CLI를 통해 스위치에서 전역 802.1x 속성 구성

소개

IEEE 802.1x는 클라이언트와 서버 간의 액세스 제어를 용이하게 하는 표준입니다. LAN(Local Access Network) 또는 스위치를 통해 클라이언트에 서비스를 제공하려면 먼저 스위치 포트에 연결된 클라이언트가 RADIUS(Remote Authentication Dial-In User Service)를 실행하는 인증 서버에서 인증되어야 합니다.

802.1x 인증은 무단 클라이언트가 공개적으로 액세스 가능한 포트를 통해 LAN에 연결하지 못하도록 제한합니다. 802.1x 인증은 클라이언트 서버 모델입니다. 이 모델에서는 네트워크 디바이스에 다음과 같은 특정 역할이 있습니다.

- 클라이언트 또는 신청자 — 클라이언트 또는 신청자는 LAN에 대한 액세스를 요청하는 네트워크 디바이스입니다. 클라이언트가 인증자에게 연결되어 있습니다.
- 인증자 — 인증자는 네트워크 서비스를 제공하고 서 폴리 컨 트 포트가 연결된 네트워크 디바이스입니다. 다음 인증 방법이 지원됩니다.

  - 802.1x 기반 — 모든 인증 모드에서 지원됩니다. 802.1x 기반 인증에서 인증자는 802.1x 메시지 또는 EAPoL(EAP over LAN) 패킷에서 EAP(Extensible Authentication Protocol) 메시지를 추출하여 RADIUS 프로토콜을 사용하여 인증 서버에 전달합니다.

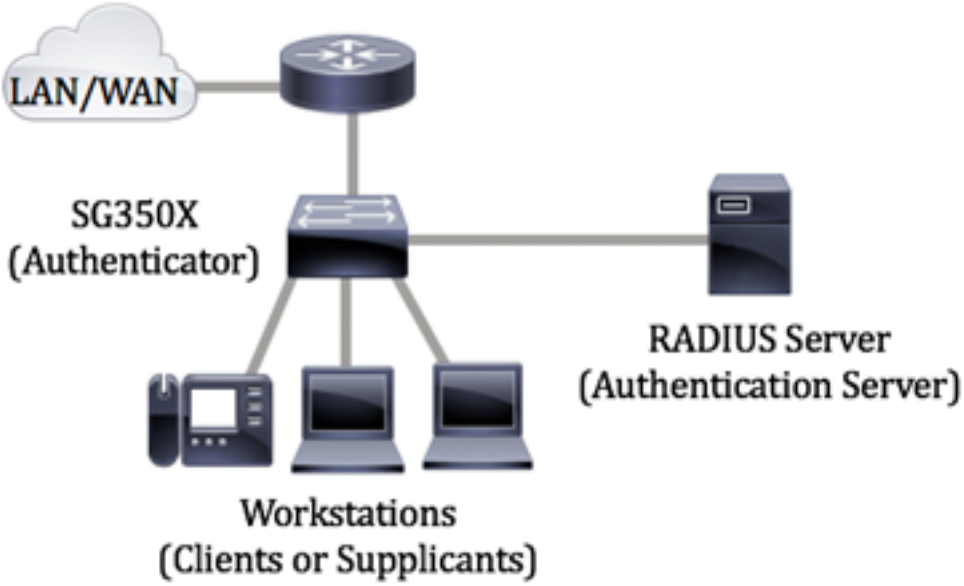
  - MAC 기반 — 모든 인증 모드에서 지원됩니다. MAC(Media Access Control) 기반의 인증자는 네트워크 액세스를 원하는 클라이언트를 대신하여 소프트웨어의 EAP 클라이언트 부분을 실행합니다.

  - 웹 기반 — 다중 세션 모드에서만 지원됩니다. 웹 기반 인증을 사용하는 인증자 자체는 네트워크 액세스를 찾는 클라이언트를 대신하여 소프트웨어의 EAP 클라이언트 부분을 실행합니다.

