census email address, mark the **Exclude email domain in username** checkbox. For example, if the user's email address is 'joetester@email.com', his generated Campus username would be 'joetester'. Usernames created via email account do not qualify for collision resolution. If the email address is missing or is already taken by an existing user account, the user account will not be created.

Field	Description

Once the user account has been created, the user will enter their email address as their username for logging into Campus via the Campus login screen (see below).

Field	Description
Use a pattern to generate username for each account created 	Selecting this option allows you to designate a pattern for how usernames are generated for each account. For example, using the criteria entered in the picture to the left (Last Name, First Name, Student Number), if the student's name is John Doe with a student number of 123456789, he would log in with a username of Doe.John.123456789

Authentication Type (Student Accounts)

The Authentication Type determines how users of the generated accounts will log into Campus.

> This option will only appear if LDAP or SAML are configured in Campus. If hidden, the default authentication type is Local Campus Authentication.

- **Local Campus Authentication Only** - This option means users will use their Campus username and password to log into Campus.
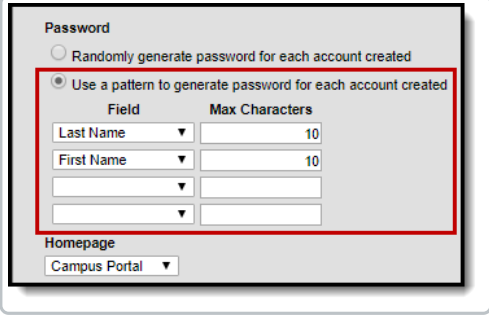- **LDAP Authentication** - This option means users will log into Campus using their LDAP username and password (controlled and maintained by their school/district's IDP). See the LDAP Authentication article for more information.
- **SAML Authentication** - This means users will log into Campus using their SAML username and password (controlled and maintained by their school/district's IDP). See the SSO Service Provider Configuration article for more information.

Password (Student Accounts)

When determining how user account passwords are created, you have the following two options:
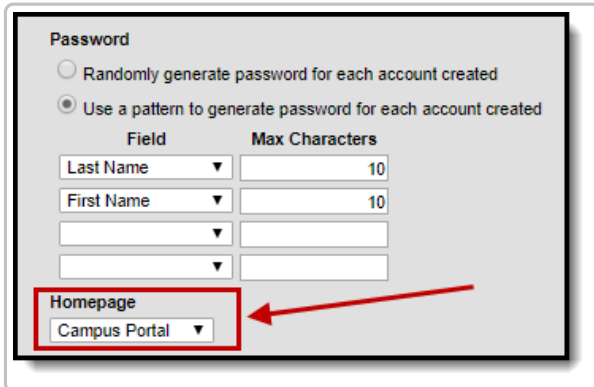
This section is not available if the Authentication Type is set to LDAP or SAML as account passwords are controlled and managed via your IDP.

Field	Description
Randomly generate password for each account created	Selecting this option means Campus will randomly generate a unique password for each account created. For more information about communicating usernames and helping users log into their new account, please see the following articles: - Notifying Users via Email - Notifying Users via Letters If generating random passwords for users, it is critical you follow the steps detailed in the article linked above. **This is the only way to properly have a users log in and set their own password if a random password was established by Campus.**

Field	Description
Use a pattern to generate password for each account created 	Selecting this option allows you to designate a pattern for how passwords are generated for each user account created. In the example to the left, based on the criteria (Last Name, First Name, 10 characters), a user named Nate Student would have a password of 'studentnate'. When automatically creating new student user account passwords containing portions or a combination of a student's PII (Personally Identifiable Information), you do so at your own risk. Often much of a student's common PII attributes are public knowledge and can be easily ascertained. Please ensure the utmost due diligence when distributing communication of a password containing portions or combinations of student PII to the applicable student(s).

Homepage (Student Accounts)

Once Username and Password criteria has been established, determine the **Homepage** of the accounts. The **Homepage** indicates whether the student will have access to Campus Student or the Campus Parent Portal.

For example, if the **Homepage** is set to 'Campus Portal', each generated student account is defaulted to a Homepage value of 'Campus Portal', meaning they will be sent to the Campus Portal when logging into Campus. This value is set on the student's User Account tab.

Automatically Disable Student Accounts

Marking the Automatically Disable Student Accounts checkbox means all student accounts tied to enrollment records with an End Date will be disabled a specified number days after the End Date.

Please consider the following:

- You must opt-in to this preference. It is not automatically turned on by default.
- The disable process is not immediate and occurs during an overnight job that is run. Students are not disabled the moment an End Date is entered on their enrollment record. Students who are given an End Date and should have their accounts disabled will have them disabled the following day.
  - If you need to immediately disable a user account, go to that student's User Account tab and mark the Disable checkbox.
- If the student has other existing and active enrollment records, their account will not be disabled.
- If the student has a future enrollment record entered within Campus their account will not be disabled.

