Security User Guide

PowerSchool 8.x
Student Information System

ALWAYS LEARNING

PEARSON

Released January 2015

Document Owner: Documentation Services

This edition applies to Release 8.2.1 of the PowerSchool software and to all subsequent releases and modifications until otherwise indicated in new editions or updates.

Contents

Preface

Use this guide to assist you while navigating PowerSchool. This guide is based on the PowerSchool online help, which you can also use to learn the PowerSchool Student Information System (SIS) and to serve as a reference.

The PowerSchool online help is updated as PowerSchool is updated. Not all versions of the PowerSchool online help are available in a printable guide. For the most up-to-date information, click **Help** on any page in PowerSchool.

Referenced Sections

This guide is based on the PowerSchool online help, and may include references to sections that are not contained within the guide. See the PowerSchool online help for the referenced section.

Security Permissions

Depending on your security permissions, only certain procedures may be available to you.

Navigation

This guide uses the > symbol to move down a menu path. If instructed to "Click **File > New > Window**," begin by clicking **File** on the menu bar. Then, click **New** and **Window**. The option noted after the > symbol will always be on the menu that results from your previous selection.

Notes

It is easy to identify notes because they are prefaced by the text "**Note:**."

Introduction

Everyone who uses PowerSchool, the PowerSchool Student and Parent portal, PowerTeacher, PowerTeacher Substitute and PowerTeacher gradebook must have a username and confidential password. Users can belong to user groups to make page permissions easier to manage. In addition, you can restrict access to PowerSchool by specific IP addresses to further promote security.

Setup

System Security

Use this page to modify system-level security settings. The settings relate to several security settings in PowerSchool, including the amount of time that can pass before a PowerSchool or the PowerSchool Student and Parent portal user is automatically signed out of the system due to inactivity; the default security level for a page when no page-specific security is set; and setting for remote support access. For more information, see *Security*.

Note: Any change will take effect on the next server restart.

How to Set System Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Server, click **System Settings**. The System Settings page appears.
3. Click **Security**. The Security Settings page appears.
4. Use the following table to enter information in the fields:

Field	Description
Maximum number of concurrent user sessions	Enter the maximum number of user sessions that can occur on PowerSchool simultaneously. **Note:** Approximately 40k of memory are used per 100 sessions.
Maximum number of concurrent student sessions	Enter the maximum number of student sessions that can occur on the PowerSchool Student and Parent portal simultaneously.
Maximum number of concurrent parent sessions	Enter the maximum number of parent sessions that can occur on the PowerSchool Student and Parent portal simultaneously. For more information, see *PowerSchool Student and Parent Portal*.
Allow users to restore session that have been timed out due to inactivity	Click the switch to **On** to allow users to restore session that have been timed out due to inactivity. Alternatively, click the switch to **Off** to disable this feature. **Note:** By default, the switch is set to **Off**.
Sign Out Administrative Users After This Many Minutes Of Inactivity	Enter the number of minutes that can pass before a PowerSchool user is automatically signed out of the system due to inactivity. This setting applies to PowerSchool, PowerTeacher, and PowerTeacher Substitute. If a value is entered, users will see one of the following messages when their sessions are close to timing out:

Field	Description
	- Several minutes before timeout, the user will see "You are about to be signed out due to inactivity. Click **Stay Signed In** or anywhere on this page to continue." - When session timeout is detected, the user will see "You have been signed out. Return to **Sign In Page**."
Sign Out Parent Users After This Many Minutes Of Inactivity	Enter the number of minutes that can pass before a PowerSchool Student and Parent portal user is automatically signed out of the system due to inactivity. For more information, see *PowerSchool Student and Parent Portal*. If a value is entered, users will see one of the following messages when their sessions are close to timing out: - Several minutes before timeout, the user will see "You are about to be signed out due to inactivity. Click **Stay Signed In** or anywhere on this page to continue." - When session timeout is detected, the user will see "You have been signed out. Return to **Sign In Page**."
Unless Specified Otherwise for an Individual Screen, Groups Have This Level Of Access	Enter a default level of access for all users for individual pages. For each user group, you can define their level of access on every PowerSchool page.
Enable Parent Single Sign-On Security	Click the switch to **On** to enable parent single sign-on security. If enabled, each parent can sign in to the PowerSchool Student and Parent portal with one account and see any and all students for whom they have legal and parental rights to. Alternatively, click the switch to **Off** to disable this feature. For more information, see *PowerSchool Student and Parent Portal*. **Note:** Once enabled, parents will receive an email notification whenever an update is made to their account.
Enable MyData Download for Parents	The MyData button is a joint project between the Office of Educational Technology and the White House Office of Science and Technology Policy that, among other goals, allows access to student data in order to create a personal learning profile that is easily portable. PowerSchool provides parents with the ability to download their students' data, including grades and attendance, in an XML-formatted file.

Field	Description
	Click the switch to **On** to display the MyData button on the PowerSchool Student and Parent portal. Alternatively, click the switch to **Off** to disable this feature. **Note:** The MyData button requires that PowerSchool is running on SSL (Secure Sockets Layer), ensuring that the data transmission is secure.
Enable PowerSchool Session Cookies to span Subdomains	If the PowerSchool session cookie needs to be submitted by the browser to another server/identity provider running on a different subdomain than the PowerSchool server for integration with external systems, click the switch to **On** to enable PowerSchool session cookies to span subdomains. If enabled, the PowerSchool session cookie will be sent by the browsers to the subdomains of the specified domain. For example, if PowerSchool is running on powerschool.com and you specify powerschool.com as the domain, then the PowerSchool session cookie will be submitted to all the subdomains ofpowerschool.com, such as school.powerschool.com or district.powerschool.com. Alternatively, click the switch to **Off** to disable this feature.
PowerSchool Domain	If the **Enable PowerSchool Session Cookies to span Subdomains** checkbox is selected, enter the valid domain name on which PowerSchool is running, such as myschooldistrict.com. **Note:** The PowerSchool Session Cookies to Span Subdomains feature will not work without a valid domain name.
Disable Remote Support	Click to disable remote support with no time limit.
Enable Remote Support	Click to enable remote support with no time limit. **Remote Support Security:** Pearson strongly recommends that SSL be enabled on your PowerSchool server to ensure all data passed between your server and Pearson technical support remains secure and private. If SSL is not enabled, data moving between your server and Pearson is unencrypted. For more information, see the *SSL Configuration* section of the *Installation Guide* available on **PowerSource**.
Temporarily Enable Remote Support	Click to enter start and end dates for remote support access. The following fields appear. • **Starting Date** - Enter a start date, or click the calendar icon to select a date. • **Ending Date** - Enter an end date, or click the

Field	Description
	calendar icon to select a date. **Note**: Date format must be one of the following: • mm/dd/yyyy • mm/dd/yy • m/d/yyyy • m/d/yy • mm-dd-yyyy • mm-dd-yy • m-d-yyyy • m-d-yy

5. Click **Submit**. The System Settings page appears.

Security Permissions

In PowerSchool, system users are considered staff members. All PowerSchool system users must be added as staff members before you can assign security permissions. When adding new staff members, you can assign permissions, as needed. Additionally, you can assign permissions by user group or set permissions at the page level. For more information about assigning permissions by user group, see *Group Security Permissions*.

