Actualizaciones de configuración de contraseña en CBS Firmware 3.2.0.84

Objetivo

El objetivo de este artículo es revisar las actualizaciones de configuración de contraseña en el firmware 3.2.0.84 de los switches Cisco Business

Dispositivos aplicables | Versión de software

CBS250 |3.2.0.84
CBS350 |3.2.0.84

Introducción

La versión de firmware 3.2.0.84 para Cisco Business Switches (CBS)250 y CBS350 Series incluye varias actualizaciones de configuración de contraseñas opcionales y obligatorias. Algunos de estos parámetros se activarán cuando actualice el switch a la versión 3.2.0.84

Los usuarios no pueden deshabilitar la configuración de contraseña obligatoria en la interfaz de usuario web (UI)I ni en la interfaz de línea de comandos (CLI).

¡Sigue leyendo para obtener más información!

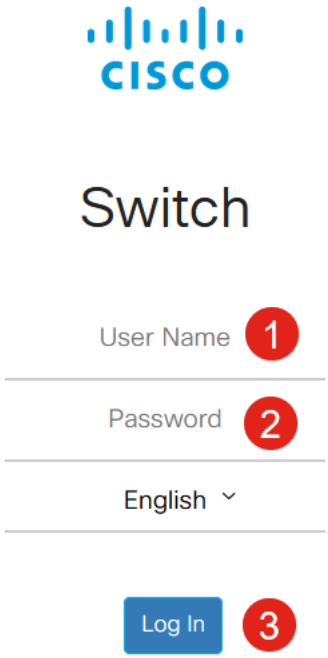
Table Of Contents

Menú Contraseña

Para acceder al menú de configuración de contraseña modificada:

Paso 1

Inicie sesión en el switch CBS.

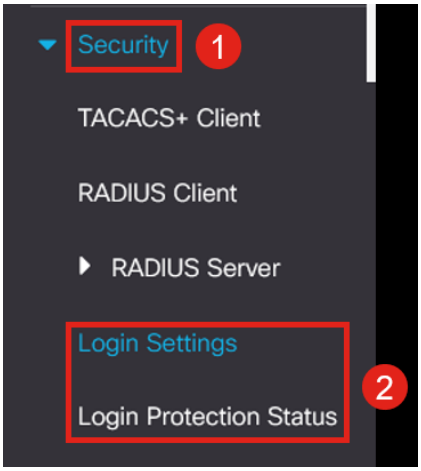


Paso 2

Elija **Advanced** en la lista desplegable de la parte superior de la interfaz de usuario web del switch.

Paso 3

Navegue hasta **Seguridad** y verá dos opciones de menú - *Configuración de inicio de sesión* que contiene las opciones de menú de la antigua Fortaleza de contraseña y algunas opciones de menú adicionales y un nuevo *menú Estado de protección de inicio de sesión*.

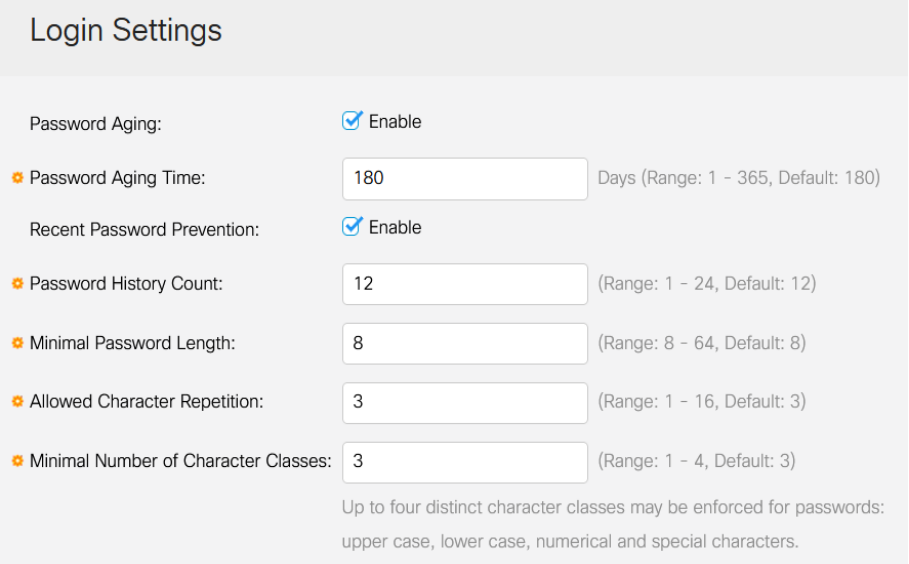


Paso 4

Haga clic en *Login Settings*. Este menú tiene dos secciones: *Configuración de inicio de sesión* y *Bloqueo de inicio de sesión*

La configuración de inicio de sesión incluye la configuración de seguridad de contraseña anterior con la configuración de protección de contraseña reciente.

