스위치에서 802.1x 포트 인증 설정 구성

목표

IEEE 802.1x는 클라이언트와 서버 간의 액세스 제어를 용이하게 하는 표준입니다.LAN(Local Area 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 퍼블릭 액세스 가능한 포트를 통해 권한이 없는 클라이언트가 LAN에 연결되는 것을 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.

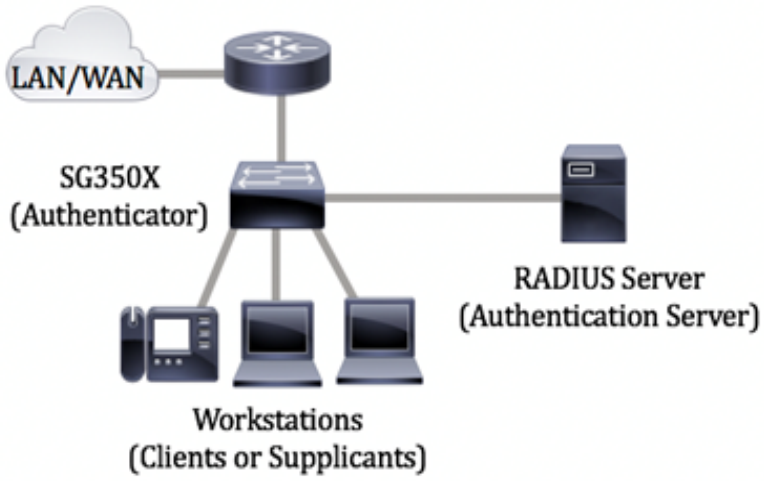
MAC 기반 — 모든 인증 모드에서 지원됩니다.MAC(Media Access Control) 기반의 인증자는 네트워크 액세스를 원하는 클라이언트를 대신하여 소프트웨어의 EAP 클라이언트 부분을 실행합니다.

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.



802.1x 구성 지침:

VLAN(Virtual Access Network)을 생성합니다. 스위치의 웹 기반 유틸리티를 사용하여 VLAN을 생성하려면 여기를 클릭합니다.CLI 기반 지침을 보려면 여기를 클릭하십시오.

스위치의 Port to VLAN 설정을 구성합니다.웹 기반 유틸리티를 사용하여 구성하려면 여기를 클릭하십시오.CLI를 사용하려면 여기를 클릭합니다.

스위치에 802.1x 속성을 구성합니다.802.1x 포트 기반 인증을 활성화하려면 스위치에서 802.1x를 전역적으로 활성화해야 합니다.자세한 내용을 보려면 여기를 클릭하십시오.

(선택 사항) 스위치에서 시간 범위를 구성합니다.스위치에서 시간 범위 설정을 구성하는 방법을 알아보려면 여기를 클릭하십시오.

802.1x 포트 인증을 구성합니다.이 문서에서는 스위치에서 802.1x 포트 인증 설정을 구성하는 방법에 대한 지침을 제공합니다.

스위치에서 mac 기반 인증을 구성하는 방법을 알아보려면 여기를 클릭하십시오.

적용 가능한 디바이스

SX300 시리즈

SX350 시리즈

SG350X 시리즈

SX500 시리즈

SX550X 시리즈

소프트웨어 버전

1.4.7.06 — SX300, SX500

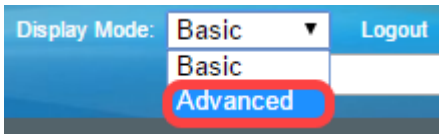
2.2.8.04 — SX350, SG350X, SX550X

스위치에서 802.1x 포트 인증 설정 구성

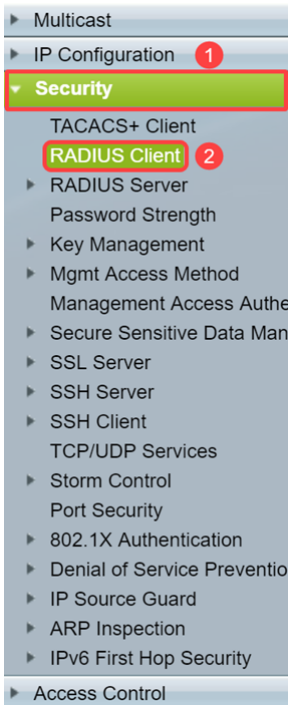
RADIUS 클라이언트 설정 구성

1단계. 스위치의 웹 기반 유틸리티에 로그인한 다음 Display Mode 드롭다운 목록에서 Advanced를 선택합니다.

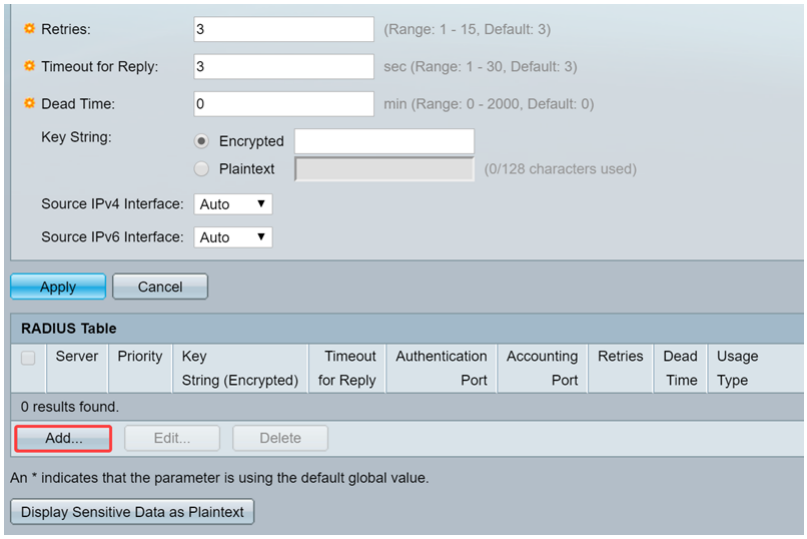
참고:사용 가능한 메뉴 옵션은 디바이스 모델에 따라 달라질 수 있습니다.이 예에서는 SG550X-24가 사용됩니다.



2단계. Security(보안) **> RADIUS Client(RADIUS 클라이언트)로 이동합니다**.

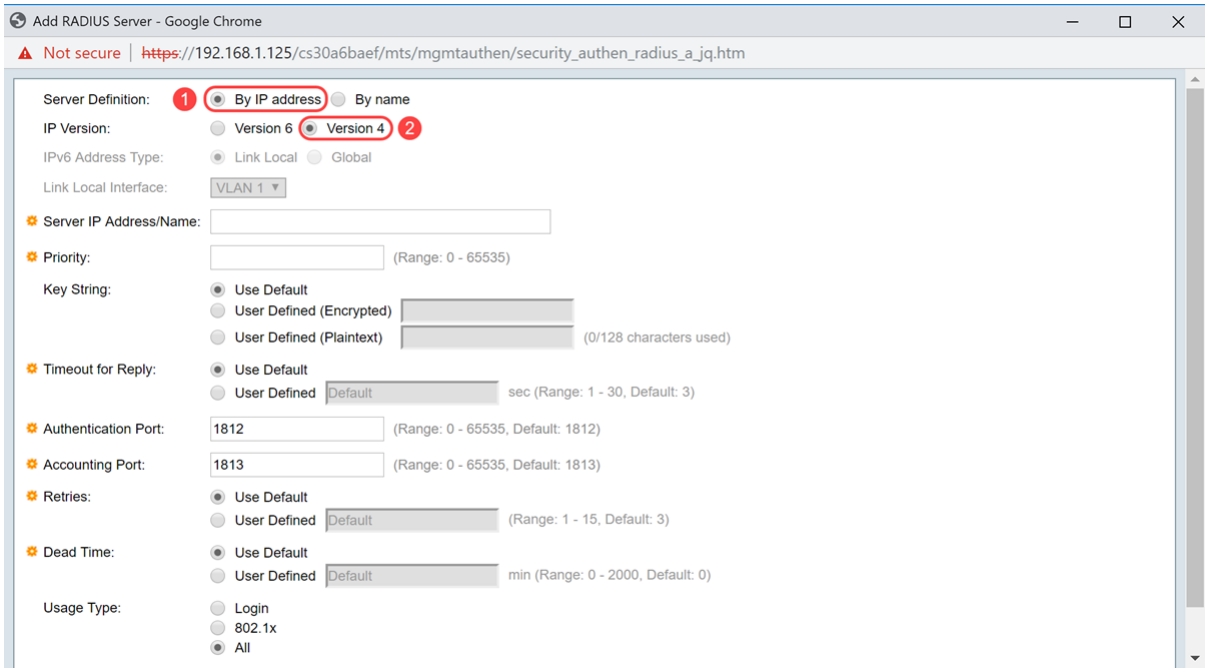


3단계. 아래로 스크롤하여 *RADIUS Table(RADIUS 테이블)* 섹션으로 이동하고 **Add...**(추가...)를 클릭하여 RADIUS 서버를 추가합니다.