When user permissions are enabled for both PowerTeacher Administrator and ReportWorks, the user account is shared. Therefore, the username and password are the same for PowerSchool, PowerTeacher Administrator, and Report Works. Due to the shared account, the PowerTeacher Administrator and ReportWorks applications cannot run simultaneously. Be sure to set appropriate PowerSchool group and page permissions for these users. For more information, see *How to Edit a Staff Member Security Settings* and ***How to Set Page-Level Permissions***.

To set up new system users, see *Add New Staff Members*. To edit or delete an existing system user account, see *How to Edit Staff Member Security Settings*.

Page-Level Permissions

To define each user group's access to individual pages within PowerSchool, use the page permissions function. The **Modify Access Privileges for this Page** link appears on every page when the page permissions are activated.

By clicking the link, you can define the access level for only that page (None, View Only, View and Modify) for each user group. If you do not define the page-level access for each group, the system uses the default access level you originally defined for the group on the Edit Group page. For more information, see *How to Edit a Staff Member Security Settings*.

After defining the access level for every group on every page, return to this page to deactivate the page permissions function.

How to Enable Page Permissions Access

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Access to Page Permissions**. The Access to Page Permissions page appears.
4. Choose **On** from the **Turn modify permissions** pop-up menu.
5. Click **Submit**. The Security page appears.
6. Proceed to ***How to Set Page-Level Permissions***.

How to Set Page-Level Permissions

1. Navigate to the PowerSchool page for which you want to define permissions.
2. Click **Modify access privileges for this page**. The Access Privileges drawer appears.
3. Use the following table to enter information in the fields:

Field	**Description**
Filter	Enter one of more search terms in the **Filter** field to narrow the list of groups. Otherwise, leave blank.
Set All Groups To	To set the level of permissions for all groups, choose one of the following: • **Group default**: Level determined as the group default on the Edit Group page for each group. For more information, see *How to Edit Security Groups*. • **None**: No access to the page. • **View-only**: Can read but not modify the information on the page. • **Full**: Can read and modify information on the page. **Note:** This setting works with the filter so that only visible (non-filtered) groups are set.
Level of Access	To set the level of permissions for a particular group, select on of the following options for the group: o **Group default**: Level determined as the group default on the Edit Group page for each group. For more information, see *How to Edit Security Groups*. o **None**: No access to the page. o **View-only**: Can read but not modify the information on the page. o **Full**: Can read and modify information on the page.

4. Click **Submit**. A confirmation message appears. The page reappears.
5. Close the Access Privileges drawer.

6. Proceed to ***How to Disable Page Permissions Access***.

How to Disable Page Permissions Access

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Access to Page Permissions**. The Access to Page Permissions page appears.
4. Choose **Off** from the **Turn modify permissions** pop-up menu.
5. Click **Submit**. The Security page appears.

Field Level Security

The Field Level Security feature provides easy-to-use tools for the PowerSchool Administrator to configure and manage field level security for PowerSchool and PowerTeacher fields that need to be limited. Users can be granted Full Access, View Only, or No Access to specific fields. It helps accomplish the following goals:

- Protect PII (Personally Identifiable Information) so that unauthorized users can not see or access it.
- Protect data integrity by limiting who can edit specific fields, even though some other users may need to view the information.

Note: For more information about common usage scenarios and provides details on how to use FLS in customizations by utilizing DATs, tlist and conditional statements, see Knowledgebase article 71873 available on **PowerSource**.

Page Level Security vs. Field Level Security

Field Level Security is not a substitute for Page Level Security, but rather complimentary to it. Users are never given more access than is granted at the page level. For example, if a user has Field Level Security set to "Full Access" on a particular field, but the page is set to "View Only" for that user, then the user will only be granted "View Only" access to the field on that page. Since Page Level Security only affects a single page, it is possible for a user to have full edit access on another page for the same field. There are some pages in PowerSchool that do not enforce FLS. These pages should continue to be secured through Page Level Security where possible:

- Autosend
- Import
- Family Management
- ReportWorks
- Reports utilizing the SRP platform.

  Note: The SRP security mechanism can be used to secure these reports.

- Reports utilizing the Reporting Engine where fields are called without DATs
- PowerTeacher Gradebook
- Health

Note: The health module has feature-level security in the Security Group settings.

- New Student Enrollment
- Transfer Out of School/Transfer Student Out

User Access Roles

User Access Roles are required to take advantage of Field Level Security. By themselves, roles are nothing more than a label. It is what you do with a role that gives it meaning in PowerSchool. Roles are very powerful tools allowing you to setup advanced security scenarios when mixed with Security Groups, Page Level Security and FLS. Users can have multiple roles tied to each of their school affiliations accommodating unique security configurations. All security roles are additive, meaning that for any particular setting users are given the highest level of access granted to any of their roles. For example, if a user has a role configured for No Access to the SSN field, but they have another role configured for View Only access, the effective security on SSN will be View Only.

Other Important Notes

- It is not recommended to set name fields to No Access. However, it is okay to secure name fields as View Only to prevent editing, but names will not be fully protected from displaying, as they are necessary for PowerSchool to function properly. Additionally, the ^(lastfirst) DAT will not be protected.
- There are some special purpose pages where users will still be able to view data even if their field access level is set to No Access. System administrators are expected to utilize Page Level Security to restrict access to these pages. For a current list of the specific areas that do not enforce field level security, see Knowledgebase article available on **PowerSource**.
- Existing tlist_sql tags used in custom pages that do not include the new FLS method tags will not be secured until they are updated with these new keywords. It is advised that you update any tlist_sql tags on custom pages that you need to be secure by FLS. For more information, see Knowledgebase article 71873 available on **PowerSource**.

How to View Field Level Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Field Level Security**. The Field Level Security page displays the following information:

Note: Click the arrow in the column heading to sort in ascending order. Click again to sort in descending order.

Field	Description
Field Name	The name of the field. **Note:** For a list of fields that are available to be secured

Field	**Description**
	through the Field Level Security system, see Knowledgebase article 72328 available on **PowerSource**.
Table	The PowerSchool table in which the field resides.
Field Security	If a green checkmark appears, field level security has been applied to this field. If a checkmark does not appear, field level security has not been applied to this field.
Actions	Click to **Edit** icon to modify field level security for the field. For more information, see ***How to Modify Field Level Security***.