- 인증 서버 — 인증 서버는 클라이언트의 실제 인증을 수행합니다. 디바이스에 대한 인증 서버는 EAP 확장이 있는 RADIUS 인증 서버입니다.

  참고: 네트워크 디바이스는 클라이언트 또는 신청자, 인증자 또는 포트당 둘 다 될 수 있습니다.

  아래 이미지는 특정 역할에 따라 디바이스를 구성한 네트워크를 표시합니다. 이 예에서는 SG350X 스위치가 사용됩니다.



지침 인 802.1x 구성:

1. RADIUS 서버를 구성합니다. 스위치에서 RADIUS 서버 설정을 구성하는 방법을 알아보려면 여기를 클릭하십시오.
2. VLAN(Virtual Local Area Network)을 구성합니다. 스위치의 웹 기반 유틸리티를 사용하여 VLAN을 생성하려면 여기를 클릭합니다. CLI 기반 지침을 보려면 여기를 클릭하십시오.
3. 스위치의 Port to VLAN 설정을 구성합니다. 웹 기반 유틸리티를 사용하여 구성하려면 여기를 클릭하십시오. CLI를 사용하려면 여기를 클릭합니다.
4. 스위치에서 전역 802.1x 속성을 구성합니다. 스위치의 웹 기반 유틸리티를 통해 전역 802.1x 속성을 구성하는 방법에 대한 지침은 여기를 클릭하십시오.
5. (선택 사항) 스위치에서 시간 범위를 구성합니다. 스위치에서 시간 범위 설정을 구성하는 방법을 알아보려면 여기를 클릭하십시오.
6. 802.1x 포트 인증을 구성합니다. 스위치의 웹 기반 유틸리티를 사용하려면 여기를 클릭하십시오.

목표

이 문서에서는 스위치의 CLI(Command Line Interface)를 통해 인증 및 게스트 VLAN 속성을 포함하는 전역 802.1x 속성을 구성하는 방법에 대한 지침을 제공합니다. 게스트 VLAN은 802.1x, MAC 기반 또는 웹 기반 인증을 통해 가입 디바이스 또는 포트를 인증 및 인증하지 않아도 되는 서비스에 대한 액세스를 제공합니다.

적용 가능한 디바이스

- SX300 시리즈
- SX350 시리즈
- SG350X 시리즈
- SX500 시리즈
- SX550X 시리즈

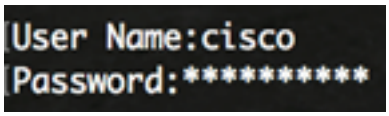
소프트웨어 버전

- 1.4.7.06 — SX300, SX500
- 2.2.8.04 — SX350, SG350X, SX550X

CLI를 통해 스위치에서 802.1x 속성 구성

802.1x 설정 구성

1단계. 스위치 콘솔에 로그인합니다. 기본 사용자 이름 및 비밀번호는 cisco/cisco입니다. 새 사용자 이름 또는 비밀번호를 구성한 경우 대신 자격 증명을 입력합니다.



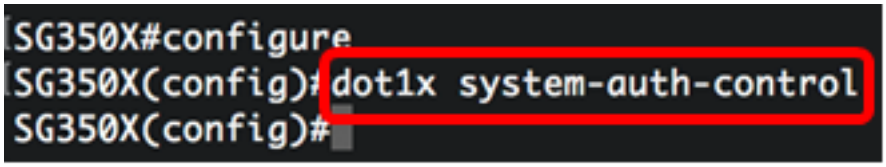
참고: 명령은 스위치의 정확한 모델에 따라 달라질 수 있습니다. 이 예에서는 텔넷을 통해 SG350X 스위치에 액세스합니다.

