스위치에서 MAC 기반 인증 구성

목표

802.1X는 목록 장치를 허용하여 네트워크에 대한 무단 액세스를 방지하는 관리 툴입니다.이 문서에서는 GUI(Graphical User Interface)를 사용하여 스위치에서 MAC 기반 인증을 구성하는 방법을 보여줍니다. CLI(Command Line Interface)를 사용하여 MAC 기반 인증을 구성하는 방법을 알아보려면 여기를 클릭하십시오.

참고:이 가이드는 9개 섹션 및 1개 섹션에 길어 호스트가 인증되었는지 확인합니다.커피, 차 또는 물을 마시고 관련 단계를 검토하고 실행할 충분한 시간을 확보하십시오.

자세한 내용은 용어집을 참조하십시오.

Radius 작동 방식

802.1X 인증, 신청자(클라이언트), 인증자(스위치 같은 네트워크 장치) 및 인증 서버(RADIUS)에 대한 세 가지 주요 구성 요소가 있습니다. RADIUS(Remote Authentication Dial-In User Service)는 네트워크 액세스를 관리하는 데 도움이 되는 AAA(Authentication, Authorization, and Accounting) 프로토콜을 사용하는 액세스 서버입니다.RADIUS는 RADIUS 서버와 하나 이상의 RADIUS 클라이언트 간에 보안 인증 정보가 교환되는 클라이언트-서버 모델을 사용합니다.클라이언트의 ID를 확인하고 클라이언트가 LAN에 액세스할 수 있는지 여부를 스위치에 알립니다.

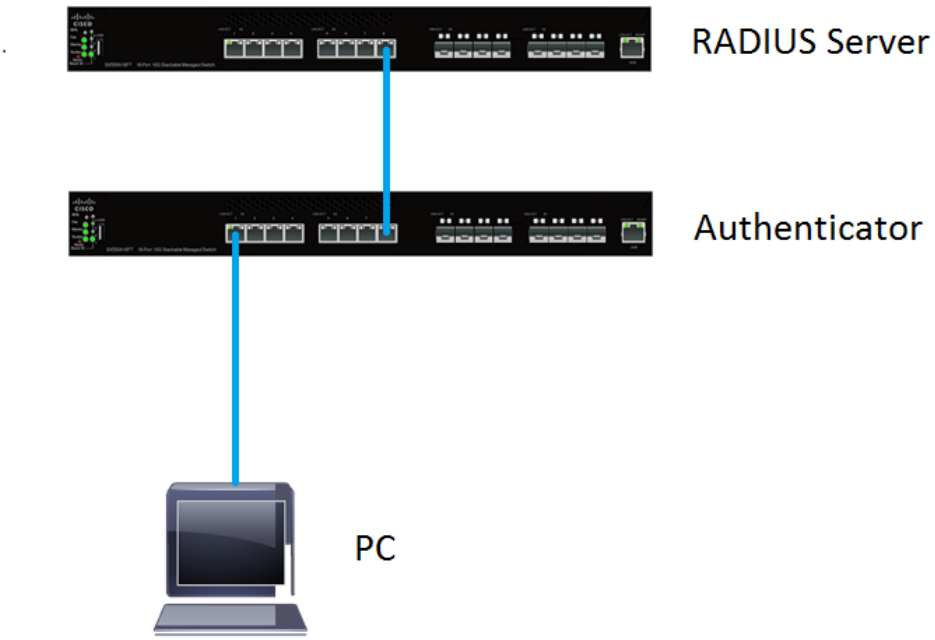
인증자는 클라이언트와 인증 서버 간에 작동합니다.먼저 클라이언트에서 ID 정보를 요청합니다.이에 대한 응답으로 인증자는 인증 서버로 정보를 확인합니다.마지막으로, 클라이언트에 응답을 릴레이합니다.이 문서에서 인증자는 RADIUS 클라이언트를 포함하는 스위치입니다.스위치는 인증 서버와 상호 작용하기 위해 EAP(Extensible Authentication Protocol) 프레임을 캡슐화하고 역캡슐화할 수 있습니다.

MAC 기반 인증은 어떻습니까?

MAC 기반 인증에서 신청자가 인증자와 통신하는 방법을 이해하지 못하거나 인증할 수 없는 경우 호스트의 MAC 주소를 사용하여 인증합니다.MAC 기반 신청자는 EAP를 사용하지 않고 순수 RADIUS를 사용하여 인증됩니다. RADIUS 서버에는 허용된 MAC 주소만 포함된 전용 호스트 데이터베이스가 있습니다.MAC 기반 인증 요청을 PAP(Password Authentication Protocol) 인증으로 처리하는 대신 서버는 특성 6 [Service-Type] = 10에 의해 이러한 요청을 인식합니다. Calling-Station-Id 특성의 MAC 주소를 호스트 데이터베이스에 저장된 MAC 주소와 비교합니다.

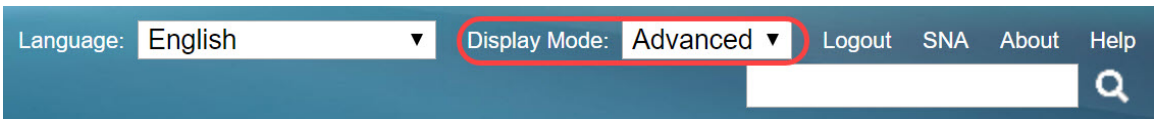
버전 2.4 릴리스는 MAC 기반 신청자를 위해 전송되고 EAP 인증 방법 또는 순수 RADIUS로 정의되는 사용자 이름의 형식을 구성하는 기능을 추가합니다.이 버전에서는 MAC 기반 신청자에 대해 사용자 이름과 다른 특정 비밀번호를 구성할 뿐만 아니라 사용자 이름의 형식을 구성할 수도 있습니다.

토폴로지:



참고:이 문서에서는 RADIUS 서버와 인증자 모두에 SG550X-24를 사용합니다.RADIUS 서버는 고정 IP 주소가 192.168.1.100이고 인증자는 고정 IP 주소가 192.168.1.101입니다.

이 문서의 단계는 **고급** 표시 모드에서 수행됩니다.모드를 고급으로 변경하려면 오른쪽 상단 모서리로 이동하여 *Display Mode* 드롭다운 목록에서 **Advanced**를 선택합니다.



목차

적용 가능한 디바이스

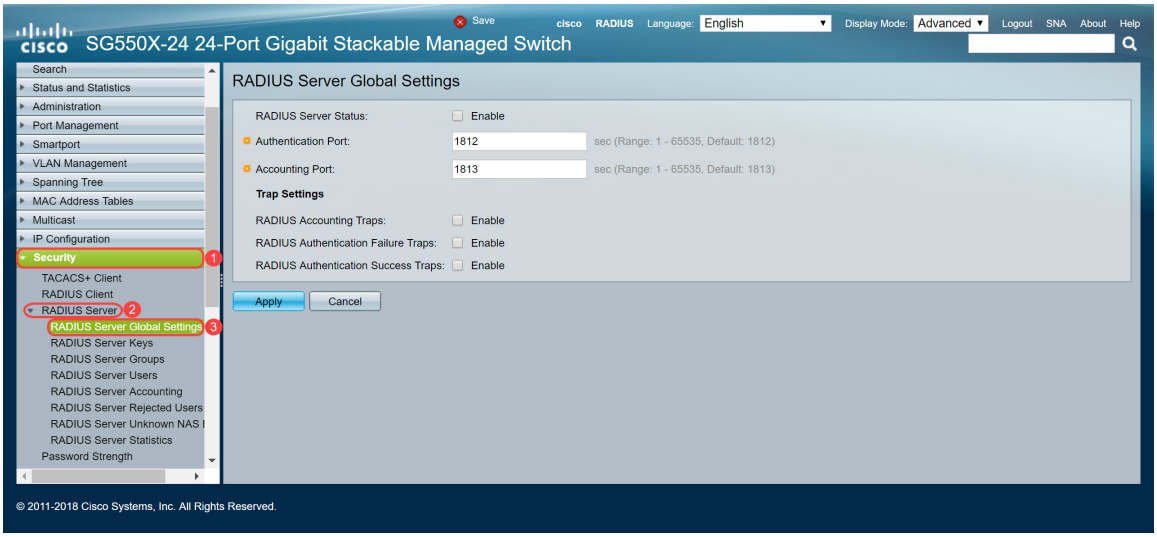
- SX350X 시리즈
- SG350XG 시리즈
- SX550X 시리즈
- SG550XG 시리즈

소프트웨어 버전

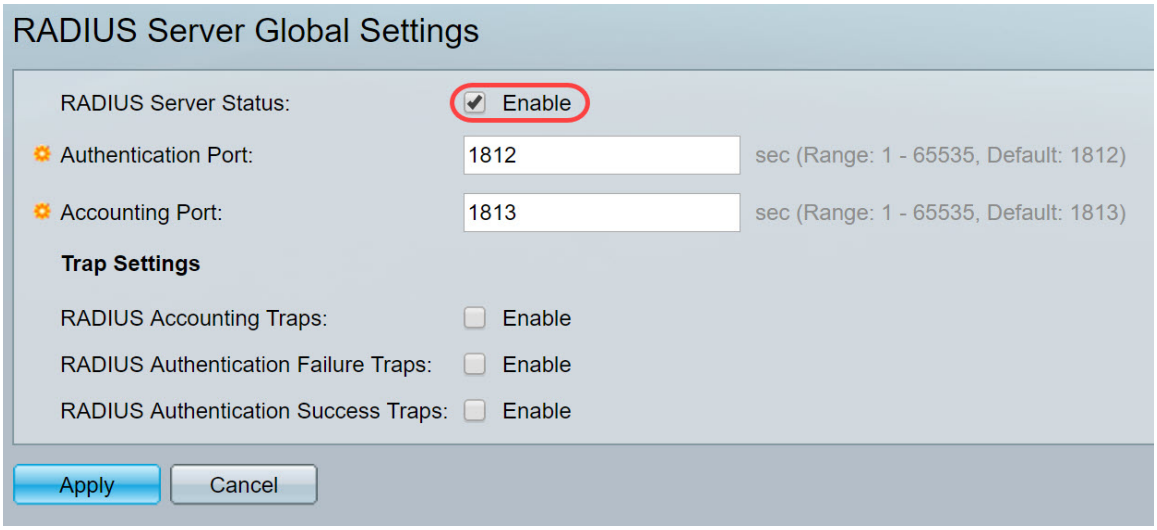
- 2.4.0.94

RADIUS 서버 전역 설정

1단계. RADIUS 서버로 구성할 스위치의 웹 기반 유틸리티에 로그인하고 **Security > RADIUS Server > RADIUS Server Global Settings로 이동합니다**.

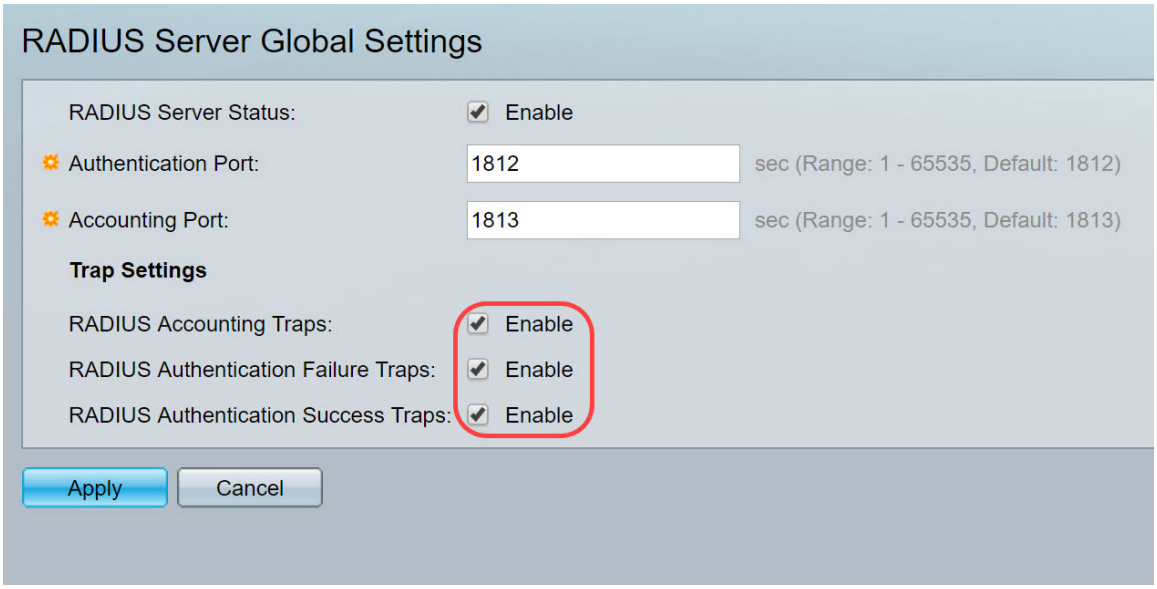


2단계. RADIUS 서버 기능 상태를 활성화하려면 RADIUS *Server Status* 필드에서 **Enable**(활성화) 확인란을 선택합니다.



3단계. RADIUS 어카운팅 이벤트, 실패한 로그인 또는 성공한 로그인에 대한 트랩을 생성하려면 원하는 **Enable** 확인란을 선택하여 트랩을 생성합니다.트랩은 SNMP(Simple Network Management Protocol)를 통해 생성되는 시스템 이벤트 메시지입니다.위반이 발생하면 스위치의 SNMP 관리자에게 트랩이 전송됩니다.다음 트랩 설정은 다음과 같습니다.

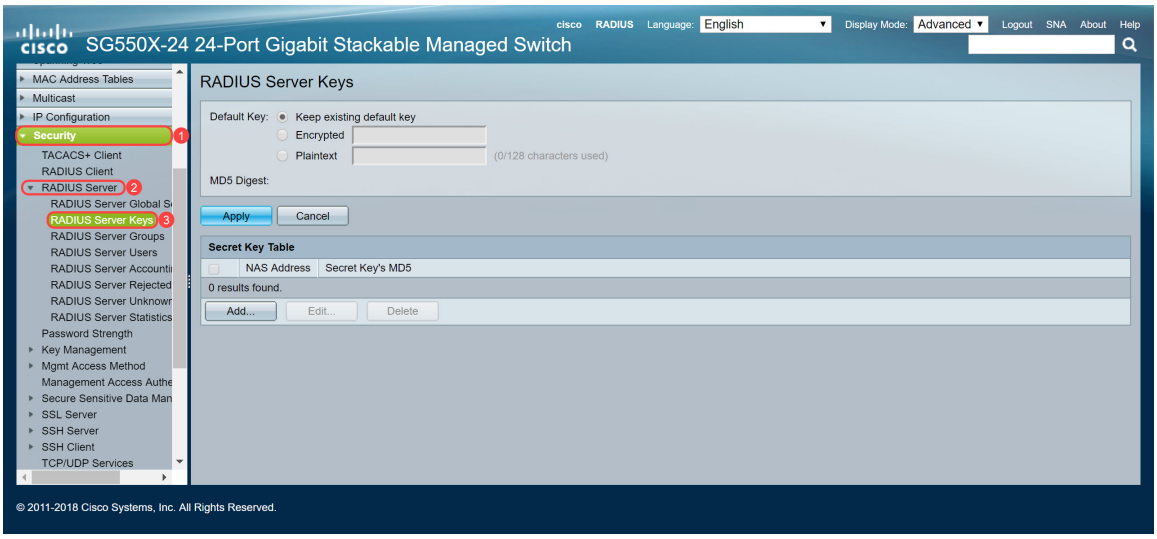
- RADIUS 어카운팅 트랩 — RADIUS 어카운팅 이벤트에 대한 트랩을 생성하려면 선택합니다.
- RADIUS 인증 실패 트랩 — 실패한 로그인에 대한 트랩을 생성하려면 선택합니다.
- RADIUS Authentication Success Traps(RADIUS 인증 성공 트랩) - 성공한 로그인에 대한 트랩을 생성하려면 선택합니다.



