

# CBS固件3.2.0.84中的密码设置更新

## 目标

本文的目的是查看思科业务交换机固件3.2.0.84中的密码设置更新

## 适用设备 | 软件版本

CBS250 | 3.2.0.84

CBS350 | 3.2.0.84

## 简介

适用于思科业务交换机(CBS)250和CBS350系列的固件版本3.2.0.84具有几个可选和强制密码设置更新。当您更新到3.2.0.84版时，其中很多设置将启用

用户无法在Web用户界面(UI)或命令行界面(CLI)中禁用强制密码设置。

继续阅读以了解更多信息！

## 目录

- [密码菜单](#)
- [新的强制密码规则](#)
- [错误消息](#)
- [密码生成器](#)

## 密码菜单

要访问更改的密码设置菜单，请执行以下操作：

### 第 1 步

登录您的CBS交换机。



# Switch

User Name **1**

---

Password **2**

---

English ▾

---

Log In **3**

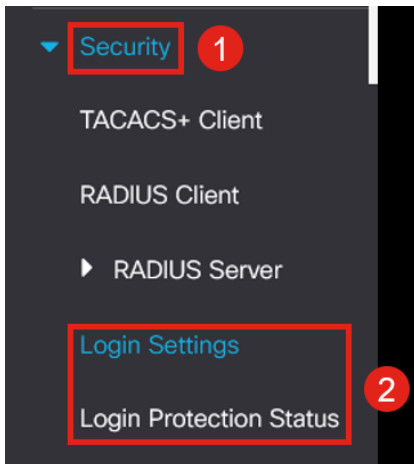
## 步骤 2

从交换机Web用户界面(UI)顶部的下拉菜单中选择**Advanced**。



## 步骤 3

导航到**Security**，您将看到两个菜单选项 — *Login Settings*，其中包含旧的“密码强度”菜单选项、一些其他菜单选项和新的*Login Protection Status*菜单。



## 步骤 4

单击*Login Settings*。此菜单包含两个部分 — *Login Settings*和*Login Lockdown*

*Login Settings*将旧密码强度设置与最近的密码保护设置相结合。

- Password Aging* — 默认情况下禁用。如果启用，则允许您设置密码老化时间(天)。
- 最近的密码防护* — 阻止用户更改其密码并立即将其密码改回旧密码。默认情况下它是禁用的。
- Password History Count* — 可以将其设置为介于1和24之间的值，默认情况下记住了12个

密码。

*Minimal Password Length* — 可用于密码的最小字符数。

*允许的字符重复* — 可在行中重复的最大字符数。例如，如果您将密码设置为TACRocks2222，则此操作会失败，因为它有四个重复的2，但TACRocks222会起作用，因为它只有三个。

*最小字符类数* — 有四个不同的字符类：大写、小写、数字和特殊字符。您可以配置密码中需要使用的此类类的数量。

### 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.

## 步骤 5

*Login Lockdown*菜单包含两个部分 — *Login Response Delay*和*Quiet Period*实施，这两个部分在默认情况下均处于禁用状态。

*Login Response Delay*强制在登录尝试和响应之间进行1到10秒的延迟。这可以显著降低对系统的自动字典攻击。

*Quiet Period Enforcement*实质上会锁定对交换机的访问，以便在用户尝试使用不正确的密码登录过多时进行管理。

设置包括：

*Quiet Period Length* — 触发访问时锁定访问的秒数。

*触发尝试*和*触发间隔*告诉您在锁定访问之前监控的期间（*触发间隔*）内失败的登录尝试（*触发尝试*）次数。

默认情况下，如果已启用，它将在六十二秒内四次登录失败后锁定系统。

*Quiet Period Access Profile*指定管理员如何在锁定期间访问设备。默认情况下，这仅通过控制台端口进行，除非用户有特定原因进行更改，否则不应进行更改。

