Cisco Business 220 Series 스위치에 802.1x 인증 구성

목표

이 문서의 목적은 Cisco Business 220 Series 스마트 스위치에 802.1x 인증을 구성하는 방법을 보여 주는 것입니다.

적용 가능한 디바이스 | 펌웨어 버전

- CBS220 시리즈(DataSheet) | 2.0.0.17

소개

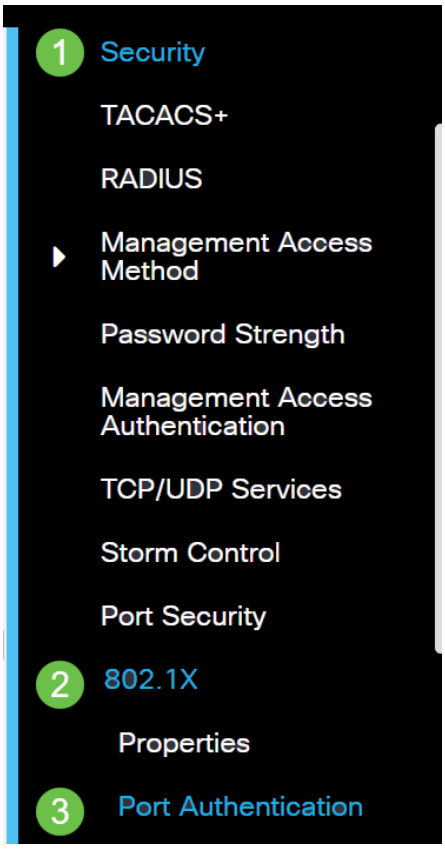
포트 인증은 각 포트에 대한 매개변수 컨피그레이션을 활성화합니다.일부 컨피그레이션 변경은 포트가 Force Authorized 상태(예: 호스트 인증)인 경우에만 가능하므로 변경하기 전에 포트 제어를 Force Authorized로 변경하는 것이 좋습니다.컨피그레이션이 완료되면 포트 제어를 이전 상태로 되돌립니다.

802.1x가 정의된 포트는 LAG의 멤버가 될 수 없습니다.802.1x와 포트 보안을 동시에 동일한 포트에서 활성화할 수 없습니다.인터페이스에서 포트 보안을 활성화하면 관리 포트 제어를 자동 모드로 변경할 수 없습니다.

포트 인증 구성

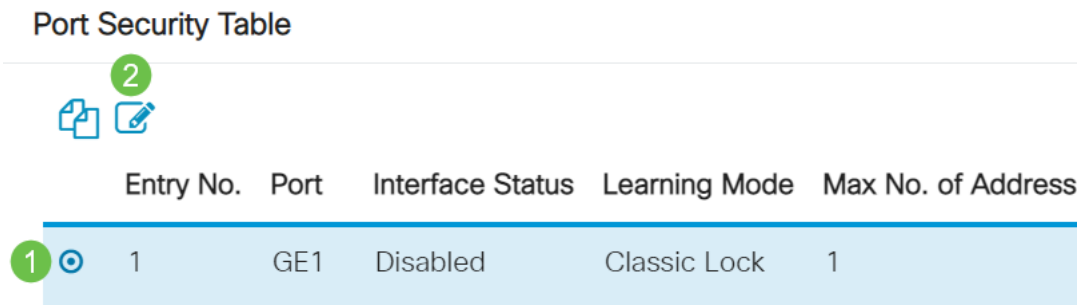
1단계

스위치 UI(Web User Interface)에 로그인하고 **Security > 802.1x > Port Authentication**을 선택합니다.



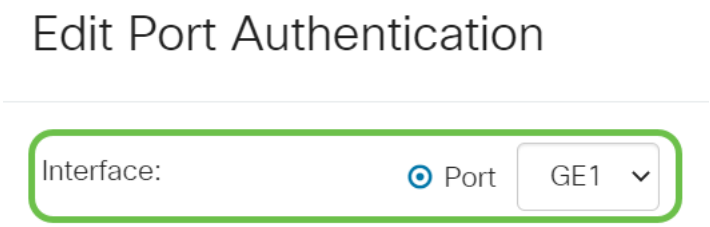
2단계

구성할 포트의 라디오 버튼을 클릭한 다음 **수정 아이콘**을 클릭합니다.



3단계

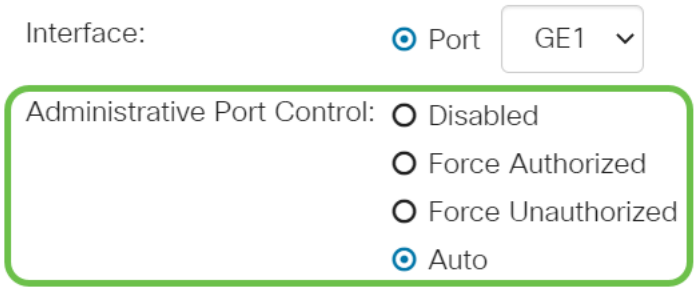
Edit *Port Authentication(포트 인증* 수정) 창이 나타납니다.Interface 드롭다운 목록에서 지정된 포트가 2단계에서 선택한 포트인지 확인합니다. 그렇지 않으면 드롭다운 화살표를 클릭하고 올바른 포트를 선택합니다.



4단계

관리 포트 컨트롤의 라디오 버튼을 선택합니다.그러면 포트 인증 상태가 결정됩니다.옵션은 다음과 같습니다.