- This preference is district-wide. This preference affects all students within a district and cannot be turned on or off at the school level.
- Disabled accounts are not stripped of their credentials. If an account is enabled after being disabled, the student can continue to use their same username and password.
- Students who have No Show marked on their enrollment record are automatically disabled the day after the No Show checkbox is marked. These accounts are NOT subject to the specified days grace period and are disabled regardless of the value entered in this field.
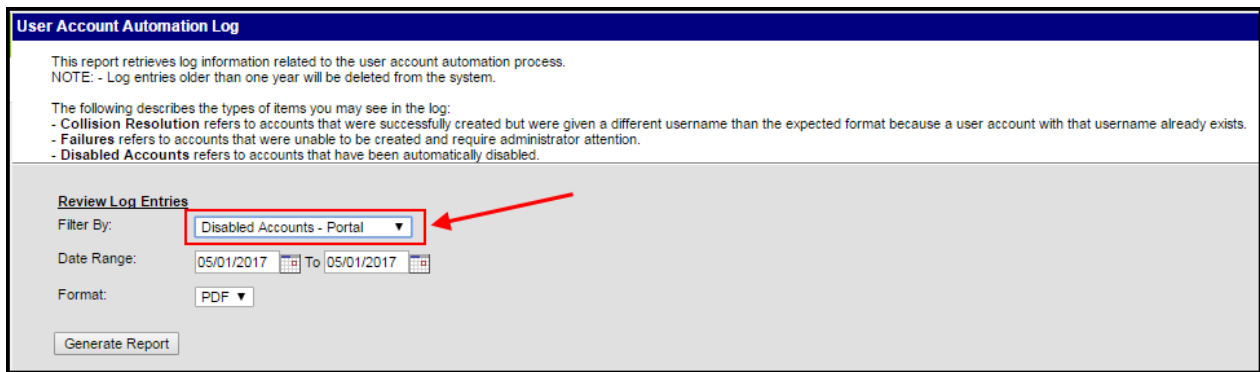
Users are allowed to enter a range of 1 to 365 days.

All parent accounts tied to the student are disabled the same day the student account is disabled unless the parent has other students tied to them who have an active or future enrollment record in the district. For example, if the district enters 60 days as the value for this field and the student is given an enrollment end date of 8/29/2019, the student and all associated parent account(s) will be disabled on 10/29/2019 (60 days after the enrollment end date).

Accounts are also disabled if **No Show** is marked on a student's enrollment record (see below). Students who have No Show marked on their enrollment record are automatically disabled the day after the No Show checkbox is marked. These accounts are NOT subject to the specified days grace period and are disabled regardless of the value entered in this field.

Each time accounts are disabled a notification will appear in the Notifications area, describing how many accounts were successfully disabled. You can click on this notification to be sent to the User Account Automation Log.

To view detailed information about each account that was disabled, select the *Disabled Accounts - Portal* option of the User Account Automation Log (see below).

Once an account is disabled, users who attempt to log into their account will receive a message indicating their account is disabled (see image below).

The student's account will have the **Disabled** checkbox marked on their User Account. To enable the account, unmark this checkbox. The user will now be able to log into their student account using the same username and password as before.

Additional Information About Generating Student Accounts

Once a new user account has been created for a student and the student logs into Campus for the first time, they will be asked to create a new account password (see image below).

If usernames get duplicated because students share the same first and last name (or same series of characters), Campus will automatically append a number to the end of the duplicate username to ensure each username is unique (e.g., If three students are named James Adams, the first username would be 'jam.ada and the second would be 'jam.ada1' and the third would be 'jam.ada2').
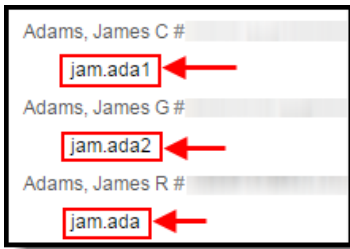
Duplicate usernames that are corrected are called Collisions within Campus. Any collision resolutions (duplicate usernames) will be indicated in the Process Alerts area and detailed information about these events can be viewed via the User Account Automation Log.

Any accounts that failed to be created are also indicated in the Process Alerts area and detailed information can be viewed via the User Account Automation Log.
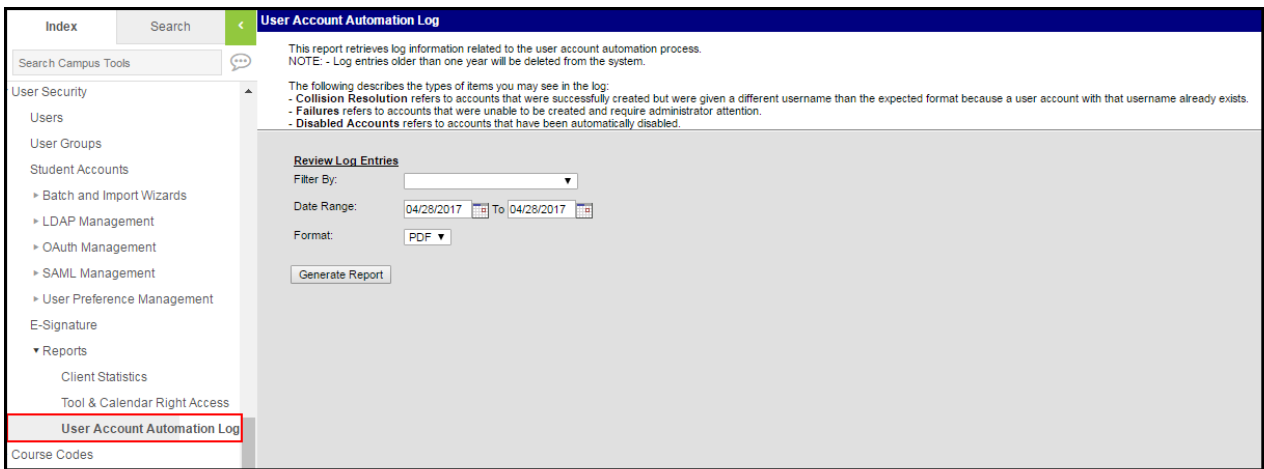
If you would like to include the student's username on printed schedules, you can mark the **Student Username** option when setting up a schedule template via the Report tool (see below).