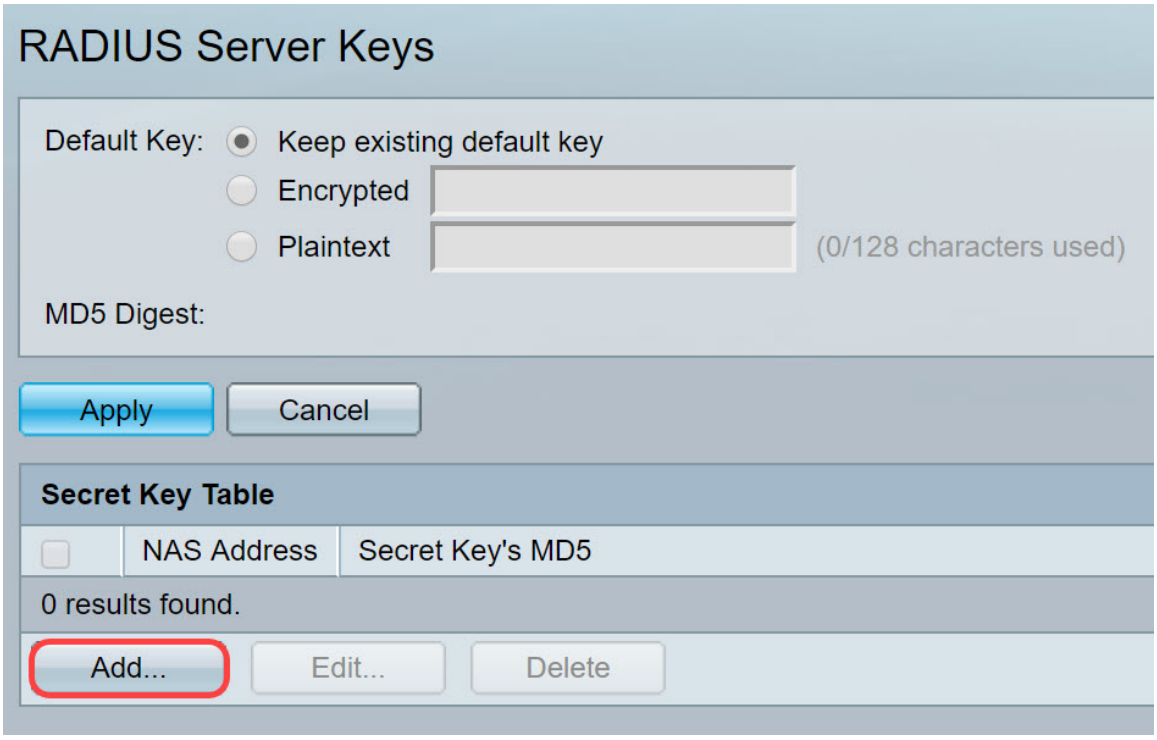
4단계. **적용**을 클릭하여 설정을 저장합니다.

RADIUS 서버 키

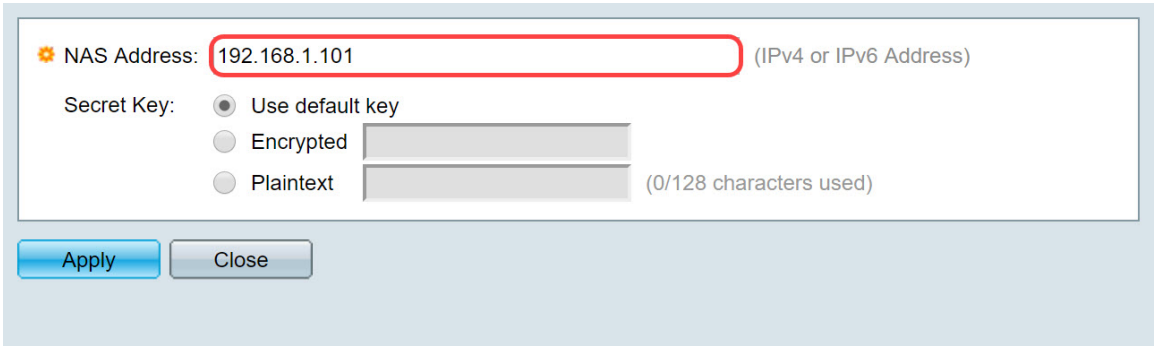
1단계. Security(보안) **> RADIUS Server(RADIUS 서버) > RADIUS Server Keys(RADIUS 서버 키)로 이동합니다**.RADIUS *Server Key* 페이지가 열립니다.



2단계. Secret *Key Table(비밀 키 테이블)* 섹션에서 Add..(추가...)를 클릭합니다. 비밀 키를 추가합니다.



3단계. Add *Secret Key*(*비밀 키 추가*) 창 페이지가 열립니다.NAS *Address* 필드에 RADIUS 클라이언트를 포함하는 스위치의 주소를 입력합니다.이 예에서는 RADIUS 클라이언트로 IP 주소 192.168.1.101을 사용합니다.

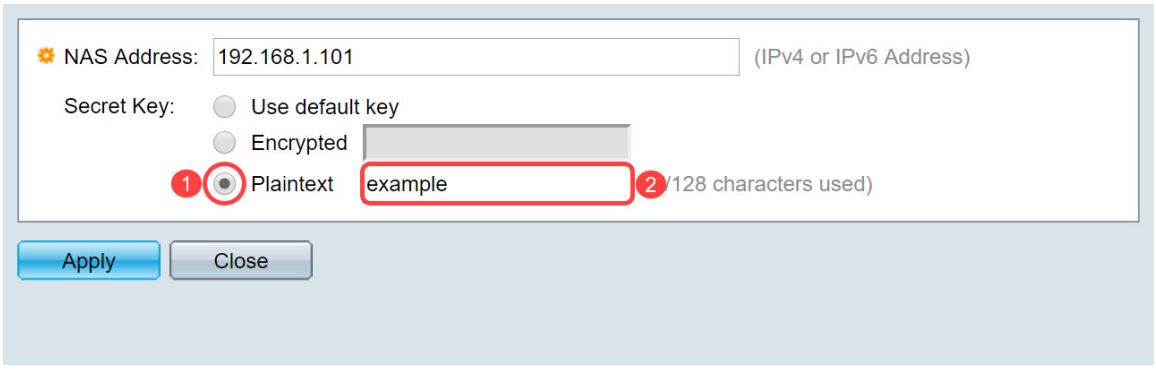


4단계. *비밀 키*로 사용되는 라디오 버튼 중 하나를 *선택합니다*.다음 옵션은 다음과 같습니다.

- 기본 키 사용 — 지정된 서버의 경우 디바이스는 기존의 기본 키 문자열을 사용하여 RADIUS 클라이언트를 인증하려고 시도합니다.
- 암호화 — MD5(Message-Digest Algorithm 5)를 사용하여 통신을 암호화하려면 암호화된 형식으로 키를 입력합니다.
- 일반 텍스트 — 일반 텍스트 모드에서 키 문자열을 입력합니다.

이 예에서는 Plaintext를 선택하고 *예*를 **예**로 *Secret Key*로 *사용합니다*.apply(적용)를 누르면 키가 암호화된 형식으로 표시됩니다.

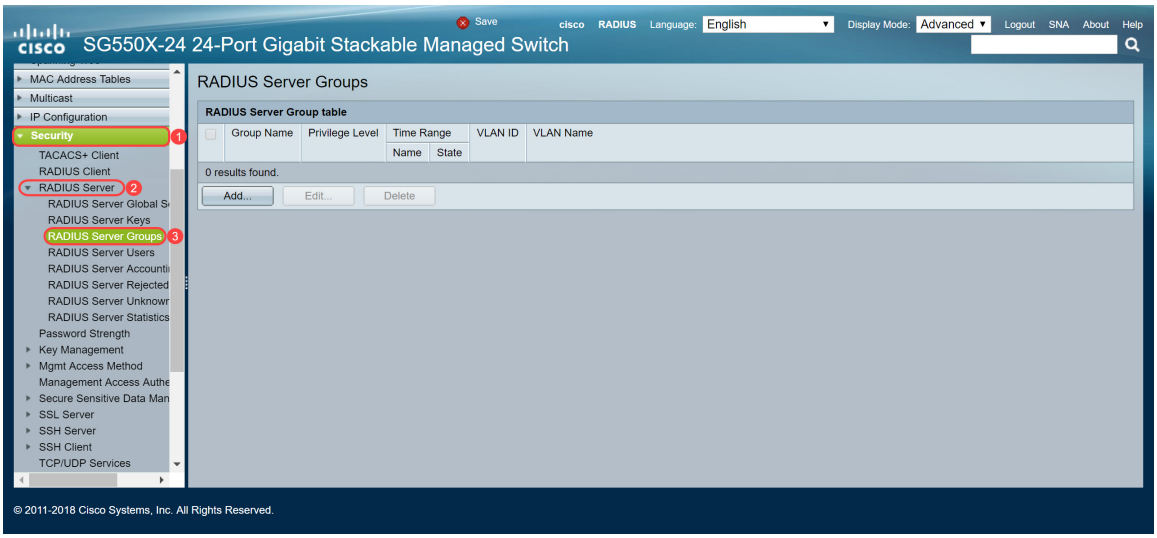
참고:example이라는 단어를 비밀 키로 사용하지 않는 것이 좋습니다.더 강력한 키를 사용하십시오.최대 128자를 사용할 수 있습니다.암호가 너무 복잡해서 기억하기 어려우면 암호이지만 특수 문자와 숫자로 암호를 기억할 수 있는 암호("P@55w0rds@reH@rdT0Remember")로 바꿀 수 있다면 더 좋습니다. 사전에서 찾을 수 있는 단어를 사용하지 않는 것이 가장 좋습니다.구 하나를 선택하고 몇 개의 문자를 특수 문자와 숫자로 바꾸는 것이 가장 좋습니다.자세한 내용은 이 Cisco 블로그 게시물을 참조하십시오.



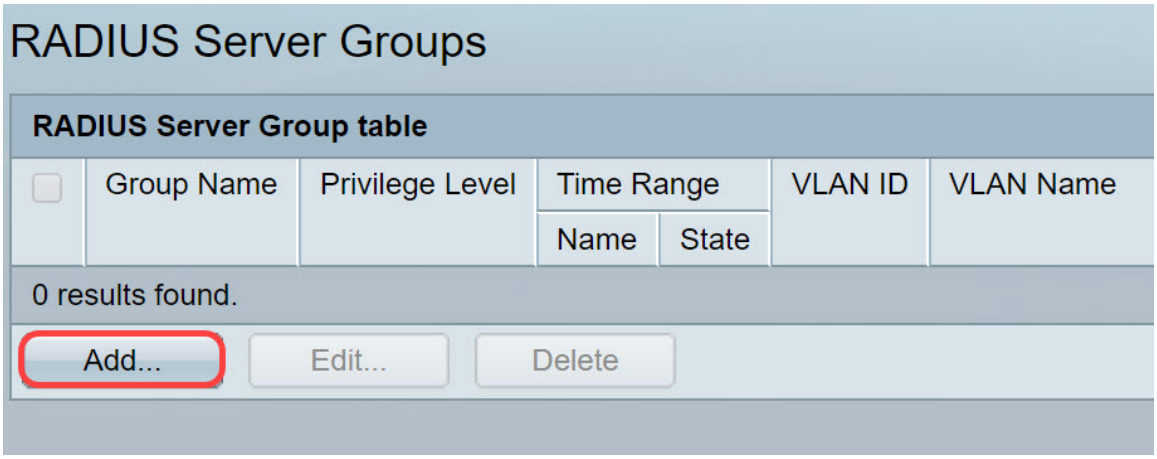
5단계. Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.비밀 키는 이제 MD5로 암호화됩니다. MD5는 데이터 조각을 가져오고 일반적으로 재생산되지 않는 고유한 16진수 출력을 만드는 암호화 해시 함수입니다.MD5는 128비트 해시 값을 사용합니다.

RADIUS 서버 그룹

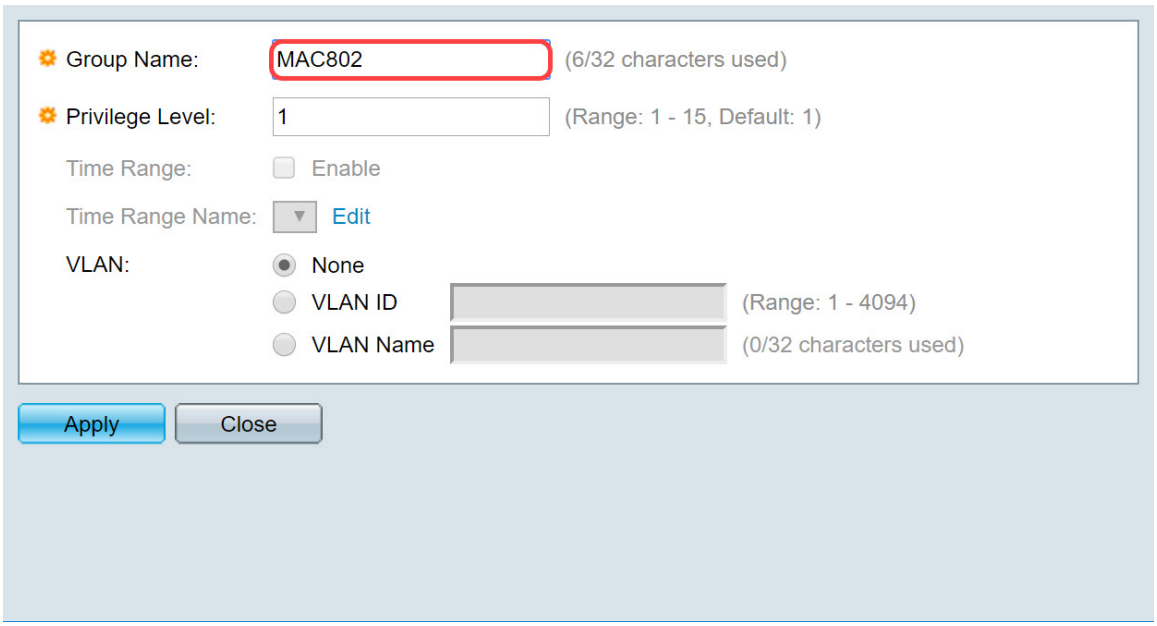
1단계. Security(보안) > **RADIUS Server(RADIUS 서버) > RADIUS Server Groups(RADIUS 서버 그룹)로 이동합니다.**



2단계. 추가**...를 클릭합니다.** 새 RADIUS 서버 그룹을 추가합니다.