How to Modify Field Level Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Field Level Security**. The Field Level Security page appears.
4. Click the **Edit** icon. The Edit [Field Name] drawer appears.
5. Use the following table to enter information in the User Access Security section:

Field	**Description**
Access	The level of permission granted to users in this role for the selected field: • Full Access - When a field is set to this setting, the field appears editable. • View Only - When a field is set to this setting, the field appears as read-only. • No Access - When a field is set to this setting, the field appears with asterisks.
Roles	The roles that have been assigned access.
Edit	1. Click to **Edit** icon to modify roles for a given access level. The Edit Roles pop-up appears. 2. Select the checkbox next to each role that you want to assign to the access level. 3. Click **OK**. The Edit Roles pop-up closes. The selected roles(s) appears in the Roles column. **Note:** A role can only be assigned to one access level. Roles will automatically be removed from any previous access level when added to a new level.
Everyone Else	The level of permission for everyone else. This setting affects all users that are not added to one of the other security levels for a field even if they do not have role

Field	Description
	associations. If no roles are configured with security exceptions, this value is automatically set to **Full Access**.

2. Click **Submit**. The Field Level Security page appears. Note a checkmark now appears in the field security column.

How to Add an Extended Schema Field to Field Level Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Field Level Security**. The Field Level Security page appears.
4. Click **Add**. The Add Fields to Set Security drawer appears.
5. Use the following table to enter information in the fields:

Field	Description
Choose Table	Choose the extended schema table you want to select fields from the pop-up menu. The Choose Fields field displays all fields for the selected extended schema table.
Choose Fields	Select the checkbox next to each field within the extended schema table you want to add to the Field Level Security page.

6. Click **Add Fields**. The Field Level Security page displays the additional field(s).

How to Delete an Extended Schema Field from Field Level Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Field Level Security**. The Field Level Security page appears.
4. Click the **Delete** icon. The Delete [Field Name] pop-up appears.
5. Click **OK**. The Delete [Field Name] pop-up closes. The Field Level Security page no longer displays the deleted field.

Plugin Security

The Plugin Security section of the [Field Name] drawer displays the plugin roles that have been granted access to the selected field. Access to the field by a plugin can only be approved or rejected by a PowerSchool Administrator when a plugin is enabled. If you need to change a plugin's access to a specific field, you must work with the plugin developer to change the field access list within the plugin xml.

When the [Field Name] drawer only displays the Plugin Security section and does not also display the User Access Security section, this indicates that the field is not a core Field Level Security field that can be secured using User Access roles. Fields of this type are only secured to plugins when those plugins are enabled, and have been granted access to the field by a PowerSchool Administrator.

For more information on a plugin's access to specific fields and how these fields are listed within the plugin xml, see the ***Plugin Management User Guide*** and the ***PowerSchool API Developer Guide*** available on **PowerSource**.

How to View Plugin Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Field Level Security**. The Field Level Security page appears.
4. Click the **Edit** icon. The Edit [Field Name] drawer appears.
5. Use the following table to view information in the Plugin Security section:

Field	**Description**
Access	The level of permission granted to users in this plugin role for the selected field: • Full Access - When a field is set to this setting, the field appears editable. • View Only - When a field is set to this setting, the field appears as read-only. • No Access - When a field is set to this setting, the field appears with asterisks.
Roles	The plugin roles that have been assigned access.

6. Click **Submit**. The Field Level Security page appears. Note a checkmark now appears in the field security column.

Group Security Permissions

PowerSchool users and staff members are assigned to groups to simplify the process of assigning and modifying permissions. Though users have the default permissions of the user group to which they belong, you can modify these permissions per user. For more information about modifying individuals' permissions, see *How to Edit a Staff Member Security Settings*.

How to Edit Security Permissions by Group

Edit the permissions of staff members and PowerSchool users.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Users by Group**. The Users by Group page appears.
4. Click the name of the user in the User Name column. The Edit Staff Security Info page appears.
5. Edit information as needed. For field descriptions, see *How to Edit Staff Member Security Settings*.
6. Click **Submit**. The Changes Recorded page appears.

How to Add Security Groups

Based on your district's needs, you can add up to 500 security groups. Adding security groups in small batches allows you to prefix the security group with a meaningful name that can help you to sort and manage security groups more easily.

Note: Once added, security groups cannot be removed. In order to remove security groups, you must contact Pearson Technical Support.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Groups**. The Groups page appears.
4. Click **Add Groups**. The Add Security Groups page appears.
5. Use the following table to enter information in the fields:

Field	**Description**
Current Number of Security Groups	The current number of security groups appears. **Note:** This field is read-only.
Number of Groups to Add	Enter the new number of security groups. The new total number of security groups appears. The minimum value that you can enter is 1. The maximum value you can enter is 500, which includes the current number of groups. For example, if the current number of groups is 100, the maximum value you can enter is 400. **Note:** This field is required.
Prefix Group Names With	Any groups that are created will use this prefix, followed by the number of the group. For example, if the current number of security groups is 50 and the number of security groups is increased to 55, then "Group 51, Group 52, Group 53, Group 54, Group 55" are created. Do one of the following • Use the default prefix setting of **Group [space].** • Replace the default prefix setting with your own prefix.

Field	**Description**
Group Name Preview	Group names appears based on the number of groups you added and the prefix you entered. Confirm that the group name is correct prior to submitting.

6. Click **Submit.** The Groups page appears along with a confirmation message.

How to Edit Security Groups

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Groups**. The Groups page appears.
4. To narrow the list of groups, enter one of more search terms in the **Filter** field. Otherwise, leave blank.
5. Click a name in the Group Name column. The Edit Group page appears.
6. Use the following table to enter information in the fields:

Field	**Description**
Copy Security Permissions	See *How to Copy Security Permissions*.
Group Number	The number of the group appears. **Note:** PowerSchool supports up to 500 security groups. For more information, see *How to Add Security Groups*.
Group Name	Edit the name of the group.
Access Level	Use the pop-up menu to choose a level of permission used as the default permissions for users in this group: • **No Access** • **View Only** • **View & Modify**
Page Level Permissions	See *How to View/Edit Overridden Page Permissions*.
Can Modify Schedules	Use the pop-up menu to choose a level of permission for modifying schedules: • **Yes, in any year** • **No, not at all** • **Only for [school years]**
PowerScheduler Access	Select the checkbox if users in this group can use the master scheduler features.