2단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 Global Configuration 모드로 들어갑니다.

```
SG350x#
```

3단계. 스위치에서 802.1x 인증을 전역적으로 활성화하려면 글로벌 컨피그레이션 모드**에서 dot1x system-auth-control** 명령을 사용합니다.

```
SG350x(config)#dotx1 system-auth-control
```



4단계. (선택 사항) 스위치에서 802.1x 인증을 전역적으로 비활성화하려면 다음을 입력합니다.

```
SG350x(config)#no dotx1 system-auth-control
```

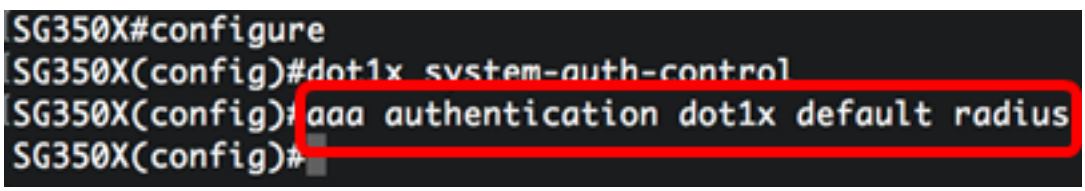
참고: 비활성화된 경우 802.1X, MAC 기반 및 웹 기반 인증이 비활성화됩니다.

5단계. 802.1x 인증이 활성화된 경우 인증에 사용할 서버를 지정하려면 다음을 입력합니다.

```
SG350x(config)#aaa authentication dot1x default [radius none] |  | ]
```

옵션은 다음과 같습니다.

- radius none — RADIUS 서버의 도움으로 먼저 포트 인증을 수행합니다. 서버가 다운된 경우와 같이 서버에서 응답이 없는 경우 인증이 수행되지 않고 세션이 허용됩니다. 서버를 사용할 수 있고 사용자 자격 증명이 올바르지 않으면 액세스가 거부되고 세션이 종료됩니다.
- radius — RADIUS 서버를 기반으로 포트 인증을 수행합니다. 인증이 수행되지 않으면 세션이 종료됩니다. 이것이 기본 인증입니다.
- none — 사용자를 인증하지 않고 세션을 허용합니다.



참고: 이 예에서 기본 802.1x 인증 서버는 RADIUS입니다.

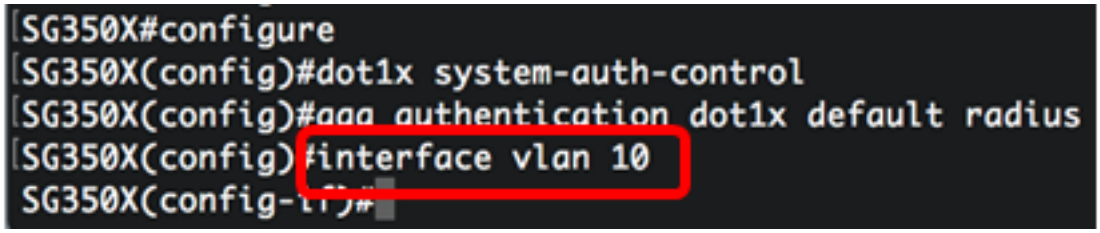
6단계. (선택 사항) 기본 인증을 복원하려면 다음을 입력합니다.

```
SG350X(config)#no aaa authentication dot1x default
```

7단계. Global Configuration(전역 컨피그레이션) 모드에서 다음을 입력하여 VLAN 인터페이스 컨피그레이션 컨텍스트를 입력합니다.

```
SG350X(config)#interface vlan [vlan-id]
```

