Cisco SX220 Series Smart Switch에서 802.1X 포트 인증 구성

목표

이 문서의 목적은 Sx220 Series 스마트 스위치에서 포트 인증을 구성하는 방법을 설명하는 것입니다.

802.1X Port Authentication(802.1X 포트 인증)을 사용하면 디바이스의 각 포트에 대해 802.1X 매개변수를 구성할 수 있습니다.인증을 요청하는 포트를 서 플리 컨 트 라고 합니다.인증자는 신청자를 위한 네트워크 가드 역할을 하는 스위치 또는 액세스 포인트입니다.인증자는 인증 메시지를 RADIUS 서버로 전달하여 포트를 인증하고 정보를 보내고 받을 수 있도록 합니다.

적용 가능한 디바이스

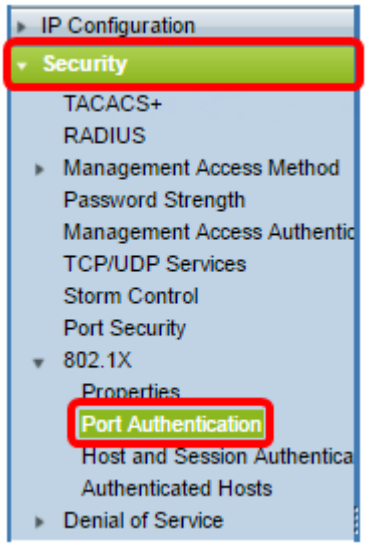
- SX220 시리즈

소프트웨어 버전

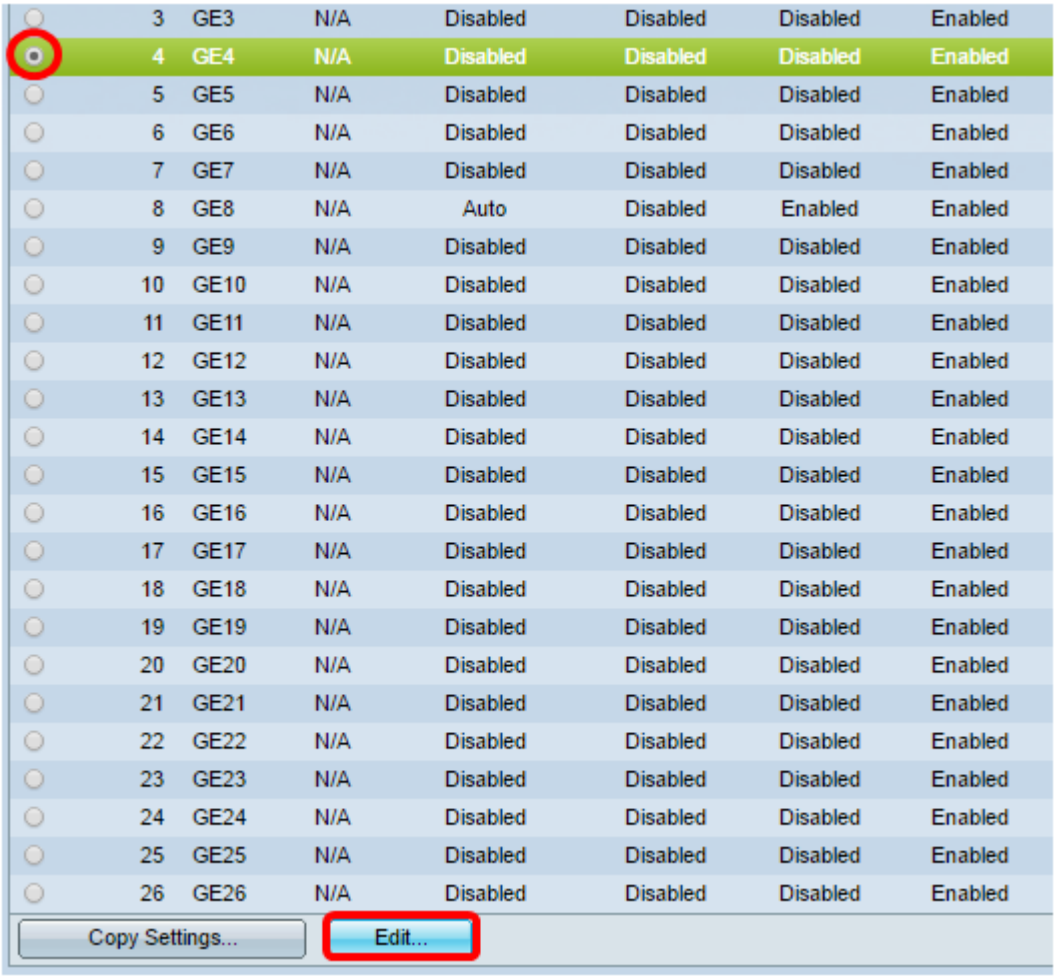
- 1.1.0.14

포트 인증 구성

1단계. 스위치 웹 기반 유틸리티에 로그인하고 **Security > 802.1X > Port Authentication**을 선택합니다.



