

Password Setting Updates in CBS Firmware 3.2.0.84

Objective

The objective of this article is to go over the password setting updates in the Cisco Business Switches Firmware 3.2.0.84

Applicable Devices | Software Version

CBS250 | 3.2.0.84

CBS350 | 3.2.0.84

Introduction

The firmware version 3.2.0.84 for Cisco Business Switches (CBS)250 and CBS350 series has several optional and mandatory password setting updates. A number of these settings will become enabled when you update your switch to version 3.2.0.84

Mandatory password settings cannot be disabled by users either in the web user interface (UI) or in the Command Line Interface (CLI).

Keep reading to find out more!

Table of Contents

- [Password Menu](#)
- [New Mandatory Password Rules](#)
- [Error Messages](#)
- [Password Generator](#)

Password Menu

To access the changed password settings menu:

Step 1

Log in to your CBS switch.



Switch

User Name **1**

Password **2**

English ▾

Log In **3**

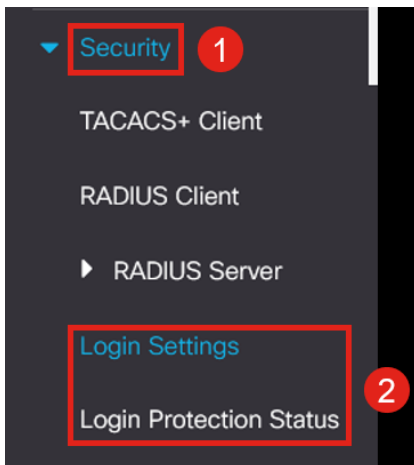
Step 2

Choose **Advanced** from the drop-down at the top of the web user interface (UI) of the switch.



Step 3

Navigate to **Security** and you will see two menu options – *Login Settings* which contains the old Password Strength menu options and some additional menu options and a new *Login Protection Status* menu.



Step 4

Click on *Login Settings*. This menu has two sections - *Login Settings* and *Login Lockdown*

The *Login Settings* include the older password strength settings with the recent password protection settings.

Password Aging - This is disabled by default. If enabled, it allows you to set a *Password Aging Time* in Days.

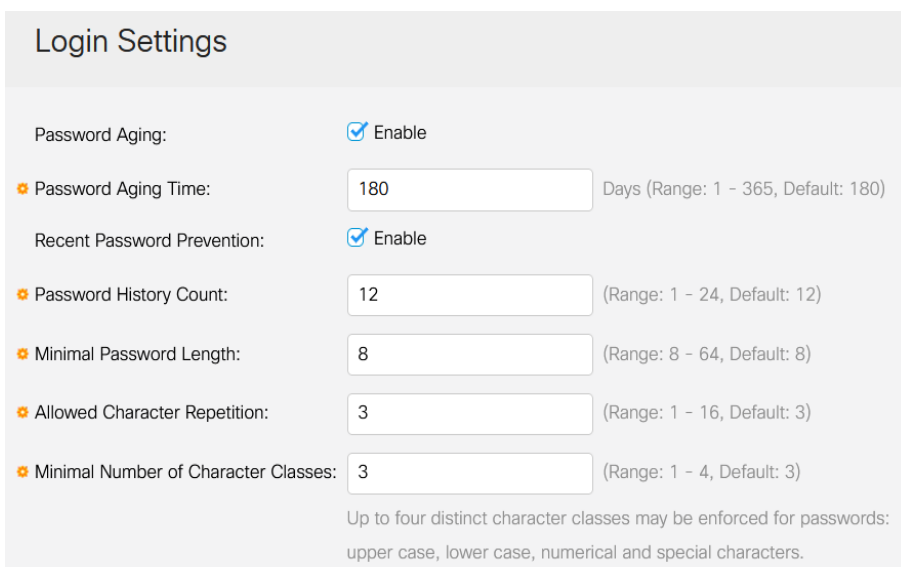
Recent Password Prevention - keeps users from changing their password and immediately changing their password back to their old password. This is disabled by default.

Password History Count – It can be set to a value between 1 and 24, with the default being 12 passwords remembered.

Minimal Password Length - the minimum number of characters that can be used for your password.

Allowed Character Repetition - the maximum number of characters that can be repeated in a row. For example, if you set your password to TACRocks2222 this would fail, because it has four repeated 2, but TACRocks222 would work, because it only has three.

Minimal Number of Character Classes – There are four distinct character classes: Upper Case, Lower Case, Number, and Special Characters. You can configure how many of these classes need to be used in a password.