Field	Description
Language Translator	Select the checkbox if users in this group can use the language translator feature. **Note:** For more information, see *Enable Language Translator Security Permissions*.
Analytics Access	Select the checkbox to allow users in this group to access Analytics. **Note**: This field only displays if Analytics is enabled. For more information, see *Enable Analytics*.
Report Queue Priority	Select the report queue priority level for this group. The report queue priority determines which reports run first, based on the user who submitted the report request.For example, a group with the priority level of 10 is the near-highest level of priority for running reports. Only groups with the level of zero would have higher priority.
Accessible Log Types	Select the checkbox next to each log type that you want to be accessible to users in this group. Click **Check All** to select all checkboxes. Click **Uncheck All** to deselect all checkboxes. **Note:** The **Check All** and **Uncheck All** buttons only appear if there are multiple log type checkboxes.
Accessible Incident Types	Select the checkbox next to each incident type that you want accessible to users in this group. **Note:** Set up Incident Types at the district level. For more information, see *Incident Types*.
Health and Immunization	Use the **Certification** pop-up menu to choose a level of permission for the Grade Level Entry Certifications tab on the District Setup Health page: • **No Access** • **View Only** • **View/Modify** • **View/Modify/Delete** Use the **Immunization** pop-up menu to choose a level of permission for the Immunizations tab on the District Setup Health page: • **No Access** • **View Only** • **View/Modify** Use the **Office Visit** pop-up menu to choose a level of permission for the Office Visits tab on the District Setup

Field	Description
	Health page: • **No Access** • **View Only** • **View / Modify** • **View / Modify / Delete** Use the **Screening** pop-up menu to choose a level of permission for the Screenings tab on the District Setup Health page: • **No Access** • **View Only** • **View / Modify** • **View / Modify / Delete** **Note:** Security for the setup Health Management pages is controlled through page-level permissions. For more information, see *Page-Level Permissions* in the *Health Management Permissions* section.
Accessible Student Screens	Select the checkbox next to each student screen that you want to be accessible to users in this group. Click **Check All** to select all checkboxes. Click **Uncheck All** to deselect all checkboxes. **Note:** The Check All and Uncheck All buttons only appear if there are multiple student screen checkboxes. The gateway to the student screens is the Quick Lookup page. Only the student screen checkboxes selected here appear as links in the main menu. If a user group is denied all access to the student screens, the system displays a message indicating access denied. If you disable access to a student screen which a user has already set as his or her default screen, the system generates an error when the user navigates to the student area. He or she can remedy this by selecting a new default screen using the Personalize function. If a security group was able to access certain student screens prior to this software update, it will still be able to do so.

7. Click **Done**. The Edit Group page appears.

How to Copy Security Permissions

Use the **Copy Security Permissions** function to copy page permissions settings and group security settings from one group to another.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Groups**. The Groups page appears.
4. Click a name in the Group Name column. The Edit Group page appears.
5. Click **Copy Security Permissions**. The Copy Security Permissions to Other Group pop-up appears.
6. Use the following table to enter information in the From Group section:

Field	**Description**
From [Name] Group	Indicates the group you selected on the previous page and the level of access.
Group Security Settings	Select the checkbox to copy group security settings. Group security settings are set using the **Edit Group page**. **Note:** This checkbox may be selected in addition to the **Page Permissions Settings** checkbox.
Page Permissions Settings	Select the checkbox to copy page permission settings. Page permission settings are set using the Access Privileges page on individual pages. **Note:** This checkbox may be selected in addition to the **Group Security Settings** checkbox.

7. Use the following table to enter information in the To Groups section:

Field	**Description**
Filter	To narrow the list of groups, begin entering the name of the group for which you want to copy security settings to.
Select All	Do one of the following: • Select the checkbox to select all groups displayed. • Deselect the checkbox to deselect all groups displayed. **Note:** This setting works with the filter so that only visible (non-filtered) groups are set.
[Individual Group]	The number, name, and default access level of each group appears. Select the checkbox of each group that you want to copy the security settings to. **Note:** Click a column heading to sort in ascending order. Click again to sort in descending order.

8. Click **Copy Settings**. The Confirm Copy Security Permissions page appears.

Note: If copying page permissions where the From Group has an access level of None or View-Only and all groups in PowerSchool are selected as To Groups, the following message appears, "You are attempting to copy a value of [View Only or No Access] to all groups. You will not be able to proceed until as least one group retains access." appears. Click **OK**.

9. Review the From Group, To Group information.

Note: Copying security settings or page permissions will replace those settings of the groups you copy to.

10. If accurate, click **Submit**. A confirmation message appears.

Note: If copying page permissions would result in one or more pages being locked out, the following message appears, "Some page permissions could not be copied because at least one user needs full access to these pages. Click here to modify the permissions to these pages manually." Click **here**. The Page Permissions that can't be Copied pop-up appears. Click the page link to adjust the page permissions for that page. The Access Privileges page appears in a separate tab on your browser. Edit the information as needed. When you click Submit, the tab on your browser closes. Repeat for each page for which you want to adjust the page permissions. When done, close the Page Permissions that Can't be Copied pop-up.

How to View/Edit Overridden Page Permissions

Use the **Overridden Page Permissions** function to view and edit pages that have a permission set to a specific level instead of the Group Access Level.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Groups**. The Groups page appears.
4. To narrow the list of groups, enter one of more search terms in the **Filter** field. Otherwise, leave blank.
5. Click a name in the Group Name column. The Edit Group page appears.
6. Click **Overridden Page Permissions**. The Overridden Page Permissions page appears.
7. Use the following table to enter information in the From Group section:

Field	Description
Filter	To locate a page, begin typing. The list of pages narrows as you enter more text.
Set All Pages To	To set all pages (on the Overridden Page Permissions page) to a specific permission level, choose one of the following from the pop-up menu: • **Group default** - Level determined as the group default on the Edit Group page for each group. For more information, see How to Edit Security Groups.

Field	Description
	- **None** - No access to the page. - **View-only** - Can read but not modify the information on the page. - **Full** - Can read and modify information on the page. **Note:** To apply, click **Submit**.
[Page]	The name of the page that has a permission set to a specific level. To define user group access: 1. Click the name of the page. The Access Privileges page appears. 2. Update the level of access for each group as needed. For field description, see *How to Set Page-Level Permissions*. 3. Click **Submit**. A confirmation message appears. 4. Close the Access Privileges page.
[Permission]	The specific permission level the page is set to. To edit, click the permission and choose one of the following from the pop-up menu: - **Group default** - Level determined as the group default on the Edit Group page for each group. For more information, see How to Edit Security Groups. - **None** - No access to the page. - **View-only** - Can read but not modify the information on the page. - **Full** - Can read and modify information on the page. **Note:** Once a page has been modified, the line item appears gray and a message displays indicating you have unsaved changes.