2단계. 구성할 포트의 라디오 버튼을 클릭한 다음 **Edit**(수정)를 클릭합니다.

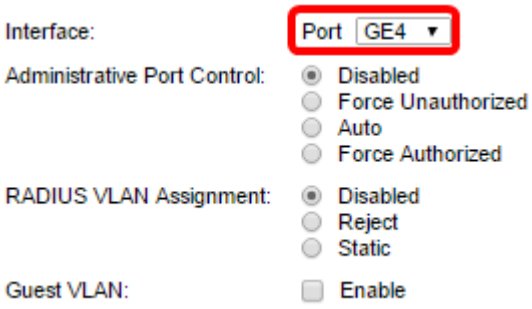


	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
◉	4	GE4	N/A	Disabled	Disabled	Disabled	Enabled
	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled

Copy Settings... Edit...

참고:이 예에서는 포트 GE4가 선택됩니다.

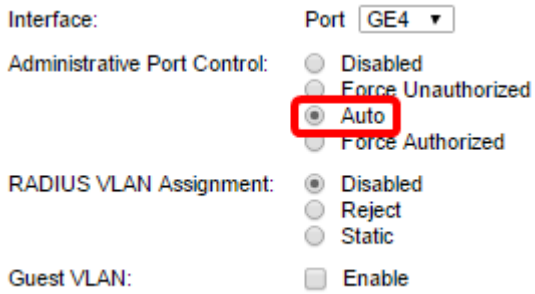
3단계. Edit Port Authentication(포트 인증 수정) 창이 나타납니다.Interface 드롭다운 목록에서 지정된 포트가 2단계에서 선택한 포트인지 확인합니다. 그렇지 않으면 드롭다운 화살표를 클릭하고 올바른 포트를 선택합니다.



4단계. 관리 포트 제어에 대한 라디오 버튼을 선택합니다.그러면 포트 인증 상태가 결정됩니다.옵션은 다음과 같습니다.

- Disabled(비활성화됨) — 802.1X를 비활성화합니다.기본 상태입니다.
- Force Unauthorized(권한 없음 강제 적용) — 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(강제 권한 부여) — 인증 없이 인터페이스를 인증합니다.

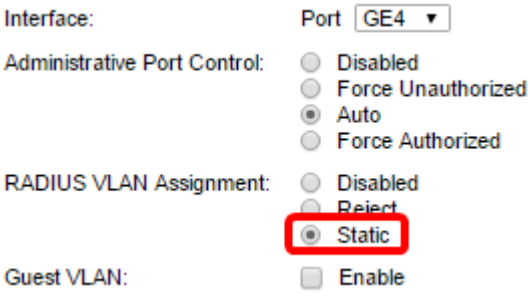


참고:이 예에서는 Auto가 선택됩니다.

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.
- Reject(거부) - 지정된 포트에서 VLAN 인증 정보를 수신하면 해당 정보를 사용합니다.그러나 VLAN 인증 정보가 없는 경우 호스트를 거부하고 승인되지 않습니다.
- Static — 지정된 포트에서 VLAN 인증 정보를 수신하면 해당 정보가 사용됩니다.그러나 VLAN 인증 정보가 없으면 호스트의 원래 VLAN이 유지됩니다.

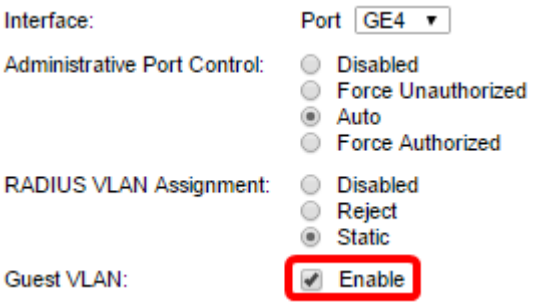
참고:RADIUS에서 VLAN 인증 정보가 있지만 DUT(Device Under Test)에서 VLAN이 관리적으로 생성되지 않은 경우 VLAN이 자동으로 생성됩니다.이 예에서는 Static이 선택됩니다.