如果需要，可以在*Security > Mgmt Access Method > Access Profiles*下添加其他访问配置文件。

### 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](#) :  ▾

## 步骤 6

新的 *Login Protection Status* 菜单是信息性显示。它显示了哪些用户未能通过控制台、SSH或Web UI登录交换机。

它还显示过去60秒发生了多少次登录失败，以及是否存在阻止新SSH或Web UI连接的锁定。

### 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

## 新的强制密码规则

这些将应用于所有新用户帐户以及对现有用户帐户所做的任何密码更改。

无法禁用新规则。

它将检验密码是否不是来自已知常用密码列表。此通用密码列表的编译方法是从一万个最常用密码的列表中选择一万个最常用密码。此列表可在[github](#)链接上找到。

常用密码不能使用大写/小写或以下字符替换：

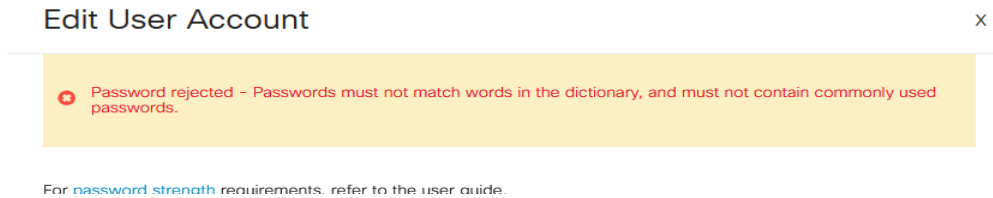
“\$”表示“s”，“@”表示“a”，“0”表示“o”，“1”表示“l”，“！”“i”表示“3”表示“e”

它将阻止连续包含两个以上连续字符的密码（再次查找常见的替换和大小写）。例如，如果密码包含`abc`，则会被阻止，因为它有三个连续字母。`@bc`也是如此，因为`@`符号常用于替换。同样，`cba`将被阻止，因为它以相反顺序排列。其他示例包括“`efg123!$`”、“`abcd765%`”、“`kji!$378`”、“`qr$58!230`”。

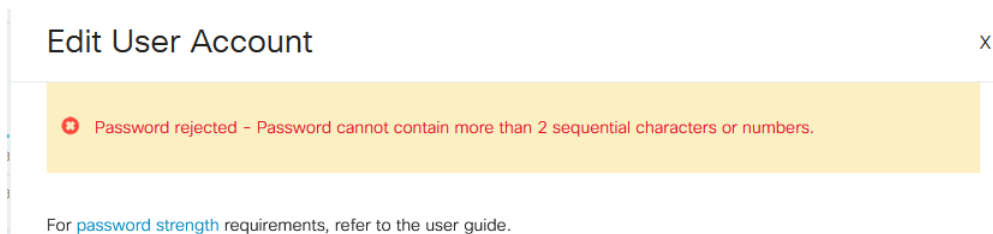
新密码不得包含用户名。例如，对于用户admin，no "Admin548"。  
新密码不得包含制造商名称。例如，no C!sc0lsCool。  
新密码不得包含产品名称。例如，no CBSCo0l\$witch

## 错误消息

如果您尝试使用字典中的密码或包含常用密码的密码，您将看到以下错误消息。



如果使用包含连续字符的密码，您将再次收到以下错误消息。

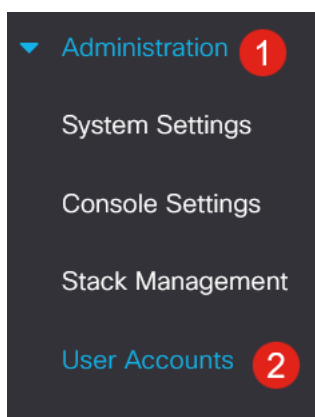


## 密码生成器

为了帮助您在创建新用户或编辑现有用户时设置有效密码，交换机的Web UI中内置了随机密码生成器。

### 第 1 步

转至**管理**>用户帐户。



### 步骤 2

*Add*或*Edit*用户帐户。

## User Accounts

Password Recovery Service:  Enable

### User Account Table

<input type="checkbox"/>	User Name	User Level
<input type="checkbox"/>	admin	Read/Write Management ...

### 步骤 3

单击Suggested Password链接。

## Edit User Account X

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

User Name:  ▼

[Suggest Password](#)

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)

### 步骤 4

将会打开一个包含密码建议的页面，您可以将此新密码复制到剪贴板。要使用帐户的密码，只需单击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

在对该帐户使用“是”之前，必须将此密码复制到剪贴板。如果在说“是”之前不保存此密码，您将无法了解密码是什么，而且您也不太可能记住它。将复制的密码保存到安全位置的文档中。

此过程将生成一个有效密码，但根据密码强度计，它生成的密码可能不是“强”密码。如果密码为“弱”，您可以尝试使用另一个建议的密码或在字符串的末尾添加字符。

## 结论

现在您已了解思科业务交换机固件3.2.0.84中的密码设置更新