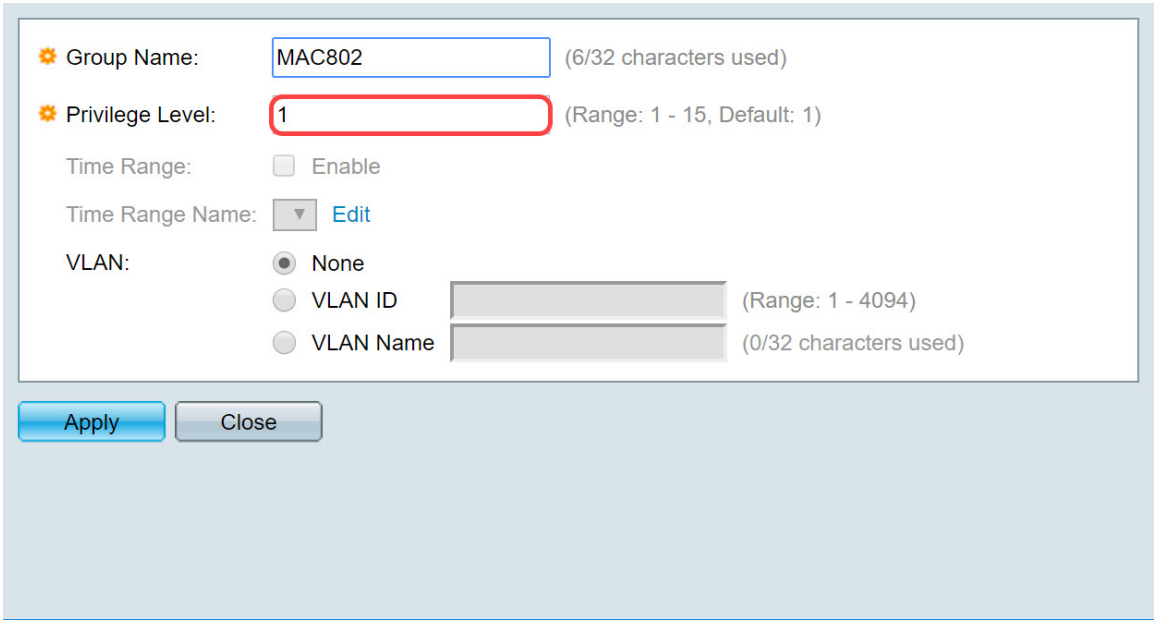


3단계. Add *RADIUS Server Group(RADIUS 서버 그룹 추가)* 페이지가 열립니다.그룹의 이름을 입력합니다.이 예에서는 그룹 이름으로 **MAC802**를 사용합니다.



4단계. 권한 레벨 필드에 그룹의 관리 액세스 권한 레벨을 입력합니다.범위는 1 — 15, 15가 가장 권한이 많고 기본값은 1입니다. 이 예에서는 권한 레벨을 1로 둡니다.

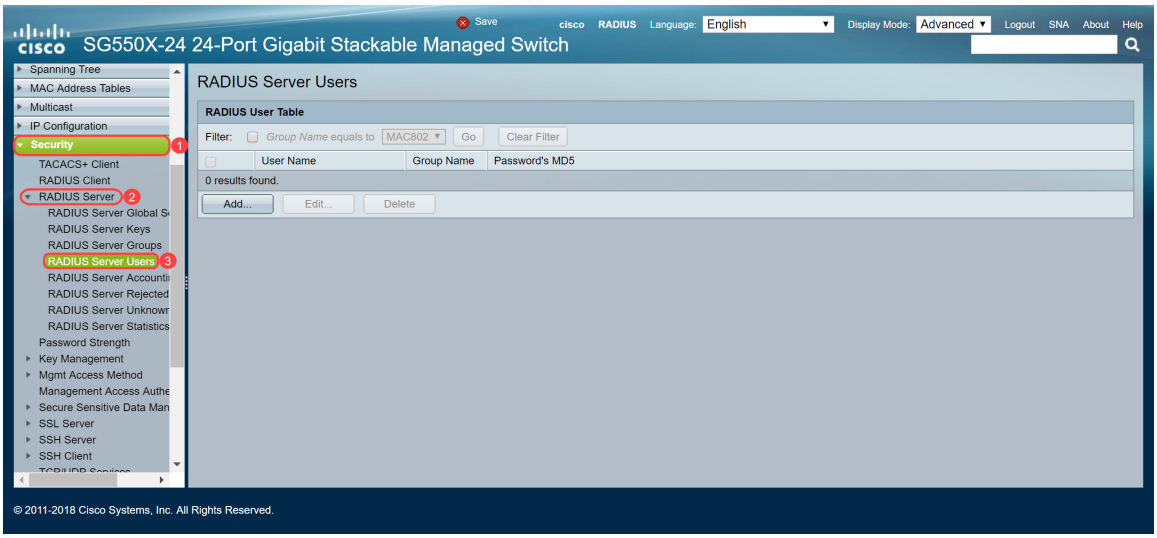
참고:이 기사에서 *시간 범위* 또는 *VLAN*을 구성하지 않습니다.



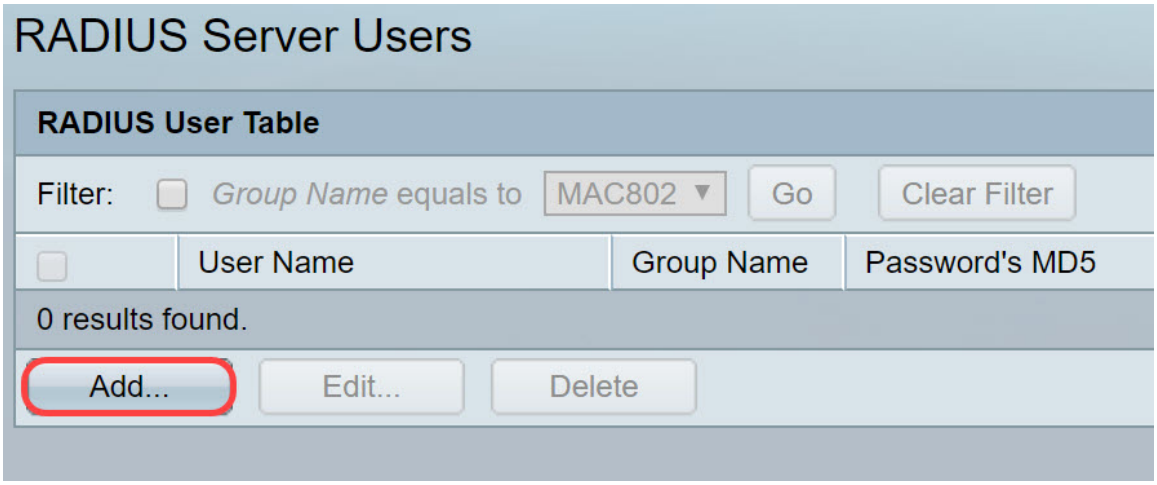
5단계. **적용**을 클릭하여 설정을 저장합니다.

RADIUS 서버 사용자

1단계. Security(**보안**) > **RADIUS Server(RADIUS 서버)** > **RADIUS Server Users(RADIUS 서버 사용자)**로 이동하여 RADIUS에 대한 사용자를 구성합니다.

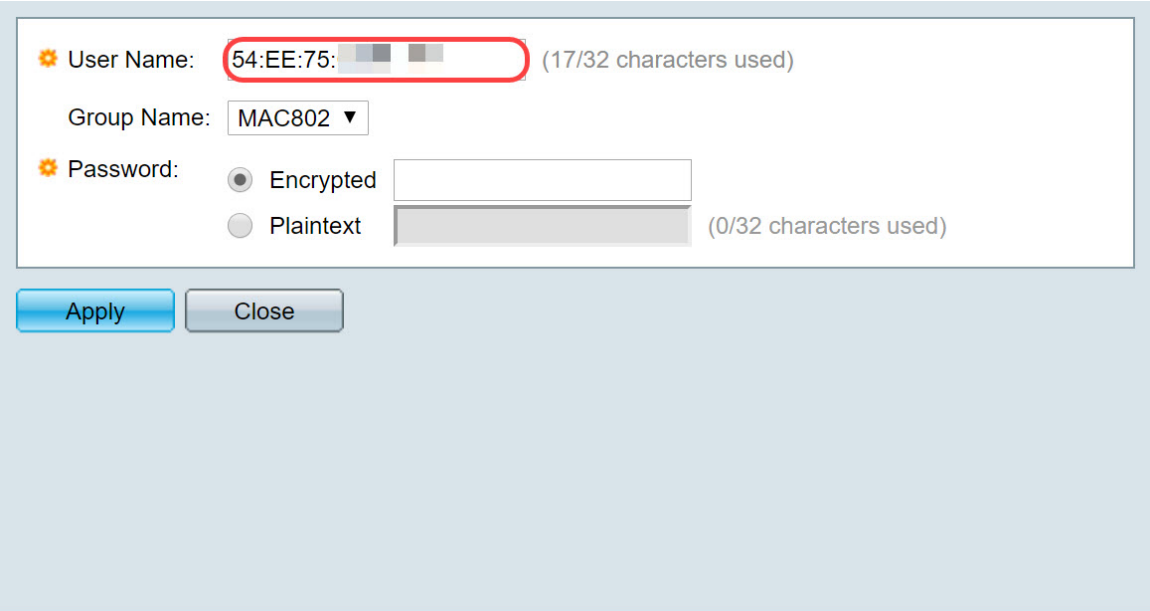


2단계. 추가**...를 클릭합니다.** 새 사용자를 추가합니다.

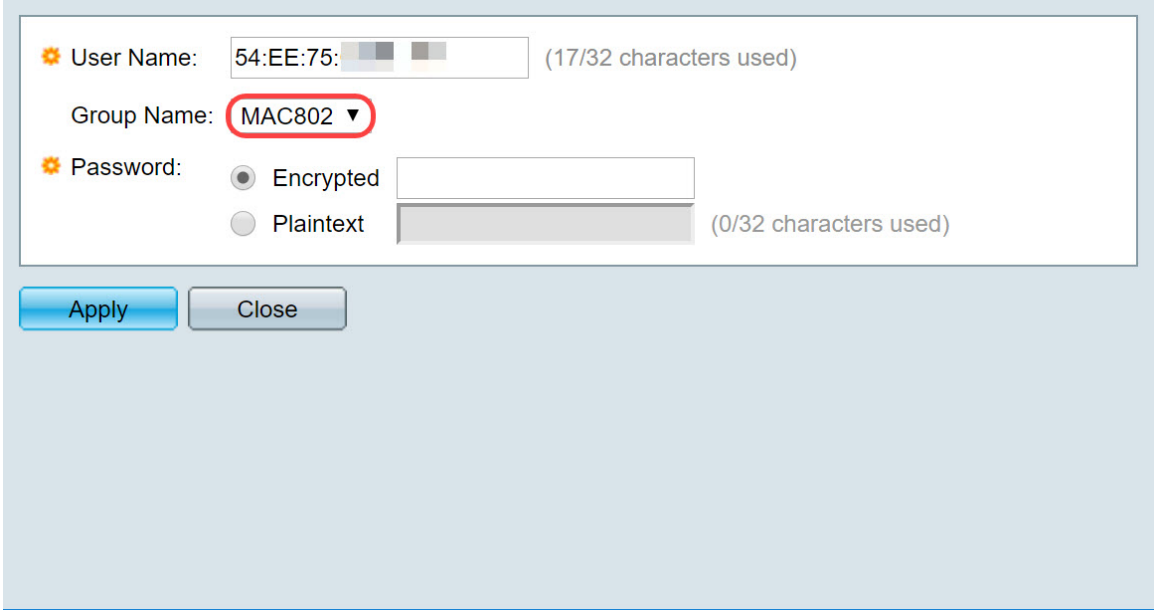


3단계. Add RADIUS *Server User(RADIUS 서버 사용자 추가)* 페이지가 열립니다.User *Name* 필드에 사용자의 MAC 주소를 입력합니다.이 예에서는 컴퓨터에서 이더넷 MAC 주소를 사용합니다.

참고:MAC 주소의 일부가 흐리게 표시되어 있습니다.



4단계. *그룹 이름* 드롭다운 목록에서 그룹을 선택합니다.RADIUS Server Group 섹션의 3단계에서 강조 표시된 대로 **MAC802**를 이 사용자의 그룹 이름으로 선택합니다.

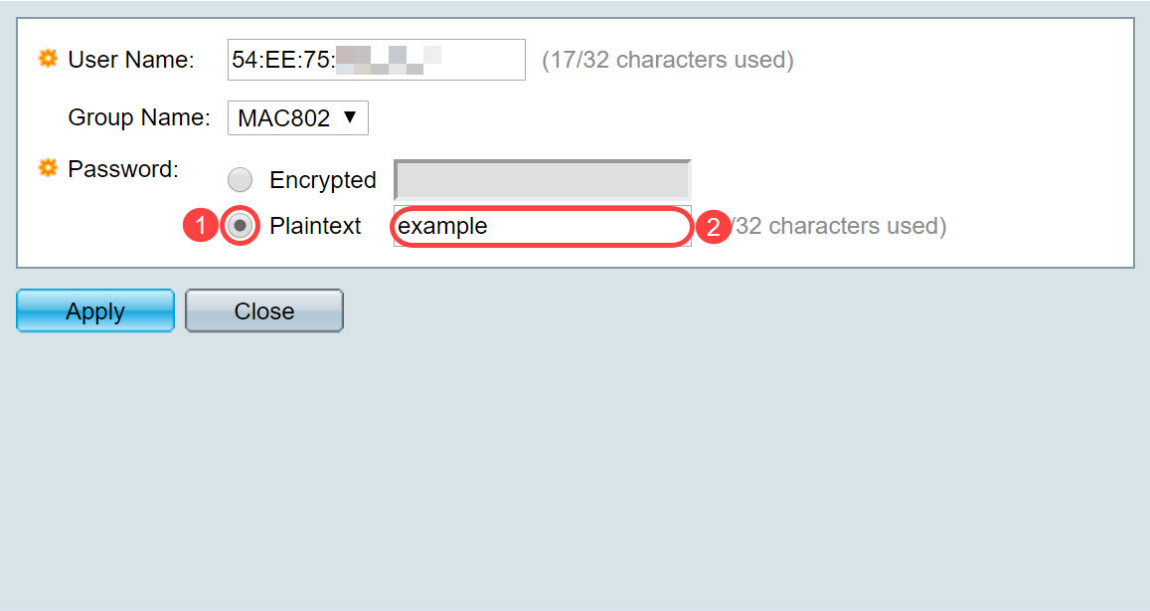


5단계. 다음 라디오 버튼 중 하나를 선택합니다.

