CLI(Command Line Interface)를 통해 스위치에서 비밀번호 설정 구성

목표

콘솔을 통해 스위치에 처음 로그인할 때는 기본 사용자 이름 및 비밀번호(*cisco*)를 사용해야 합니다. 그런 다음 Cisco 어카운트에 대한 새 비밀번호를 입력하고 구성하라는 메시지가 표시됩니다. 비밀번호 복잡성은 기본적으로 활성화되어 있습니다. 선택하는 암호가 복잡하지 않으면 다른 암호를 만들라는 메시지가 표시됩니다.

비밀번호는 디바이스에 액세스하는 사용자를 인증하는 데 사용되므로 단순 비밀번호는 잠재적인 보안 위험입니다. 따라서 비밀번호 복잡성 요구 사항은 기본적으로 적용되며 필요에 따라 구성할 수 있습니다.

이 문서에서는 CLI(Command Line Interface)를 통해 기본 비밀번호 설정, 회선 비밀번호, 비밀번호 활성화, 서비스 비밀번호 복구, 사용자 계정의 비밀번호 복잡성 규칙, 스위치의 비밀번호 에이징 설정을 정의하는 방법에 대한 지침을 제공합니다.

참고: 스위치의 웹 기반 유틸리티를 통해 비밀번호 강도 및 복잡성 설정을 구성할 수도 있습니다. 여기를 클릭하여 지침을 확인하십시오.

적용 가능한 디바이스 | 소프트웨어 버전

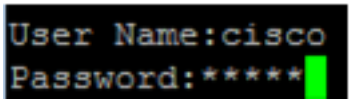
- SX300 시리즈 | 1.4.7.06(최신 다운로드)
- SX350 시리즈 | 2.2.8.04(최신 다운로드)
- SG350X 시리즈 | 2.2.8.04(최신 다운로드)
- SX500 시리즈 | 1.4.7.06(최신 다운로드)
- SX550X 시리즈 | 2.2.8.04(최신 다운로드)

CLI를 통해 비밀번호 설정 구성

아래 옵션에서 구성할 비밀번호 설정을 선택합니다.

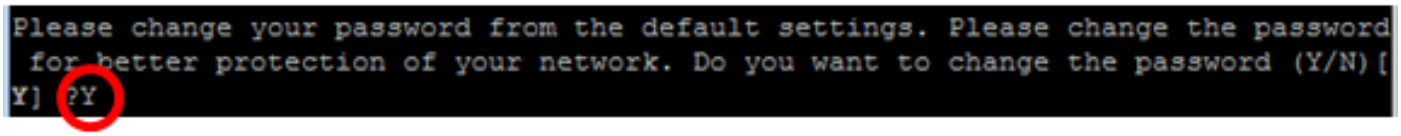
기본 비밀번호 설정 구성

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다.



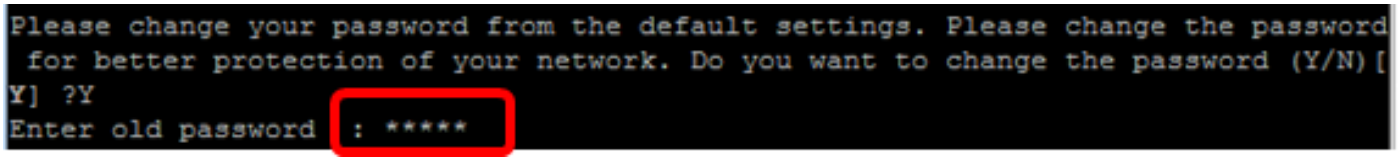
참고: 사용 가능한 명령 또는 옵션은 디바이스의 정확한 모델에 따라 달라질 수 있습니다. 이 예에서는 SG350X 스위치가 사용됩니다.

2단계. 네트워크 보호를 개선하기 위해 새 비밀번호를 구성하라는 메시지가 표시됩니다. 키보드에서 **Y**를 Yes로, **N**을 **누릅니다**.