Antigüedad de contraseña: esta opción está desactivada de forma predeterminada. Si está activado, le permite establecer una *hora de caducidad de la contraseña* en días.
Prevención de contraseñas reciente: evita que los usuarios cambien su contraseña y la cambien inmediatamente a la antigua. Esto está desactivado de forma predeterminada.
Recuento de historial de contraseñas: se puede establecer en un valor entre 1 y 24, siendo el valor predeterminado 12 contraseñas recordadas.
Longitud mínima de la contraseña: el número mínimo de caracteres que se puede utilizar para la contraseña.
Repetición de caracteres permitida: el número máximo de caracteres que se pueden repetir en una fila. Por ejemplo, si configura su contraseña en TACRocks2222 esto fallaría, porque tiene cuatro repeticiones 2, pero TACRocks222 funcionaría, porque sólo tiene tres.
Número mínimo de clases de caracteres: hay cuatro clases de caracteres diferentes: Mayúsculas, minúsculas, números y caracteres especiales. Puede configurar cuántas de estas clases deben utilizarse en una contraseña.



Paso 5

El menú *Login Lockdown* tiene dos secciones: *Login Response Delay* y *Quiet Period* En,ambas desactivadas de forma predeterminada.

El *retraso de respuesta de inicio de sesión* fuerza un retraso de 1 a 10 segundos entre el intento de inicio de sesión y la respuesta. Esto puede ralentizar drásticamente los ataques automatizados de diccionario contra el sistema.

La *Aplicación de Periodo Tranquilo* bloquea esencialmente el acceso al switch para la administración si un usuario intenta iniciar sesión demasiadas veces con una contraseña incorrecta.

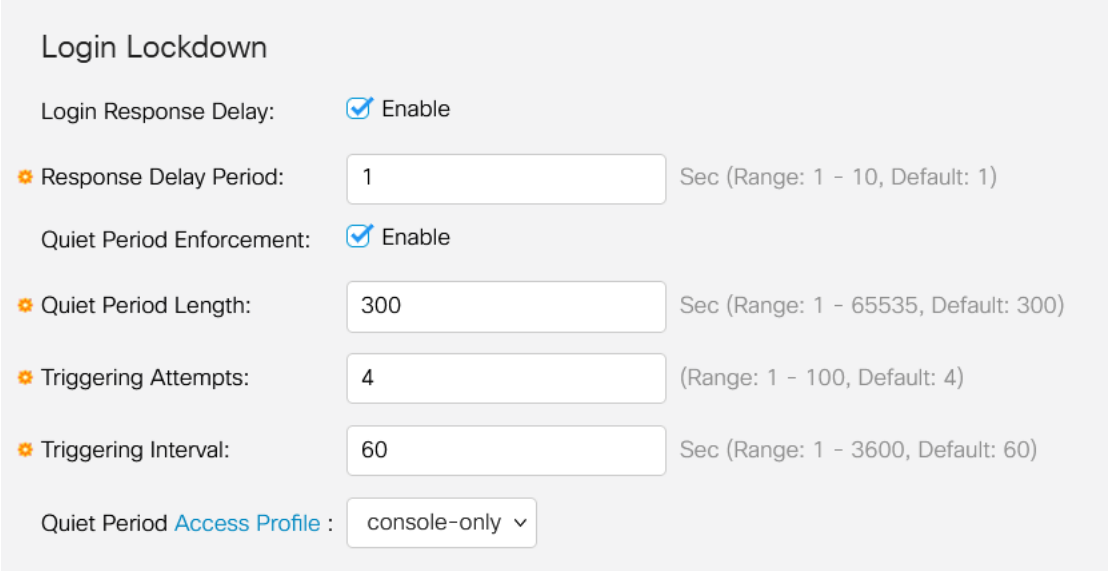
La configuración incluye:

Duración del período silencioso: el número de segundos que se debe bloquear el acceso cuando se activa.
El desencadenado de intentos y el *intervalo de desencadenado* le indica el número de intentos de inicio de sesión fallidos (los intentos de desencadenado) en el período que se está supervisando (el intervalo de activación) antes de que bloquee el acceso.