- Encrypted — 키는 MD5를 사용하여 통신을 암호화하는 데 사용됩니다. 암호화를 사용하려면 암호화된 형식으로 키를 입력합니다.
- Plaintext — 암호화된 키 문자열(다른 디바이스에서)이 없는 경우 일반 텍스트 모드에서 키 문자열을 입력합니다.암호화된 키 문자열이 생성되고 표시됩니다.

Plaintext를 이 사용자의 비밀번호로 선택하고 **예**를 일반 텍스트 비밀번호로 입력합니다.

참고:example을 일반 텍스트 비밀번호로 사용하지 않는 것이 좋습니다.더 강력한 비밀번호를 사용하는 것이 좋습니다.

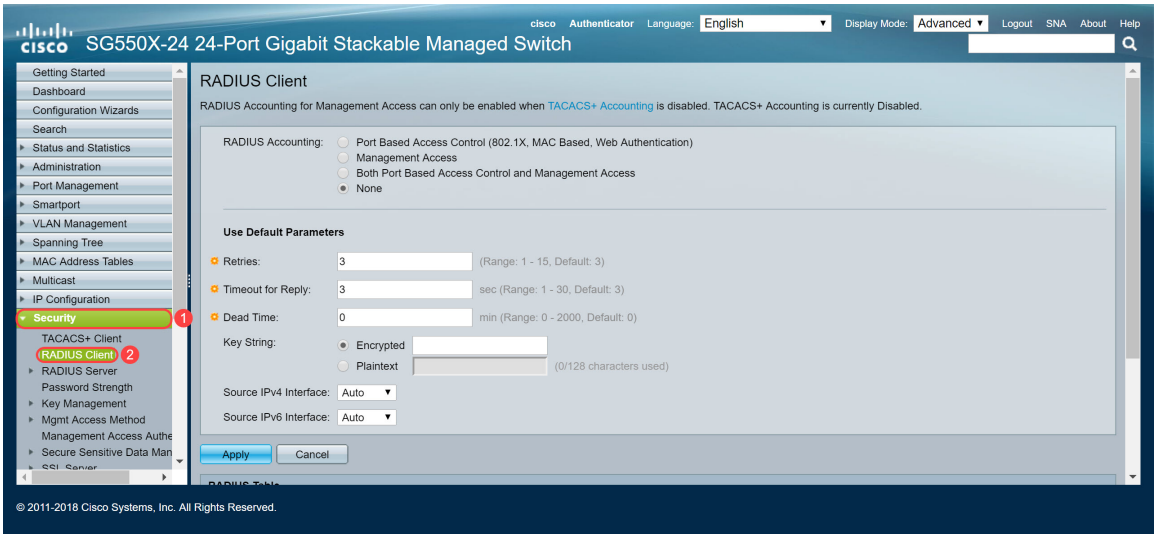


6단계. 구성을 완료한 후 Apply를 클릭합니다.

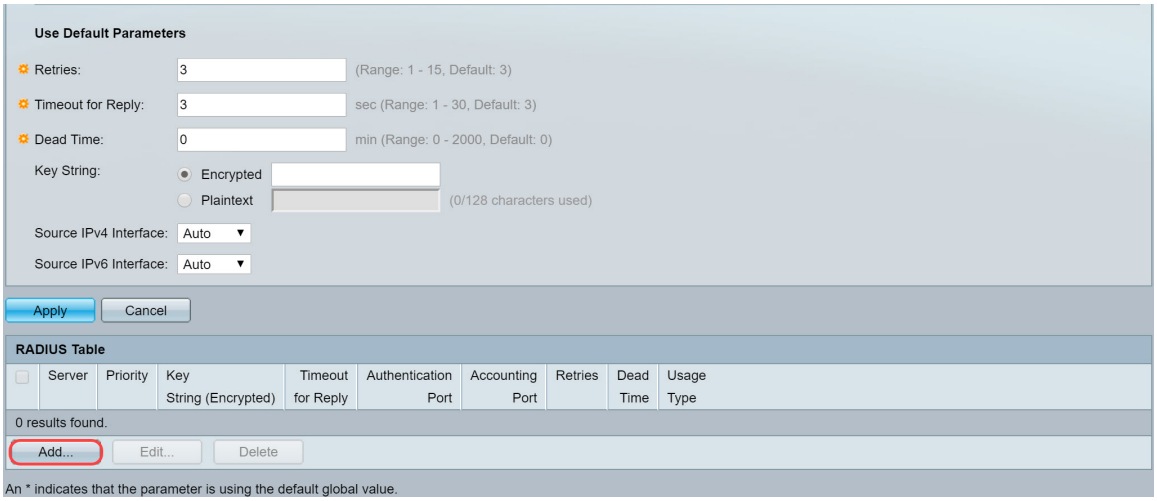
이제 RADIUS 서버 구성을 마쳤습니다.다음 섹션에서는 두 번째 스위치를 인증자로 구성합니다.

RADIUS 클라이언트

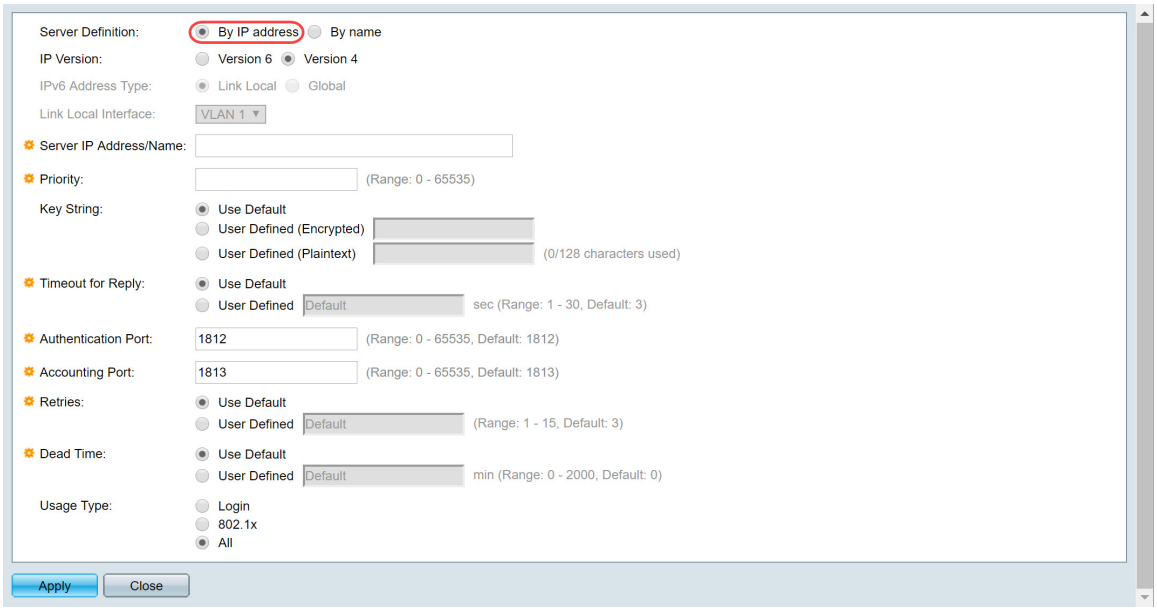
1단계. 인증자로 구성될 스위치의 웹 기반 유틸리티에 로그인하고 **Security(보안) > RADIUS Client(RADIUS 클라이언트)로 이동합니다**.



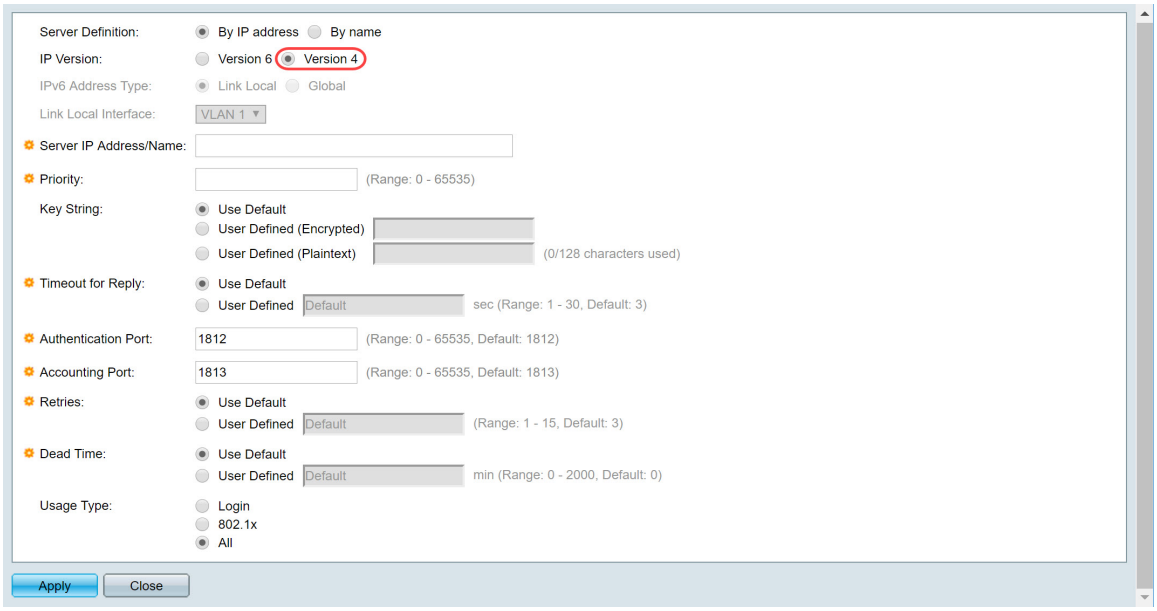
2단계. 아래로 스크롤하여 *RADIUS Table(RADIUS 테이블)* 섹션으로 이동한 다음 Add...(추가...)**를 클릭합니다.** RADIUS 서버를 추가합니다.



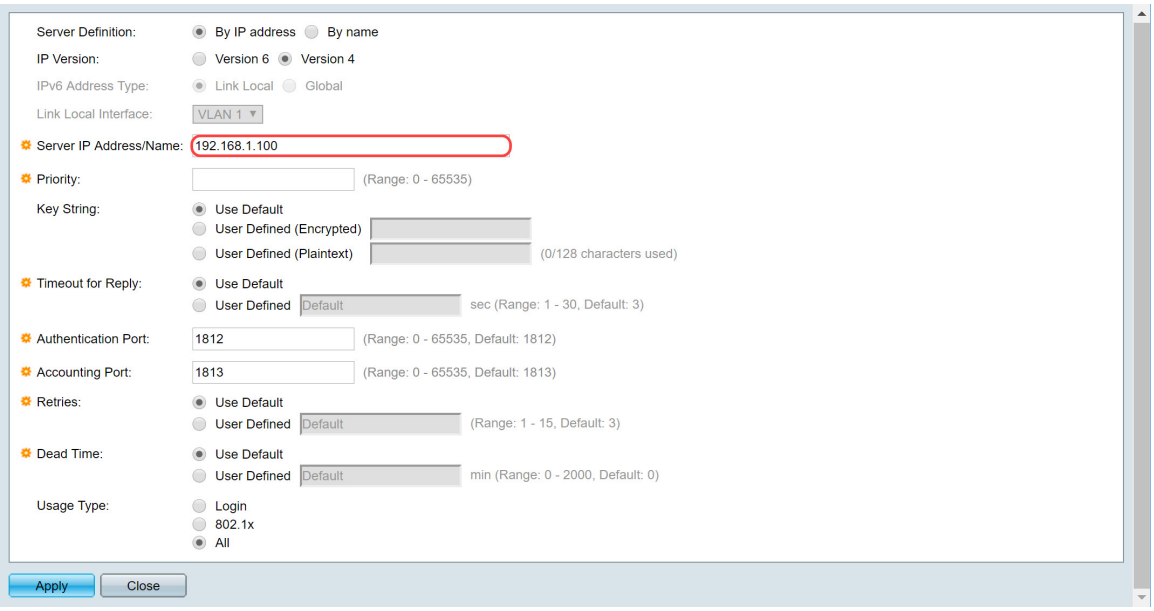
3단계. (선택 사항) Server Definition(서버 정의) 필드에서 IP 주소 또는 이름으로 RADIUS 서버를 지정할지 여부를 *선택합니다*.이 예제에서는 기본 선택 항목인 **IP 주소**를 **그대로 유지합니다**.



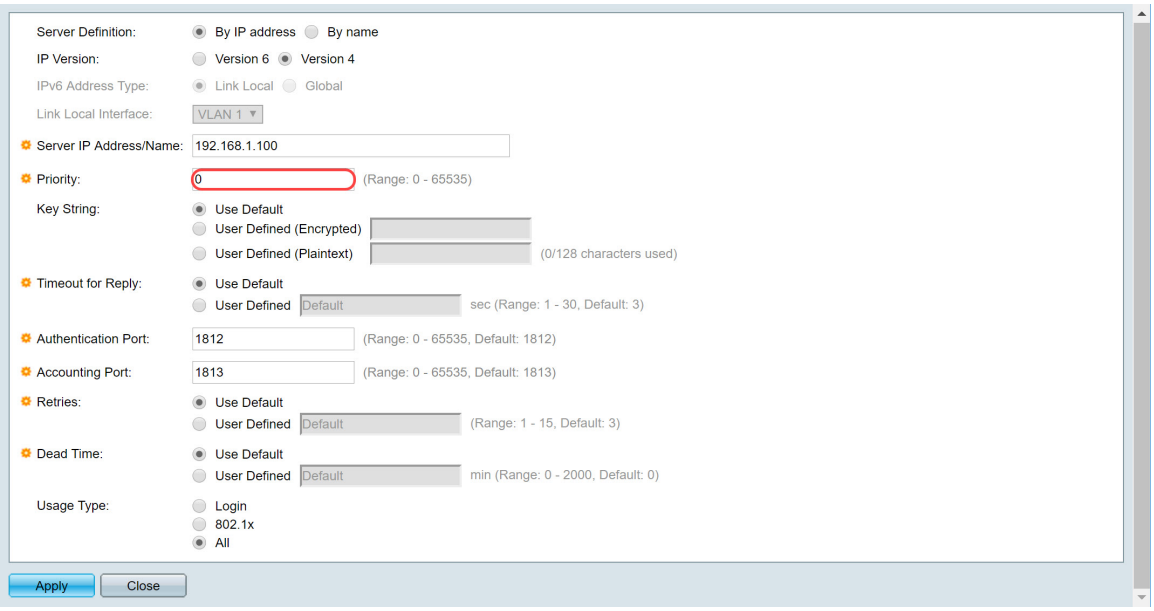
4단계. (선택 사항) *IP Version* 필드에서 RADIUS 서버의 IP 주소 버전을 선택합니다.이 예제에서는 **버전 4**의 기본 선택을 유지합니다.