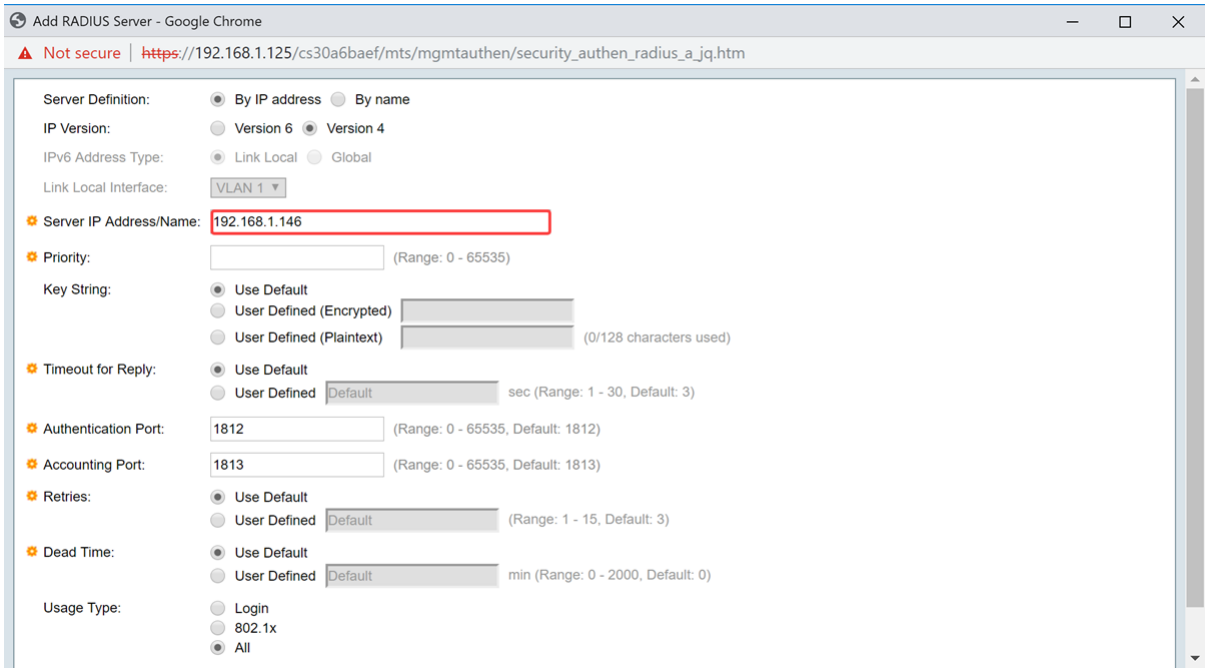
4단계. Server Definition(서버 정의) 필드에서 IP 주소 또는 이름으로 RADIUS 서버를 지정할지 여부를 *선택합니다.IP Version* 필드에서 RADIUS 서버의 IP 주소 버전을 선택합니다.

참고:이 예에서는 **By IP address** 및 **Version 4**를 사용합니다.

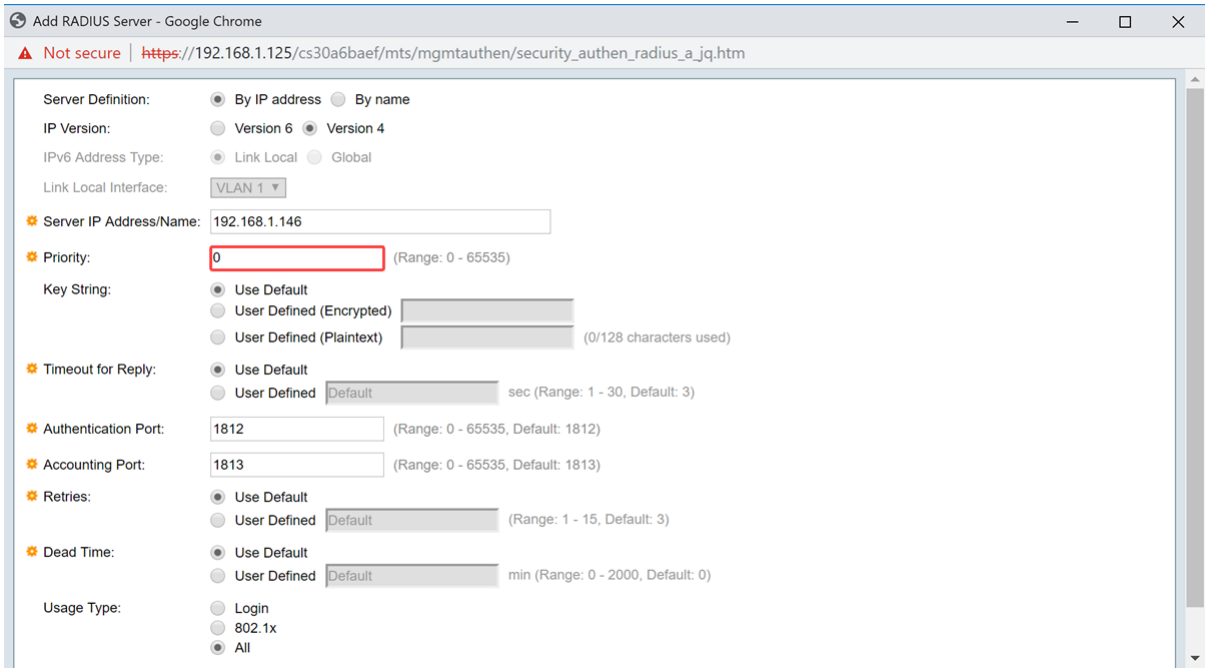


5단계. IP 주소 또는 이름으로 RADIUS 서버에 입력합니다.

참고: Server *IP Address/Name* 필드에 **192.168.1.146**의 IP 주소를 입력하겠습니다.



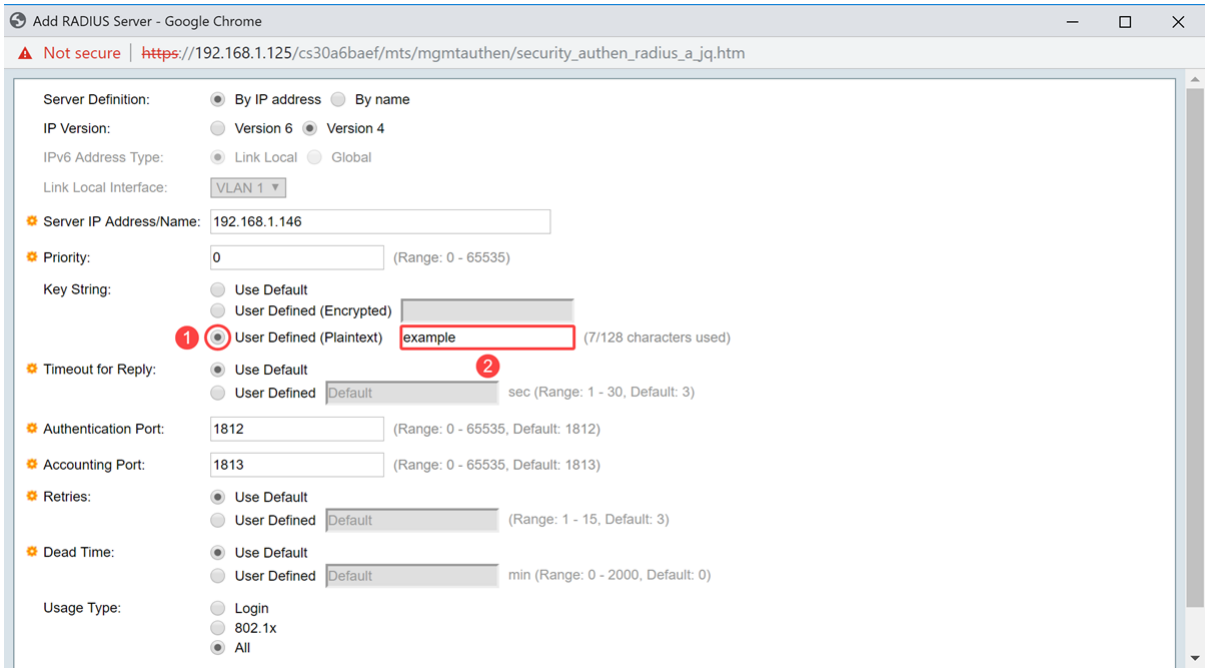
6단계. 서버의 우선순위를 입력합니다.우선순위는 디바이스가 사용자를 인증하기 위해 서버에 연결하려고 시도하는 순서를 결정합니다.디바이스가 우선 순위가 가장 높은 RADIUS 서버로 먼저 시작됩니다.0이 가장 높은 우선 순위입니다.



