

CBSファームウェア3.2.0.84のパスワード設定の更新

目的

この記事の目的は、Cisco Business Switchesファームウェア3.2.0.84のパスワード設定のアップデートを確認することです

該当するデバイス | ソフトウェアバージョン

CBS250 | 3.2.0.84

CBS350 | 3.2.0.84

概要

Cisco Business Switch(CBS)250およびCBS350シリーズ用のファームウェアバージョン3.2.0.84には、オプションおよび必須のパスワード設定のアップデートがいくつか含まれています。これらの設定の多くは、スイッチをバージョン3.2.0.84にアップデートすると有効になります

Webユーザインターフェイス(UI)またはコマンドラインインターフェイス(CLI)でユーザが必須パスワード設定を無効にすることはできません。

詳細を見つけるために読み続ける！

目次

- [パスワードメニュー](#)
- [新しい必須パスワードルール](#)
- [エラーメッセージ](#)
- [パスワードジェネレータ](#)

パスワードメニュー

変更されたパスワード設定メニューにアクセスするには、次の手順に従います。

手順 1

CBSスイッチにログインします。



Switch

User Name **1**

Password **2**

English ▾

Log In **3**

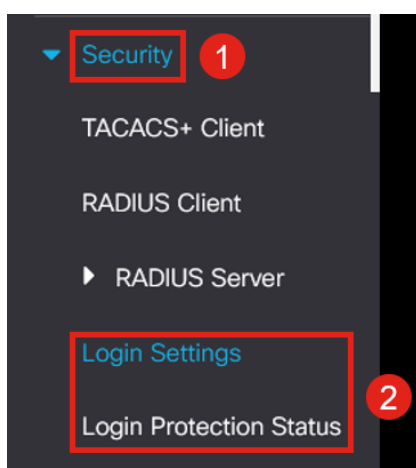
手順 2

スイッチのWebユーザインターフェイス(UI)の上部にあるドロップダウンから [Advanced] を選択します。



手順 3

[Security] に移動すると、[Login Settings] の2つのメニューオプションが表示されます。このメニューオプションには、古い[Password Strength]メニューオプションといくつかの追加メニューオプションが含まれており、新しい[Login Protection Status]メニューが含まれています。



手順 4

[Login Settings] をクリックします。このメニューには、[Login Settings] と [Login Lockdown] の2つのセクションがあります

[Login Settings] には、最新のパスワード保護設定を使用した古いパスワードの強度設定が含まれています。

Password Aging : デフォルトでは無効になっています。有効になっている場合は、パスワードのエイジングタイム (日数) を設定できます。

最近のパスワード防止 : ユーザがパスワードを変更したり、すぐにパスワードを古いパスワードに戻したりすることを防ぎます。これは、デフォルトでは無効になっています。

Password History Count: 1 ~ 24の値に設定できます。デフォルトは12個のパスワードが記憶されています。

Minimum Password Length : パスワードに使用できる最小文字数。

Allowed Character Repetition: 1行に繰り返し可能な最大文字数。たとえば、パスワードをTACRocks2222に設定した場合、2が4回繰り返されるため失敗しますが、TACRocks222は3回しか繰り返されないため動作します。

文字クラスの最小数: 4つの異なる文字クラスがあります。大文字、小文字、数字、および特殊文字。これらのクラスのうち、パスワードで使用する必要のあるクラスの数を設定できます。

Login Settings

Password Aging:	<input checked="" type="checkbox"/> Enable
✦ Password Aging Time:	<input type="text" value="180"/> Days (Range: 1 - 365, Default: 180)
Recent Password Prevention:	<input checked="" type="checkbox"/> Enable
✦ Password History Count:	<input type="text" value="12"/> (Range: 1 - 24, Default: 12)
✦ Minimal Password Length:	<input type="text" value="8"/> (Range: 8 - 64, Default: 8)
✦ Allowed Character Repetition:	<input type="text" value="3"/> (Range: 1 - 16, Default: 3)
✦ Minimal Number of Character Classes:	<input type="text" value="3"/> (Range: 1 - 4, Default: 3)

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

手順 5

[Login Lockdown] メニューには、[Login Response Delay] と [Quiet Period] [Enforcement] の2つのセクションがあり、デフォルトではどちらも無効になっています。