5단계. IP 주소 또는 이름으로 RADIUS 서버에 입력합니다.Server *IP Address/Name* 필드에 **192.168.1.100**의 IP 주소*를* 입력하겠습니다.

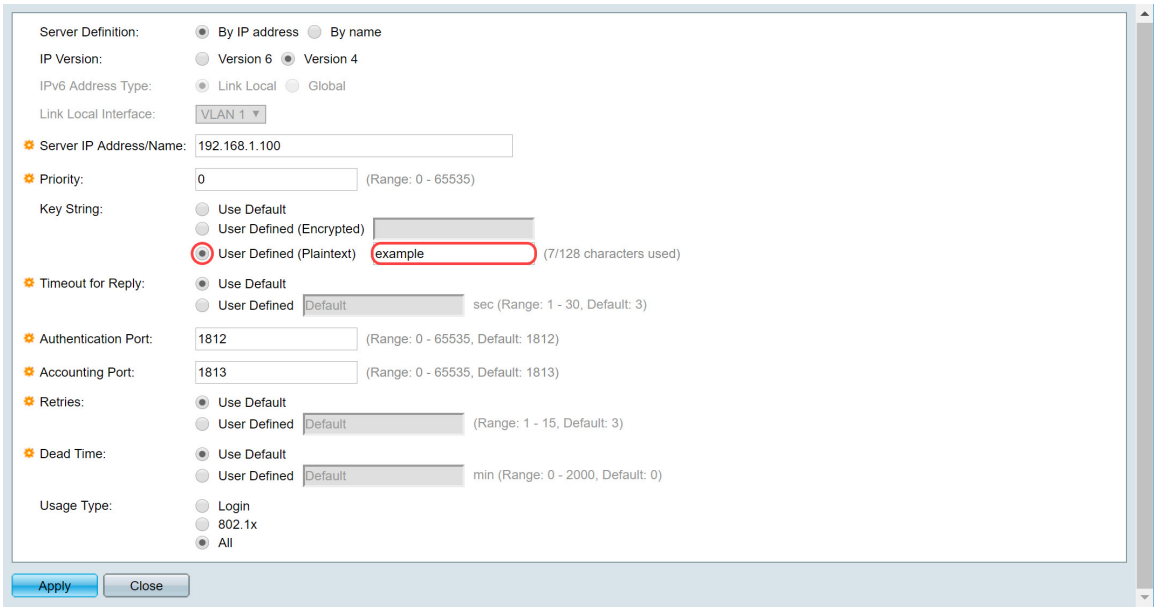


6단계. 서버의 우선순위를 입력합니다.우선순위는 디바이스가 사용자를 인증하기 위해 서버에 연결하려고 시도하는 순서를 결정합니다.디바이스가 우선 순위가 가장 높은 RADIUS 서버로 먼저 시작됩니다.0이 가장 높은 우선 순위입니다.



7단계. 디바이스와 RADIUS 서버 간의 통신을 인증하고 암호화하는 데 사용되는 키 문자열을 입력합니다.이 키는 RADIUS 서버에 구성된 키와 일치해야 합니다.**암호화** 또는 일반 텍스트 형식으로 입력할 수 **있습니다**.Use **Default**(기본값 사용)를 선택하면 디바이스는 기본 키 문자열을 사용하여 RADIUS 서버에 인증하려고 시도합니다.User Defined(Plaintext)**를** 사용하고 주요 **예**를 입력하겠습니다.

참고:나머지 컨피그레이션은 기본값으로 둡니다.원하는 경우 구성할 수 있습니다.

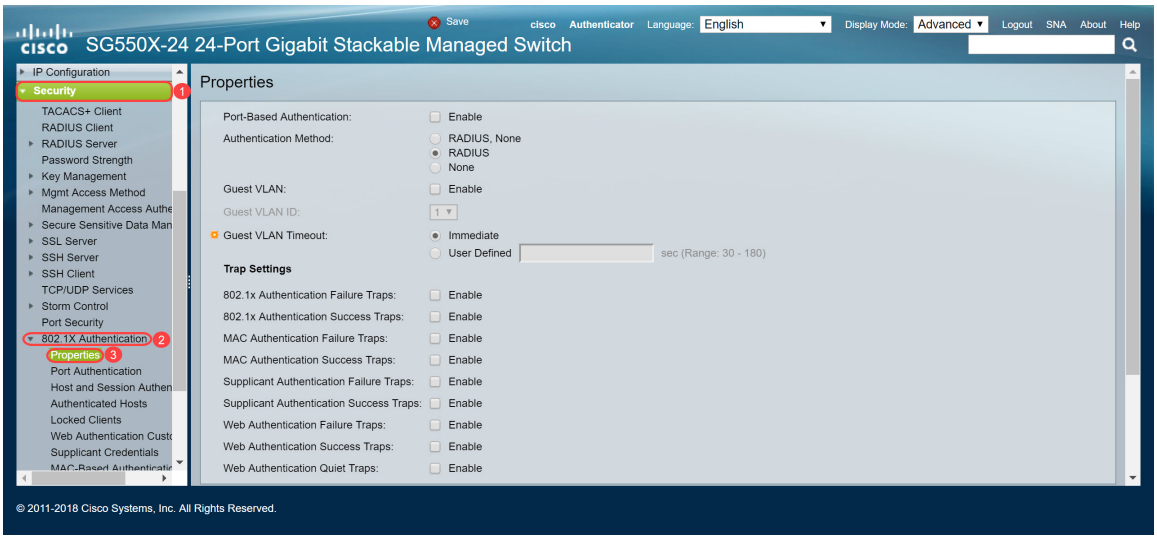


8단계. Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.

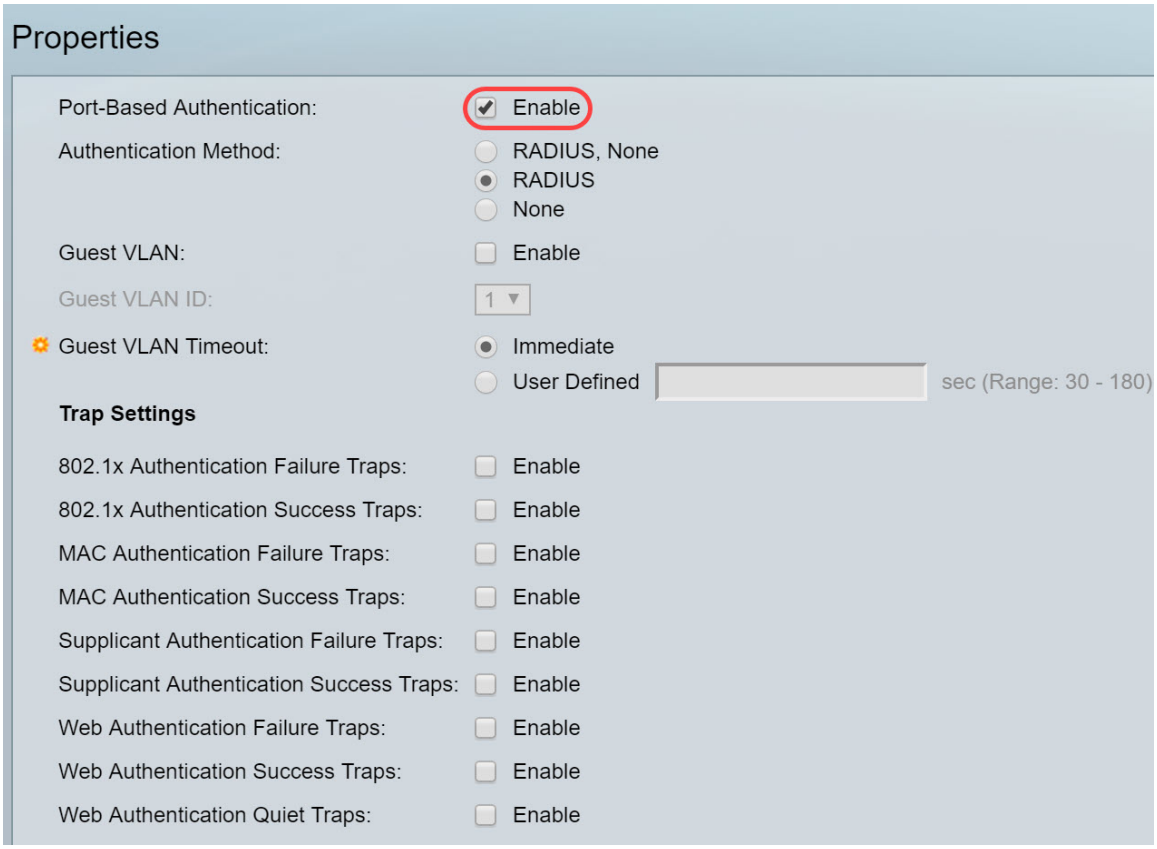
802.1X 인증 속성

속성 페이지는 포트/디바이스 인증을 전역적으로 활성화하는 데 사용됩니다.인증이 작동하려면 전역적으로 그리고 각 포트에서 개별적으로 활성화되어야 합니다.

1단계. Security(**보안**) > **802.1X Authentication(802.1X 인증) > Properties(속성)로 이동합니다**.

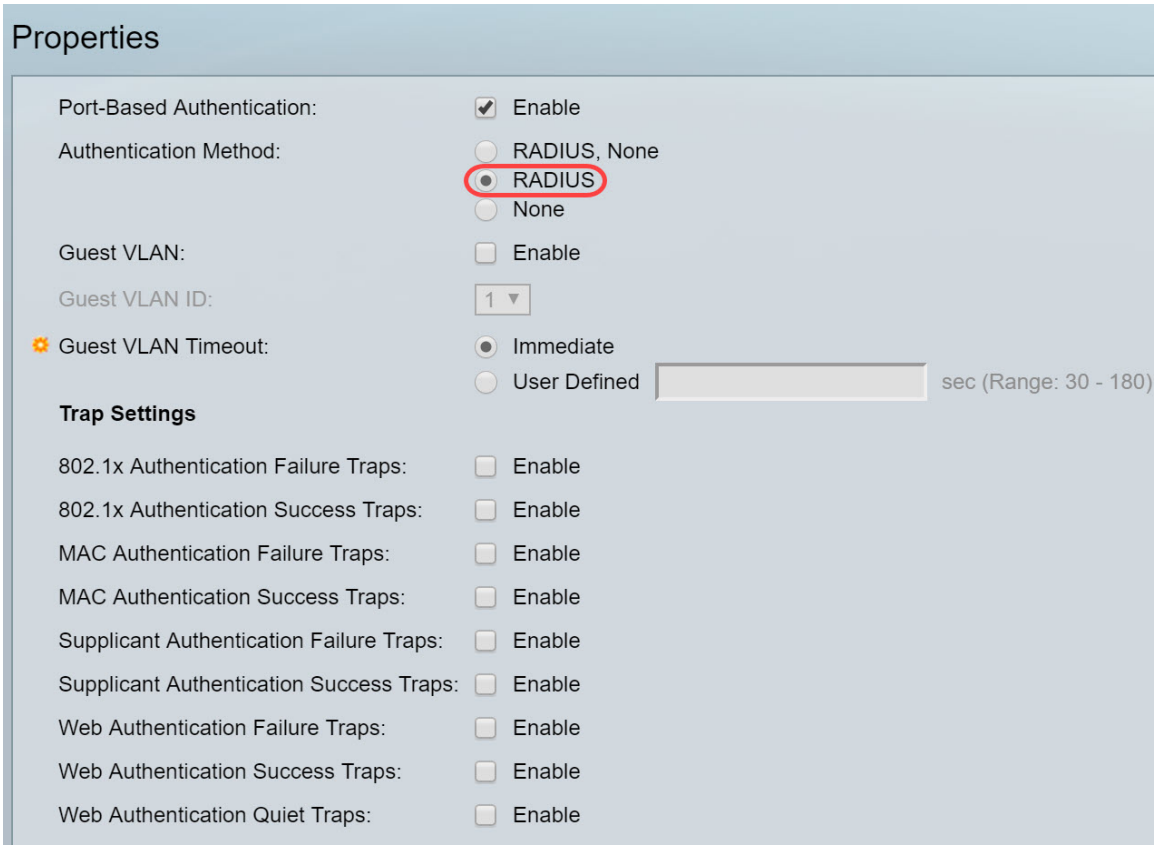


2단계. 포트 기반 인증을 활성화하려면 Enable 확인란을 선택합니다.

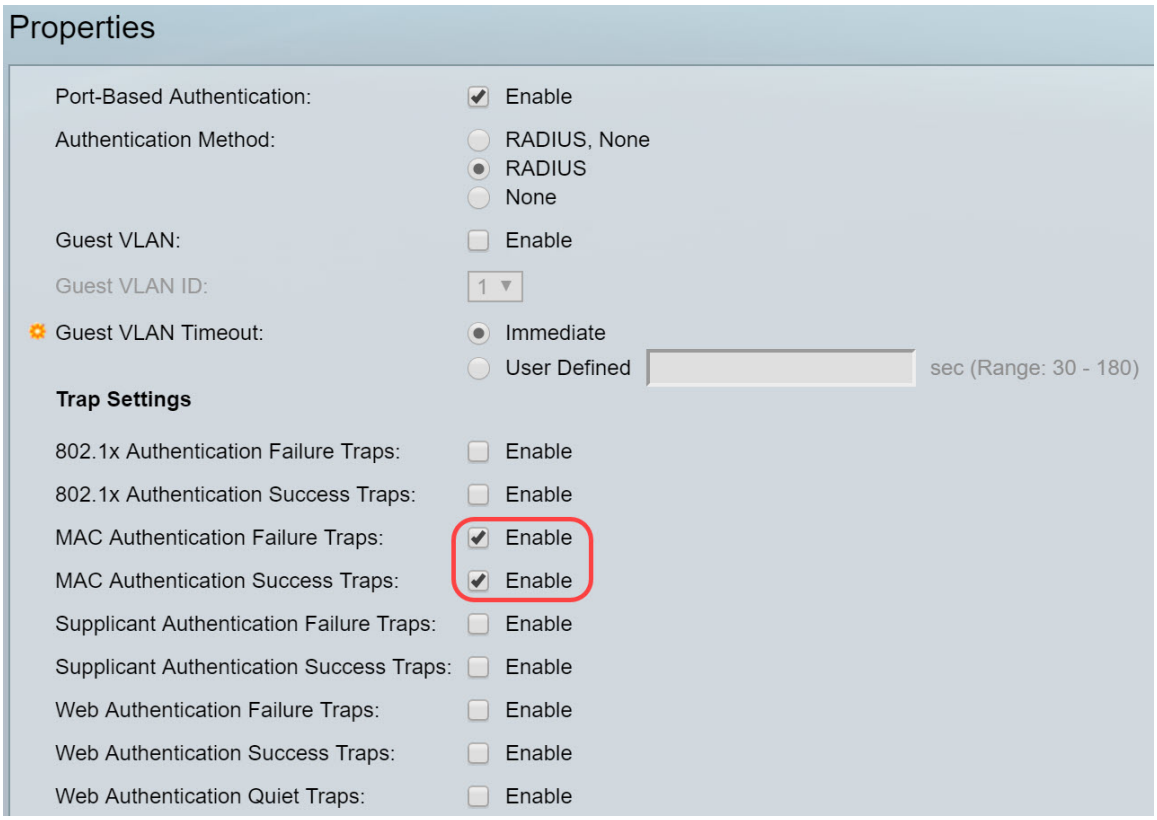


3단계. 사용자 인증 방법을 선택합니다.인증 방법으로 RADIUS를 선택하겠습니다.다음 옵션은 다음과 같습니다.