De forma predeterminada, si está activado, bloqueará el sistema después de cuatro inicios de sesión fallidos en un período de sesenta segundos.

El *perfil de acceso de período tranquilo* especifica cómo un administrador puede acceder al dispositivo durante el bloqueo. De forma predeterminada, esto sólo se realiza a través del puerto de la consola y no se debe cambiar a menos que el usuario tenga un motivo específico para cambiarlo.

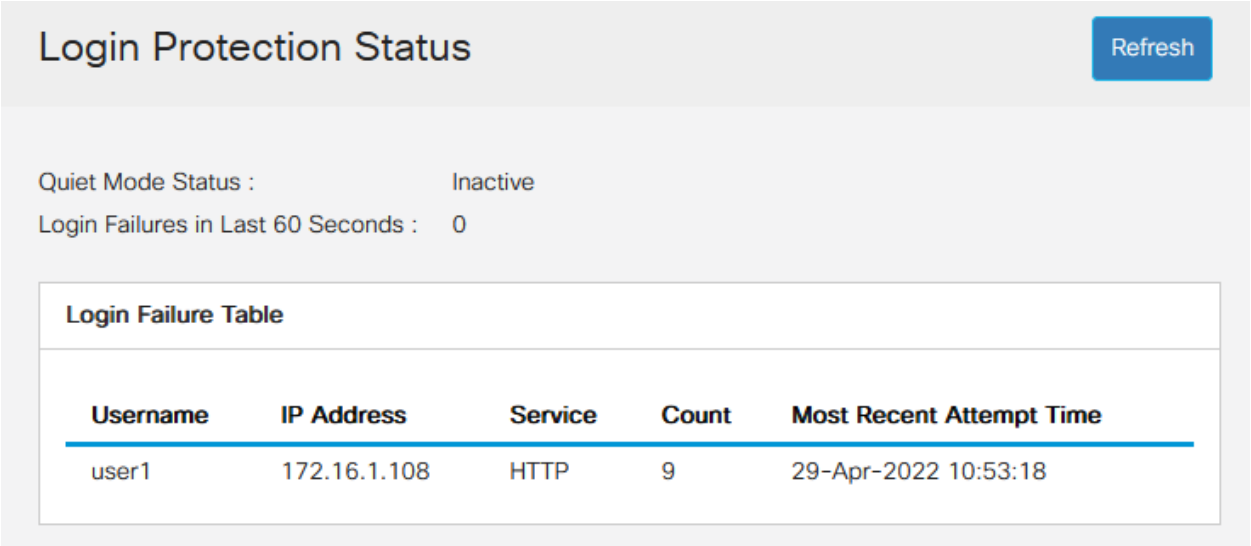
Se pueden agregar perfiles de acceso adicionales si es necesario en *Seguridad > Método de acceso de administración > Perfiles de acceso.*



Paso 6

El nuevo menú *Estado de protección de inicio de sesión* es una visualización informativa. Muestra lo que los usuarios no han podido iniciar sesión en el switch a través de la consola, SSH o la interfaz de usuario web.

También muestra cuántos fallos de inicio de sesión han ocurrido en los últimos 60 segundos y si hay un bloqueo que bloquea nuevas conexiones SSH o de interfaz de usuario web.



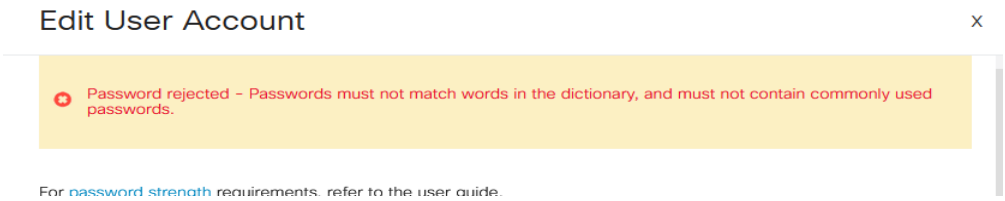
Nuevas reglas de contraseña obligatorias

Se aplicarán a todas las cuentas de usuario nuevas y a los cambios de contraseña realizados en las cuentas de usuario existentes.