8. Click **Submit**. A confirmation message appears.

   Note: When visiting these pages they may only partially render. These links are only to be used to alter page level permissions, and not for entering data.

Substitute Sign In Settings

Substitute teachers at your school can use PowerTeacher Substitute to enter attendance and lunch counts for the classes they are covering. In order for substitute teachers to sign in to PowerTeacher Substitute, you will need to provide them with the school's PowerTeacher Substitute URL, the name of the school, the name of the teacher for whom you are substituting, and a password. For more information, see the PowerTeacher Substitute online help or the *PowerTeacher Substitute User Guide*.

How to Set Substitute Sign In Settings

1. On the start page, choose **School** under Setup the main menu. The School Setup page appears.
2. Under General, click **Sub Sign In Settings**. The Substitute Sign In Settings page appears.
3. Use the following table to enter information in the fields:

Field	**Description**
Sub Sign In Password	Enter the substitute password.
Include current date?	Select the checkbox to include the current date as a prefix to the password.

4. Click **Submit**. The School Setup page appears.

IP Address Restrictions

Use this function to restrict PowerSchool permissions to certain IP addresses. Depending on the network used to access PowerSchool, this can limit the PowerSchool permissions to only selected computers.

How to Restrict IP Addresses

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **IP Address Restrictions**. The IP Address Restrictions page appears.
4. Click **New**. The Edit IP Address Range page appears.
5. Use the following table to enter information in the fields:

Field	**Description**
Start of IP Range	Enter the starting IP address in the range.
End of IP Range	Enter the ending IP address in the range.

6. Click **Submit**. The IP Address Restrictions page appears.
7. Repeat steps 4-6 for each IP address range.

How to Edit IP Address Restrictions

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **IP Address Restrictions**. The IP Address Restrictions page appears.
4. Click the IP address in the Start of IP Range column that you want to edit. The Edit IP Address Range page appears.
5. Use the following table to edit information in the fields:

Field	Description
Start of IP Range	Edit the starting IP address in the range.
End of IP Range	Edit the ending IP address in the range.

6. Click **Submit**. The IP Address Restrictions page displays the edited IP address range.

How to Delete IP Address Restrictions

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **IP Address Restrictions**. The IP Address Restrictions page appears.
4. Click the IP address in the Start of IP Range column that you want to delete. The Edit IP Address Range page appears.
5. Click **Delete**.
6. Click **Confirm Delete**. The Selection Delete page appears.

Sign In Attempts Restrictions

Restrict the number of times an administrative user can unsuccessfully attempt to sign in to PowerSchool. Restricting sign in attempts is a security precaution to minimize the risk of unauthorized persons entering your PowerSchool system. To remove the restriction, reset the user's disabled IP address.

How to Restrict Sign In Attempts

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Sign In Attempts Restrictions**. The Sign In Attempts Restrictions page appears.
4. Use the following table to enter information in the fields:

Field	Description

Field	Description
Disable IP address	Select the checkbox to activate the function.
Failed sign in attempts	Enter the number of failed sign in attempts possible.
Send security e-mail notification to	Enter the email address of the person monitoring security.

5. Click **Submit**. The Sign In Attempts Restrictions page displays the new settings.
6. Restart the server to activate the settings.

How to Reset Disabled IP Addresses

Reset a user's IP address after being disabled from too many unsuccessful sign in attempts.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Sign In Attempts Restrictions**. The Sign In Attempts Restrictions page appears.
4. Click **View Disabled IP Addresses**. The Disabled IP Addresses page appears.
5. Click an IP address to reset that address and enable additional sign in attempts. The Edit Disabled IP Address page appears.
6. Click **Delete**.
7. Click **Confirm Delete**. The Selection Delete page appears.

Password Rules Management

With the introduction of Password Rules Management, PowerSchool now provides PowerSchool administrators the ability to configure various rules that are applicable when Students, Admins and Teachers, and Parents establish and maintain their passwords, including:

- Password Reset Rule
- Password Complexity Rules
- Password Expiration Rule
- Password Reuse Rule
- Account Lockout Rule

For detailed information, see *Password Rules Management*.

State Report Security

Using the Edit State Report Security page, you can restrict access to certain PowerSchool state reports to further promote security. When working with the access restriction matrix, note the following:

- Restrict Report Access must be enabled in order to edit the access restriction matrix.
- A green checkmark indicates that a security group can access a report.
- A red circle with a line through it indicates that a security group cannot access a report. If restrictions have been applied, the red circle with a line through appears in the Reports cell, the security group cell, and the report name cell.
- A pencil indicates that access restrictions have been modified from their original state but have not yet been saved. If restrictions have been modified, the pencil appears in the Reports cell, the security group cell, and the report name cell.
- Use the access restriction matrix scroll bars to see portions of the access restriction matrix that are not within view.
- Access restrictions that have been modified from their original state appear highlighted in yellow until you click **Refresh** or **Submit**.

How to Edit State Report Security

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **State Report Security**. The Edit State Report Security page appears.
4. Use the following table to enter information in the fields:

Field	**Description**
Restrict Report Access	Do one of the following: • Choose **Yes** from the pop-up menu to enable the access restriction matrix. When enabled, restrictions can be applied. • Choose **No** from the pop-up menu to disable the access restriction matrix. When disabled, all security groups have access to all reports. This is the default setting.
Reports	In the first cell of the header row, Reports appears. To edit all reports for all security groups: 1. When hovering over the Reports cell, all security groups and all reports appear highlighted. 2. Double-click the **Reports** cell to toggle the access restriction.
[Security Group]	In the subsequent cells of the header row, the name of each security group appears. To edit all reports for a selected security group: 1. When hovering over a security group cell, all reports for the selected security group appear highlighted. 2. Double-click the security group name to toggle the

Field	Description
	access restriction.
[Report Category]	In the first column, the name of each report category appears in alphabetically ascending order. To edit all reports within a report category for all security groups: 1. When hovering over a report category cell, all reports within the report category and all security groups appear highlighted. 2. Double-click the report category cell to toggle the access restriction. To edit all reports within a report category for a security group: 1. When hovering over a column cell in the report category row, all reports within the report category for the respective security group appear highlighted. 2. Double-click the column cell in the report category row to toggle the access restriction.
[Report Name]	In the first column, report names appear under their respective report categories in alphabetically ascending order. To edit a report for all security groups: 1. When hovering over a report name cell, all security groups appear highlighted. 2. Double-click the report name cell to toggle the access restriction. To edit a report for a security group: 1. When hovering over the intersecting cell of a report and security group, the cell appears highlighted. 2. Double-click the intersecting cell of the report and security group to toggle the access restriction.

