

CBS 펌웨어 3.2.0.84의 비밀번호 설정 업데이트

목표

이 문서의 목적은 Cisco Business Switches 펌웨어 3.2.0.84의 비밀번호 설정 업데이트를 살펴보는 것입니다

적용 가능한 장치 | 소프트웨어 버전

CBS250 | 3.2.0.84

CBS350 | 3.2.0.84

소개

Cisco Business Switches(CBS)250 및 CBS350 시리즈용 펌웨어 버전 3.2.0.84에는 몇 가지 선택적 및 필수 비밀번호 설정 업데이트가 있습니다. 스위치를 버전 3.2.0.84로 업데이트하면 이러한 설정 중 다수가 활성화됩니다

웹 UI(사용자 인터페이스) 또는 CLI(명령줄 인터페이스)에서 사용자가 필수 비밀번호 설정을 비활성화할 수 없습니다.

더 많은 것을 알아보려면 계속 읽으세요!

목차

- [암호 메뉴](#)
- [새 필수 비밀번호 규칙](#)
- [오류 메시지](#)
- [비밀번호 생성기](#)

암호 메뉴

변경된 비밀번호 설정 메뉴에 액세스하려면

1단계

CBS 스위치에 로그인합니다.



Switch

User Name **1**

Password **2**

English ▾

Log In **3**

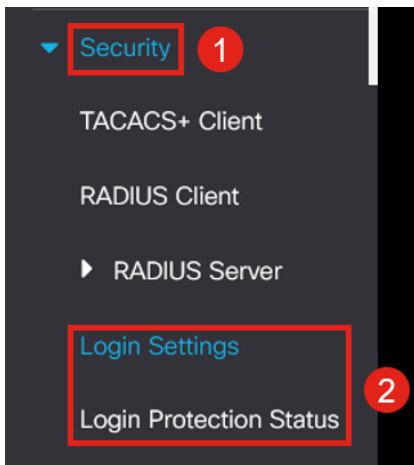
2단계

스위치의 웹 UI(사용자 인터페이스) 상단에 있는 드롭다운에서 **Advanced**(고급)를 선택합니다.



3단계

Security(보안)로 이동하면 *Login Settings*(로그인 설정)의 두 가지 메뉴 옵션이 표시됩니다. 이 옵션에는 이전 Password Strength(비밀번호 강도) 메뉴 옵션과 일부 추가 메뉴 옵션 및 새 *Login Protection Status*(로그인 보호 상태) 메뉴가 포함됩니다.



4단계

Login Settings(로그인 설정)를 클릭합니다. 이 메뉴에는 *Login Settings*(로그인 설정)와 *Login Lockdown*(로그인 잠금)의 두 섹션이 있습니다

Login Settings(로그인 설정)에는 최근 비밀번호 보호 설정과 함께 이전 비밀번호 강도 설정이 포함됩니다.

비밀번호 에이징 - 기본적으로 비활성화되어 있습니다. 활성화하면 비밀번호 에이징 시간(일)을 설정할 수 있습니다.

최신 비밀번호 방지 - 사용자가 비밀번호를 변경하고 즉시 이전 비밀번호로 다시 변경할 수 없게 합니다. 이는 기본적으로 비활성화되어 있습니다.

Password History Count(비밀번호 기록 수) - 1~24 사이의 값으로 설정할 수 있으며 기본값은 12개의 비밀번호가 기억됩니다.

최소 비밀번호 길이 - 비밀번호에 사용할 수 있는 최소 문자 수입니다.

Allowed Character Repetition - 한 행에서 반복할 수 있는 최대 문자 수입니다. 예를 들어 비밀번호를 TACRocks222로 설정하면 4개의 반복 2가 있으므로 이 작업은 실패하지만 TACRocks222는 3개만 있으므로 작동합니다.

최소 문자 클래스 수 - 네 가지 문자 클래스가 있습니다. 대문자, 소문자, 숫자 및 특수 문자입니다. 비밀번호에 이러한 클래스를 몇 개 사용해야 하는지 구성할 수 있습니다.