Login Settings

Password Aging: Enable

✦ Password Aging Time: Days (Range: 1 - 365, Default: 180)

Recent Password Prevention: Enable

✦ Password History Count: (Range: 1 - 24, Default: 12)

✦ Minimal Password Length: (Range: 8 - 64, Default: 8)

✦ Allowed Character Repetition: (Range: 1 - 16, Default: 3)

✦ Minimal Number of Character Classes: (Range: 1 - 4, Default: 3)

Up to four distinct character classes may be enforced for passwords:
upper case, lower case, numerical and special characters.

Step 5

The *Login Lockdown* menu has two sections - the *Login Response Delay* and the *Quiet Period Enforcement*, both of which are disabled by default.

The *Login Response Delay* forces a 1 to 10 second delay between the login attempt and the response. This can dramatically slow automated dictionary attacks against the system.

The *Quiet Period Enforcement* essentially locks down access to the switch for management if a user attempts to login too many times with an incorrect password.

The settings include:

Quiet Period Length - the number of seconds to lock down access when it's triggered.
Triggering Attempts and the *Triggering Interval* tells you the number of failed login attempts (the triggering attempts) in the period being monitored (the triggering interval) before it locks down access.

By default, if it's enabled, it will lock down the system after four failed logins in a sixty second period.

The *Quiet Period Access Profile* specifies how an admin can access the device during the lockdown. By default, this is only via the console port and should not be changed unless the user has a specific reason to change it.

Additional Access Profiles can be added if needed under *Security > Mgmt Access Method > Access Profiles*.

Login Lockdown

Login Response Delay: Enable

✱ Response Delay Period: Sec (Range: 1 - 10, Default: 1)

Quiet Period Enforcement: Enable

✱ Quiet Period Length: Sec (Range: 1 - 65535, Default: 300)

✱ Triggering Attempts: (Range: 1 - 100, Default: 4)

✱ Triggering Interval: Sec (Range: 1 - 3600, Default: 60)

Quiet Period [Access Profile](#) : ▾

Step 6

The new *Login Protection Status* menu is an informational display. It shows what users have failed to log into the switch through either the console, SSH, or the Web UI.

It also shows how many login failures have happened in the last 60 seconds, and if there is a lockdown blocking new SSH or Web UI connections.

Login Protection Status Refresh

Quiet Mode Status : Inactive

Login Failures in Last 60 Seconds : 0

Login Failure Table				
Username	IP Address	Service	Count	Most Recent Attempt Time
user1	172.16.1.108	HTTP	9	29-Apr-2022 10:53:18

New Mandatory Password Rules

These will apply to all new user accounts and any password changes made to existing user accounts.

New Rules **CANNOT** be disabled.

It will verify that the password is not from a list of known common passwords. This common password list was compiled by choosing the 10,000 most used passwords from a list of the 10,000,000 most common passwords. This list can be found on the [github](#) link.

No variations of the common passwords using upper/lower case or using the following character substitutions:

"\$" for "s", "@" for "a", "0" for "o", "1" for "l", "!" for "i", "3" for "e"

It will block passwords that include more than two sequential characters in a row (again looking for common substitutions and case). For example, if a password contains *abc*, it will be blocked as it has three sequential letters. So would *@bc* since there is the common substitution of the @ symbol for a. Similarly, *cba* will be blocked as it is sequential in reverse order. Other examples include "efg123!\$", "abcd765%", "kji!\$378", "qr\$58!230".

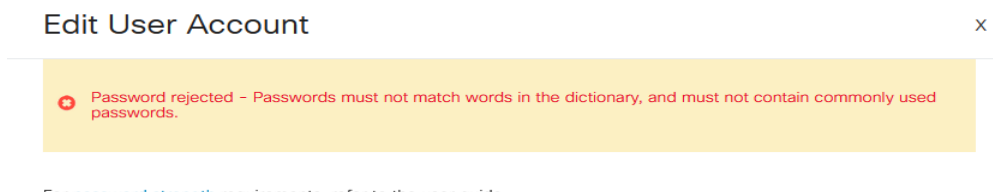
New password must not contain the username. For example, no "Admin548" for user admin.

New password must not contain the manufacturer name. For example, no C!sc0lsCool.

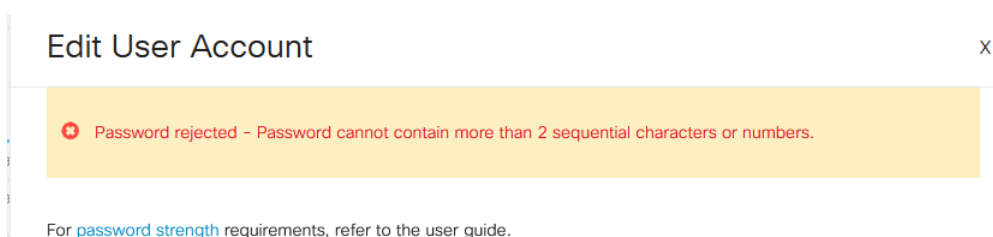
New password must not contain the product name. For example, no CBSCo0l\$witch

Error Messages

If you try to use a password that is either in the dictionary or contains commonly used passwords, you will see the following error message.