7단계. 디바이스와 RADIUS 서버 간의 통신을 인증하고 암호화하는 데 사용되는 키 문자열을 입력합니다.이 키는 RADIUS 서버에 구성된 키와 일치해야 합니다.**암호화된** 또는 **일반 텍스트** 형식**으로** 입력할 수 있습니다.Use **Default**(기본값 사용)를 선택하면 디바이스는 기본 키 문자열을 사용하여 RADIUS 서버에 대한 인증을 시도합니다.

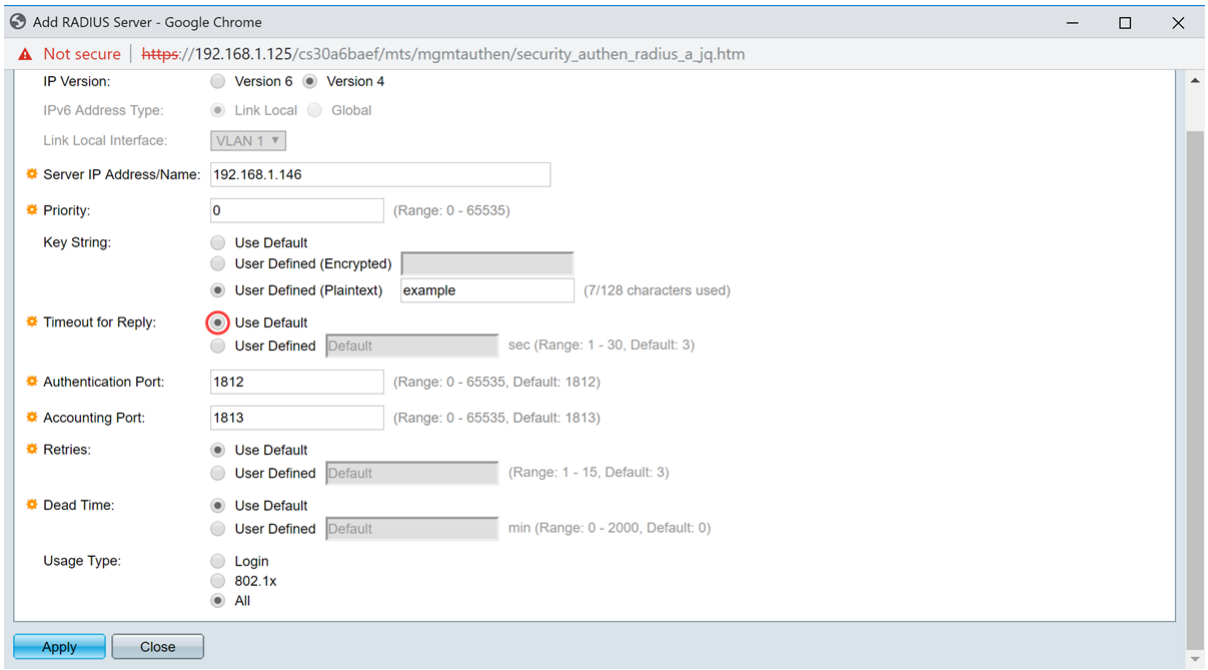
참고: User Defined(Plaintext)**를** 사용하고 주요 **예**를 입력하겠습니다.

스위치에서 RADIUS 서버 설정을 구성하는 방법을 알아보려면 여기를 클릭하십시오.



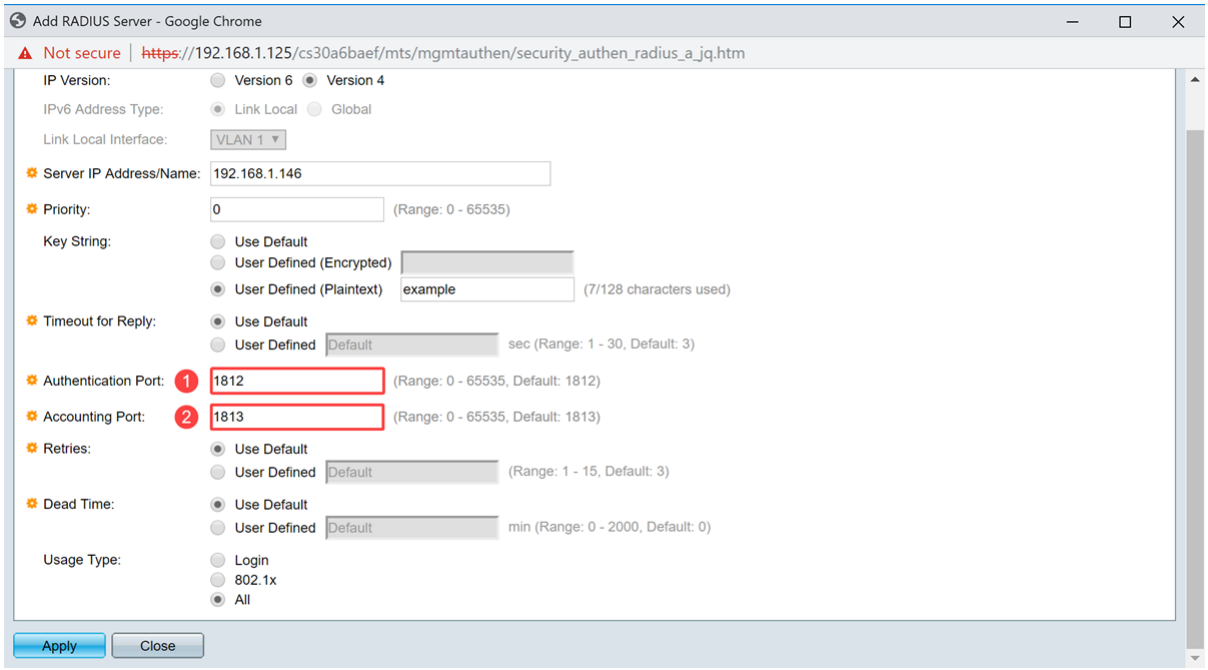
8단계. Timeout for *Reply* 필드*에서 Use Default* 또**는 User Defined**를 선택합니다.**User Defined(사용자 정의)**를 선택한 경우 디바이스가 쿼리를 재시도하기 전에 RADIUS 서버의 응답을 기다리는 시간(초)을 입력하거나 최대 재시도 횟수만큼 다음 서버로 전환합니다.Use **Default(기본값 사용)**를 선택하면 디바이스에서 기본 시간 제한 값을 사용합니다.

참고:이 예에서는 **Use Default(기본값 사용)**가 선택되었습니다.



9단계. 인증 요청을 위한 RADIUS 서버 포트의 UDP 포트 번호를 Authentication *Port* 필드에 입력합니다.어카운팅 요청을 위한 RADIUS 서버 포트의 UDP 포트 번호를 Accounting *Port* 필드에 입력합니다.