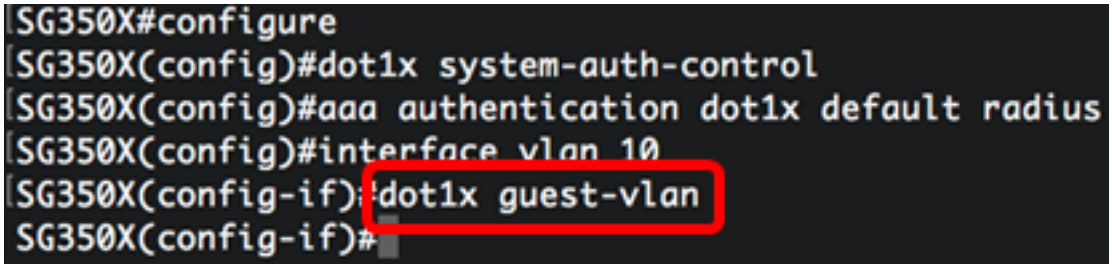
- vlan-id — 구성할 VLAN ID를 지정합니다.



8단계. 무단 포트에 게스트 VLAN을 사용하도록 설정하려면 다음을 입력합니다.

```
SG350X(config-if)#dot1x guest-vlan
```

참고: 게스트 VLAN이 활성화된 경우, 모든 권한이 없는 포트는 게스트 VLAN에서 선택한 VLAN에 자동으로 조인합니다. 포트가 나중에 인증되면 게스트 VLAN에서 제거됩니다.



9단계. 인터페이스 컨피그레이션 컨텍스트를 종료하려면 다음을 입력합니다.

```
SG350X(config-if)#exit
```

10단계. 802.1X(또는 포트 업)를 활성화하고 게스트 VLAN에 포트를 추가하는 시간 지연을 설정하려면 다음을 입력합니다.

```
SG350X(config)#dot1x guest-vlan timeout [timeout]
```

- timeout — 802.1X(또는 포트 업)를 활성화하고 게스트 VLAN에 포트를 추가하는 시간 지연(초)을 지정합니다. 범위는 30~180초입니다.

참고: 링크 업 후, 소프트웨어에서 802.1x 신청자를 탐지하지 않거나 포트 인증에 실패한 경우 게스트 VLAN 시간 초과 기간이 만료된 후에만 포트가 게스트 VLAN에 추가됩니다. 포트가 Authorized(권한 있음)에서 Not Authorized(권한 없음)로 변경되면 게스트 VLAN Timeout(게스트 VLAN 시간 제한) 기간이 만료된 후에만 포트가 게스트 VLAN에 추가됩니다. VLAN 인증에서 VLAN 인증을 활성화 또는 비활성화할 수 있습니다.

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#
```

참고: 이 예에서 사용된 게스트 VLAN 시간 제한은 60초입니다.

11단계. 트랩을 활성화하려면 다음 옵션 중 하나 이상을 선택합니다.

```
SG350X(config)# dot1x traps  [ |  | ] [802.1x | mac | ]
```

옵션은 다음과 같습니다.

- 802.1x 인증 실패 트랩 — 802.1x 인증에 실패할 경우 트랩을 보냅니다.
- 802.1x 인증 성공 트랩 — 802.1x 인증이 성공하면 트랩을 보냅니다.
- mac 인증 실패 트랩 — MAC 인증이 실패할 경우 트랩을 전송합니다.
- mac authentication success traps — MAC 인증이 성공하면 traps를 보냅니다.
- 웹 인증 실패 트랩 — 웹 인증이 실패할 경우 트랩을 보냅니다.
- 웹 인증 성공 트랩 — 웹 인증이 성공하면 트랩을 보냅니다.
- 웹 인증 quiet traps — 조용한 기간이 시작되는 경우 트랩을 보냅니다.

참고: 이 예에서는 802.1x 인증 실패 및 성공 트랩을 입력합니다.

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#
```