- RADIUS, None — RADIUS 서버를 사용하여 먼저 포트 인증을 수행합니다.RADIUS에서 응답이 수신되지 않으면(예: 서버가 다운된 경우) 인증이 수행되지 않으며 세션이 허용됩니다.서버를 사용할 수 있지만 사용자 자격 증명이 올바르지 않으면 액세스가 거부되고 세션이 종료됩니다.
- RADIUS — RADIUS 서버에서 사용자를 인증합니다.인증이 수행되지 않으면 세션이 허용되지 않습니다.
- 없음 — 사용자를 인증하지 않습니다.세션을 허용합니다.



4단계. (선택 사항) *MAC 인증 실패 트랩* 및 *MAC 인증 성공 트랩*에 대한 **Enable**(활성화) 확인란을 *선택합니다*.MAC 인증이 실패하거나 성공할 경우 트랩이 생성됩니다.이 예에서는 MAC *Authentication Failure Traps* 및 *MAC Authentication Success Traps*를 모두 *활성화합니다*.

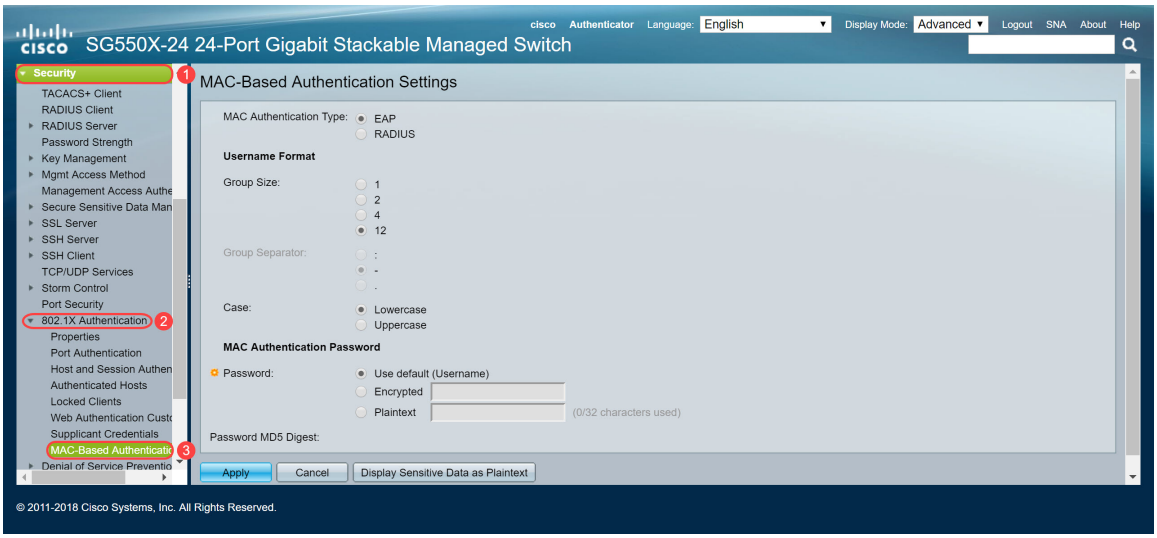


5단계. 적용을 **누릅니다**.

802.1X 인증 MAC 기반 인증 설정

이 페이지에서는 MAC 기반 인증에 적용할 수 있는 다양한 설정을 구성할 수 있습니다.

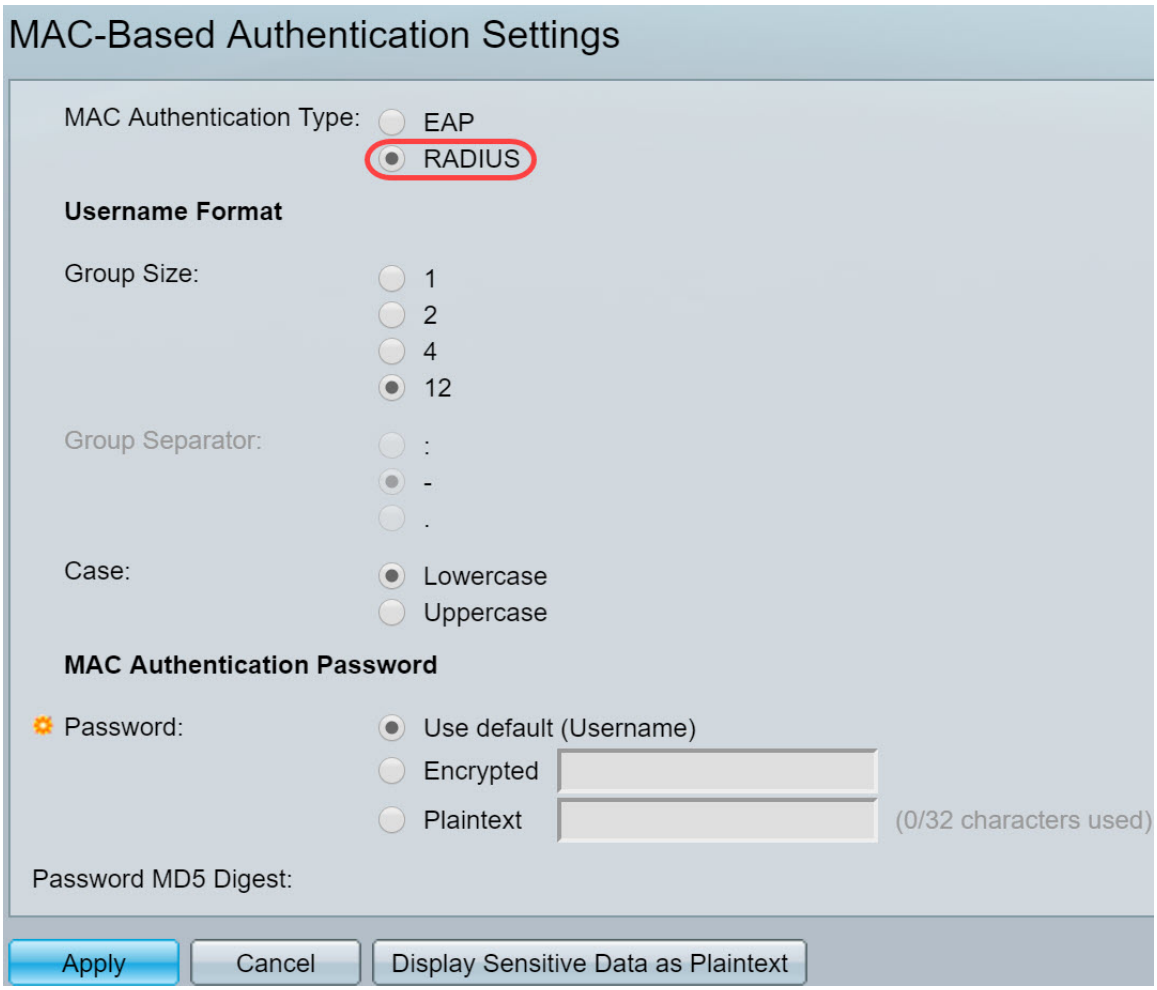
1단계. Security(**보안**) > **802.1X Authentication(802.1X 인증)** > **MAC-Based Authentication Settings(MAC 기반 인증 설정)**로 이동합니다.



2단계. *MAC Authentication Type(MAC 인증 유형)*에서 다음 중 하나를 선택합니다.

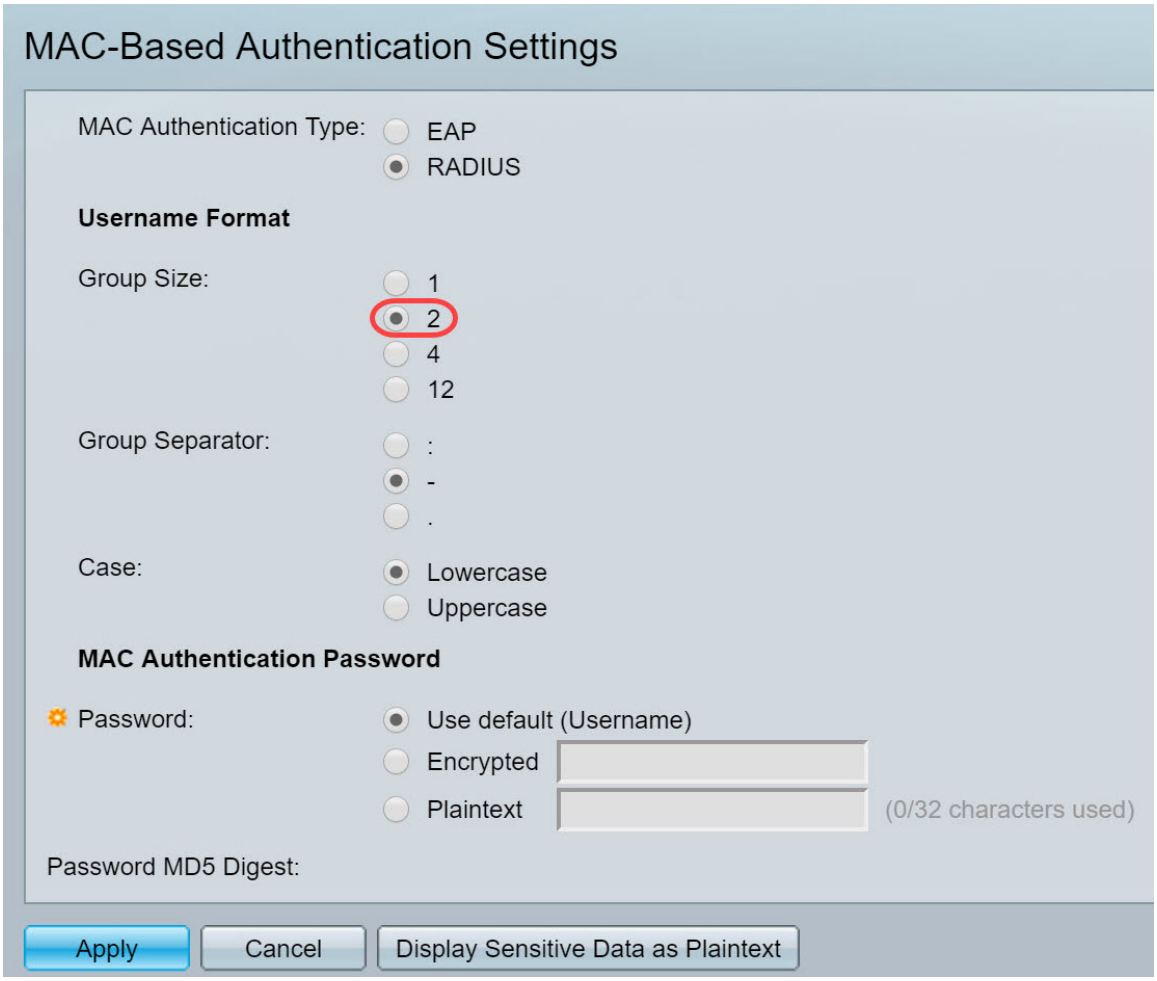
- EAP — MAC 기반 신청자를 인증하는 스위치(RADIUS 클라이언트)와 RADIUS 서버 간의 트래픽에 대해 EAP 캡슐화와 함께 RADIUS를 사용합니다.
- RADIUS — MAC 기반 신청자를 인증하는 스위치(RADIUS 클라이언트)와 RADIUS 서버 간의 트래픽에 대해 EAP 캡슐화 없이 RADIUS를 사용합니다.

이 예에서는 MAC 인증 유형으로 RADIUS를 선택합니다.

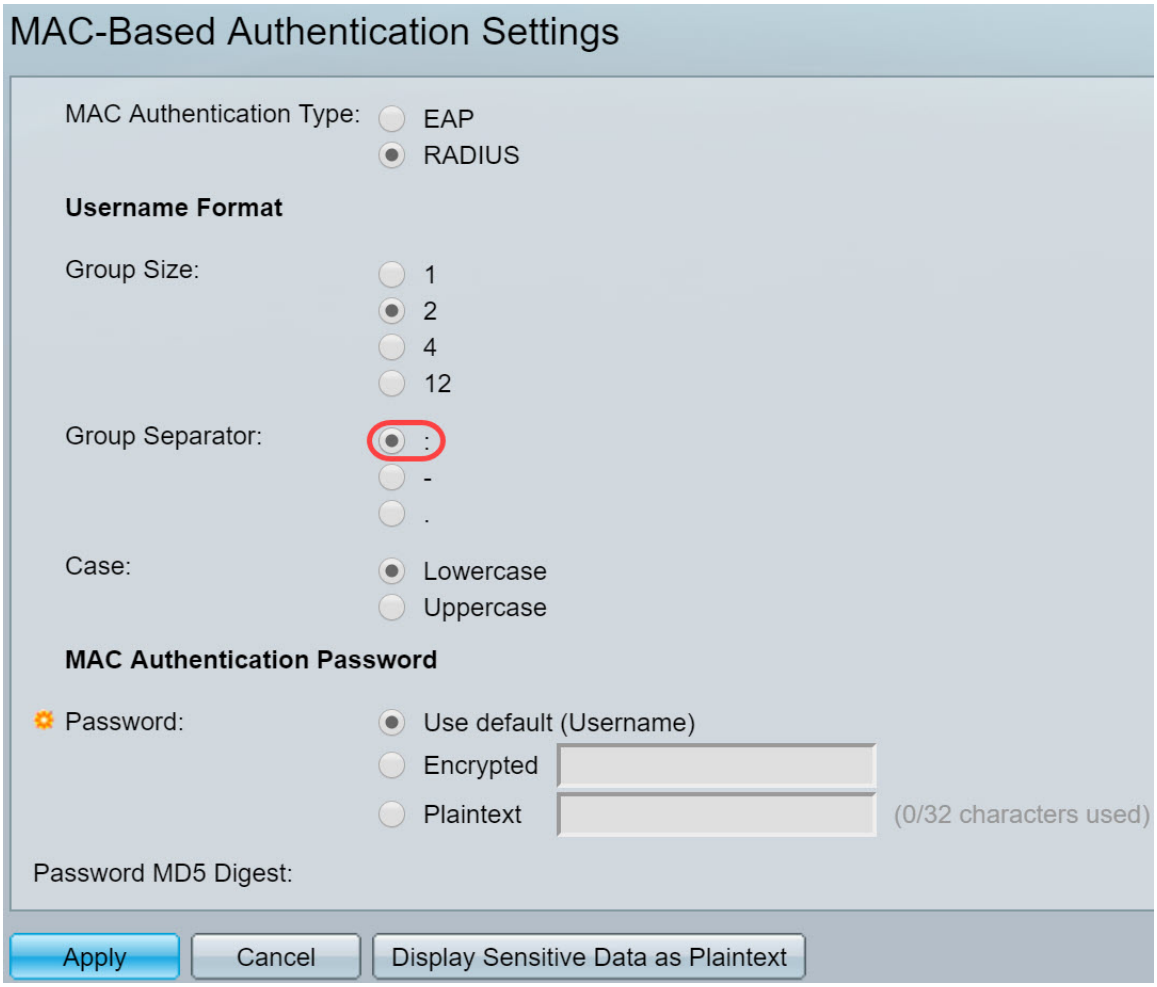


3단계. *사용자 이름 형식*에서 사용자 이름으로 전송된 MAC 주소의 구분 기호 사이에 ASCII 문자 수를 선택합니다.이 경우 그룹 크기로 2를 선택합니다.