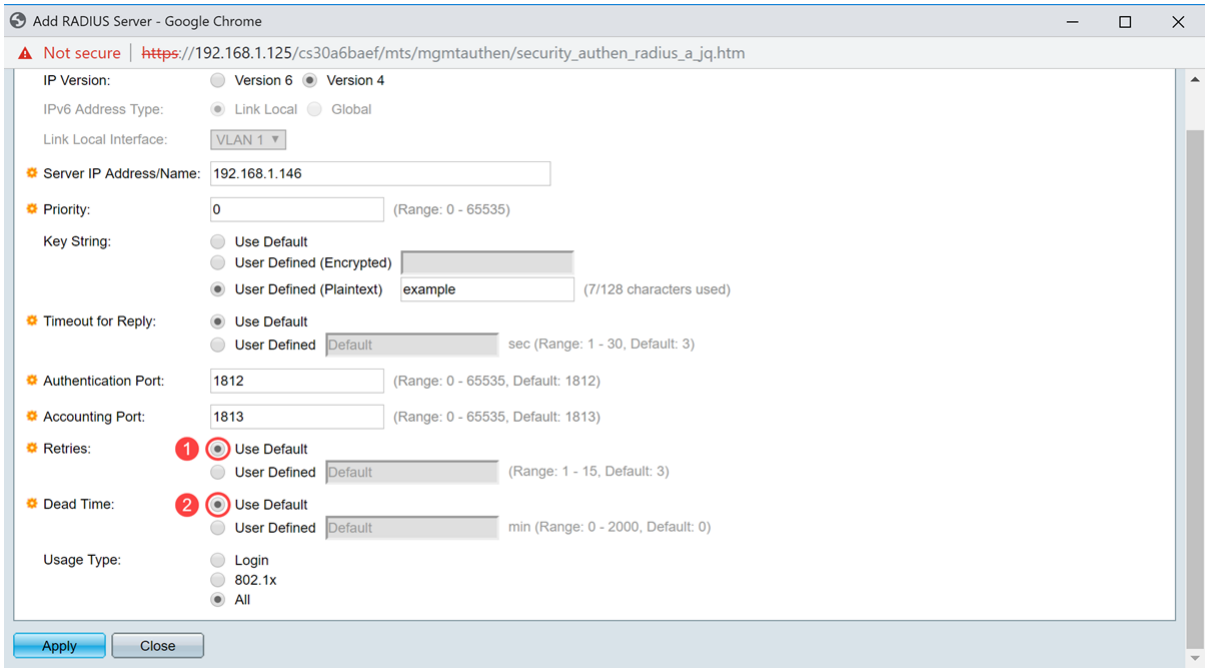
참고:이 예에서는 인증 포트 및 어카운팅 포트 모두에 기본값을 사용합니다.



10단계. **User Defined(사용자 정의)**가 Retries(재시도) 필드에 대해 선택된 경우 오류가 발생한 것으로 간주되기 전에 RADIUS 서버로 전송된 요청 수를 입력합니다.Use **Default(기본값 사용)**를 선택한 경우 디바이스는 재시도 횟수에 기본값을 사용합니다.

User Defined(**사용자 정의**)가 Dead *Time*(데드 *타임)*에 대해 선택된 경우, 서비스 요청에 대해 응답하지 않는 RADIUS 서버를 우회하기 전에 경과해야 하는 시간(분)을 입력합니다.Use **Default(기본값 사용)**를 선택한 경우 디바이스는 데드 시간의 기본값을 사용합니다.0분을 입력하면 데드 타임이 없습니다.

참고:이 예에서는 두 필드에 **대해 기본값 사용**을 선택하겠습니다.

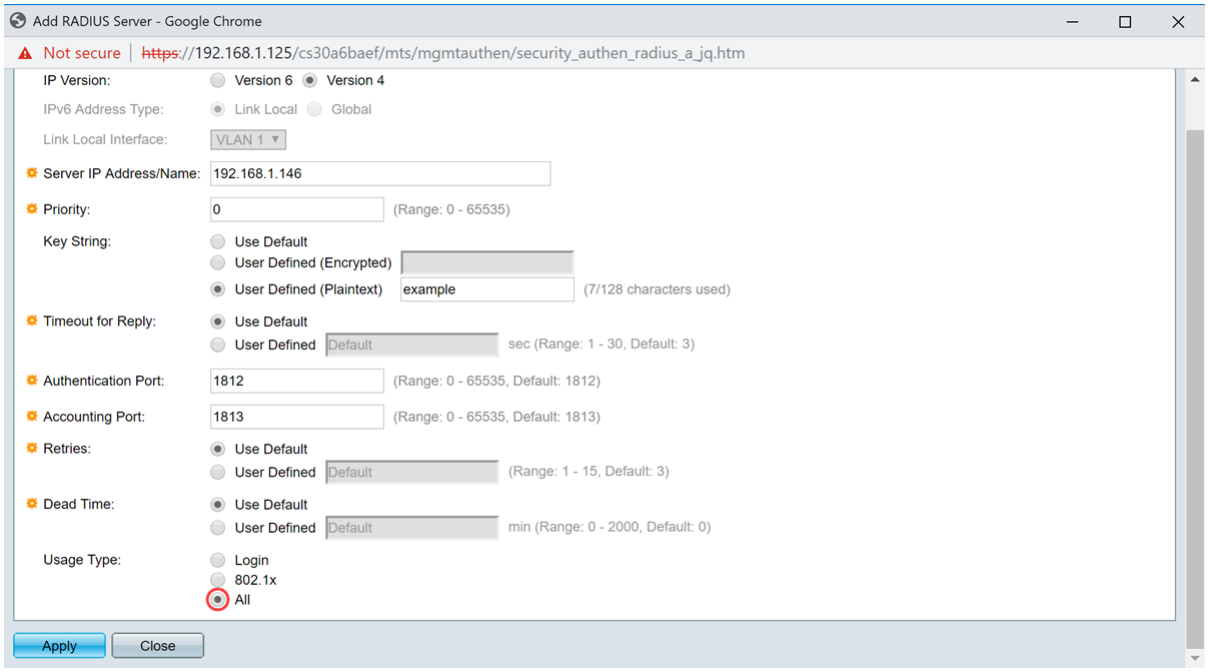


11단계. Usage *Type*(사용 유형) 필드에 RADIUS 서버 인증 유형을 입력합니다.옵션은 다음과 같습니다.

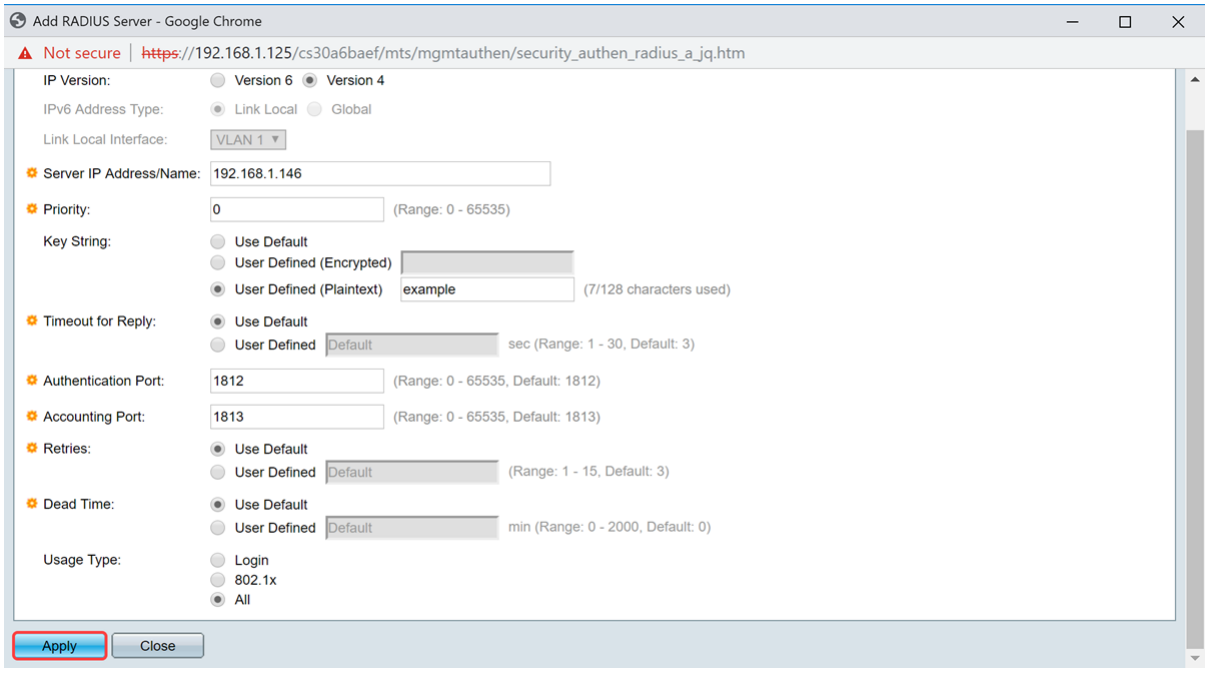
로그인 - RADIUS 서버는 디바이스 관리를 요청하는 사용자를 인증하는 데 사용됩니다.