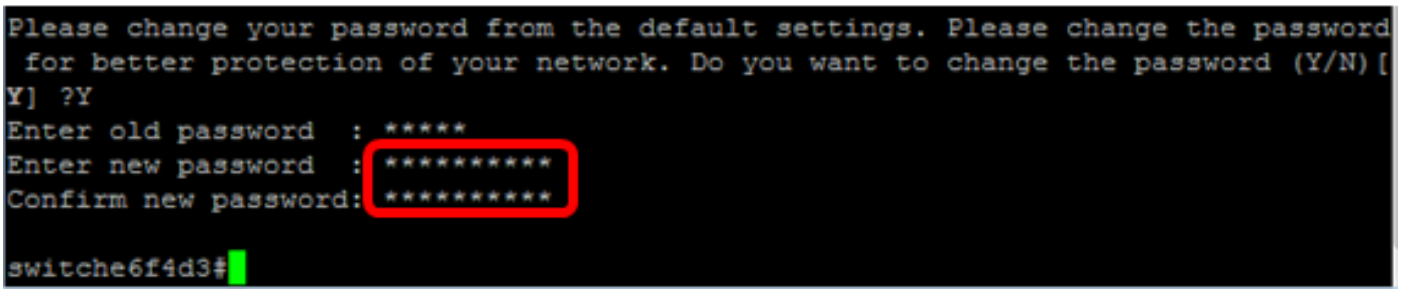


참고: 이 예에서는 Y를 누릅니다.

3단계. 이전 비밀번호를 입력한 다음 키보드에서 Enter를 누릅니다.

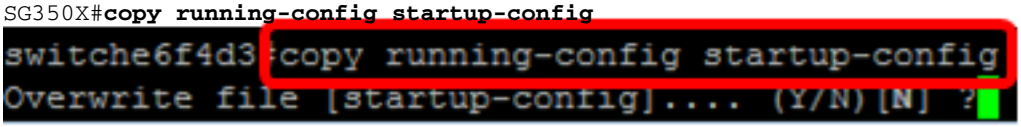


4단계. 새 비밀번호를 입력하고 확인한 다음 키보드에서 **Enter**를 누릅니다.

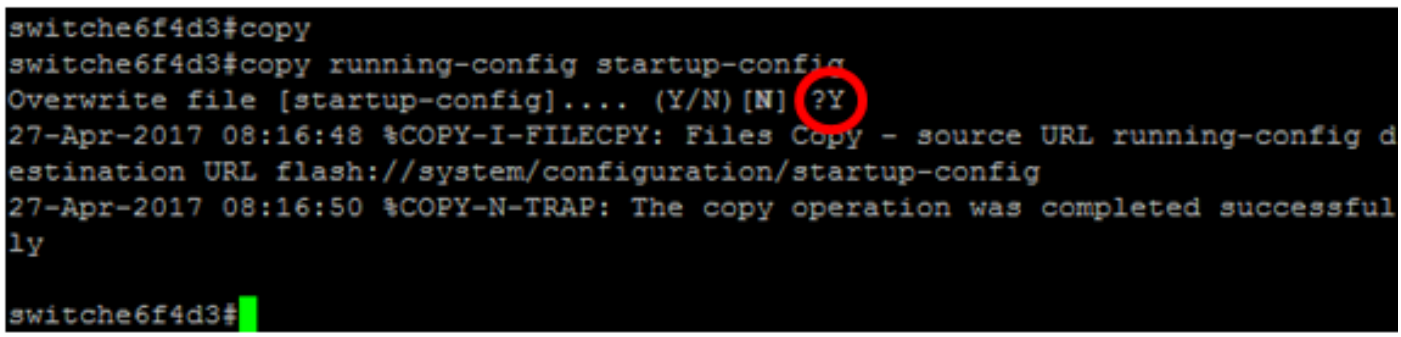


5단계. enable 명령을 사용하여 특별 권한 EXEC 모드를 입력합니다. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

```
SG350X#copy running-config startup-config
```



6단계. (선택 사항) Overwrite file [startup-config]... 프롬프트가 나타나면 키보드에서 Y 또는 **N**을 누릅니다.



이제 CLI를 통해 스위치에서 기본 비밀번호 설정을 구성해야 합니다.

회선 암호 설정 구성

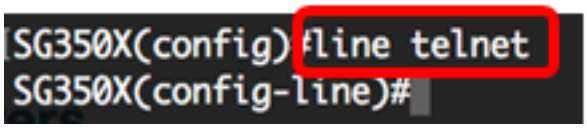
1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 해당 자격 증명을 입력합니다.

2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 글로벌 컨피그레이션 모드로 들어갑니다.

```
SG350X#configure terminal
```

3단계. 콘솔, 텔넷, SSH(Secure Shell) 등의 행에서 비밀번호를 구성하려면 다음을 입력하여 비밀번호 라인 컨피그레이션 모드를 입력합니다.

```
SG350X(config)#line [line-name]
```



참고: 이 예에서 사용된 라인은 텔넷입니다.