The student username will appear in the header of printed schedules (see below).

Schedules can be generated/printed for a student via the Schedule tab or en masse via the Schedule Batch tool.

Automatically created student accounts will indicate they were Created By the person who initially created the student within Campus.

Communicating New User Accounts to Students

For more information about communicating usernames and helping students log into their new

account, please see the following articles:

- Informing Users of Newly Created User Accounts
- Scheduling a Recurring User Account Message
- Notifying Users via Letters

If generating random passwords for users, it is critical you follow the steps detailed in the articles linked above. **This is the only way to properly have a users log in and set their own password if a random password was established by Campus.**

Campus highly recommends you establish a recurring user account activation message. Please see the User Account Messenger Scheduler article for more information about this process.

Staff Account Automation

Staff Account Automation allows you to enable the automatic creation of staff accounts and control how usernames, passwords, and the default homepage is established for each account created.

See the following sections below for more information about setting up this preference:

- Enable Automatic Creation of Staff Accounts
- Username (Staff Accounts)
- Authentication Type (Staff Accounts)
- Password (Staff Accounts)
- Rules
- Automatically Disable Accounts After Staff Member is No Longer Employed by the District
- Help! The Rules Editor is Saying There is an Invalid Configuration
- Communicating New User Accounts to Staff Members
- Reviewing User Group Calendar/Tool Rights and Associated Rules

Enable Automatic Creation of Staff Accounts

Marking the **Enable automatic creation of staff accounts** checkbox will turn on staff account automation functionality within Campus.

This preference will automatically create a user account for staff members who are given an active district assignment. Staff who already have a district assignment record but no user account will automatically have user accounts created 24 hours after the the preference is enabled (a nightly job is run to generate these accounts).

Once this preference is enabled, people who are given a district assignment record with at least a School, Start Date, Title and/or a role checkbox (e.g., Teacher, Special Ed, Program, etc) entered and saved will have a user account generated.

Staff Account Automation
☑ Enable automatic creation of staff accounts
Note: Staff accounts will be created based on district assignment

This preference does not re-enable or re-activate any existing deactivated accounts.

Username (Staff Accounts)

Usernames are generated based on two available options: the email address of the staff member or a pattern used to create usernames for each account. The table below describes each option.

Field	Description
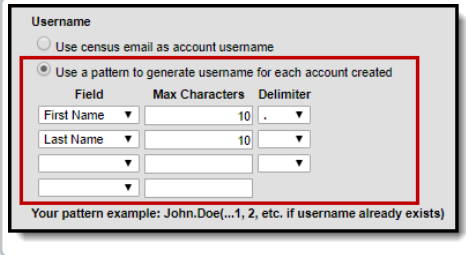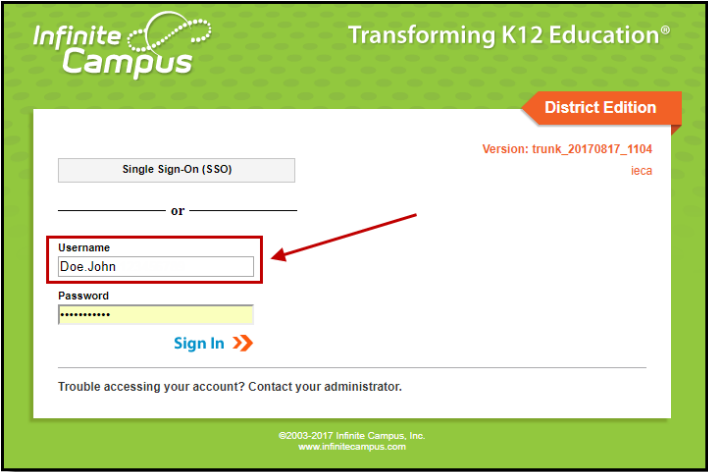
Field	Description
Use census email as account username 	Selecting this option means usernames will be generated to match the email address listed in the **Email** field on the staff member's Demographics tab (see below). If you would like to remove the domain from usernames generated from a staff member's census email address, mark the **Exclude email domain in username** checkbox. For example, if the user's email address is 'joetester@email.com', his generated Campus username would be 'joetester'. Once the user account has been created, the user will enter their email address as their username for logging into Campus via the Campus login screen (see below).

Field	Description
Use a pattern to generate username for each account created 	Selecting this option allows you to designate a pattern for how usernames are generated for each account. For example, using the criteria entered in the picture to the left (First Name, Last Name, 10 characters, Delimiter of .), if the staff member's name is John Doe, he would log in with a username of Doe.John

Authentication Type (Staff Accounts)

The Authentication Type determines how users of the generated accounts will log into Campus.

This option will only appear if LDAP or SAML are configured in Campus. If hidden, the default authentication type is Local Campus Authentication.