802.1x - 802.1x 인증에 RADIUS 서버가 사용됩니다.

모두 - RADIUS 서버는 디바이스 관리 및 802.1x 인증을 요청하는 사용자를 인증하는 데 사용됩니다.



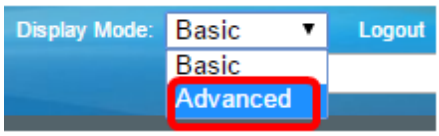
12단계. 적용을 **누릅니다**.



802.1x 포트 인증 설정 구성

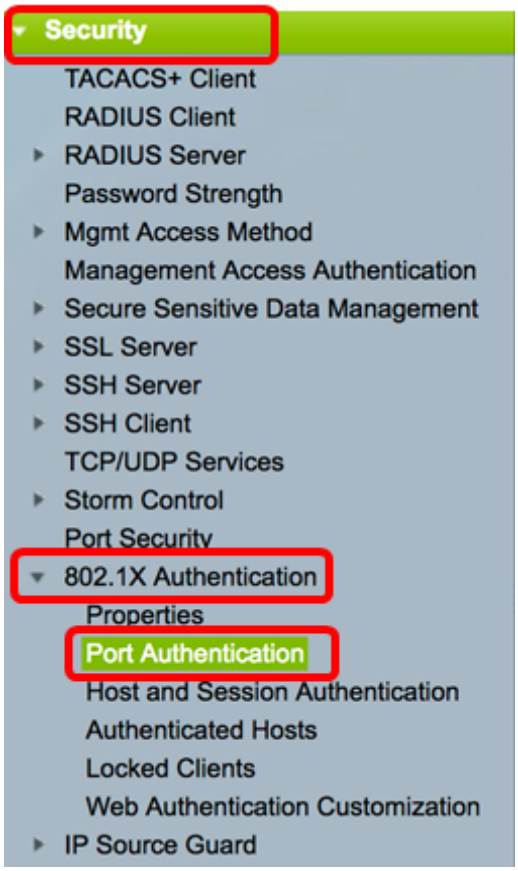
1단계. 스위치의 웹 기반 유틸리티에 로그인한 다음 Display Mode 드롭다운 목록에서 Advanced를 선택합니다.

참고:사용 가능한 메뉴 옵션은 디바이스 모델에 따라 달라질 수 있습니다.이 예에서는 SG350X-48MP가 사용됩니다.



참고: Sx300 또는 SX500 Series 스위치가 있는 경우 2단계로 건너뜁니다.

2단계. **Security > 802.1X Authentication > Port Authentication을 선택합니다.**

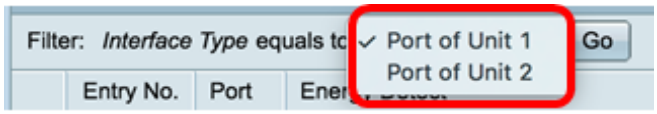


3단계. *Interface Type* 드롭다운 목록에서 인터페이스를 선택합니다.

Port — Interface *Type* 드롭다운 목록에서 단일 포트만 선택해야 하는 **Port**를 선택합니다.

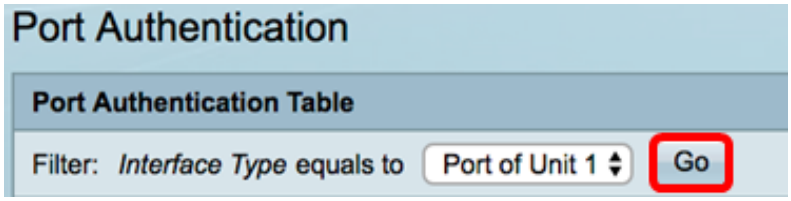
LAG — Interface *Type* 드롭다운 목록에서 구성할 LAG를 선택합니다.이는 LAG 컨피그레이션에 정의된 포트 그룹에 영향을 미칩니다.

참고:이 예에서는 Port of Unit 1이 선택됩니다.

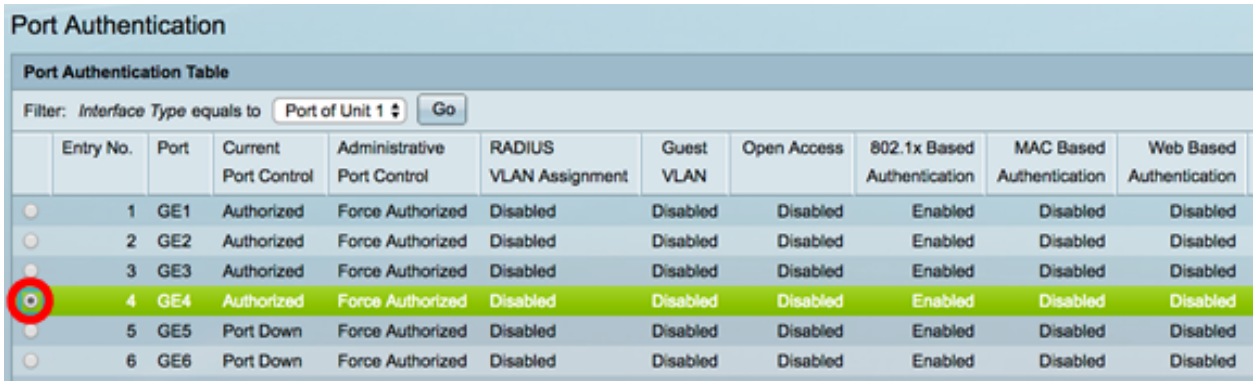


참고: Sx300 Series 스위치와 같이 스택이 아닌 스위치가 있는 경우 5단계로 건너뜁니다.

4단계. **Go(이동)**를 클릭하여 인터페이스에 포트 또는 LAG의 목록을 표시합니다.



5단계. 구성할 포트를 클릭합니다.



참고:이 예에서는 GE4가 선택됩니다.

6단계. 페이지를 아래로 스크롤한 다음 편집을 **클릭합니다**.

7단계. (선택 사항) 다른 인터페이스를 수정하려면 Unit and Port 드롭다운 목록에서 선택합니다.

참고:이 예에서는 유닛 1의 포트 GE4가 선택됩니다.

8단계. Administrative Port Control(관리 포트 제어) 영역에서 원하는 포트 제어에 해당하는 라디오 버튼을 클릭합니다.옵션은 다음과 같습니다.

Force Unauthorized(권한 없음 강제 적용) - 포트를 무단 상태로 전환하여 인터페이스 액세스를 거부합니다.포트가 트래픽을 삭제합니다.

Auto — 포트는 신청자의 인증을 기반으로 권한 있는 상태 또는 권한 없는 상태 사이를 이동합니다.

Force Authorized(강제 권한 부여) - 인증 없이 포트를 인증합니다.포트가 트래픽을 전달합니다.

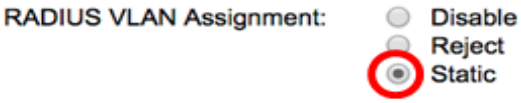
참고:이 예에서는 Auto가 선택됩니다.

9단계. 선택한 포트에서 동적 VLAN 할당을 구성하려면 RADIUS VLAN Assignment 라디오 버튼을 클릭합니다.옵션은 다음과 같습니다.

Disable(비활성화) - 기능이 활성화되지 않았습니다.

거부 — RADIUS 서버가 신청자를 승인했지만 신청자 VLAN을 제공하지 않은 경우 신청자가 거부됩니다.