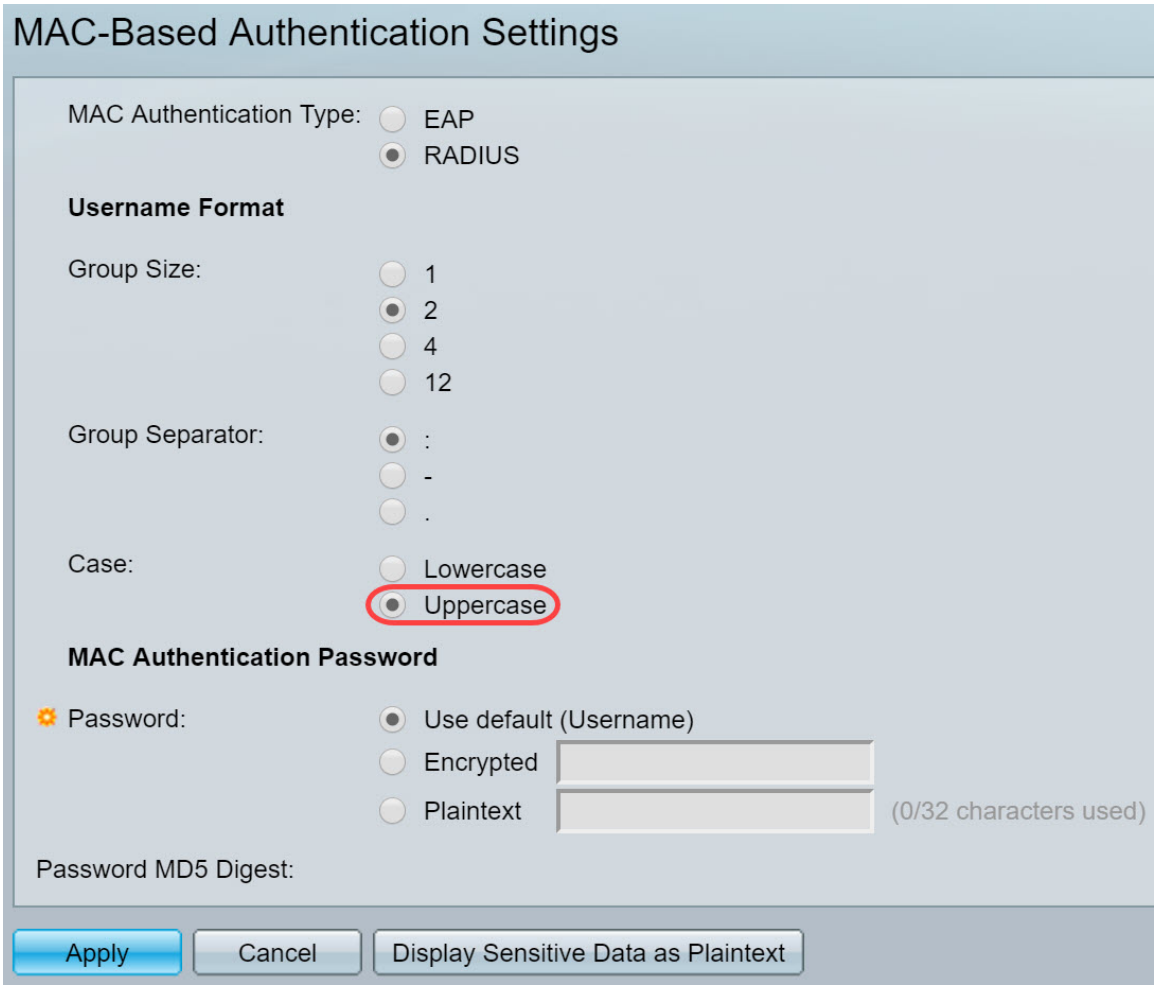
참고:사용자 이름 형식이 Radius *Server Users* 섹션에서 MAC 주소를 입력하는 방법과 동일한지 확인합니다.



4단계. MAC 주소의 정의된 문자 그룹 사이에 구분 기호로 사용되는 문자를 선택합니다.이 예에서는 다음을 선택합니다.그룹 구분 기호로 사용됩니다.

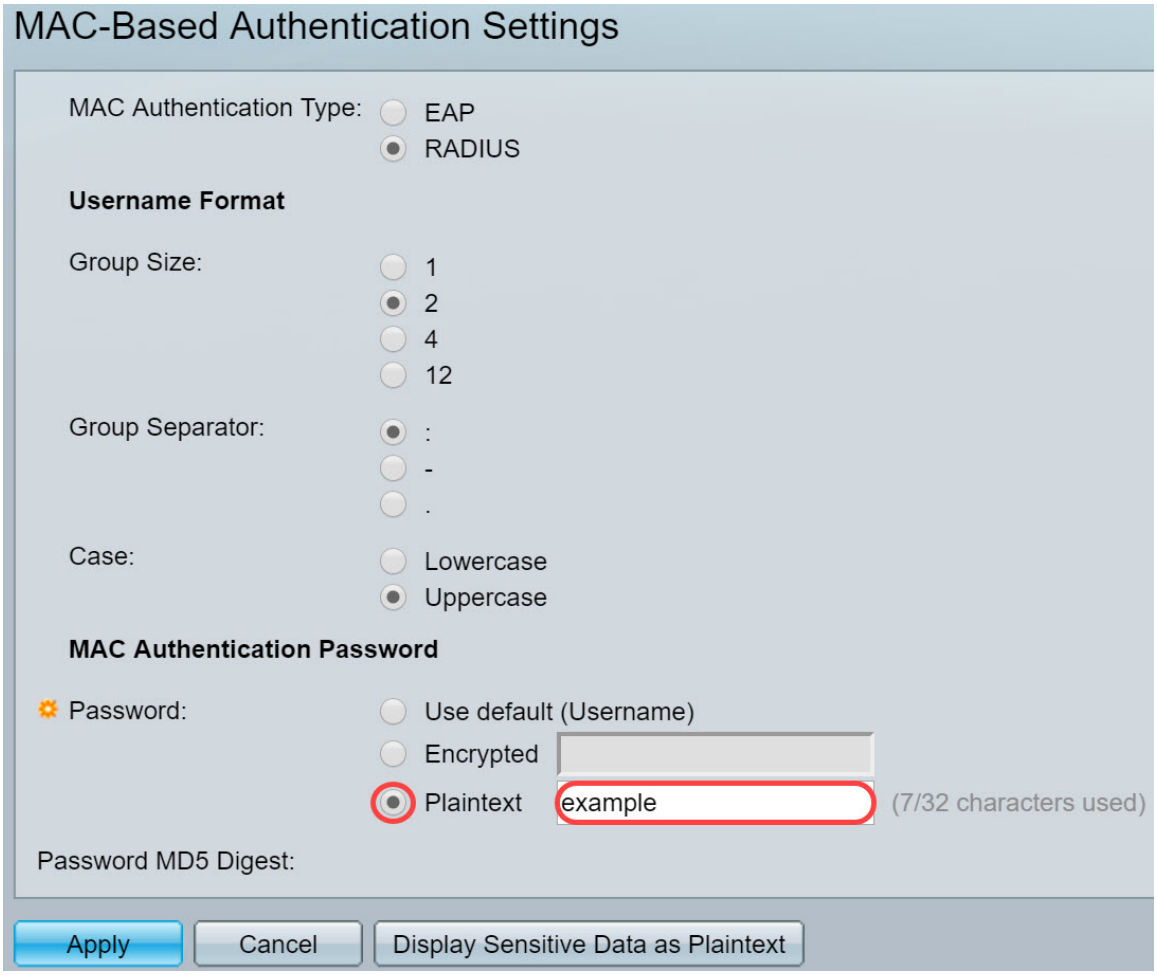


5단계. *Case* 필드에서 **Lowercase** 또는 **Uppercase**를 선택하여 사용자 이름을 소문자 또는 대문자로 보냅니다.



6단계. 비밀번호는 스위치가 RADIUS 서버를 통한 인증에 사용하는 방법을 정의합니다.다음 옵션 중 하나를 선택합니다.

- 기본값 사용(사용자 이름) — 정의된 사용자 이름을 비밀번호로 사용하려면 선택합니다.
- Encrypted — 암호화된 형식으로 비밀번호를 정의합니다.
- 일반 텍스트 — 일반 텍스트 형식으로 비밀번호를 정의합니다.



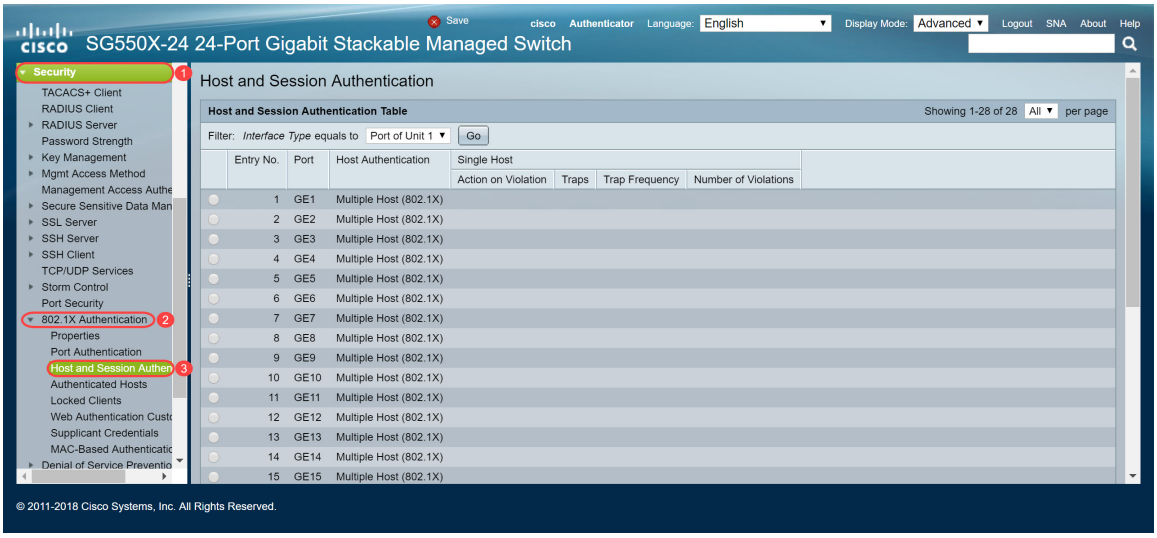
참고:*MD5(Password Message-Digest Algorithm 5) Digest(비밀번호 메시지 다이제스트 알고리즘 5) Digest(다이제스트)*에 MD5 다이제스트 비밀번호가 표시됩니다.MD5는 데이터 일부를 가져와 일반적으로 재생산되지 않는 고유한 16진수 출력을 만드는 암호화 해시 함수입니다.MD5는 128비트 해시 값을 사용합니다.

7단계. Apply(**적용**)를 클릭하면 설정이 Running Configuration(실행 중인 컨피그레이션) 파일에 저장됩니다.

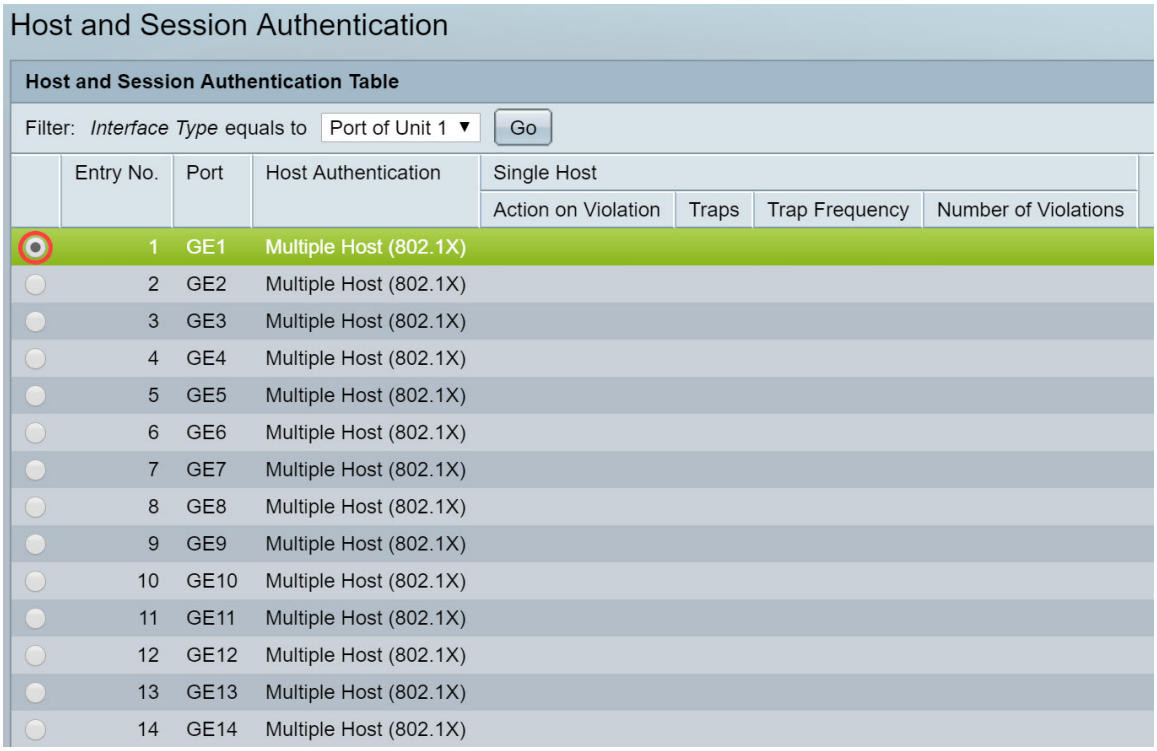
802.1X 인증 호스트 및 세션 인증

Host *and Session Authentication(호스트 및 세션 인증)* 페이지에서는 802.1X가 포트에서 작동하는 모드를 정의하고 위반이 탐지된 경우 수행할 작업을 정의할 수 있습니다.