- **Disabled**(비활성화됨) — 802.1x를 비활성화합니다.기본 상태입니다.
- **Force Unauthorized** — 인터페이스를 무단 상태로 전환하여 인터페이스 액세스를 거부합니다.스위치는 인터페이스를 통해 클라이언트에 인증 서비스를 제공하지 않습니다.
- **Auto** — 스위치에서 포트 기반 인증 및 권한 부여를 활성화합니다.인터페이스는 스위치와 클라이언트 간의 인증 교환을 기반으로 권한 있는 상태 또는 권한 없는 상태 사이를 이동합니다.
- **Force Authorized** — 인증 없이 인터페이스를 인증합니다.



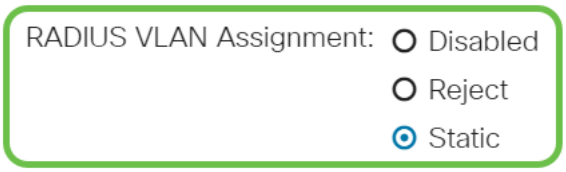
5단계(선택 사항)

RADIUS VLAN 할당에 대한 라디오 버튼을 선택합니다.그러면 지정된 포트에서 동적 VLAN 할당이 활성화됩니다.옵션은 다음과 같습니다.

- **Disabled**(비활성화됨) — VLAN 권한 부여 결과를 무시하고 호스트의 원래 VLAN을 유지합니다.이것이 기본 작업입니다.

- **거부** — 지정된 포트에서 VLAN 인증 정보를 수신하면 해당 정보가 사용됩니다.그러나 VLAN 인증 정보가 없는 경우 호스트를 거부하고 승인되지 않습니다.
- **고정** — 지정된 포트가 VLAN 인증 정보를 수신하면 해당 정보를 사용합니다.그러나 VLAN 인증 정보가 없으면 호스트의 원래 VLAN이 유지됩니다.

RADIUS에서 VLAN 인증 정보가 있지만 DUT(Device Under Test)에서 VLAN이 관리적으로 생성되지 않은 경우 VLAN이 자동으로 생성됩니다.



빠른 팁: 동적 VLAN 할당 기능이 작동하려면 스위치에서 RADIUS 서버에서 다음 VLAN 특성을 전송해야 합니다.

- [64] 터널 유형 = VLAN(유형 13)
- [65] 터널 중간 유형 = 802(유형 6)
- [81] Tunnel-Private-Group-Id = VLAN ID

6단계(선택 사항)

게스트 VLAN이 권한 없는 포트에 게스트 VLAN을 사용하려면 Enable 확인란을 선택합니다.

7단계

Periodic **Reauthentication**(주기적 재인증 활성화) 확인란을 선택합니다.이렇게 하면 지정된 재인증 기간 이후 포트 재인증 시도가 활성화됩니다.

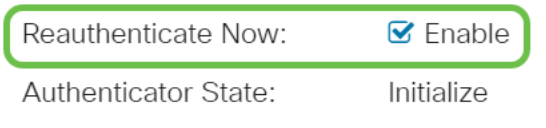
8단계

Reauthentication Period(재인증 기간) 필드에 값을 입력합니다.포트를 재인증하는 데 걸리는 시간(초)입니다.

9단계(선택 사항)

Reauthenticate Now(지금 **재인증**) 확인란을 선택하여 즉시 포트 재인증을 활성화합니다.

Authenticator State(인증자 상태) 필드에는 현재 인증 상태가 표시됩니다.



포트가 Force Authorized(강제 권한 부여) 또는 Force Unauthorized(강제 권한 없음) 상태가 아닌 경우 자동 모드이며 인증자가 진행 중인 인증 상태를 표시합니다.포트가 인증되면 상태가 Authenticated로 표시됩니다.

10단계

Max *Hosts* 필드에 특정 포트에서 허용되는 인증된 호스트의 최대 수를 입력합니다.이 값은 다중 세션 모드에만 적용됩니다.

11단계

Quiet *Period* 필드에 인증 교환 실패 후 스위치가 자동 상태로 유지되는 시간(초)을 입력합니다.스위치가 조용한 상태이면 스위치가 클라이언트의 새 인증 요청을 수신하지 않음을 의미합니다.

12단계

Resending *EAP* 필드에 스위치가 요청을 다시 보내기 전에 서 플리 컨 트 (클라이언트)로부터 EAP (Extensible Authentication Protocol) 요청 또는 ID 프레임에 대한 응답을 기다리는 시간(초)을 입력합니다.

13단계

Max EAP *Requests(최대 EAP 요청*) 필드에 전송할 수 있는 최대 EAP 요청 수를 입력합니다.정의된 기간(서 플리 컨 트 시간 초과) 후에 응답을 받지 못하면 인증 프로세스가 다시 시작됩니다.

14단계

Supplicant *Timeout*(신청자 시간 초과) 필드에 EAP 요청이 신청자에게 재전송되기 전에 경과된 시간(초)을 입력합니다.

15단계

Server *Timeout* 필드에 스위치가 인증 서버에 요청을 재전송하기 전에 경과하는 시간(초)을 입력합니다.

16단계

Apply를 **클릭합니다**.

이제 스위치에서 802.1x 인증을 성공적으로 구성해야 합니다.

자세한 컨피그레이션은 Cisco Business 220 Series 스위치 관리 가이드를 참조하십시오.

다른 문서를 보려면 Cisco Business 220 Series 스위치 지원 페이지를 확인하십시오.