Password Rules Management User Guide

PowerSchool
Student Information System

Released June 2016

Document Owner: Documentation Services

This edition applies to Release 10 of the PowerSchool software and to all subsequent releases and modifications until otherwise indicated in new editions or updates.

The data and names used to illustrate the reports and screen images may include names of individuals, companies, brands, and products. All of the data and names are fictitious; any similarities to actual names are entirely coincidental.

Table of 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

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

Once Password Rules Management is configured, Password Rules Management functionality appears throughout PowerSchool, the PowerSchool Student and Parent portal, PowerTeacher, PowerTeacher Administrator and PowerTeacher Gradebook.

Quick Start

To get started immediately, perform the following tasks to set up and begin using Password Rules Management:

- Password Rules Management Configuration
- Configure Password Rules
- Configure Student Password Rules (optional)
- Work with Password Rules

Setup

Password Rules Management provides PowerSchool administrators the ability to configure various rules that are applicable when Students, Parents, Admins, and Teachers establish and maintain their passwords. The rules can be configured separately for each group of user types, as follows:

- Students
- Admins and Teachers
- Parents

Upgrading PowerSchool

When upgrading, Password Rules Management is automatically set to the following default values for students, admins and teachers, and parents:

- Password Reset Rule – Disabled.
- Password Complexity Rules (Minimum characters) – Set to **1** for students, admins, and teachers. Set to **6** for parents.
- Password Complexity Rules (Password contains) – Disabled.
- Password Expiration Rule – Disabled.
- Password Reuse Rule – Disabled.
- Account Lockout Rule – Disabled.

Once you have configured Password Rules Management, subsequent upgrades will preserve your configurations.

During the upgrade, user account data is migrated into the new Password Rules Management PCAS tables. Once the upgrade is completed, a comma-delimited file is created in the PowerSchool logs folder (the same folder containing pslog.txt and dalx.log) called PCAS_Migrate.csv. The file only contains errors and modified usernames. If the file appears empty, all accounts migrated successfully and without change. To open the file, use a spreadsheet application, such as Excel. The file displays original usernames, new usernames where the original usernames had to be modified, and any errors that were encountered during the migration. Possible errors include:

- Failed to migrate: Indicates that the account could not be migrated for unexpected reasons.
- Truncated password to 40 characters: Indicates that the user's password was too long for an admin-entered password and has been truncated to the first 40 characters of the password.

- Failed Rename in Legacy Table (PCAS and Legacy out of sync!): Indicates that the new username was created in PCAS, but was not copied back over to the legacy table overwriting the original username; as a result, the user will not be able to sign in; therefore, manually change the user's username via the appropriate PowerSchool page.

Note: If you are unable to identify a user by their username, the DCID value for that particular row in the appropriate table is given; you can use the DCID value to bring up the matching record in USM.

Using the information provided, you can notify users who usernames had to be modified (user names are modified to prevent duplicate user names from migrating to the new Password Rules Management PCAS tables, as well as to troubleshoot any data migration issues.

Installing PowerSchool

When installing, Password Rules Management is automatically set to the following default values for students, admins and teachers, and parents:

- Password Reset Rule – Enabled.
- Password Complexity Rules (Minimum characters) – Set to **7**.
- Password Complexity Rules (Password contains) – Enabled.
- Password Expiration Rule – Set to **60** days.
- Password Reuse Rule – Set to **5**.
- Account Lockout Rule – Set to **5**.

Configure Password Rules

Using Password Rules Management, you define password reset, complexity, expiration, reuse, and lockout rules based on your district’s needs. Once configured, user may encounter the following messages:

Occurs	Message	Action
Sign In	Your password was set by the system administrator. Please change your password.	User to reset their password. Refer them to appropriate *How to Reset Your Password* procedure.

Sign In	Your password has expired. Please create a new password.	User to reset their password. Refer them to appropriate *How to Reset Your Password* procedure.
Sign In	The number of sign in attempts for this account has been exceeded. Contact your school directly for assistance.	User to contact you to unlock their account. See *How to Unlock an Account*.
Reset Password Change Password	Current password is not correct.	User to re-enter password accordingly.
Reset Password Change Password	New password must be at least [number] characters long.	User to re-enter password accordingly.
Reset Password Change Password	New password must contain at least one uppercase and one lowercase letter.	User to re-enter password accordingly.
Reset Password Change Password	New password must contain at least one letter and one number.	User to re-enter password accordingly.
Reset Password Change Password	New password must contain at least one special character.	User to re-enter password accordingly.
Reset Password Change Password	The verification password you enter must match the new password.	User to re-enter password accordingly.
Reset Password Change Password	The password entered was previously used. Please enter a new password.	User to re-enter password accordingly.