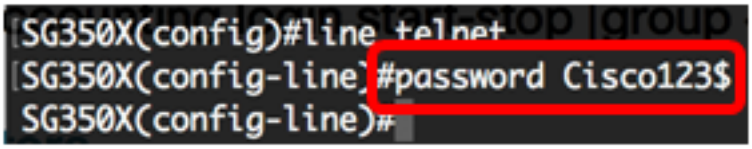
4단계. 다음을 입력하여 라인에 대한 비밀번호 명령을 입력합니다.

```
SG350X(config-line)#password [password][encrypted]
```

옵션은 다음과 같습니다.

- password — 회선의 비밀번호를 지정합니다. 길이는 0~159자입니다.
- encrypted — (선택 사항) 비밀번호가 암호화되어 다른 디바이스 컨피그레이션에서 복사되도록 지정합니다.

참고: 이 예에서는 텔넷 라인에 대해 비밀번호 Cisco123$가 지정됩니다.



5단계. (선택 사항) 회선 비밀번호를 기본 비밀번호로 되돌리려면 다음을 입력합니다.

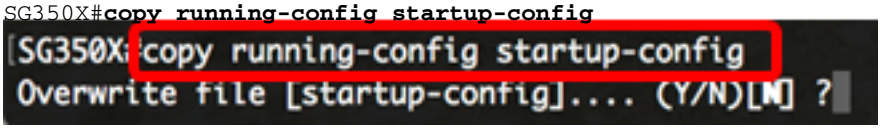
```
SG350X(config-line)#no password
```

6단계. **end** 명령을 입력하여 스위치의 Privileged EXEC 모드로 돌아갑니다.

```
SG350X(config)#end
```

7단계. (선택 사항) 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

```
SG350X#copy running-config startup-config
```



8단계. (선택 사항) Overwrite file [startup-config]... 프롬프트가 나타나면 키보드에서 Y 또는 **N**을 누릅니다.

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
27-Apr-2017 07:33:50 %COPY-I-FILECPY: Files Copy - source URL running-config destina
tion URL flash://system/configuration/startup-config
27-Apr-2017 07:33:52 %COPY-N-TRAP: The copy operation was completed successfully

SG350X#
```

이제 CLI를 통해 스위치에 회선 비밀번호 설정을 구성해야 합니다.

비밀번호 설정 활성화 구성

새 enable 비밀번호를 구성하면 자동으로 암호화되어 실행 중인 컨피그레이션 파일에 저장됩니다. 비밀번호가 어떻게 입력되었든, 이 비밀번호는 **암호화된** 키워드와 함께 실행 중인 컨피그레이션 파일에 나타납니다.

CLI를 통해 스위치에서 enable 비밀번호 설정을 구성하려면 다음 단계를 수행합니다.

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 해당 자격 증명을 입력합니다.

```
User Name:cisco
Password:**********
```

2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 글로벌 컨피그레이션 모드로 들어갑니다.

```
SG350X#configure terminal
```

3단계. 스위치의 특정 사용자 액세스 레벨에 대한 로컬 비밀번호를 구성하려면 다음을 입력합니다.

```
SG350X(config)#enable password [level privilege-level] [unencrypted-password | encrypted
encrypted-password]
```

옵션은 다음과 같습니다.

- **level privilege**-level — 비밀번호가 적용되는 레벨을 지정합니다. 레벨 범위는 1~15입니다. 지정하지 않으면 레벨이 기본값인 15로 설정됩니다. 사용자 레벨은 다음과 같습니다.

  - 읽기 전용 CLI 액세스(1) — 사용자는 GUI에 액세스할 수 없으며 디바이스 컨피그레이션을 변경하지 않는 CLI 명령만 액세스할 수 있습니다.

  - 읽기/제한된 쓰기 CLI 액세스(7) — 사용자는 GUI에 액세스할 수 없으며 디바이스 컨피그레이션을 변경하는 일부 CLI 명령에만 액세스할 수 있습니다. 자세한 내용은 CLI 참조 설명서를 참조하십시오.

  - 읽기/쓰기 관리 액세스(15) - 사용자가 GUI에 액세스하고 디바이스를 구성할 수 있습니다.

```
SG350X(config)#enable password level 7 Cisco123$
```

참고: 이 예에서 비밀번호 Cisco123$는 레벨 7 사용자 계정에 대해 설정됩니다.

- unencrypted-password — 현재 사용 중인 사용자 이름의 비밀번호입니다. 길이는

0~159자입니다.