- **Local Campus Authentication Only** - This option means users will use their Campus username and password to log into Campus.
- **LDAP Authentication** - This option means users will log into Campus using their LDAP username and password (controlled and maintained by their school/district's IDP). See the LDAP Authentication article for more information.
- **SAML Authentication** - This means users will log into Campus using their SAML username and password (controlled and maintained by their school/district's IDP). See the SSO Service Provider Configuration article for more information.

Password (Staff Accounts)

Each account created will require the staff member go through the account activation process. During this process, their password will be established.

See the **Informing Users of their New User Account** article for more information on contacting staff about the user account activation process.

You can also establish a recurring message sent to any new users about activating their user account via the User Account Messenger Scheduler tool. See this article for more information: **Scheduling a Recurring User Account Message**

Rules

Rules are used to designate what calendar rights, tool rights, and homepage settings are automatically applied to user accounts based on the Title and/or Role(s) designated on their District Assignment.

You must designate at least 1 rule in order to generate staff accounts via this tool.

Title/Role values are entered on the District Assignment tab (Census > People > District Assignment) (select image below).

To view or modify an existing rule, select the rule from the Staff Account Automation Rule Settings window. Once a rule is selected, a pop-up will appear, displaying all selected Calendar User Groups and Tool User Groups with an ability to assign additional calendar and tool user groups (see image below).
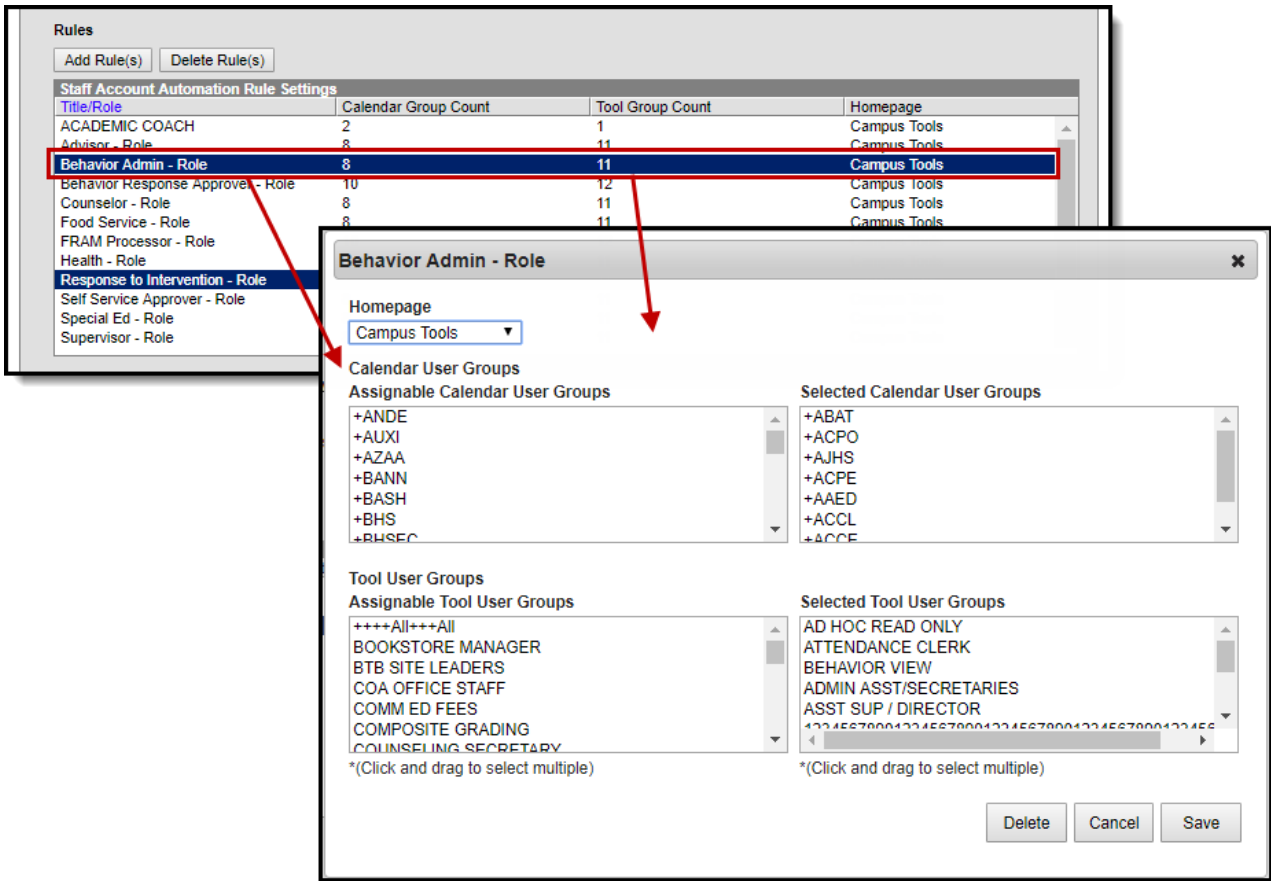
To create a new rule, click the **Add Rule(s)** button. The **Staff Account Automation Setup** window will appear (see below).