Static — RADIUS 서버가 신청자를 승인했지만 신청자 VLAN을 제공하지 않은 경우 신청자가 수락됩니다.



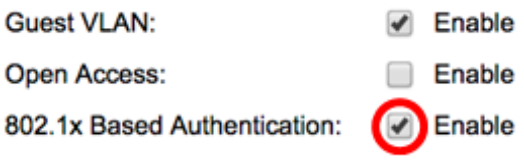
참고:이 예에서는 Static이 선택됩니다.

10단계. Guest **VLAN(게스트 VLAN)** 확인란을 선택하여 권한이 없는 포트에 대해 게스트 VLAN을 활성화합니다.게스트 VLAN은 802.1 속성의 게스트 VLAN ID 영역에서 선택한 VLAN에 무단 포트가 자동으로 조인하도록 합니다.

11단계. (선택 사항) **Enable** Open Access 확인란을 선택하여 열린 액세스를 활성화합니다 .Open Access를 사용하면 네트워크에 연결하는 호스트의 구성 문제를 이해하고, 잘못된 상황을 모니터링하며, 이러한 문제를 해결할 수 있습니다.

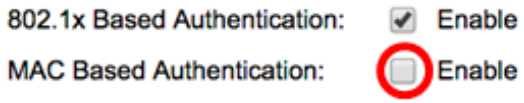
참고:인터페이스에서 Open Access가 활성화된 경우 스위치는 RADIUS 서버에서 수신한 모든 장애를 성공으로 간주하며 인증 결과와 상관없이 인터페이스에 연결된 스테이션의 네트워크에 대한 액세스를 허용합니다.이 예에서는 Open Access가 비활성화됩니다.

12단계. 포트에서 802.1X 인증을 활성화하려면 **Enable** 802.1x Based Authentication 확인란을 선택합니다.



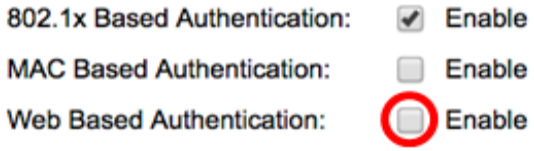
13단계. 서 플리 컨 트 MAC 주소를 기반으로 포트 인증을 활성화 하려면 **Enable** MAC Based Authentication 확인란을 선택 합니다.8개의 MAC 기반 인증만 포트에서 사용할 수 있습니다.

참고:MAC 인증이 성공하려면 RADIUS 서버 신청자 사용자 이름 및 비밀번호가 신청자 MAC 주소여야 합니다.MAC 주소는 소문자 및 를 포함하지 않고 입력해야 합니다.또는 - 구분 기호 (예: 0020aa00bbcc)



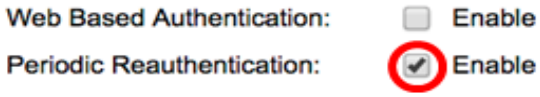
참고:이 예에서는 MAC 기반 인증이 비활성화됩니다.

14단계. Enable Web Based Authentication(웹 기반 인증 활성화) 확인란을 선택하여 스위치에서 웹 기반 인증을 활성화합니다.이 예에서는 웹 기반 인증이 비활성화됩니다.



참고:이 예에서는 웹 기반 인증이 비활성화됩니다.

15단계. (선택 사항) Enable Periodic **Reauthentication** 확인란을 선택하여 지정된 시간 후에 포트를 재인증합니다.이 시간은 Reauthentication Period(재인증 *기간)* 필드에 정의되어 있습니다.



참고:이 예에서는 기간 재인증이 활성화됩니다.

16단계(선택 사항) Reauthentication Period(재인증 기간) 필드에 값을 입력합니다.이 값은 인터페이스가 포트를 다시 인증하기 전 시간(초)을 나타냅니다.기본값은 3600초이며 범위는 300~4294967295초입니다.

참고:이 예에서는 6000초가 구성됩니다.

17단계. (선택 사항) Enable **Reauthenticate** Now 확인란을 선택하여 즉시 포트를 재인증합니다.이 예에서는 즉시 재인증이 비활성화됩니다.

Authenticator State(인증자 상태) 영역에는 포트의 인증 상태가 표시됩니다.

18단계. (선택 사항) **Enable** Time Range 확인란을 선택하여 포트가 인증된 시간에 대한 제한을 활성화합니다.

참고:이 예에서는 시간 범위가 활성화됩니다.이 기능을 건너뛰려면 20단계로 진행합니다.

19단계. (선택 사항) Time Range Name 드롭다운 목록에서 사용할 시간 범위를 선택합니다.

참고:이 예에서는 Dayshift가 선택됩니다.

20단계. Maximum WBA Login Attempts(최대 WBA 로그인 시도) 영역에서 Infinite for no limit(무제한) 또는 User Defined(사용자 정의)를 클릭하여 제한을 설정합니다.User Defined(사용자 정의)를 선택한 경우 웹 기반 인증에 허용되는 최대 로그인 시도 횟수를 입력합니다.

참고:이 예에서는 Infinite가 선택됩니다.

21단계. Maximum WBA Silence Period(최대 WBA 무음 기간) 영역에서 Infinite for no limit(무제한) 또는 User Defined(사용자 정의)를 클릭하여 제한을 설정합니다.User Defined(사용자 정의)를 선택한 경우 인터페이스에서 허용되는 웹 기반 인증을 위한 무음 기간의 최대 길이를 입력합니다.

참고:이 예에서는 Infinite가 선택됩니다.

22단계. Max Hosts(최대 호스트) 영역에서 Infinite for no limit(무제한)을 클릭하고 User Defined(사용자 정의)를 클릭하여 제한을 설정합니다.User Defined(사용자 정의)를 선택한 경우 인터페이스에서 허용되는 인증된 호스트의 최대 수를 입력합니다.

참고:다중 세션 모드에서 웹 기반 인증을 위한 단일 호스트 모드를 시뮬레이션하려면 이 값을 1로 설정합니다.이 예에서는 Infinite가 선택됩니다.

23단계. Quiet *Period* 필드에 인증 교환 실패 후 스위치가 조용한 상태로 유지되는 시간을 입력합니다.스위치가 조용한 상태이면 스위치가 클라이언트의 새 인증 요청을 수신하지 않음을 의미합니다.기본값은 60초이며 범위는 1~65535초입니다.

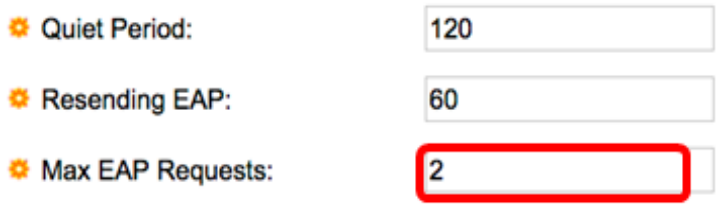
참고:이 예에서는 자동 기간이 120초로 설정됩니다.

24단계. Resending EAP(*EAP 재전송*) 필드에 스위치가 요청을 재전송하기 전에 신청자의 응

답 메시지를 기다리는 시간을 입력합니다.기본값은 30초이며 범위는 1~65535초입니다.

참고:이 예에서는 EAP를 다시 보내는 것이 60초로 설정됩니다.

25단계. *Max EAP Requests(최대 EAP 요청)* 필드에 전송할 수 있는 최대 EAP 요청 수를 입력합니다.EAP는 스위치와 클라이언트 간 인증 정보 교환을 제공하는 802.1X에서 사용되는 인증 방법입니다.이 경우 EAP 요청은 인증을 위해 클라이언트로 전송됩니다.그런 다음 클라이언트는 인증 정보에 응답하고 일치해야 합니다.클라이언트가 응답하지 않으면 Resending EAP 값을 기반으로 다른 EAP 요청이 설정되고 인증 프로세스가 다시 시작됩니다.기본값은 2이고 범위는 1에서 10까지입니다.