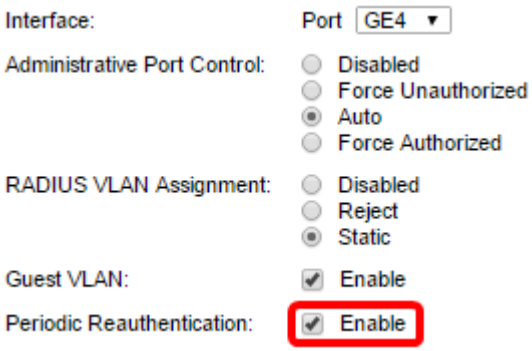
빠른 팁: 동적 VLAN 할당 기능이 작동하려면 스위치에서 RADIUS 서버에서 다음 VLAN 특성을 전송해야 합니다.

- [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.

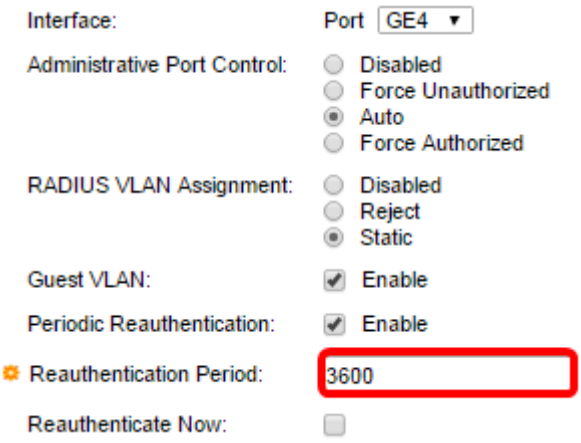


7단계. Periodic Reauthentication(주기적 재인증)에 대해 Enable(활성화) 확인란을 선택합니다.이렇게 하면 지정된 재인증 기간 이후 포트 재인증 시도가 활성화됩니다.



참고:이 기능은 기본적으로 활성화되어 있습니다.

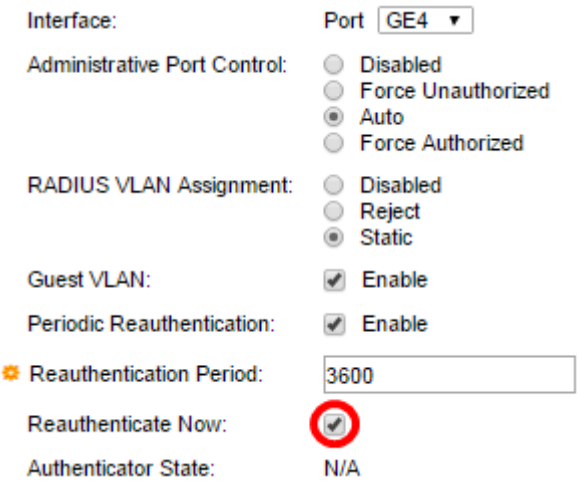
8단계. 재인증 기간 필드에 값을 입력합니다.포트를 재인증하는 데 걸리는 시간(초)입니다.



참고:이 예에서는 기본값 3600이 사용됩니다.

9단계. (선택 사항) Reauthenticate Now(지금 **재인증**) 확인란을 선택하여 즉시 포트 재인증을 활성화합니다.

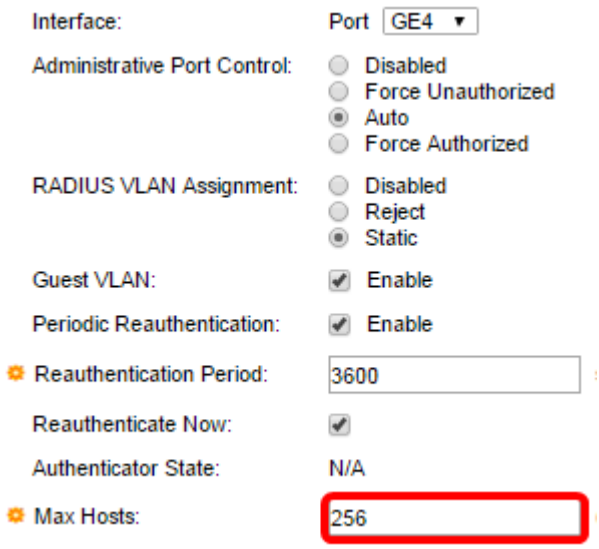
참고: Authenticator State(인증자 상태) 필드에는 현재 인증 상태가 표시됩니다.



참고: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

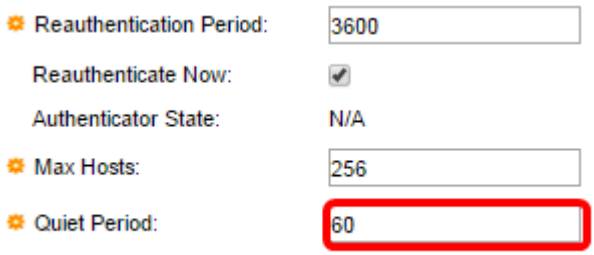
상태가 Authenticated로 표시됩니다.