If you use a password that contains sequential characters, you will again get the following error message.

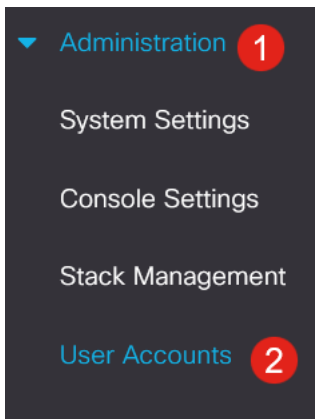


Password Generator

To help you come up with valid passwords when either creating new users or editing existing user, a random password generator has been built into the web UI of the switch.

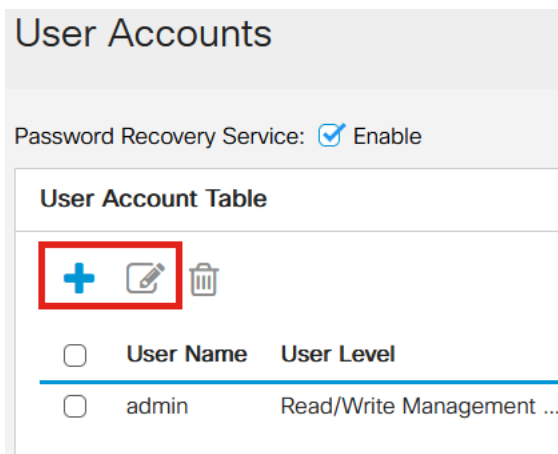
Step 1

Go to **Administration > User Accounts**.



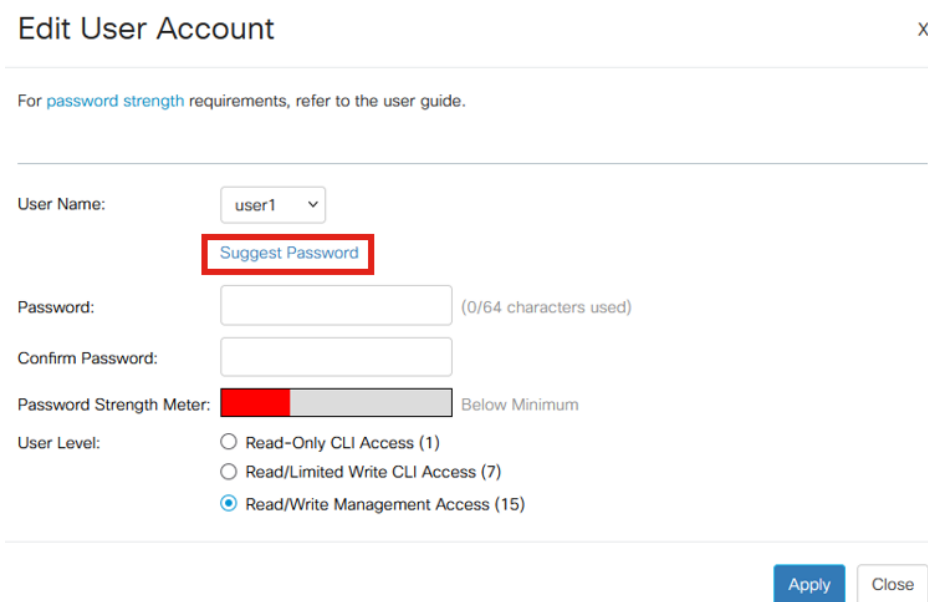
Step 2

Either *Add* or *Edit* a user account.



Step 3

Click on the **Suggest Password** link.



Step 4

A page will open with the password suggestion, and you can copy this new password to the clipboard. To use the password for the account, simply click **Yes**.

Suggest Password

X

The following strong password has been generated:

 eAnU&bM5#fh3 Copy to Clipboard **1**

Would you like to use it for this account?

2

It is VERY important that you copy this password to the clipboard before you say Yes to use it for the account. If you do not save this password before saying yes, you will not be able to find out what the password is, and it is unlikely that you will remember it. Save the copied password to a document in a safe location.

This process will generate a valid password, but it is possible that the password it generates might not be a "Strong" password according to the password strength meter. If it says the password is 'Weak', you can try another suggested password or add characters to the end of the string.

Conclusion

Now you know all about the password setting updates in Cisco Business Switches Firmware 3.2.0.84