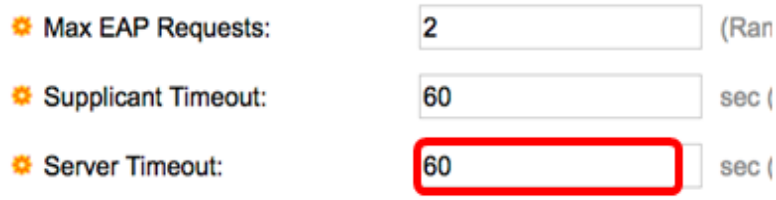


참고:이 예에서는 기본값인 2가 사용됩니다.

26단계. Supplicant *Timeout(신청자 시간 초과)* 필드에 EAP 요청이 신청자에게 재전송되기 전의 시간을 입력합니다.기본값은 30초이며 범위는 1~65535초입니다.

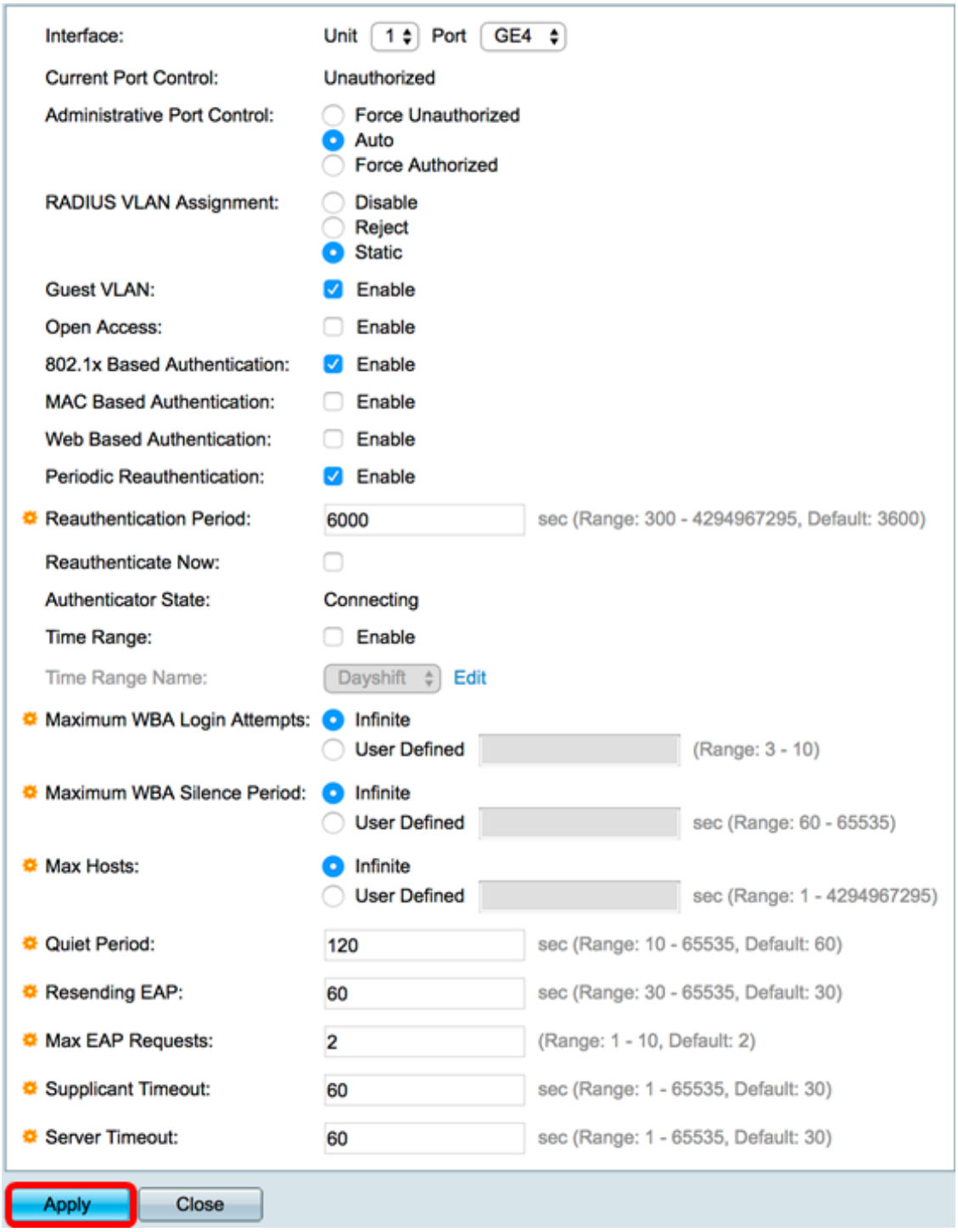
참고:이 예에서 신청자 시간 제한은 60초로 설정됩니다.

27단계. *Server Timeout* 필드에 스위치가 RADIUS 서버에 요청을 다시 보내기 전에 경과된 시간을 입력합니다.기본값은 30초이며 범위는 1~65535초입니다.

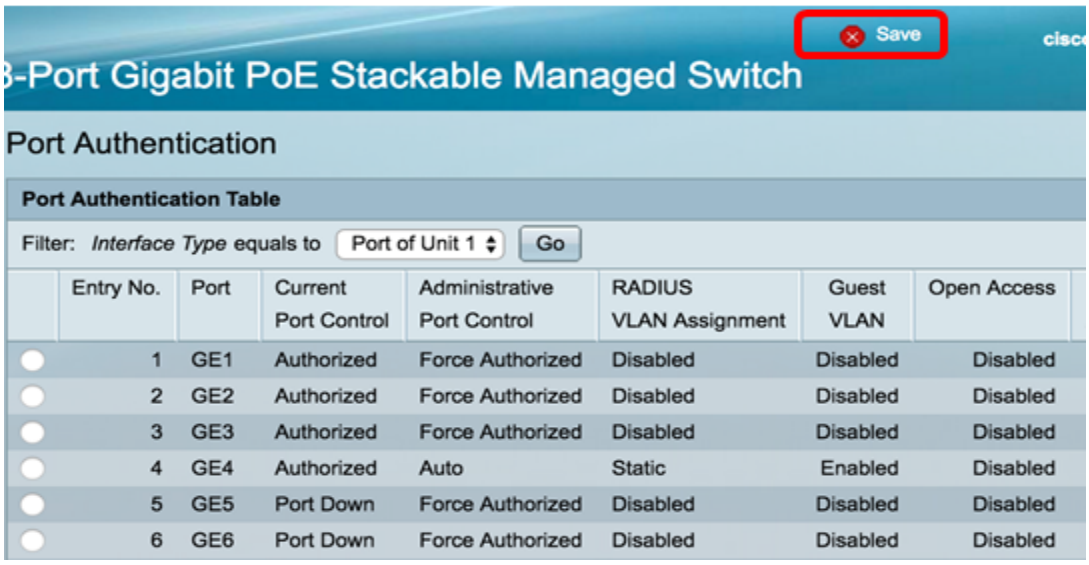


참고:이 예에서는 서버 시간 초과가 60초로 설정됩니다.

28단계. **적용**을 클릭한 다음 **닫기를 클릭합니다**.



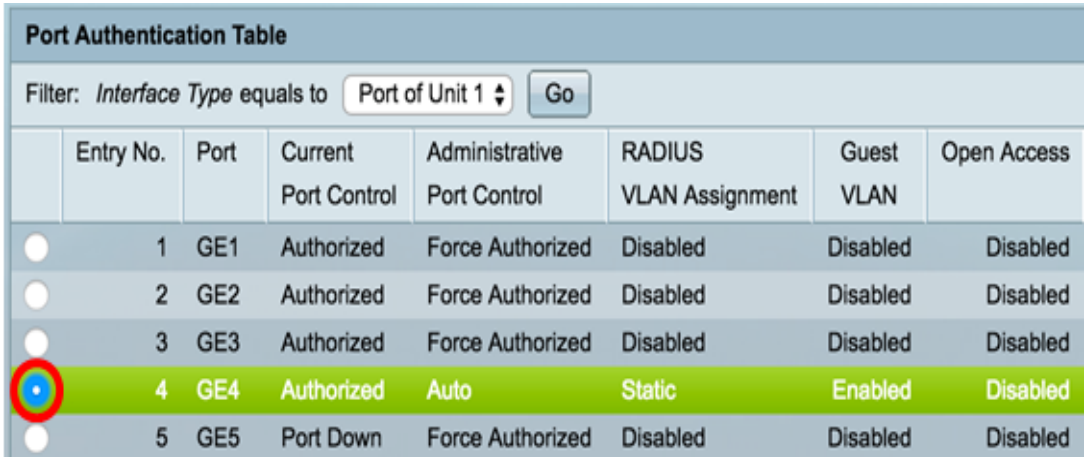
29단계. (선택 사항) **Save**를 클릭하여 시작 컨피그레이션 파일에 설정을 저장합니다.