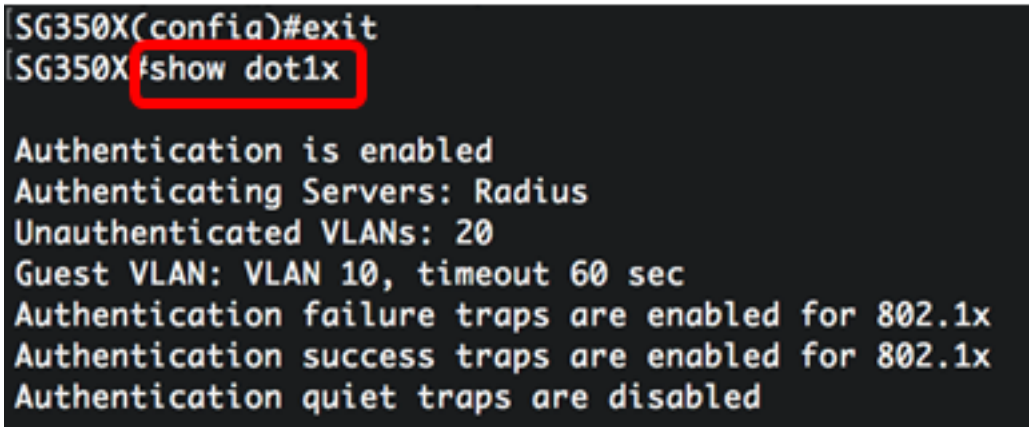
12단계. 인터페이스 컨피그레이션 컨텍스트를 종료하려면 다음을 입력합니다.

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

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#exit
SG350X#
```

13단계. (선택 사항) 스위치에 구성된 전역 802.1x 속성을 표시하려면 다음을 입력합니다.

```
SG350X#show dot1x
```



이제 스위치에서 802.1x 속성을 성공적으로 구성했어야 합니다.

VLAN 인증 구성

802.1x가 활성화되면 게스트 VLAN 또는 인증되지 않은 VLAN의 일부가 아닌 한, 인증되지 않은 포트 또는 디바이스는 VLAN에 액세스할 수 없습니다. 포트를 VLAN에 수동으로 추가해야 합니다.

VLAN에서 인증을 비활성화하려면 다음 단계를 수행합니다.

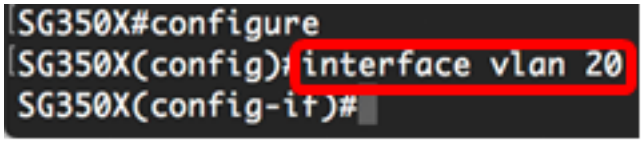
1단계. 스위치의 Privileged EXEC 모드에서 다음을 입력하여 Global Configuration 모드로 들어갑니다.

```
SG350X#configure
```

2단계. Global Configuration(전역 컨피그레이션) 모드에서 다음을 입력하여 VLAN 인터페이스 컨피그레이션 컨텍스트를 입력합니다.