5. Do one of the following:

   - Click **Refresh** to revert any pending changes highlighted in yellow.
   - Click **Submit** to save your changes.

A confirmation message appears.

6. Click **OK**.

Roles Administration

Roles Administration provides you with a central location from which to manage roles.

User Access

User Access provides PowerSchool administrators with the ability to create their own roles that control user access to PowerSchool or external applications. When a role is created, you can assign a security group to that role, which can be used to override the default security group for a user within a specific school context.

The roles are assigned to the teacher or staff member on the Admin Access and Roles tab of the Staff Security Settings page. Teacher and staff members can have multiple school affiliations. Each school affiliation can have a different role assignment. Note that all roles assignments are configured on the Admin Access and Roles tab, whether the user is a teacher or administrative staff.

It is important to understand that the security group is the backbone of a role. A role that has a PowerSchool security group can be used to override a users default security group for any school affiliation. Users can have multiple role/group combinations for each of their schools, but can only have one default security group. If a user has no roles with a PowerSchool security group, PowerSchool recognizes the users default security group. The security group determines if the user can access the administrative portion of PowerSchool, external systems, or both.

For more information on assigning roles, see *Staff Security Settings*.

How to Create a User Access Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click **New**. The Edit User Access Role page appears.
5. Use the following table to enter information in the fields:

Field	Description
Name	Enter the name of the role.
Description	Enter a description of the role.
Enabled	Select the checkbox to enable the role. Alternatively, deselect the checkbox to disable the role. When disabled, the role can still be assigned to a user, however PowerSchool will treat the role as if it does not exist. Disabled roles are preceded with a “Disabled:” prefix.
Security group assigned to the role	Select the security group you want to assign to this role. This security group will override the user default security group when this role is associated to a school on the user account. For more information, see *Role Assignments*.

Field	**Description**
Categories	Using document attachment categories, you can control user access of document attachments by associating categories with roles. By default the **Use Default** checkbox is selected for all roles when a document attachment category is created. For more information about creating categories, see *Document Attachment Categories*. 1. To modify the permissions for a document attachment category, click the **Edit** icon. The Categories - Set Category Permissions drawer appears. 2. Select one or more of the following: ▪ Select the **Download** checkbox to allow a user to download attachments for a given category. ▪ Select the **Update Details** checkbox to allow a user to edit attachments for a given category. ▪ Select the **Delete** checkbox to allow a user to delete attachments for a given category. 3. Click **Ok**. The Categories - Set Category Permissions drawer closes. **Note:** If all permissions on a given category are removed from a role, including **Use Default**, users assigned that role will have no access to documents with that category (even when other roles assigned to the user would have otherwise granted them access).

6. Click **Submit**. A confirmation message appears.

How to Edit a User Access Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click the name of the role you want to edit. The Edit User Access Role page appears.
5. Edit information as needed. For field descriptions, see *How to Create a User Access Role*.

   Note: One of the following messages may appear if the **Enabled** checkbox is deselected:

"This role is associated with fields in the field level security setup area. These associations will be disabled if you continue." For information, see *Field Level Security*.

"This role is associated with users on the Staff Security Settings page. These associations will be disabled if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Admin Access Roles*.

"User and field level security is associated with this role. These associations will be disabled if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Field Level Security* and *Admin Access Roles*.

6. Click **Submit**. A confirmation message appears.

How to Delete a User Access Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click the name of the role you want to delete. The Edit User Access Role page appears.
5. Click **Delete**.

Note: One of the following messages may appear:

"This role is associated with fields in the field level security setup area. These associations will be permanently deleted if you continue." For information, see *Field Level Security*.

"This role is associated with users on the Staff Security Settings page. These associations will be permanently deleted if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Admin Access Roles*.

"User and field level security is associated with this role. These associations will be permanently deleted if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Field Level Security* and *Admin Access Roles*.

6. Click **Confirm Delete**. The User Access Roles page appears.

How to Configure the User Access Matrix View

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click **Configure Table**. The User Access Configure Matrix View page appears.
5. Use the following table to enter information in the fields:

Field	Description
Description	The description entered for the role appears.
Short Name	For each permission, enter the text you want to display on the column heading on the User Access Roles page.
Show in Matrix	For each permission, do one of the following: • Select the checkbox to display the permission on the User Access Roles page. • Deselect the checkbox to hide the permission.

6. Click **Submit**. A confirmation message appears.

How to Sort User Access Roles

Use the following procedure to arrange the roles into the order in which you want the roles to appear on the User Access Roles page.

Note: This procedure may only be performed at the district level.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Drag and drop the role you want to move. A message appears indicating the role is being updated.
5. Repeat Step 4 for each role you want to move. When you are done, the changes are automatically saved.

   Note: If a role is added, it appears as the last item in the sort order. If a role is deleted, the sort order is automatically updated and re-sequenced as needed.

How to Search for Staff by User Access Roles

Using the Search Staff function, you can search for staff members that are assigned to a particular role.

1. On the start page, choose **Staff Search** under People in the main menu. The Search Staff page appears.
2. In the **Search Staff** field, enter the role of a staff member whose record you want to review using the format Role.useraccess= [Role Name].

   Note: Leading and trailing spaces are removed from the value for which you are searching, embedded spaces are not, and considered part of the term to match.

3. Click the **Search** icon. Staff members associated to the role appears.
4. Click the name of the individual whose record you want to review. To work with the entire group of staff members, click **Functions** at the bottom of the list to display the Group Staff Functions page. For more information about the group staff functions, see *Work With Staff Groups*.

Working With Roles Administration

Using the Roles Administration page, you can view and edit roles for Schoolnet, Co-Teaching, and User Access.

Note: This procedure may only be performed at the district level.

How to Access the Roles Administration Page

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Use the following table to enter information in the fields:

Field	**Description**
Schoolnet	Click to view and edit Schoolnet roles. For more information, see *Schoolnet*.
Co-Teaching	Click to view and edit Co-Teaching roles. For more information, see *Co-Teaching*.
User Access	Click to view and edit User Access roles. For more information, see *User Access*.

How to Create a User Access Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click **New**. The Edit User Access Role page appears.
5. Use the following table to enter information in the fields:

Field	Description
Name	Enter the name of the role.
Description	Enter a description of the role.
Enabled	Select the checkbox to enable the role. Alternatively, deselect the checkbox to disable the role. When disabled, the role can still be assigned to a user, however PowerSchool will treat the role as if it does not exist. Disabled roles are preceded with a “Disabled:” prefix.
Security group assigned to the role	Select the security group you want to assign to this role. This security group will override the user default security group when this role is associated to a school on the user account. For more information, see *Role Assignments*.