1. First, select the **Homepage**. This will determine if users will be automatically sent to Campus tools or Campus Instruction upon login.
2. Select which **Titles** are tied to this rule. Users who have this title selected on their District Assignment will be granted the calendar and tool rights assigned within this rule.
3. Select which **Roles** are tied to this rule. Users who have this role selected on their District Assignment will be granted the calendar and tool rights assigned within this rule.
4. Click the **Next** button.

Once titles and roles have been selected, you now need to determine which calendar user groups will be assigned to the rule. This step is optional.

If no calendar or tool rights groups are assigned to the rule, users tied to the titles/roles selected in the rule will not receive tool rights or calendar rights during account creation.

In this scenario, users will have to be granted tool rights and calendar rights manually via the Tool Rights and Calendar Rights tabs within System Administration > User Security > Users > Tool Rights, Calendar Rights
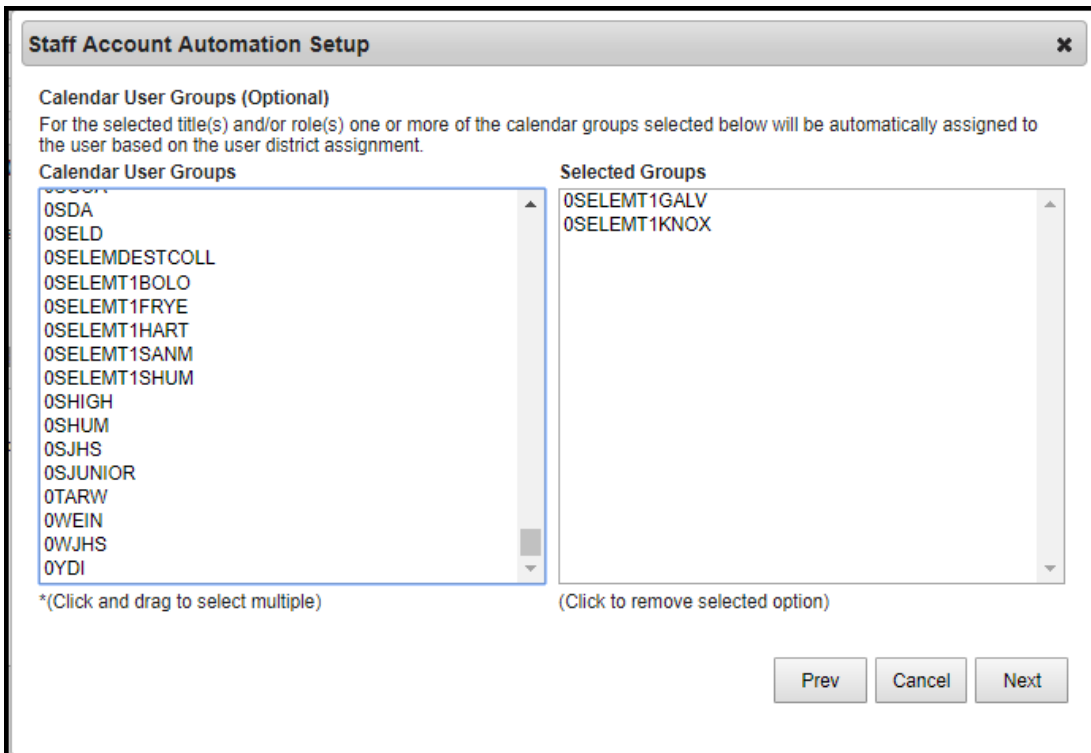
Calendar User Groups contain permissions for accessing all calendars assigned the selected user group.

Calendars are assigned to User Groups via the Calendar Rights tab (System Administration > User Security > User Group > Calendar Rights)

Select which Calendar User Groups to assign and once selected, click the **Next** button.

Please consider the following:

- Only User Groups containing only calendar rights will appear for selection within the Calendar User Groups window. User Groups containing a combination of tool rights and calendar rights ARE NOT available for selection.
- Rule functionality requires calendar rights be assigned only to Calendar User Groups and tool rights only be assigned to Tool User Groups.
- Calendar User Groups must be assigned to a single school. User groups containing calendar rights for 2 or more schools will not appear in the Calendar User Groups window.
- Users who need calendar rights to more than one school will need to be granted these rights either by adding additional Calendar User Groups to the rule or manually via the Calendar Rights tab.
- Calendar rights are assigned based on the person's District Assignment record. If a user is given rights based on a Rule, even if the rule contains several Calendar User Groups, the user will only receive calendar rights for schools matching their existing District Assignment record(s).
- The Tool Rights tool will prevent users from adding tool rights to calendar user groups.
- User groups containing all schools/all calendars are not available for use in the Staff Account Automation tool. Each user account requiring access to all schools/all calendars must be handled manually.


Select which **Tool User Groups** should be assigned to the rule. All tool rights assigned to the user group selected will be applied to user accounts tied to the rule.

Tool rights are assigned to User Groups via the Tool Rights tab (System Administration > User Security > Users > Tool Rights)

Select user groups from the **Tool User Groups** window. Each selected user group will appear in the **Selected Groups** window. Once all groups have been selected, click the **Finish** button. The Rule has been created and will now assign the selected user group calendar and tool rights to users who have matching District Assignment Role and/or Title values.