```
SG350X(config)#enable password level Cisco123$
```

참고: 이 예에서는 비밀번호 Cisco123$가 사용됩니다.

- **encrypted**-password — 비밀번호가 암호화되도록 지정합니다. 이 명령을 사용하여 다른 디바이스의 다른 컨피그레이션 파일에서 이미 암호화된 비밀번호를 입력할 수 있습니다. 이렇게 하면 동일한 비밀번호로 두 스위치를 구성할 수 있습니다.

```
SG350X(config)#enable password encrypted 6f43205030a2f3a1e243873007370fab
```

참고: 이 예에서 사용된 암호화된 비밀번호는 6f43205030a2f3a1e243873007370fab입니다. Cisco123$ 의 암호화된 버전입니다.

참고: 위의 예에서 enable 비밀번호 Cisco123$는 레벨 7 액세스에 대해 설정됩니다.

4단계. (선택 사항) 사용자 비밀번호를 기본 비밀번호로 되돌리려면 다음을 입력합니다.

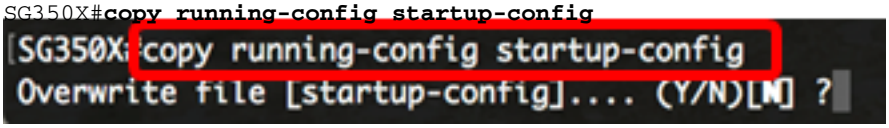
```
SG350X(config)#no enable password
```

5단계. **exit** 명령을 입력하여 스위치의 Privileged EXEC 모드로 돌아갑니다.

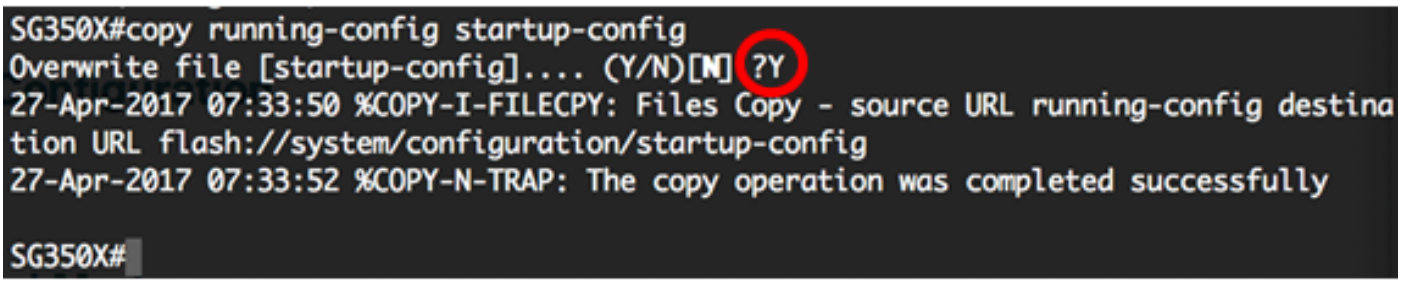
```
SG350X(config)#exit
```

6단계. (선택 사항) 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

```
SG350X#copy running-config startup-config
```



7단계. (선택 사항) Overwrite file [startup-config]... 프롬프트가 나타나면 키보드에서 Y 또는 **N**을 누릅니다.



이제 CLI를 통해 스위치에서 enable 비밀번호 설정을 구성해야 합니다.

서비스 비밀번호 복구 설정 구성

서비스 비밀번호 복구 메커니즘은 다음 조건을 사용하여 디바이스의 콘솔 포트에 대한 물리적 액세스를 제공합니다.

- 비밀번호 복구가 활성화된 경우 부팅 메뉴에 액세스하고 부팅 메뉴에서 비밀번호 복구

를 트리거할 수 있습니다. 모든 컨피그레이션 파일 및 사용자 파일이 보관됩니다.
- 비밀번호 복구가 비활성화된 경우 부팅 메뉴에 액세스하고 부팅 메뉴에서 비밀번호 복구를 트리거할 수 있습니다. 구성 파일과 사용자 파일이 제거됩니다.
- Secure Sensitive Data에 대해 사용자 정의 패스프레이즈로 민감한 데이터를 보호하도록 디바이스가 구성된 경우 비밀번호 복구가 활성화된 경우에도 부팅 메뉴에서 비밀번호 복구를 트리거할 수 없습니다.

서비스 비밀번호 복구는 기본적으로 활성화되어 있습니다. CLI를 통해 스위치에서 서비스 비밀번호 복구 설정을 구성하려면 다음 단계를 수행합니다.

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 해당 자격 증명을 입력합니다.

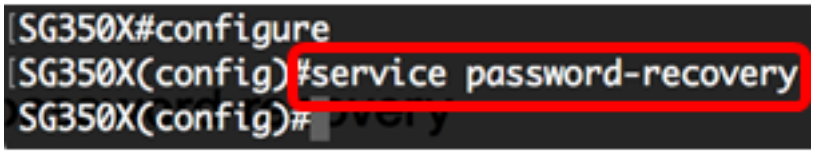
```
User Name:cisco
Password:**********
```

2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 글로벌 컨피그레이션 모드로 들어갑니다.