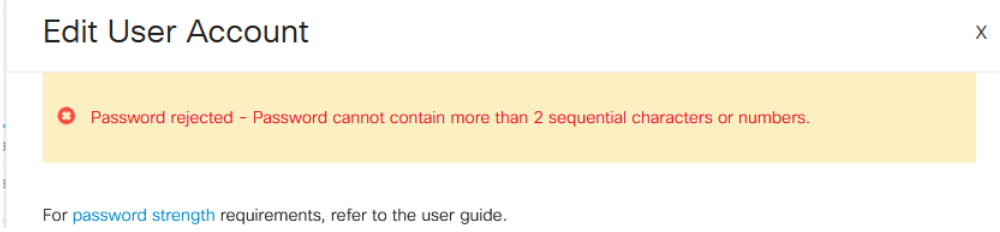
Las nuevas reglas **NO PUEDEN** desactivarse.
Comprobará que la contraseña no pertenece a una lista de contraseñas comunes conocidas. Esta lista común de contraseñas se compiló eligiendo las 10.000 contraseñas más usadas de una lista de las 10.000.000 contraseñas más comunes. Esta lista se puede encontrar en el enlace **github**.
Ninguna variación de las contraseñas comunes utilizando mayúsculas/minúsculas o utilizando las siguientes sustituciones de caracteres:
"$" por "s", "@" por "a", "0" por "o", "1" por "l", "!" para "i", "3" para "e"
Bloqueará las contraseñas que incluyen más de dos caracteres secuenciales en una fila (buscando de nuevo las sustituciones y casos comunes). Por ejemplo, si una contraseña contiene *abc*, se bloqueará porque tiene tres letras secuenciales. Así que *@bc* ya que hay la sustitución común del símbolo @ por un. De manera similar, *cba* se bloqueará porque es secuencial en orden inverso. Otros ejemplos incluyen "efg123!$", "abcd765%", "kji!$378", "qr$58!230".
La nueva contraseña no debe contener el nombre de usuario. Por ejemplo, no hay "Admin548" para el usuario admin.
La nueva contraseña no debe contener el nombre del fabricante. Por ejemplo, no C!sc0IsCool.
La nueva contraseña no debe contener el nombre del producto. Por ejemplo, no CBSCo0l$witch

Mensajes de error

Si intenta utilizar una contraseña que se encuentra en el diccionario o que contiene contraseñas comúnmente utilizadas, verá el siguiente mensaje de error.



Si utiliza una contraseña que contiene caracteres secuenciales, volverá a recibir el siguiente mensaje de error.

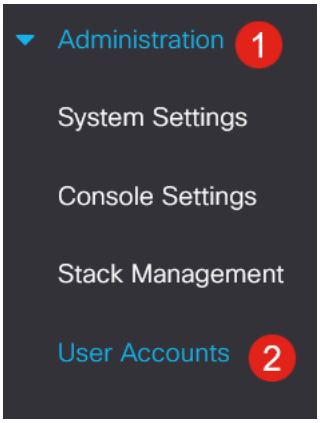


Generador de contraseñas

Para ayudarle a obtener contraseñas válidas al crear nuevos usuarios o editar usuarios existentes, se ha incorporado un generador de contraseñas aleatorio en la interfaz de usuario web del switch.

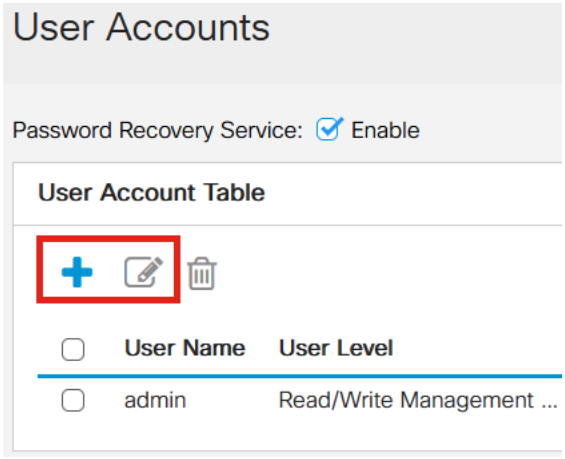
Paso 1

Vaya a **Administración > Cuentas de usuario**.