How to Configure Password Rules

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 **Password Rules Management**. The Password Rules Management page appears. By default, the Password Rules tab is selected.
4. Use the following table to enter information in the fields:

Field	Description
Password Reset Rule	To require a user to reset their password upon first signing in, select the applicable checkboxes: **Note:** If you do not want to apply this rule, leave the checkbox blank. • Select the **Students** checkbox to apply this rule to students' passwords. • Select the **Admins and Teachers** checkbox to apply this rule to administrators' and teachers' passwords. • Select the **Parents** checkbox to apply this rule to parents' passwords.
Password Complexity Rules	Indicate the minimum number of characters a password must contain (value between 1 and 24): • Enter the desired number in the **Students** field to apply this rule to students' passwords. • Enter the desired number in the **Admins and Teachers** field to apply this rule to administrators' and teachers' passwords. • Enter the desired number in the **Parents** field to apply this rule to parents' passwords. To require a user's password contain at least 1 uppercase letter, 1 lowercase letter, 1 special character, and 1 numeric character, select the applicable checkboxes:

	Note: If you do not want to apply this rule, leave the checkbox blank. • Select the **Students** checkbox to apply this rule to students' passwords. • Select the **Admins and Teachers** checkbox to apply this rule to administrators' and teachers' passwords. • Select the **Parents** checkbox to apply this rule to parents' passwords.
Password Expiration Rule	Indicate the number of days a user may use a password before being required to enter a new password: **Note:** If you do not want to apply this rule, enter **0**. • Enter the desired number in the **Students** field to apply this rule to students' passwords. • Enter the desired number in the **Admins and Teachers** field to apply this rule to administrators' and teachers' passwords. • Enter the desired number in the **Parents** field to apply this rule to parents' passwords.
Password Reuse Rule	Indicate the number of different passwords a user must use before a password may be reused after resetting the password: **Note:** If you do not want to apply this rule, enter **0**. • Enter the desired number in the **Students** field to apply this rule to students' passwords. • Enter the desired number in the **Admins and Teachers** field to apply this rule to administrators' and teachers' passwords. • Enter the desired number in the **Parents** field to apply this rule to parents' passwords.
Account Lockout Rule	Indicate the number of times users may enter an incorrect password before being locked out:

	Note: If you do not want to apply this rule, enter **0**. • Enter the desired number in the **Students** field to apply this rule to students' passwords. • Enter the desired number in the **Admins and Teachers** field to apply this rule to administrators' and teachers' passwords. • Enter the desired number in the **Parents** field to apply this rule to parents' passwords.

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

How to Reset Password Rules Default Settings

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 **Password Rules Management**. The Password Rules Management page appears. By default, the Password Rules tab is selected.
4. Click **Load Default Settings**. A confirmation message appears indicating the default settings have been loaded.

   Note: For details about default values, see *Installing PowerSchool*.

5. Click **Submit**. A confirmation message appears indicating your changes have been saved.

Configure Student Password Rules

Once password rules are established, you have the option to provide students with the ability to change their own passwords when using the PowerSchool Student and Parent portal. Settings on this page affect the ability of students to change their own passwords based on their school and grade level. If a student is able to change their password, any password rules settings enabled for students will be enforced for the password they choose.

Note: By default, students may not change their passwords, This feature must be enabled.

How to Configure Student Password Rules

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 **Password Rules Management**. The Password Rules Management page appears. By default, the Password Rules Management tab is selected.
4. Click the **Student Password Management** tab. The Student Password Management tab appears selected.
5. Locate the name of the school for which you want students to be able to change their own passwords.
6. For the selected school, choose the grade level for which you want students to be able to change their own passwords from the **Enable At and Above Grade** pop-up menu.
7. Repeat Step 5 through Step 6 for each school for which you want students to be able to change their own passwords
8. Click **Submit**. A confirmation message appears.

Invalid Sign In Attempts

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

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 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
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, or the PowerSchool Student and 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**.

Work with Password Rules

Once Password Rules Management is configured, Password Rules Management functionality appears throughout PowerSchool, the PowerSchool Student and Parent Portal, PowerTeacher, PowerTeacher Administrator and PowerTeacher Gradebook.

PowerSchool

Note: Information in this section appears in the PowerSchool online help, as well as *The Basics User Guide* available on PowerSource.

- *How to Sign In to PowerSchool*
- *How to Reset Your Password*
- *How to Change Your Password*

PowerSchool Student and Parent Portal Administrator

Note: Information in this section appears in the PowerSchool online help, as well and the *PowerSchool Student and Parent Portal Administrator Guide* available on PowerSource.

- *How to Create a Parent Account*
- *How to Reset a Parent Account Password*

PowerSchool Student and Parent Portal

Note: Information in this section appears in the PowerSchool Student and Parent portal online help, as well as in the *PowerSchool Student and Parent Portal User Guide* available on PowerSource.

- *How to Sign In to PowerSchool Student and Parent Portal*
- *How to Reset Your Password*
- *How to Recover Your Password*
- *How to Create a Parent Account*
- *How to Change Your Account Preferences*

PowerTeacher

Note: Information in this section appears in the PowerTeacher online help, as well as the *PowerTeacher Portal User Guide* available on PowerSource.

- *How to Sign In to PowerTeacher*
- *How to Reset Your Password*
- *How to Change Your Password*