이제 스위치에서 802.1x 포트 인증 설정을 성공적으로 구성했어야 합니다.

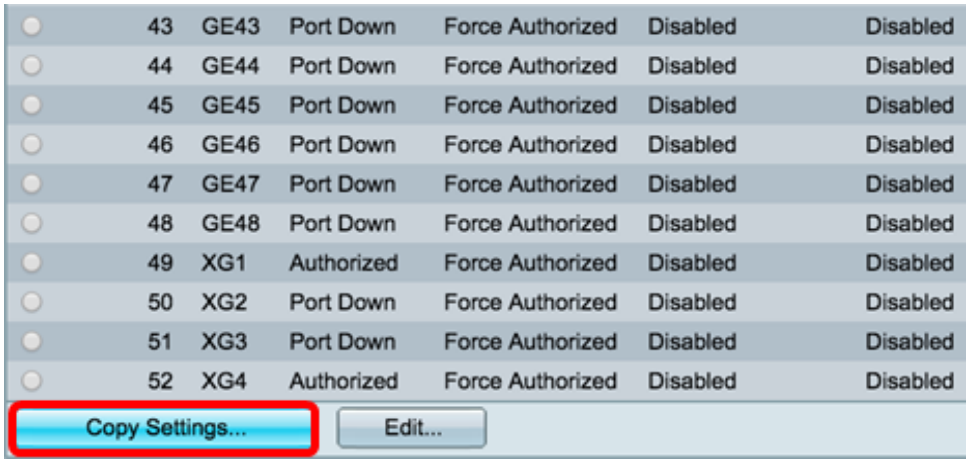
여러 인터페이스에 인터페이스 컨피그레이션 설정 적용

1단계. 여러 인터페이스에 인증 컨피그레이션을 적용할 인터페이스의 라디오 버튼을 클릭합니다.



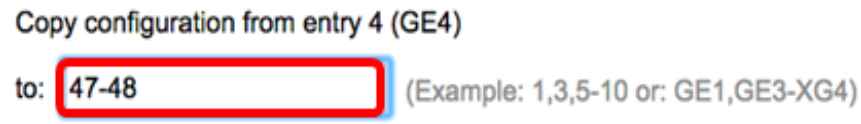
참고:이 예에서는 GE4가 선택됩니다.

2단계. 아래로 스크롤한 다음 **Copy Settings(설정 복사)**를 클릭합니다.



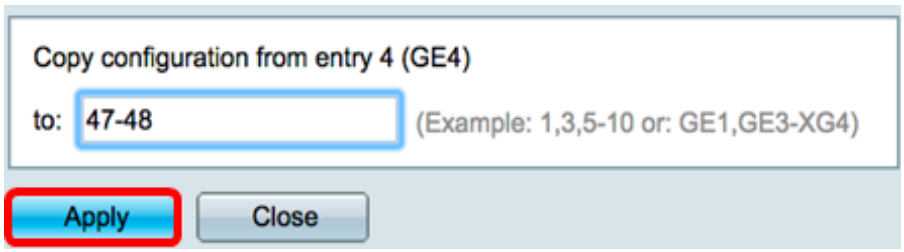
3단계. *to* 필드에 선택한 인터페이스의 컨피그레이션을 적용할 인터페이스 범위를 입력합니다.인터페이스 번호 또는 인터페이스의 이름을 입력으로 사용할 수 있습니다.각 인터페이스를

쉼표로 구분하여 입력할 수 있습니다(예: 1, 3, 5 또는 GE1, GE3, GE5). 또는 인터페이스 범위(예: 1-5 또는 GE1-GE5)를 입력할 수 있습니다.

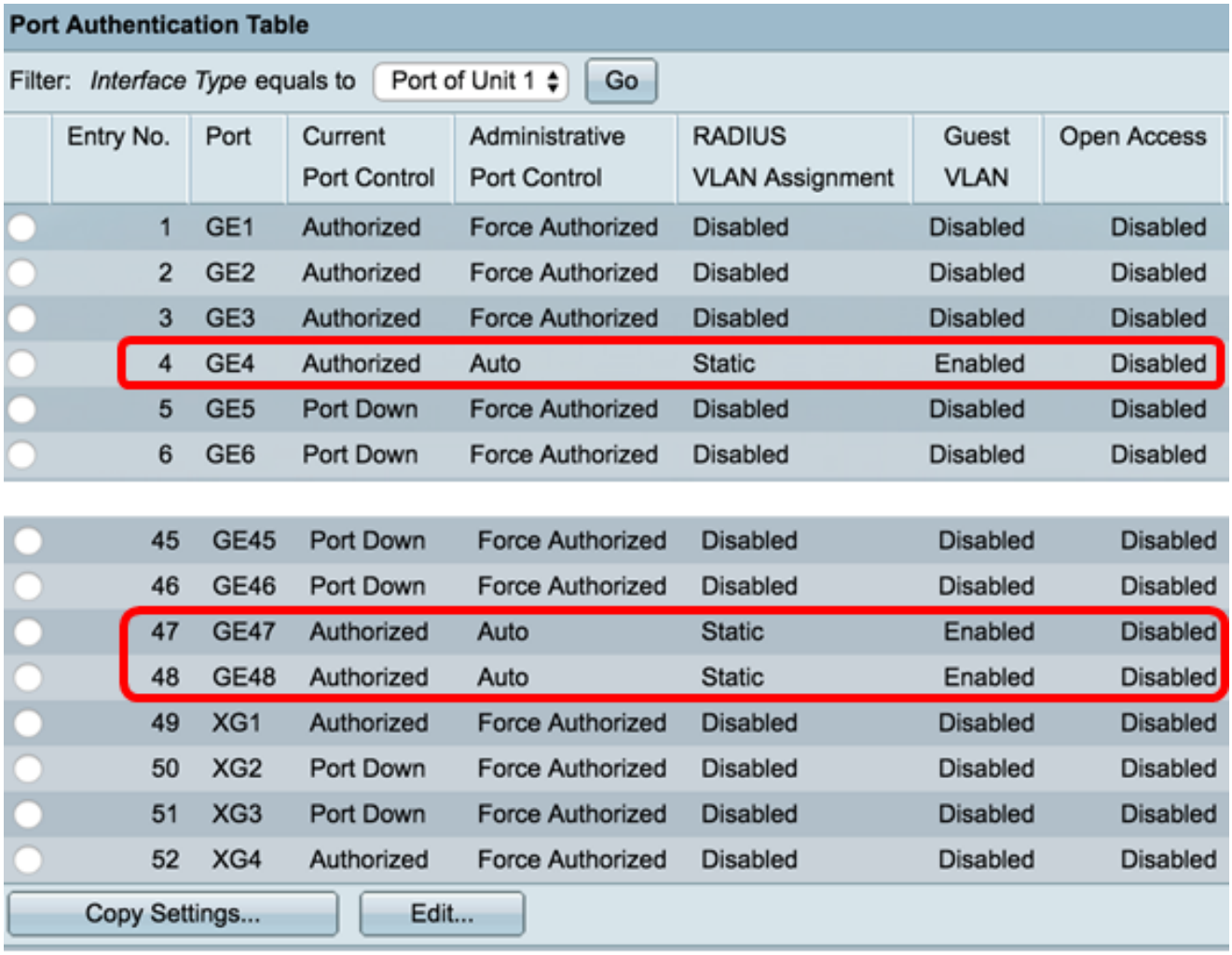


참고:이 예에서는 컨피그레이션 설정이 포트 47~48에 적용됩니다.

4단계. Apply(적용)를 **클릭한** 다음 **Close(닫기)**를 클릭합니다.



아래 이미지는 컨피그레이션 후의 변경 사항을 나타냅니다.



이제 한 포트의 802.1x 인증 설정을 성공적으로 복사하고 스위치의 다른 포트 또는 포트에 적용했어야 합니다.