```
SG350X#configure terminal
```

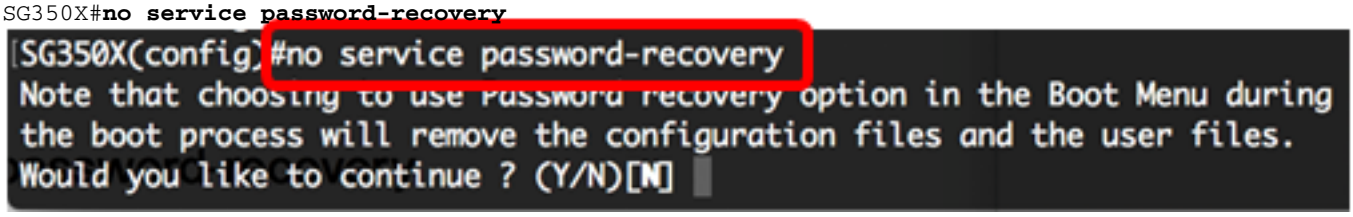
3단계. (선택 사항) 스위치에서 비밀번호 복구 설정을 활성화하려면 다음을 입력합니다.

```
SG350X#service password-recovery
```

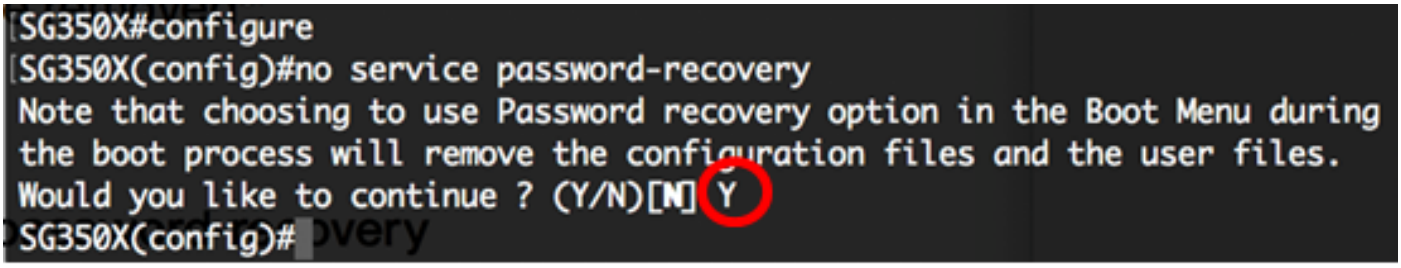


4단계. (선택 사항) 스위치에서 비밀번호 복구 설정을 비활성화하려면 다음을 입력합니다.