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.

5단계

Login Lockdown 메뉴에는 **Login Response Delay** 및 **Quiet Period Enforcement**의 두 섹션이 있으며, 둘 다 기본적으로 비활성화되어 있습니다.

Login Response Delay(로그인 응답 지연)는 로그인 시도와 응답 사이에 1초에서 10초의 지연을 강제합니다. 이는 시스템에 대한 자동화된 사전 공격을 극적으로 늦출 수 있습니다.

자동 기간 적용은 사용자가 잘못된 비밀번호로 너무 많이 로그인을 시도할 경우 관리를 위해 스위치에 대한 액세스를 기본적으로 차단합니다.

다음과 같은 설정이 포함됩니다.

Quiet Period Length - 트리거될 때 액세스를 잠글 시간(초)입니다.

Triggering Attempts 및 **Triggering Interval**은 액세스를 잠그기 전에 모니터링되는 기간(트리거링 간격) 동안 실패한 로그인 시도(트리거링 시도) 수를 알려줍니다.

기본적으로 활성화되어 있으면 60초 동안 4번의 로그인이 실패한 후 시스템이 잠깁니다.

Quiet Period Access Profile(자동 기간 액세스 프로파일)은 잠금 중에 관리자가 디바이

스에 액세스하는 방법을 지정합니다. 기본적으로 이 작업은 콘솔 포트를 통해서만 수행되며 사용자가 변경할 특별한 사유가 없는 한 변경할 수 없습니다.

필요한 경우 Security(보안) > Management Access Method(관리 액세스 방법) > Access Profiles(액세스 프로필)에서 추가 액세스 프로필을 추가할 수 있습니다.

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 :

6단계

새로운 *Login Protection Status* 메뉴는 정보 표시입니다. 사용자가 콘솔, SSH 또는 웹 UI를 통해 스위치에 로그인하지 못한 내용을 표시합니다.

또한 지난 60초 동안 발생한 로그인 실패 횟수와 새 SSH 또는 웹 UI 연결을 차단하는 잠금이 있는 경우에도 표시됩니다.

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

새 필수 비밀번호 규칙

이는 모든 새 사용자 계정 및 기존 사용자 계정의 암호 변경 사항에 적용됩니다.

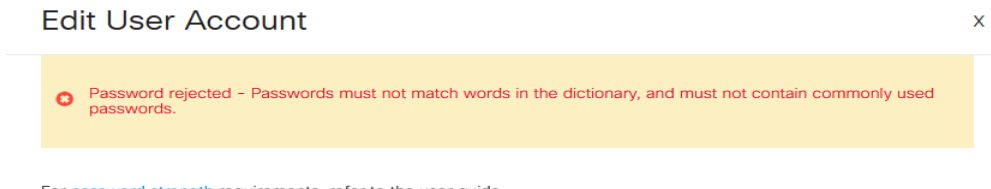
새 규칙을 비활성화할 수 없습니다.

알려진 일반 비밀번호 목록에서 비밀번호가 아닌지 확인합니다. 이 공통 비밀번호 목록은 가장 많이 사용되는 비밀번호 10,000,000개의 목록에서 가장 많이 사용되는 비밀번호