Please consider the following:

- Only User Groups containing only tool rights will appear for selection within the Tool User Groups window. User Groups containing a combination of tool rights and calendar rights ARE NOT available for selection.
- Rule functionality requires calendar rights be assigned only to Calendar User Groups and tool rights only be assigned to Tool User Groups.
- The Calendar Rights tool will prevent users from adding calendar rights to tool user groups.
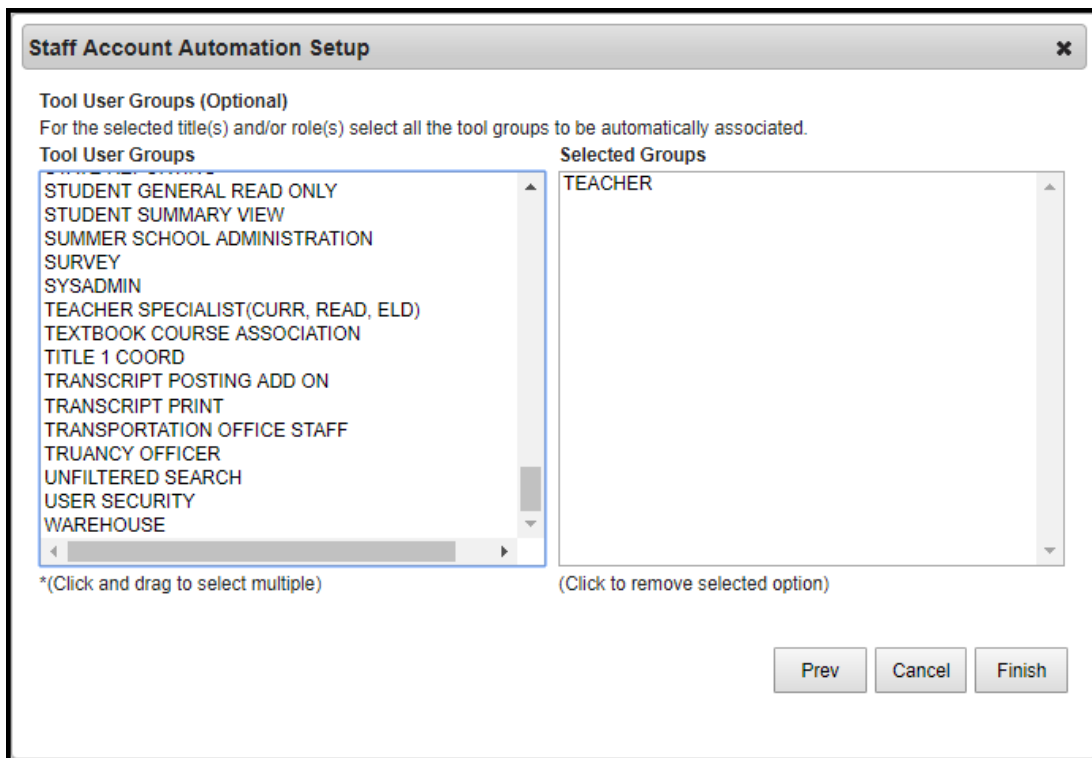

To delete an existing rule, click the **Delete Rule(s)** button. The **Delete Titles And/Or Rules** window will appear. From the **Current Titles and Roles** window, select which titles or roles (Rules) should be deleted and once all have been selected, click the **Delete** button.

You can also delete a rule by selecting the rule from the Staff Account Automation Rule Settings

window and selecting the **Delete** button.

The selected Rules have been deleted from Campus and will no longer be applied to generated staff user accounts.

Deleting a rule has no effect on already created user accounts.
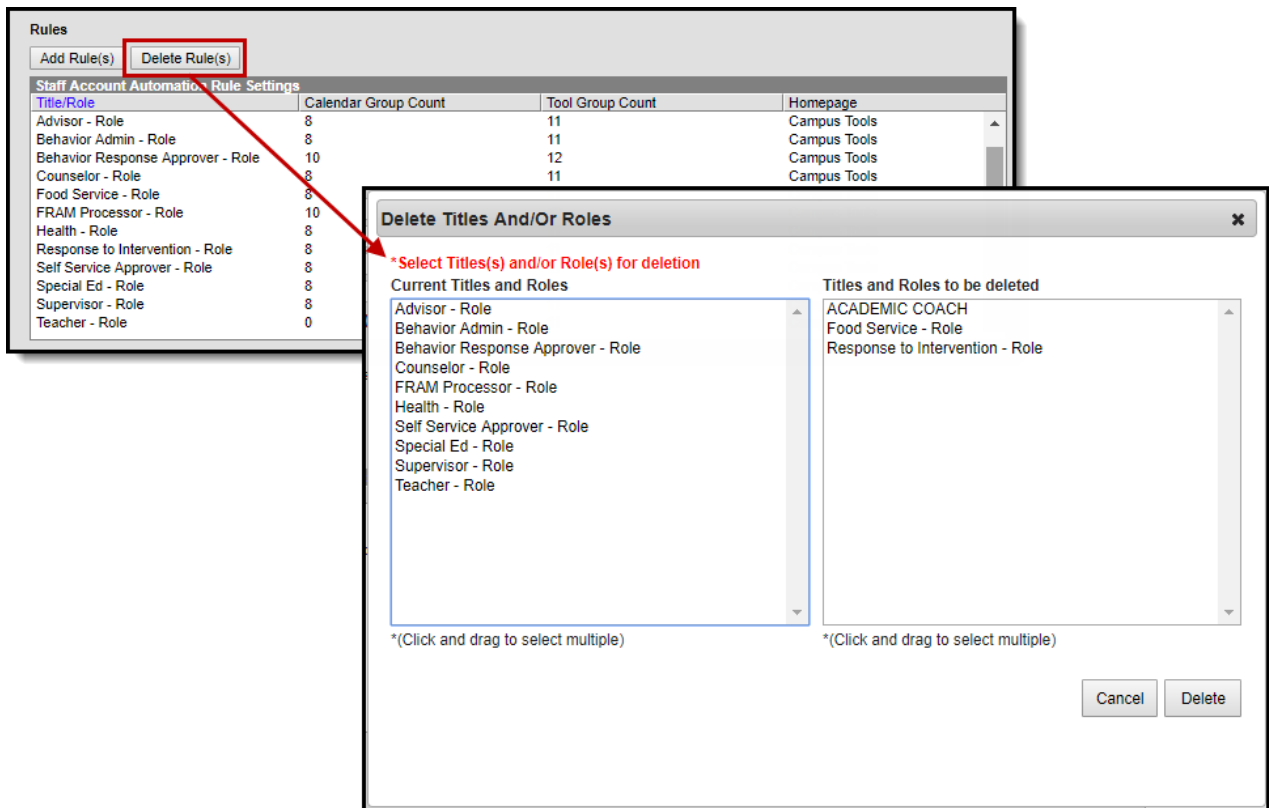
Automatically Disable Accounts After Staff Member is No Longer Employed by the District