```
SG350X#no service password-recovery
```



5단계. (선택 사항) **Y**를 Yes(예)로, **N**을 누르면 키보드에 No(아니요)가 나타납니다.



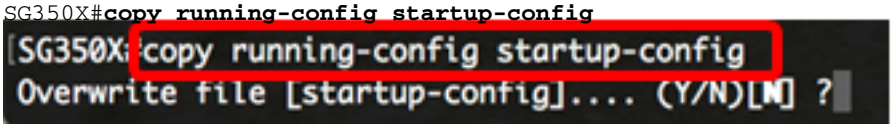
참고: 이 예에서는 Y를 누릅니다.

6단계. **exit** 명령을 입력하여 스위치의 Privileged EXEC 모드로 돌아갑니다.

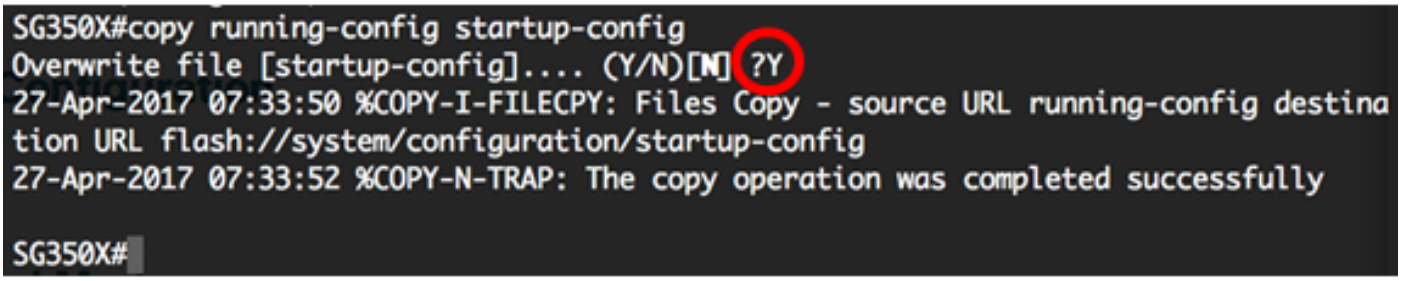
```
SG350X(config)#exit
```

7단계. (선택 사항) 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

```
SG350X#copy running-config startup-config
```



8단계. (선택 사항) Overwrite file [startup-config]... 프롬프트가 나타나면 키보드에서 Y 또는 **N**을 누릅니다.



이제 CLI를 통해 스위치에서 비밀번호 복구 설정을 구성해야 합니다.

비밀번호 복잡성 설정 구성

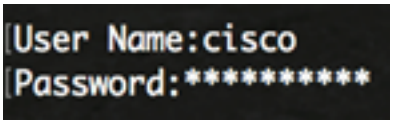
스위치의 비밀번호 복잡성 설정은 비밀번호에 대한 복잡성 규칙을 활성화합니다. 이 기능이 활성화된 경우 새 비밀번호는 다음 기본 설정을 따라야 합니다.

- 최소 8자의 길이를 가집니다.
- 표준 키보드에서 사용할 수 있는 대문자, 소문자, 숫자, 특수 문자 등 4개 이상의 문자 클래스의 문자를 포함합니다.
- 현재 비밀번호와 다릅니다.
- 연속적으로 3번 이상 반복되는 문자를 포함하지 않습니다.
- 문자의 대/소문자를 변경하여 사용자 이름 또는 도달한 모든 변형을 반복하거나 역행하지 마십시오.
- 문자의 대/소문자를 변경하여 제조업체 이름 또는 찾은 변형을 반복하거나 반대로 만들지 마십시오.

특정 명령을 사용하여 위의 비밀번호 복잡성 특성을 제어할 수 있습니다. 이전에 다른 복잡성 설정을 구성한 경우 해당 설정이 사용됩니다.

이 기능은 기본적으로 활성화되어 있습니다. CLI를 통해 스위치에서 비밀번호 복잡성 설정을 구성하려면 다음 단계를 수행합니다.

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 해당 자격 증명을 입력합니다.

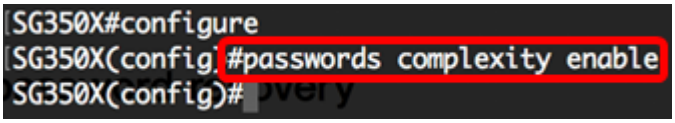


2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 글로벌 컨피그레이션 모드로 들어갑니다.

```
SG350X#configure terminal
```

3단계. (선택 사항) 스위치에서 비밀번호 복잡성 설정을 활성화하려면 다음을 입력합니다.

```
SG350X(config)#passwords complexity enable
```



4단계. (선택 사항) 스위치에서 비밀번호 복잡성 설정을 비활성화하려면 다음을 입력합니다.

```
SG350X(config)#no passwords complexity enable
```

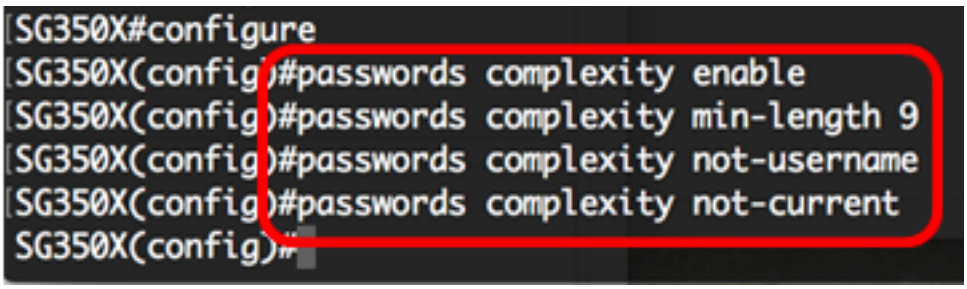
5단계. (선택 사항) 비밀번호에 대한 최소 요구 사항을 구성하려면 다음을 입력합니다.