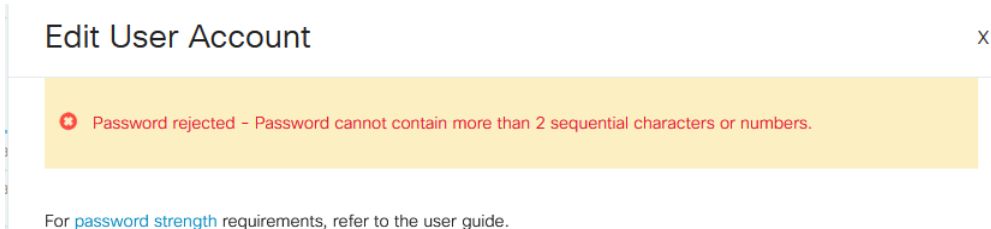
10,000개를 선택하여 컴파일했습니다. 이 목록은 github 링크에서 찾을 수 있습니다.
대문자/소문자 또는 다음 문자 대체를 사용하는 일반 비밀번호의 변형은 없습니다.
"s"의 경우 "\$", "a"의 경우 "@", "o"의 경우 "0", "l"의 경우 "1", "!" "!"의 경우 "3"의 경우 "e"
이 명령은 연속되는 두 개 이상의 문자가 포함된 비밀번호를 차단합니다(일반적인 대용과 대소문자를 다시 찾음). 예를 들어 비밀번호에 abc가 포함되어 있으면 세 개의 연속된 문자가 있으므로 비밀번호가 차단됩니다. 또한 @bc는 @ 기호를 a로 대체한다는 공통점이 있으므로 마찬가지로 cba는 역순으로 순차적이므로 차단됩니다. 다른 예에는 "efg123!\$", "abcd765%", "kjl!\$378", "qr\$58!230"이 포함됩니다.
새 비밀번호는 사용자 이름을 포함할 수 없습니다. 예를 들어 사용자 admin에 대해 "Admin548"이 없습니다.
새 암호는 제조업체 이름을 포함할 수 없습니다. 예를 들어, C!sc0!sCool이 없습니다.
새 암호는 제품 이름을 포함할 수 없습니다. 예를 들어, CBSCo0!\$witch가 없습니다.

오류 메시지

사전에 있거나 일반적으로 사용되는 비밀번호를 포함하는 비밀번호를 사용하려고 하면 다음 오류 메시지가 표시됩니다.



순차 문자가 포함된 비밀번호를 사용하는 경우 다음 오류 메시지가 다시 표시됩니다.

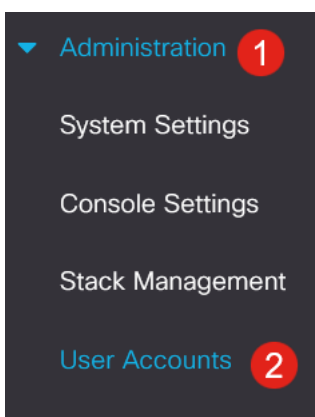


비밀번호 생성기

새 사용자를 만들거나 기존 사용자를 편집할 때 유효한 암호를 만들 수 있도록 스위치의 웹 UI에 임의 암호 생성기가 내장되어 있습니다.

1단계

Administration(관리) > User Accounts(사용자 계정)로 이동합니다.






2단계

사용자 계정 추가 또는 편집

User Accounts

Password Recovery Service: Enable

User Account Table



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

3단계

Suggest Password(비밀번호 제안) 링크를 클릭합니다.

Edit User Account

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)

4단계

암호 제안과 함께 페이지가 열리며 이 새 암호를 클립보드에 복사할 수 있습니다. 계정의 암호를 사용하려면 [예]를 클릭하십시오.

Suggest Password

The following strong password has been generated:

 eAnU&bM5#fh3 [Copy to Clipboard](#) 1

Would you like to use it for this account?

2

이 암호를 계정에 사용하려면 [예]라고 말하기 전에 클립보드에 복사하는 것이 매우 중요합니다. 이 비밀번호를 저장하지 않고 예라고 말하면 비밀번호가 무엇인지 알 수 없으며 기억될 가능성이 거의 없습니다. 복사한 암호를 안전한 위치에 문서에 저장합니다.

이 프로세스에서는 유효한 비밀번호를 생성하지만, 비밀번호 강도 측정기에 따라 "Strong" 비밀번호가 아닐 수 있습니다. 비밀번호가 'Weak'으로 표시되면 다른 권장 비밀번호를 시도하거나 문자열의 끝에 문자를 추가할 수 있습니다.

결론

이제 Cisco Business Switches Firmware 3.2.0.84의 비밀번호 설정 업데이트에 대해 모두 알 수 있습니다