6. Click **Submit**. A confirmation message appears.

How to Edit a User Access Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click the name of the role you want to edit. The Edit User Access Role page appears.
5. Edit information as needed. For field descriptions, see *How to Create a User Access Role*.

   Note: One of the following messages may appear if the **Enabled** checkbox is deselected:

   "This role is associated with fields in the field level security setup area. These associations will be disabled if you continue." For information, see *Field Level Security*.

   "This role is associated with users on the Staff Security Settings page. These associations will be disabled if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Admin Access Roles*.

   "User and field level security is associated with this role. These associations will be disabled if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Field Level Security* and *Admin Access Roles*.

6. Click **Submit**. A confirmation message appears.

How to Delete a User Access Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click the name of the role you want to delete. The Edit User Access Role page appears.
5. Click **Delete**.

   Note: One of the following messages may appear:

   "This role is associated with fields in the field level security setup area. These associations will be permanently deleted if you continue." For information, see *Field Level Security*.

   "This role is associated with users on the Staff Security Settings page. These associations will be permanently deleted if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Admin Access Roles*.

   "User and field level security is associated with this role. These associations will be permanently deleted if you continue. If this is a user's only role at a school, then their PowerSchool security will revert to their default security group for that school. The following users will be affected: [List of Users]." For information, see *Field Level Security* and *Admin Access Roles*.

6. Click **Confirm Delete**. The User Access Roles page appears.

How to Configure the User Access Matrix View

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Click **Configure Table**. The User Access Configure Matrix View page appears.
5. Use the following table to enter information in the fields:

Field	**Description**
Description	The description entered for the role appears.
Short Name	For each permission, enter the text you want to display on the column heading on the User Access Roles page.
Show in Matrix	For each permission, do one of the following: • Select the checkbox to display the permission on the User Access Roles page.

Field	Description
	• Deselect the checkbox to hide the permission.

6. Click **Submit**. A confirmation message appears.

How to Sort User Access Roles

Use the following procedure to arrange the roles into the order in which you want the roles to appear on the User Access Roles page.

Note: This procedure may only be performed at the district level.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **User Access**. The User Access Roles page appears.
4. Drag and drop the role you want to move. A message appears indicating the role is being updated.
5. Repeat Step 4 for each role you want to move. When you are done, the changes are automatically saved.

   Note: If a role is added, it appears as the last item in the sort order. If a role is deleted, the sort order is automatically updated and re-sequenced as needed.

How to Search for Staff by User Access Roles

Using the Search Staff function, you can search for staff members that are assigned to a particular role.

1. On the start page, choose **Staff Search** under People in the main menu. The Search Staff page appears.
2. In the **Search Staff** field, enter the role of a staff member whose record you want to review using the format Role.useraccess= [Role Name].

   Note: Leading and trailing spaces are removed from the value for which you are searching, embedded spaces are not, and considered part of the term to match.

3. Click the **Search** icon. Staff members associated to the role appears.
4. Click the name of the individual whose record you want to review. To work with the entire group of staff members, click **Functions** at the bottom of the list to display the Group Staff Functions page. For more information about the group staff functions, see *Work With Staff Groups*.

Co-Teaching

Co-Teaching provides PowerSchool administrators with the ability to assign multiple lead and additional staff/teachers to a section. The teacher-of-record is the lead teacher, and other staff/teachers are the "additional" teachers.

The administrator can select additional teachers, indicating the role, the percent allocation to the role, and the start and end dates, along with an optional note for each teacher. A visual indicator is available on several pages in PowerSchool to alert you that more than one teacher shares a section. A Section Teachers icon appears next to a shared section on the Quick Lookup, Bell Schedule, and Modify Schedule pages.

If a section is shared between multiple teachers, teachers can generate section-specific reports even if they are not the lead teacher of a section in PowerTeacher gradebook. For more information, see the *PowerTeacher Gradebook User Guide* available on **PowerSource**. Some System Reports in PowerSchool will display section and teacher association data. For more information, see *System Reports.*

Setup

PowerSchool comes with default roles, which should be sufficient for most configurations. If additional roles are needed, you may setup roles with the applicable access for PowerTeacher portal and PowerTeacher gradebook.

Once the roles are defined, you can assign the roles to teachers and staff on the affected section. For more information, see *Assign Teachers to a Section*.

Co-Teaching Roles

Configure Co-Teaching Roles

Using Co-Teaching roles, you can control the level of access given to teachers who access PowerTeacher. By default, there are four predefined roles that you can assign to teachers: Lead Teacher, Co-Teacher, Teacher Aide, and Observer. You can edit or delete any of these roles except for the special “Lead Teacher” role. You can create as many other roles as needed based on your district’s needs.

Using the Co-Teaching Roles page, you can view the role assignment at a glance. A chart displays each role and the assigned properties.

Using the on the Co-Teaching Configure Matrix View page, you can customize which role assignments appear on the Co-Teaching Roles page, as well as edit the names of the properties assigned to each role.

How to Create a Co-Teaching Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.

3. Click **Co-Teaching**. The Co-Teaching Roles page appears.
4. Click **New**. The Edit Co-Teaching Role page appears.
5. Use the following table to enter information in the fields:

Field	**Description**
Name	Enter the name of the role, such as Teacher's Aide.
Description	Enter a description of the role.
Enabled	Select the checkbox to enable the role. Alternatively, deselect the checkbox to disable the role. **Note:** Disabling a role only prevents it from being selected for newly added teachers. Any teacher already assigned a role that has been disabled will continue to show as assigned to the role for reporting purposes
View sections in PowerTeacher	Select the checkbox to allow this role to view sections in PowerTeacher portal.
View sections in PowerTeacher Gradebook	Select the checkbox to allow this role to view sections in PowerTeacher Gradebook.
Edit sections in PowerTeacher Gradebook	Select the checkbox to allow this role to edit sections in PowerTeacher Gradebook.
Access sections past the end date	Select the checkbox to allow this role to access sections past their role end date. When this option is enabled, the level of access persists on the assigned section until a new role for the teacher is assigned.
Display this role in Parent/Student Portal	Select the checkbox to display this role in the PowerSchool Student and Parent portal.
Display this role in PowerSchool Admin	Select the checkbox to display this role in PowerSchool.
Display this role in PowerTeacher	Select the checkbox to display this role in PowerTeacher portal.
Display this role on reports	Select the checkbox to display this role on reports.
Default allocation percent	Enter the default allocation percent for this role.
Reference code	Enter a reference code for this role.
Alt. code 1	Enter an alternate code for this role.

Field	Description
Alt. code 2	Enter an alternate code for this role.