```
SG350X(config)#passwords complexity [min-length number] [min-classes number] [not-current] [no-repeat number] [not-username] [not manufacturer-name]
```

옵션은 다음과 같습니다.

- min-length number — 비밀번호의 최소 길이를 설정합니다. 범위는 0~64자입니다. 기본값은 8입니다.
- min-classes number — 표준 키보드에서 사용할 수 있는 대문자, 소문자, 숫자 및 특수 문자와 같은 최소 문자 클래스를 설정합니다. 범위는 0~4개 클래스입니다. 기본값은 3입니다.
- not-current — 새 비밀번호가 현재 비밀번호와 같을 수 없도록 지정합니다.
- no-repeat number — 새 비밀번호의 최대 문자 수를 지정하여 연속적으로 반복할 수 있습니다. 0은 반복되는 문자에는 제한이 없음을 지정합니다. 범위는 0~16자입니다. 기본값은 3입니다.
- not-username — 비밀번호가 문자의 대/소문자를 변경하여 사용자 이름 또는 도달한 모든 변형을 반복하거나 역전할 수 없도록 지정합니다.
- not-manufacturer-name — 비밀번호가 제조업체의 이름 또는 문자의 대/소문자를 변경하여 접촉하는 모든 변형을 반복하거나 역행하지 않도록 지정합니다.

참고: 이러한 명령은 다른 설정을 지우지 않습니다. 비밀번호 복잡성 설정 구성은 토글로만 작동합니다.



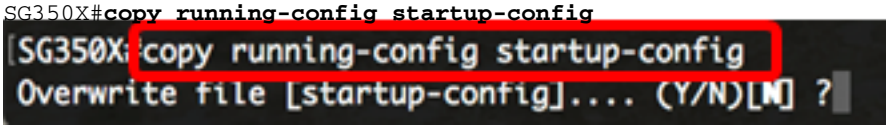
참고: 이 예에서는 비밀번호 복잡성이 9자 이상으로 설정되고 사용자 이름을 반복하거나 취소할 수 없으며 현재 비밀번호와 같을 수 없습니다.

6단계. **exit** 명령을 입력하여 스위치의 Privileged EXEC 모드로 돌아갑니다.

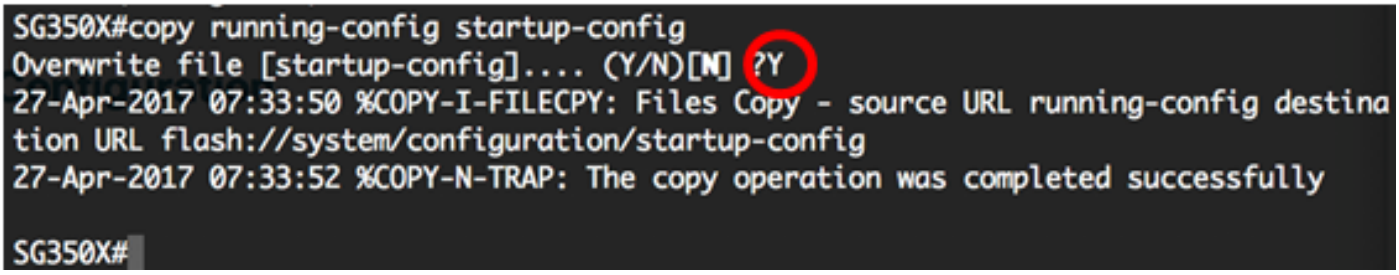
```
SG350X(config)#exit
```

7단계. (선택 사항) 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