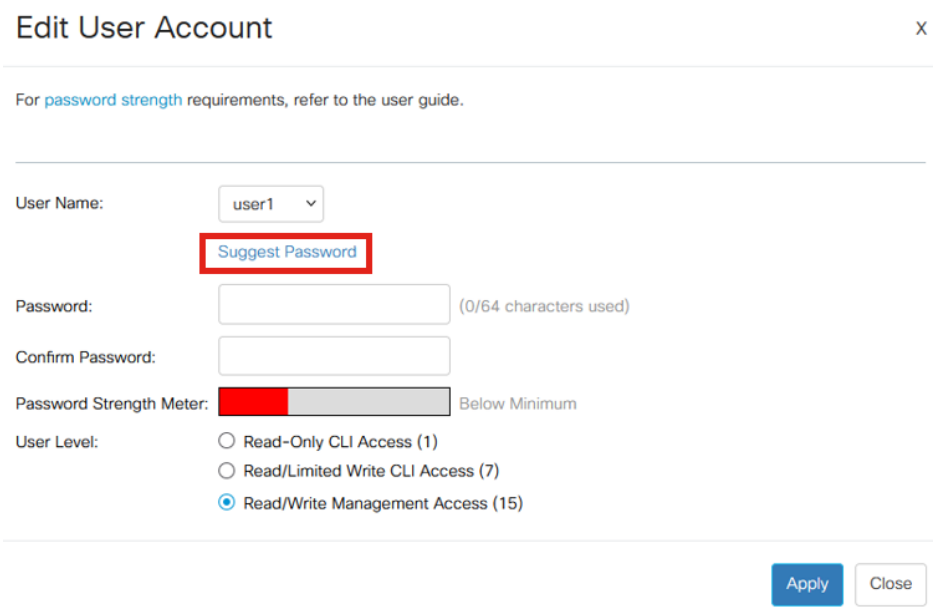
Paso 2

Agregar o *Editar* una cuenta de usuario.



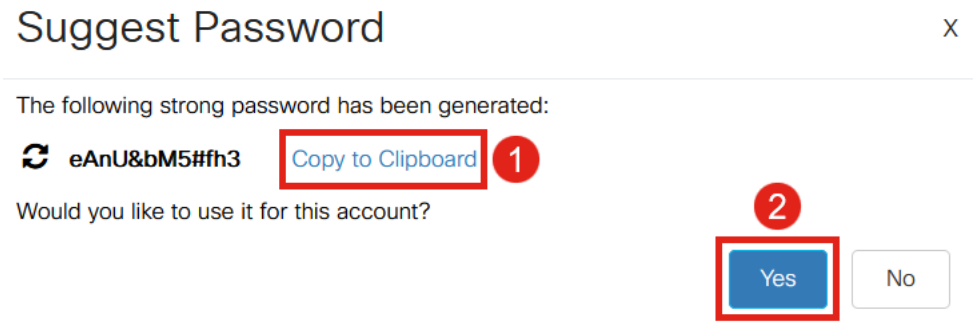
Paso 3

Haga clic en el enlace **Sugerir contraseña**.



Paso 4

Se abrirá una página con la sugerencia de contraseña y podrá copiar esta nueva contraseña en el portapapeles. Para utilizar la contraseña de la cuenta, simplemente haga clic en **Yes**.



Es MUY importante que copie esta contraseña en el portapapeles antes de decir Sí para utilizarla en la cuenta. Si no guarda esta contraseña antes de decir sí, no podrá averiguar cuál es la contraseña y es poco probable que la recuerde. Guarde la contraseña copiada en un documento en una ubicación segura.

Este proceso generará una contraseña válida, pero es posible que la contraseña que genera no sea una contraseña "segura" según el medidor de seguridad de la contraseña. Si dice que la contraseña es "débil", puede probar otra contraseña sugerida o agregar caracteres al final de la cadena.

Conclusión

Ahora sabe todo sobre las actualizaciones de configuración de contraseñas en el firmware 3.2.0.84 de los switches Cisco Business