Marking this checkbox means all staff accounts will be disabled based on the following logic:

- Accounts will be disabled as of the End Date entered on their district assignment record (if the person does not have an active district employment record).
- If an End Date is entered on a person's district assignment record but they have an active district employment record, the user will be disabled as of the End Date entered on their district employment record.
- If an End Date is entered on a person's district employment record but they have an active district assignment record, the user will be disabled as of the End Date entered on their district assignment record.
  - In order for a user to be disabled, they must no longer have an active district employment or district assignment record. If an End Date is entered on both a user's district

employment and district assignment record, logic uses the latest date of the two dates as the account disable date.

Automatically disable accounts after staff member is no longer employed by the district
(Note: Some staff accounts will not be automatically disabled with this functionality. Districts should check the "Accounts Requiring Review" option within the "User Account Automation Log" report to keep track of those accounts and manually disable them when no longer needed.)

Please consider the following:

- You must opt-in to this preference. It is not automatically turned on by default.
- The disable process is not immediate and occurs during an overnight job that is run. Staff are not disabled the moment an End Date is entered on their district assignment/district employment record (based on the logic mentioned above).
  - If you need to immediately disable a user account, go to that user's User Account tab and mark the Disable checkbox.
- If the staff member has other existing and active District Assignment records, their account will not be disabled.
- If the staff member has a future District Assignment record entered within Campus their account will not be disabled.
- This preference is district-wide. This preference affects all staff within a district and cannot be turned on or off at the school level.
- Disabled accounts are not stripped of their credentials. If an account is enabled after being disabled, the staff member can continue to use their same username and password.
- Users with a Product Security Role will have their account disabled when their District Assignment and District Employment record expire.

This preference **DOES NOT** disable user accounts which have no employment records (district employment or district assignment records). These accounts must be manually disabled via the Disabled checkbox on the User Account tab.

To view a list of all user accounts which do not have employment records, please see the 'Accounts Requiring Review - Staff' option of the User Account Automation Log.

User Account Automation Log

This report retrieves log information related to the user account automation process.
NOTE: - Log entries older than one year will be deleted from the system.

The following describes the types of items you may see in the log:
- **Collision Resolution** refers to accounts that were successfully created but were given a different username than the expected format because a user account with that username already exists.
- **Failures** refers to accounts that were unable to be created and require administrator attention.
- **Disabled Accounts** refers to accounts that have been automatically disabled.
- **Accounts Requiring Review - Staff** refers to those accounts where the user does not have any history of employment with the district. (Note: Accounts Requiring Review will not be disabled by the automation. Any accounts listed in this report will need to be disabled manually. For security purposes, we recommend the district review these accounts on a regular basis, as there should not be more than a handful of these accounts.)