*Login Response Delay*は、ログイン試行と応答の間に1 ~ 10秒の遅延を強制します。これにより、システムに対する自動化された辞書攻撃が大幅に遅くなる可能性があります。

*Quiet Period Enforcement*は、ユーザが誤ったパスワードで何度もログインを試みた場合、基本的に管理のためにスイッチへのアクセスをロックします。

設定は次のとおりです。

Quiet Period Length : トリガーされたときにアクセスをロックダウンする秒数。

*Triggering Attempts*および*Triggering Interval*は、監視対象の期間 (トリガー間隔) 内でログイン試行の失敗 (トリガー試行) の回数を示します。この回数を超えると、アクセスがロックされます。

デフォルトでは、この機能が有効になっている場合、ログインに60秒間に4回失敗す

ると、システムがロックダウンされます。

*Quiet Period Access Profile*は、ロックダウン中に管理者がデバイスにアクセスする方法を指定します。デフォルトでは、これはコンソールポートを介してのみであり、ユーザが変更する特定の理由がない限り変更しないでください。

必要に応じて、[Security] > [Mgmt Access Method] > [Access Profiles] でアクセスプロファイルを追加できます。

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](#) : ▾

手順 6

新しい[Login Protection Status] メニューは情報を表示するメニューです。コンソール、SSH、またはWeb UIを介してスイッチにログインできなかったユーザを表示します。

また、過去60秒間に発生したログイン障害の数と、新しいSSHまたはWeb UI接続をブロックするロックダウンが存在するかどうかを示します。

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

新しい必須パスワードルール

これらは、すべての新規ユーザアカウントと、既存のユーザアカウントに加えられたパスワード変更に応用されます。

新しいルールを無効にすることはできません。

パスワードが既知の共通パスワードのリストに含まれていないことを確認します。この共通パスワードリストは、10,000,000の最も一般的なパスワードのリストから10,000の最も頻繁に使用されるパスワードを選択することによってコンパイルされました。このリストは[github](#)リンクにあります。

大文字と小文字を使用したり、次の文字を置き換えたりして、一般的なパスワードを変更することはできません。

"\$" ("s"用)、"@ ("a"用)、"0" ("o"用)、"1" ("l"用)、"! "i"は"3"は"e"です。

連続する2つ以上の文字を含むパスワードをブロックします (共通の置換と大文字と小文字を再度検索します)。たとえば、パスワードにabcが含まれている場合は、連続する3文字が含まれているためブロックされます。@bcも同様です。これは、aの@記号の共通置換があるためです。同様に、cbaは順番が逆であるためブロックされます。その他の例としては、「efg123!\$」、「abcd765%」、「kji!\$378」、「qr\$58!230」などがあります。

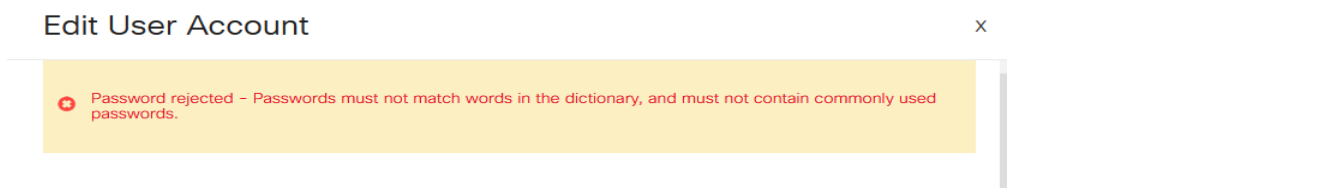
新しいパスワードにユーザ名を含めることはできません。たとえば、ユーザadminには「Admin548」はありません。