```
SG350X#copy running-config startup-config
```



8단계. (선택 사항) Overwrite file [startup-config]... 프롬프트가 나타나면 키보드에서 Y 또는 **N**을 누릅니다.



이제 CLI를 통해 스위치에서 비밀번호 복잡성 설정을 구성해야 합니다.

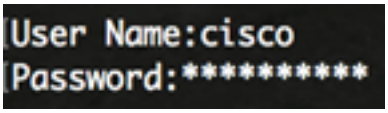
스위치의 CLI에 비밀번호 컨피그레이션 설정을 표시하려면 Show Passwords Configuration Settings(비밀번호 컨피그레이션 설정 표시)로 건너뜁니다.

비밀번호 에이징 설정 구성

에이징은 권한 레벨이 15이고 권한 레벨 15의 비밀번호를 사용하도록 구성된 로컬 데이터베이스의 사용자에게만 해당됩니다. 기본 컨피그레이션은 180일입니다.

CLI를 통해 스위치에서 비밀번호 에이징 설정을 구성하려면 다음 단계를 수행합니다.

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름과 비밀번호는 *cisco*입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 해당 자격 증명을 입력합니다.



2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 글로벌 컨피그레이션 모드로 들어갑니다.

```
SG350X#configure terminal
```

3단계. 스위치에서 비밀번호 에이징 설정을 지정하려면 다음을 입력합니다.

```
SG350X(config)#passwords aging [days]
```

- days — 비밀번호 변경이 강제 적용되기 전까지의 일 수를 지정합니다. 0을 사용하여 에이징을 비활성화할 수 있습니다. 범위는 0~365일입니다.

참고: 이 예에서는 비밀번호 에이징이 60일로 설정됩니다.

4단계. (선택 사항) 스위치에서 비밀번호 에이징을 비활성화하려면 다음을 입력합니다.

```
SG350X(config)#no passwords aging 0
```

5단계. (선택 사항) 비밀번호 에이징을 기본 설정으로 되돌리려면 다음을 입력합니다.

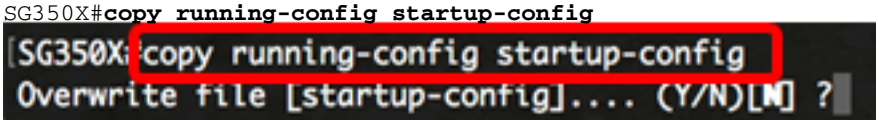
```
SG350X(config)#no passwords aging [days]
```

6단계. **exit** 명령을 입력하여 스위치의 Privileged EXEC 모드로 돌아갑니다.

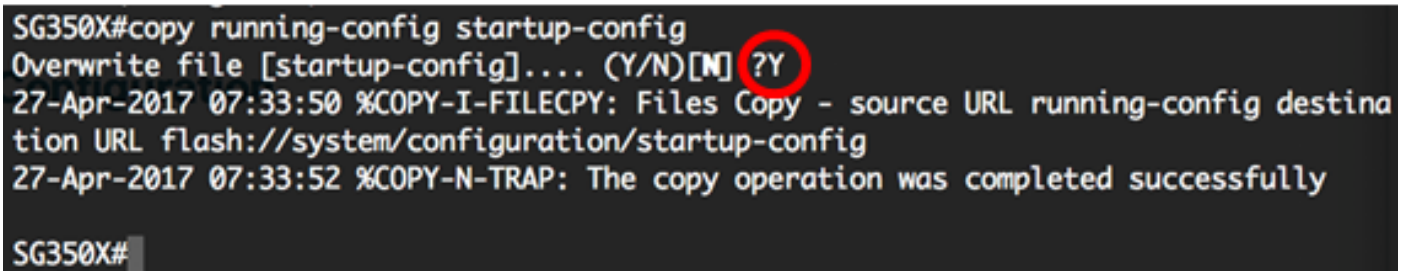
```
SG350X(config)#exit
```

7단계. (선택 사항) 스위치의 Privileged EXEC 모드에서 다음을 입력하여 구성된 설정을 시작 구성 파일에 저장합니다.

```
SG350X#copy running-config startup-config
```



8단계. (선택 사항) Overwrite file [startup-config]... 프롬프트가 나타나면 키보드에서 Y 또는 **N**을 누릅니다.



이제 CLI를 통해 스위치에서 비밀번호 에이징 설정을 구성해야 합니다.

스위치의 CLI에 비밀번호 컨피그레이션 설정을 표시하려면 Show Passwords Configuration Settings(비밀번호 컨피그레이션 설정 표시)로 건너뜁니다.

암호 구성 설정 표시

에이징은 권한 레벨이 15이고 권한 레벨 15의 비밀번호를 사용하도록 구성된 로컬 데이터베이스의 사용자에게만 해당됩니다. 기본 컨피그레이션은 180일입니다.

1단계. 스위치의 Privileged EXEC 모드에서 다음을 입력합니다.

SG350X(config)#**show passwords configuration**