```
KSG350x(config)# interface vlan [vlan-id]
```

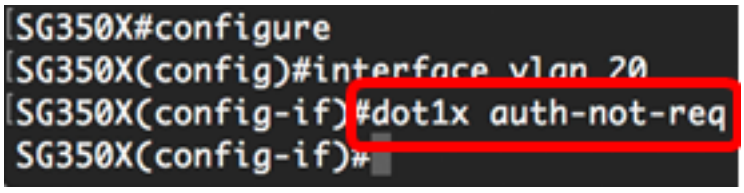
- vlan-id — 구성할 VLAN ID를 지정합니다.



참고: 이 예에서는 VLAN 20이 선택됩니다.

3단계. VLAN에서 802.1x 인증을 비활성화하려면 다음을 입력합니다.

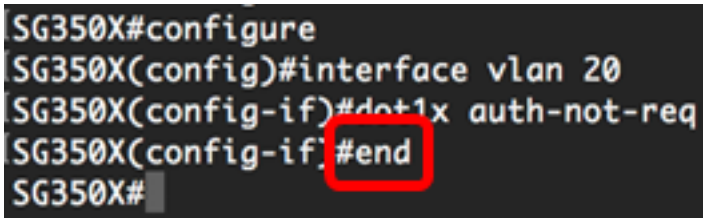
SG350X(config-if)#dot1x auth-not-req



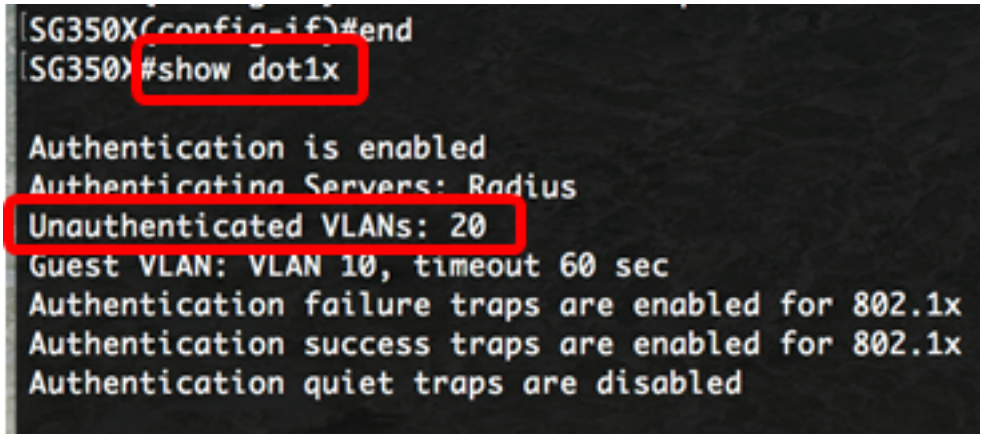
4단계. (선택 사항) VLAN에서 802.1x 인증을 활성화하려면 다음을 입력합니다.

SG350X(config-if)#no dot1x auth-not-req

5단계. 인터페이스 컨피그레이션 컨텍스트를 종료하려면 다음을 입력합니다.



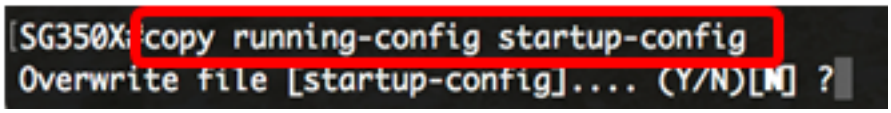
6단계. (선택 사항) 스위치에 802.1x 전역 인증 설정을 표시하려면 다음을 입력합니다.



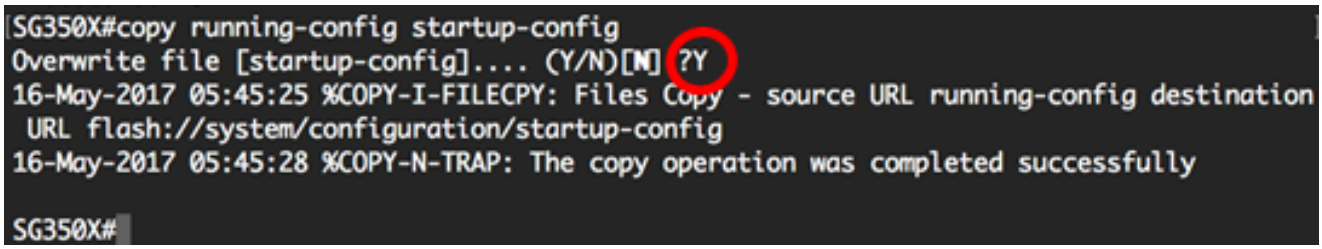
참고: 이 예에서는 VLAN 20이 인증되지 않은 VLAN으로 표시됩니다.

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 스위치의 VLAN에 802.1x 인증 설정을 성공적으로 구성했어야 합니다.

중요: 스위치에서 802.1x 포트 인증 설정을 구성하려면 위 지침을 따르십시오.