6. Click **Submit**. A confirmation message appears.

How to Sort Co-Teaching Roles

Use the following procedure to arrange the roles into the order in which you want the role to appear on the Co-Teaching Roles page, as well as the Manage Roles pop-up on the Section Edit page.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **Co-Teaching**. The Co-Teaching Roles page appears.
4. Drag and drop the role you want to move. A message appears indicating the role is being updated.
5. Repeat Step 4 for each role you want to move. When you are done, the changes are automatically saved.

   Note: If a role is added, it appears as the last item in the sort order. If a role is deleted, the sort order is automatically updated and re-sequenced as needed.

How to Edit a Co-Teaching Role

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **Co-Teaching**. The Co-Teaching Roles page appears.
4. Click the name of the role you want to edit. The Edit Co-Teaching Role page appears.
5. Edit information as needed. For field descriptions, see *How to Create a Role*.
6. Click **Submit**. A confirmation message appears.

How to Delete a Co-Teaching Role

Note: Roles can only be deleted if they are not in use anywhere in PowerSchool. If the role is assigned to a teacher, it will need to be reassigned to another role before you will be able to delete.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **Co-Teaching**. The Co-Teaching Roles page appears.
4. Click the name of the role you want to edit. The Edit Co-Teaching Role page appears.
5. Click **Delete**.

6. Click **Confirm Delete**. The Co-Teaching Roles page appears.

How to Configure the Co-Teaching Matrix View

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Roles Administration**. The Roles Administration page appears.
3. Click **Co-Teaching**. The Co-Teaching Roles page appears.
4. Click **Configure Table**. The Co-Teaching Configure Matrix View appears.
5. Use the following table to enter information in the fields:

Field	**Description**
Short Name	Enter the text you want to display on the column heading on the Co-Teaching Roles page. Maximum length is 100 characters.
Show in Matrix	Next to the applicable assignment, do one of the following: • Select the checkbox to display the role assignment on the Co-Teaching Roles page. • Deselect the checkbox to hide the role assignment.

6. Click **Submit**. The Co-Teaching Roles page appears.

Monitor Activity

Current Users

The Current Users page displays information about users that are currently signed in to PowerSchool, including their name, IP address, and time they last signed in to the system.

How to View a List of Current Users

The list of current users is view-only for all users.

1. On the start page, choose **Special Functions** under Functions in the main menu. The Special Functions page appears.
2. Click **Current Users**. The Current Users page appears.
3. Use the following table to understand the information in the fields:

Field	Description
Type	The user group that this user belongs to appears.
User	The name of the user appears.
Sign In	The time the user last signed in to the system appears.
Hits	The number of page item requests since the user last signed in to the system appears.
Last	The time of user's last hit appears.
IP Address	The user's computer IP address appears. This field also displays the user's operating system and Web browser type and version.
Platform	The user's hardware system.
Browser	The user's software application used to locate and display Web pages.

Invalid Sign In Attempts

Using the Invalid Sign In Attempts Report, you can monitor sign in attempts to ensure system security.

Note: Password Rules Management is only applicable to parents if parent single sign-on is enabled. For more information, see *Parent Access Management*.

How to View Invalid Sign In Attempts

1. On the start page, choose **System** under Setup in the main menu. The System Administrator Page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Report of Invalid Sign In Attempts**. The Report of Invalid Sign In Attempts page appears.
4. Use the following table to enter information in the fields:

Field	**Description**
Start Date	To search for invalid sign in attempts for a specified date range, enter the start date using the format mm/dd/yyyy. Otherwise, leave the field blank. **Note:** If you only enter a start date, the system searches from that date to today's date.
End Date	To search for invalid sign in attempts for a specified date range, enter the end date using the format mm/dd/yyyy. Otherwise, leave the field blank.
Source IP Address	To search for invalid sign in attempts using a specific IP address, enter the IP address in the field. Otherwise, leave the field blank.
Minimum Invalid Attempts	To search for invalid sign in attempts based on a minimum number of sequential attempts, enter a number in the field. Otherwise, leave the field blank.
User Type	To search for invalid sign in attempts by a specific portal, choose the appropriate portal from the pop-up menu: • **Parent** • **PowerSchool Administrator** • **PowerTeacher Administrator** • **Student** • **System Management Console Administrator** • **Teacher** Otherwise, leave the default setting of **All Users** selected.
Attempted User Name	To search for invalid sign in attempts based on specific user, enter the user's username in the field. Otherwise, leave the field blank.
Attempt Type	To search for sign in attempts based on validity, select the appropriate option: • Select **Valid Users** to search for invalid sign in attempts where the user name entered matches a user name in the system. • Select **Invalid Users** to search for invalid sign in

Field	**Description**
	attempts where the user name entered does not match a user name in the system. Otherwise, leave the default setting of **All Users** selected.

5. Click the **Search** icon. The following search results display based on the criteria you entered:

   - User Name – Click to view user account details. If the account is locked, you can unlock the account by clicking the **Unlock** button.
   - Valid User
   - User Type
   - Source IP Address
   - Attempt Date
   - Attempt Time

   Note: Click the name of a column to sort by that column in ascending order. Click again to sort in descending order. If many results appear, use the quick navigation links such as **<< first** and **next >** to navigate between the different pages of results.

Locked Accounts

Using the Locked Accounts Report, you can monitor locked accounts to ensure system security. A user account may be locked automatically if **Account Lockout Rules** is enabled and the user has exceeded the number of sign in attempts allowed. For more information, see *Password Rules Configuration*. Accounts only appear on this page if they have been automatically locked.

How to View Locked Accounts

1. On the start page, choose **System** under Setup in the main menu. The System Administrator Page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Locked Accounts**. The Manage Locked Accounts page appears.
4. Click the appropriate portal from the pop-up menu:

   - **All**
   - **Admins**
   - **Teachers**
   - **Parents**
   - **Students**

5. The following information appears for each locked account:

Field	**Description**

Field	Description
Username	The last name, first name, and username of the user that is locked out. Click to access the Security Settings page.
Account Type	Indicates the portal for which the user has an account.
Lock Details	The date, time, and reason the user is locked out of account.

How to Unlock an Account

Use this procedure to unlock a user’s account whereby allowing them access to PowerSchool, PowerTeacher, Parent Portal, or PowerSchool Parent Portal.

1. On the start page, choose **System** under Setup in the main menu. The System Administrator page appears.
2. Under Security, click **Security**. The Security page appears.
3. Click **Locked Accounts**. The Manage Locked Accounts page appears.
4. Click the appropriate portal from the pop-up menu:
    - **All**
    - **Admins**
    - **Teachers**
    - **Parents**
    - **Students**
5. Do one of the following:
    - Click **Unlock** next to each account you want to unlock.
    - Click **Unlock All [Name of Selected Portal] Accounts** to unlock all locked accounts for the selected portal.
6. Click **Submit**.