Review Log Entries

Filter By: Account Requiring Review - Staff ▼

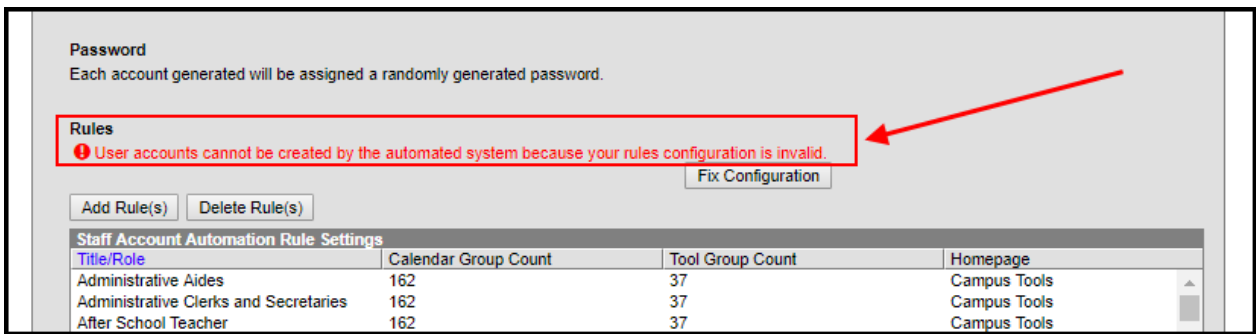Date Range: 11/27/2017 To 11/27/2017

Format: PDF ▼

Generate Report

Help! The Rules Editor is Saying There is an Invalid

Configuration

If incorrect modifications were made to the attribute dictionaries for Titles or Roles or if calendar rights or other items were modified in the back-end of Campus, this may cause existing Rules to become corrupt and thus cause your automation configuration to no longer be valid. If this occurs, an error message will appear in the Staff Account Automation area stating "User accounts cannot be created by the automated system because your rules configuration is invalid" (see image below).

Staff account automation is disabled until the configuration is corrected. Once corrected, any users added during the down period will have a user account automatically created and the user can access their new user account the day following the day the configuration was corrected (user accounts are created during an overnight job).

To view a list of the misconfigured data and to potentially delete the data from the system, click the **Fix Configuration** button (see below). The Fix Configuration window will appear, displaying all misconfigured data and the reason the data is considered invalid.

To correct this issue, you can either modify/update these items one by one within Campus and set them to their correct values or you can have the Fix Configuration tool delete them from the system by clicking the **Delete** button.

Once all items have been corrected and/or deleted, the error message will go away and staff account automation will resume working within Campus.

Communicating New User Accounts to Staff Members

For more information about communicating usernames and helping staff members log into their new account, please see the following articles:

- Notifying Users via Email
- Notifying Users via Letters
- Scheduling a Recurring User Account Message

If generating random passwords for users, it is critical you follow the steps detailed in the articles linked above. **This is the only way to properly have a users log in and set their own password if a random password was established by Campus.**

Campus highly recommends you establish a recurring user account activation message. Please see the User Account Messenger Scheduler article for more information about this process.
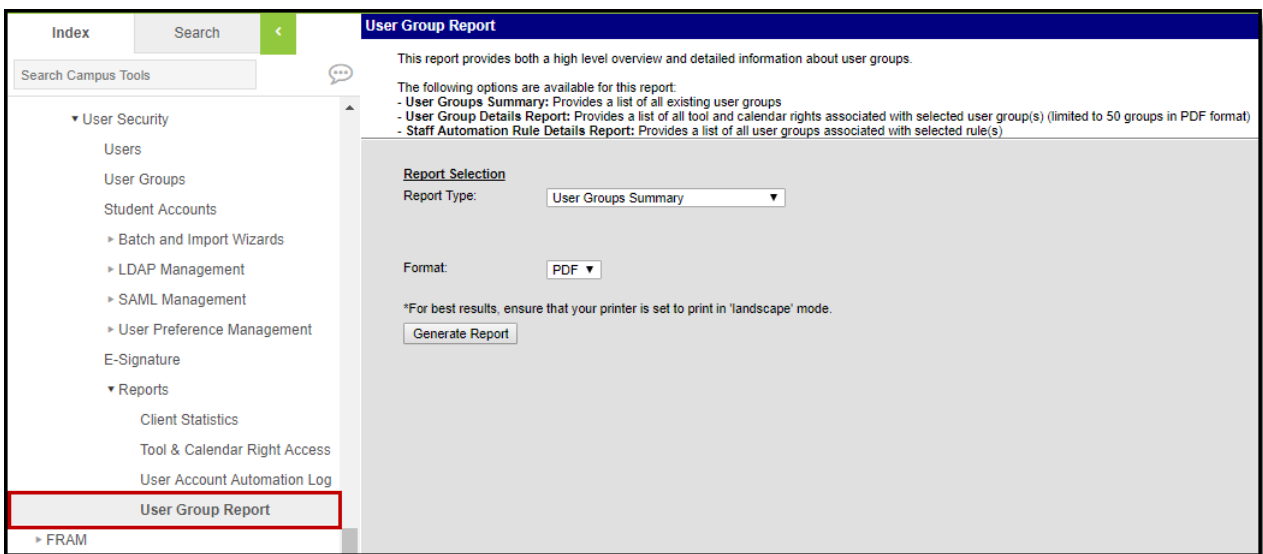
This section is not available if the **Authentication Type** is set to LDAP or SAML as account passwords are controlled and managed via your IDP.

Reviewing User Group Calendar/Tool Rights and Associated Rules

PATH: *System Administration > User Security > Reports > User Group Report*

Users can generate the User Group Report to assist in creating and modifying Rules. This report details all existing user groups, tool and calendar rights associated to specific user groups, and user groups associated with specific Rules.

For more information about this report, please see the User Group Report article.

Related Tools

Tool	Description
User Account Batch Wizard	This tool allows users 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, force a password reset for student and staff user accounts, and add or remove user groups for user accounts en masse.
User Account Automation Log	This tool allows you to view detailed information about user account username modifications, user account creation failures, accounts automatically disabled via preferences set in the Account Security Preferences tool, and staff accounts not automatically disabled by Account Security Preferences.
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.

Tool	Description
User Account Messenger Scheduler	The User Account Messenger Scheduler allows you to establish recurring user account messages which can be sent daily, weekly, or monthly to users who meet message template criteria.