新しいパスワードに製造元名を含めることはできません。たとえば、no C!sc0lsCoolと指定します。

新しいパスワードに製品名を含めることはできません。たとえば、no CBSCo0l\$witchと入力します。

エラーメッセージ

辞書に登録されているパスワード、または一般的に使用されるパスワードを使用しようとすると、次のエラーメッセージが表示されます。

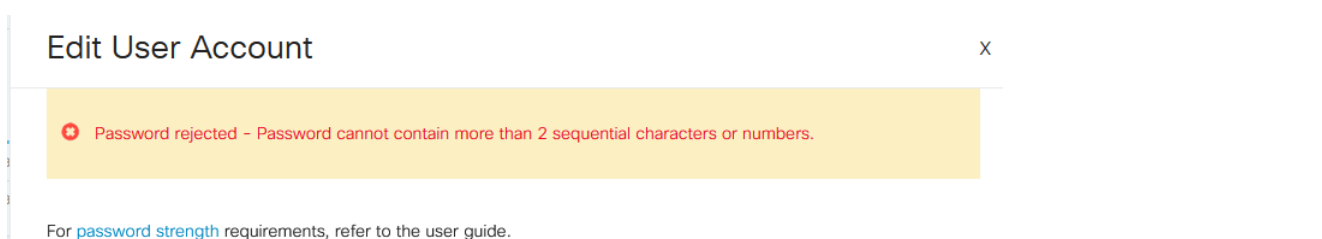


Edit User Account x

✘ Password rejected - Passwords must not match words in the dictionary, and must not contain commonly used passwords.

For [password strength](#) requirements, refer to the user guide.

連続した文字を含むパスワードを使用すると、次のエラーメッセージが再び表示されます。



Edit User Account x

✘ Password rejected - Password cannot contain more than 2 sequential characters or numbers.

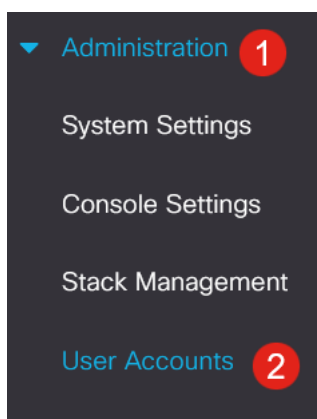
For [password strength](#) requirements, refer to the user guide.

パスワードジェネレータ

新規ユーザの作成または既存ユーザの編集の際に有効なパスワードを見つけやすくするため、スイッチのWeb UIにはランダムパスワードジェネレータが組み込まれています。

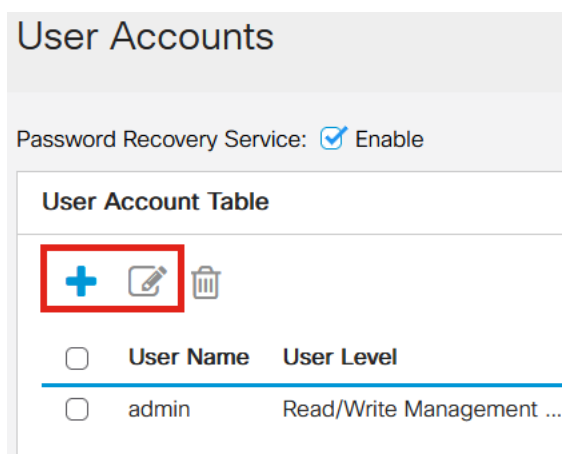
手順 1

[Administration] > [User Accounts] に移動します。



手順 2

ユーザアカウントを追加または編集します。



手順 3


[Suggest Password] リンクをクリックします。

For password strength requirements, refer to the user guide.

User Name:

Password: (0/64 characters used)

Confirm Password:

Password Strength Meter:  Below Minimum

User Level:

- Read-Only CLI Access (1)
- Read/Limited Write CLI Access (7)
- Read/Write Management Access (15)

手順 4

パスワードの提案を含むページが開き、この新しいパスワードをクリップボードにコピーできます。アカウントのパスワードを使用するには、**Yes**をクリックします。

Suggest Password

The following strong password has been generated:

 eAnU&bM5#fh3 1

Would you like to use it for this account?

2

このパスワードをアカウントに使用するには、「はい」と言う前にクリップボードにコピーすることが非常に重要です。「はい」と言う前にこのパスワードを保存しないと、パスワードが何であるかを知ることができず、パスワードを覚えている可能性はほとんどありません。コピーしたパスワードを安全な場所の文書に保存します。

このプロセスでは有効なパスワードが生成されますが、パスワード強度メーターによると、生成されるパスワードが「強力な」パスワードではない可能性があります。パスワードが「Weak」と表示されている場合は、別の推奨パスワードを試すか、文字列の末尾に文字を追加します。

結論

これで、Cisco Business Switchesファームウェア3.2.0.84のパスワード設定の更新に関するすべての情報が得られました