10단계. Max *Hosts* 필드에 특정 포트에서 허용되는 인증된 호스트의 최대 수를 입력합니다 .이 값은 다중 세션 모드에만 적용됩니다.



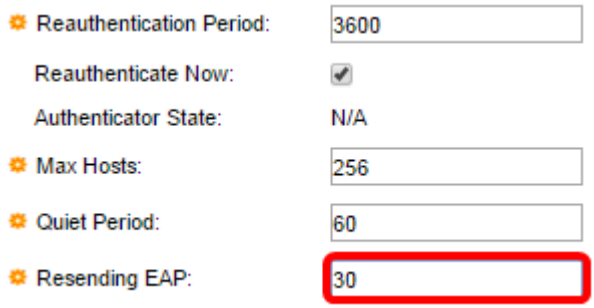
참고:이 예에서는 기본값 256이 사용됩니다.

11단계. Quiet *Period* 필드에 인증 교환 실패 후 스위치가 조용한 상태로 유지되는 시간(초)을 입력합니다.스위치가 조용한 상태이면 스위치가 클라이언트의 새 인증 요청을 수신하지 않음을 의미합니다.



참고:이 예에서는 기본값 60이 사용됩니다.

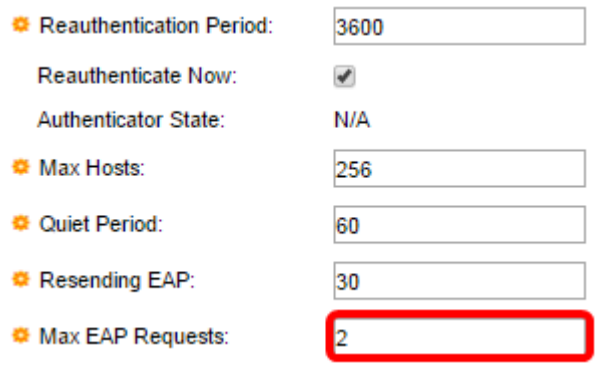
12단계. Resending EAP(*EAP* 재전송) 필드에 스위치가 요청을 다시 보내기 전에 신청자(클라이언트)로부터 EAP(Extensible Authentication Protocol) 요청 또는 ID 프레임에 대한 응답을 기다리는 시간(초)을 입력합니다.



참고:이 예에서는 기본값 30이 사용됩니다.

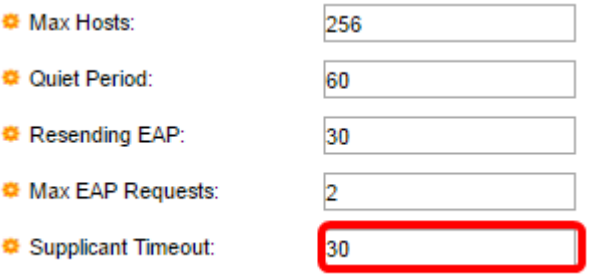
13단계. *Max EAP Requests(최대 EAP 요청)* 필드에 전송할 수 있는 최대 EAP 요청 수를 입력

합니다.정의된 기간(서 플리 컨 트 시간 초과) 후에 응답을 받지 못하면 인증 프로세스가 다시 시작됩니다.



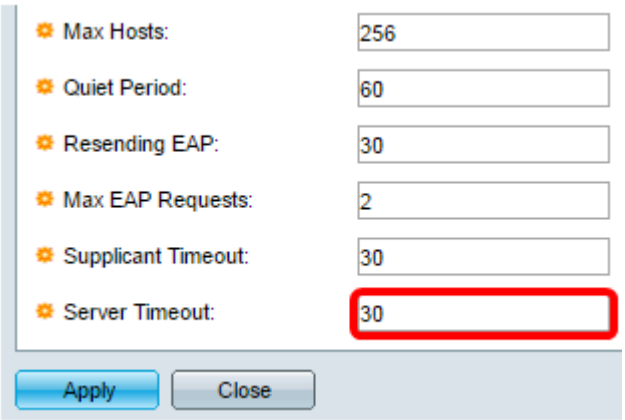
참고:이 예에서는 기본값 2가 사용됩니다.

14단계. Supplicant *Timeout* 필드에 EAP 요청이 신청자에게 재전송되기 전에 경과된 시간(초)을 입력합니다.



참고:이 예에서는 기본값 30이 사용됩니다.

15단계. *Server Timeout* 필드에 스위치가 인증 서버에 요청을 재전송하기 전에 경과된 시간(초)을 입력합니다.



참고:이 예에서는 기본값 30이 사용됩니다.

16단계. 적용을 **누릅니다**.

이제 스위치에서 포트 인증을 성공적으로 구성해야 합니다.