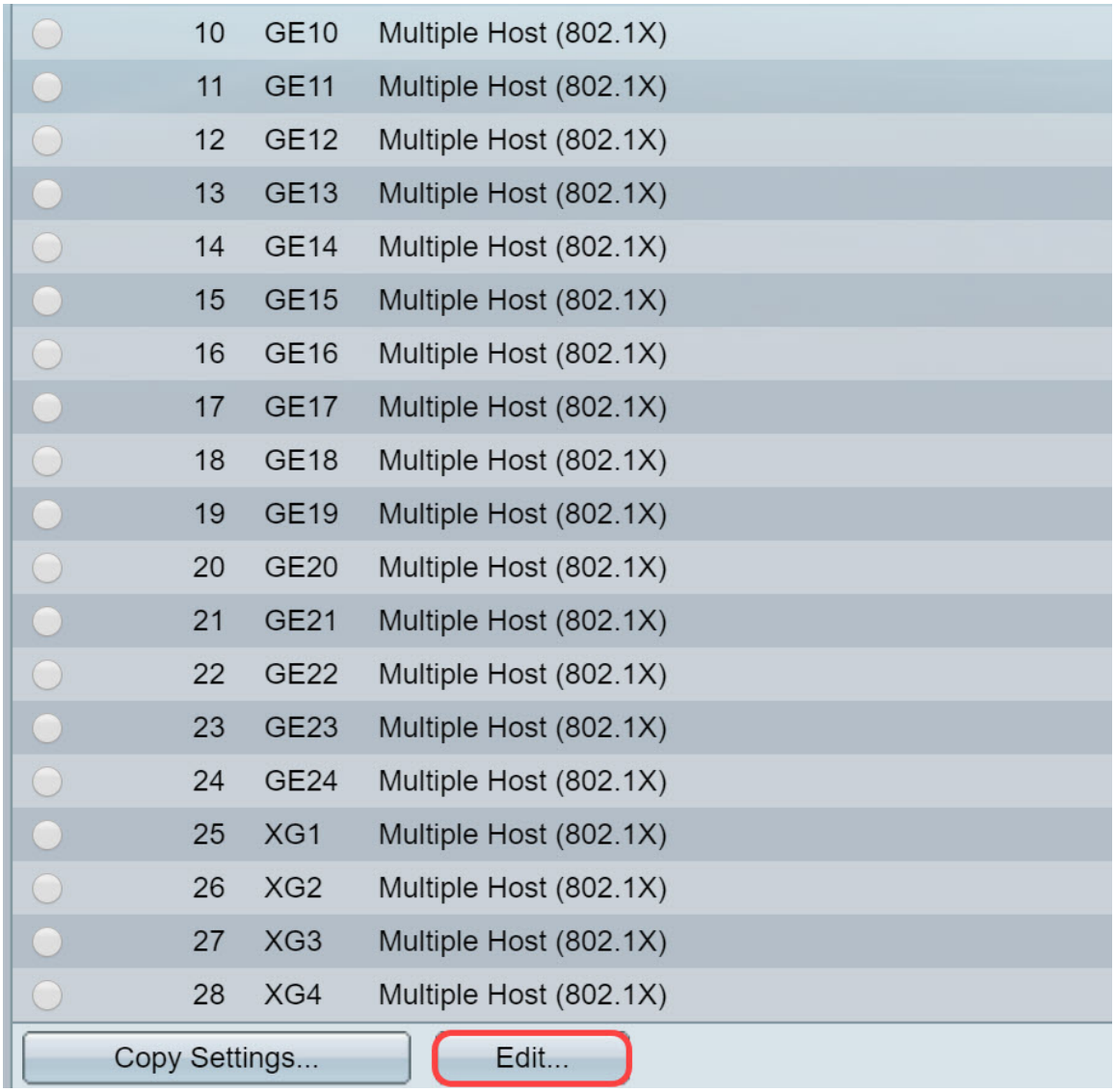
1단계. Security(**보안**) > **802.1X Authentication(802.1X 인증)** > **Host and Session Authentication(호스트 및 세션 인증)으로 이동합니다**.



2단계. 호스트 인증을 구성할 포트를 선택합니다.이 예에서는 GE1이 최종 호스트에 연결되어 있으므로 구성합니다.



3단계. **편집...을 클릭합니다.** 포트를 구성합니다.

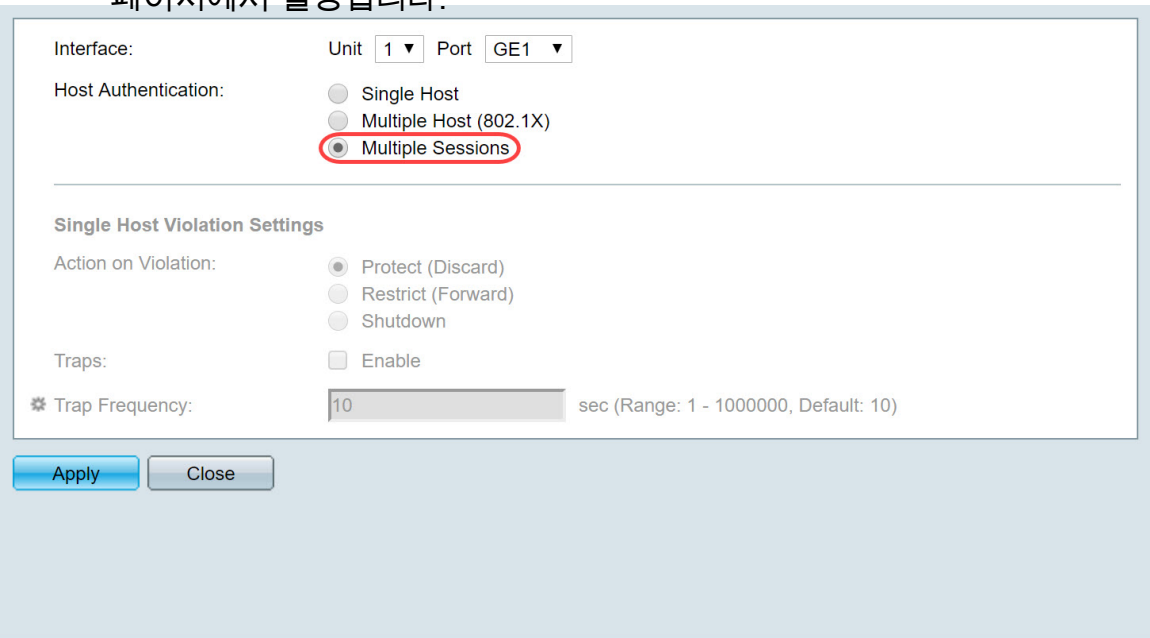


4단계. Host *Authentication*(호스트 인증) 필드에서 다음 옵션 중 하나를 선택합니다.

1. 단일 호스트 모드
   - 인증된 클라이언트가 있는 경우 포트가 인증됩니다.한 포트에서 하나의 호스트만 인증할 수 있습니다.
   - 포트가 승인되지 않고 게스트 VLAN이 활성화되면 태그 없는 트래픽은 게스트 VLAN에 다시 매핑됩니다.태그가 지정된 트래픽은 게스트 VLAN 또는 인증되지 않은 VLAN에 속하지 않는 한 삭제됩니다.게스트 VLAN이 포트에서 활성화되지 않은 경우 인증되지 않은 VLAN에 속한 태그 처리된 트래픽만 브리징됩니다.
   - 포트가 인증되면, 인증된 호스트의 태그 없는 트래픽 및 태그가 지정된 트래픽은 고정 VLAN 멤버십 포트 컨피그레이션을 기반으로 브리지됩니다.다른 호스트의 트래픽이 삭제됩니다.
   - 사용자는 인증 프로세스 중에 RADIUS 서버에서 할당한 VLAN에 인증된 호스트의 태그 없는 트래픽을 다시 매핑하도록 지정할 수 있습니다.태그가 지정된 트래픽은 RADIUS 할당 VLAN 또는 인증되지 않은 VLAN에 속하지 않는 한 삭제됩니다.포트의 RADIUS VLAN 할당은 *Port Authentication* Page*에서* 설정됩니다.
2. 다중 호스트 모드
   - 하나 이상의 인증된 클라이언트가 있는 경우 포트가 인증됩니다.
   - 포트가 승인되지 않고 게스트 VLAN이 활성화되면 태그 없는 트래픽은 게스트 VLAN에 다시 매핑됩니다.태그가 지정된 트래픽은 게스트 VLAN 또는 인증되지 않은 VLAN에 속하지 않는 한 삭제됩니다.게스트 VLAN이 포트에서 활성화되지 않은 경우 인증되지 않은 VLAN에 속한 태그 처리된 트래픽만 브리징됩니다.
   - 포트가 인증되면 고정 VLAN 멤버십 포트 컨피그레이션을 기반으로, 포트에 연결된 모든 호

스트의 태그 없는 트래픽 및 태그가 지정된 트래픽이 브리지됩니다.
- 인증 프로세스 중에 RADIUS 서버에서 할당한 VLAN에 태그가 지정되지 않은 트래픽이 리디렉션되도록 지정할 수 있습니다.태그가 지정된 트래픽은 RADIUS 할당 VLAN 또는 인증되지 않은 VLAN에 속하지 않는 한 삭제됩니다.포트의 RADIUS VLAN 할당은 Port *Authentication* 페이지에서 설정됩니다.

3. 다중 세션 모드
   - 단일 호스트 및 다중 호스트 모드와 달리 다중 세션 모드의 포트에는 인증 상태가 없습니다.이 상태는 포트에 연결된 각 클라이언트에 할당됩니다.
   - 인증되지 않은 VLAN에 속하는 태그 처리된 트래픽은 호스트의 권한 부여 여부에 관계없이 항상 브리징됩니다.
   - 인증되지 않은 VLAN에 속하지 않은 호스트의 태그 지정 및 태그가 지정되지 않은 트래픽은 VLAN에서 정의 및 활성화된 경우 게스트 VLAN에 다시 매핑되거나, 게스트 VLAN이 포트에서 활성화되지 않은 경우 삭제됩니다.
   - 인증 프로세스 중에 RADIUS 서버에서 할당한 VLAN에 태그가 지정되지 않은 트래픽이 리디렉션되도록 지정할 수 있습니다.태그가 지정된 트래픽은 RADIUS 할당 VLAN 또는 인증되지 않은 VLAN에 속하지 않는 한 삭제됩니다.포트의 RADIUS VLAN 할당은 *Port Authentication* 페이지에서 설정됩니다.



5단계. Apply(**적용**)를 클릭하여 컨피그레이션을 저장합니다.

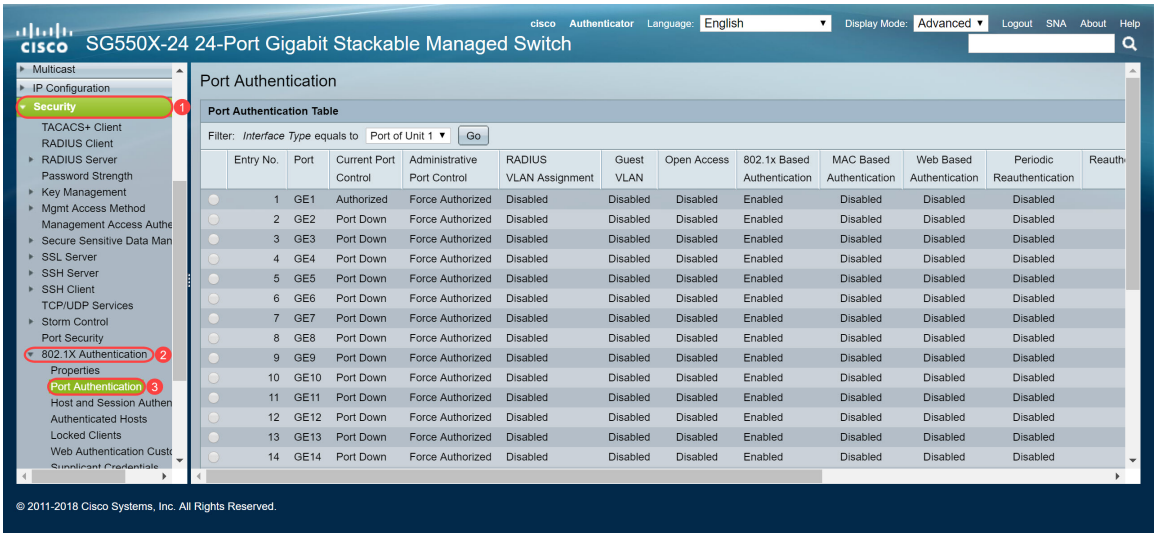
참고:설정 *복사 사용...* 동일한 GE1 구성을 여러 포트에 적용합니다.RADIUS 서버에 연결된 포트를 *다중 호스트(802.1X)로 둡니다*.

802.1X 인증 포트 인증

Port *Authentication(포트 인증)* 페이지에서는 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.

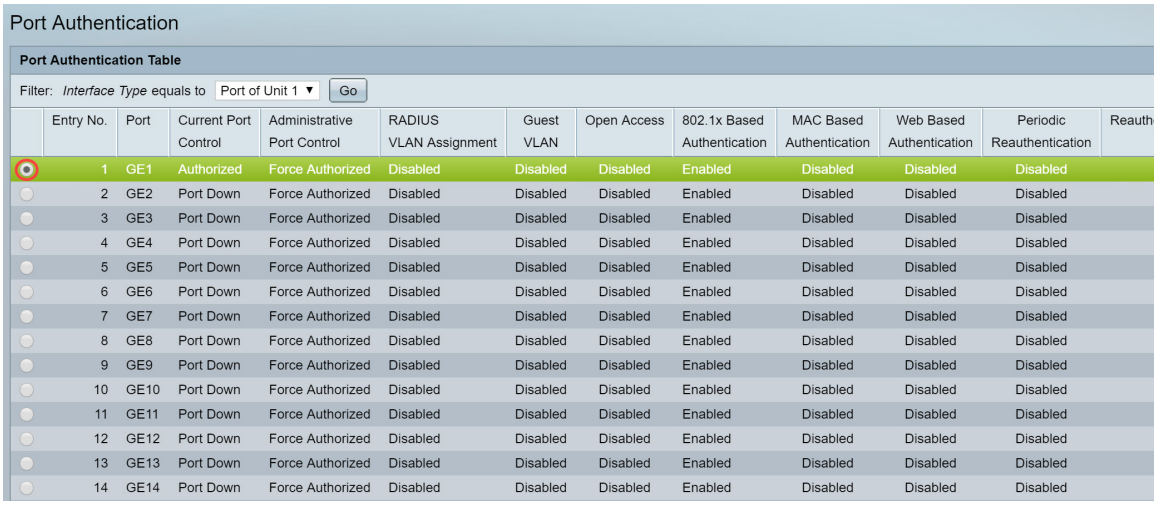
참고:MAC 기반 인증에 필요한 설정만 구성합니다.나머지 컨피그레이션은 기본값으로 유지됩니다.

1단계. **Security > 802.1X Authentication > Port Authentication으로 이동합니다**.

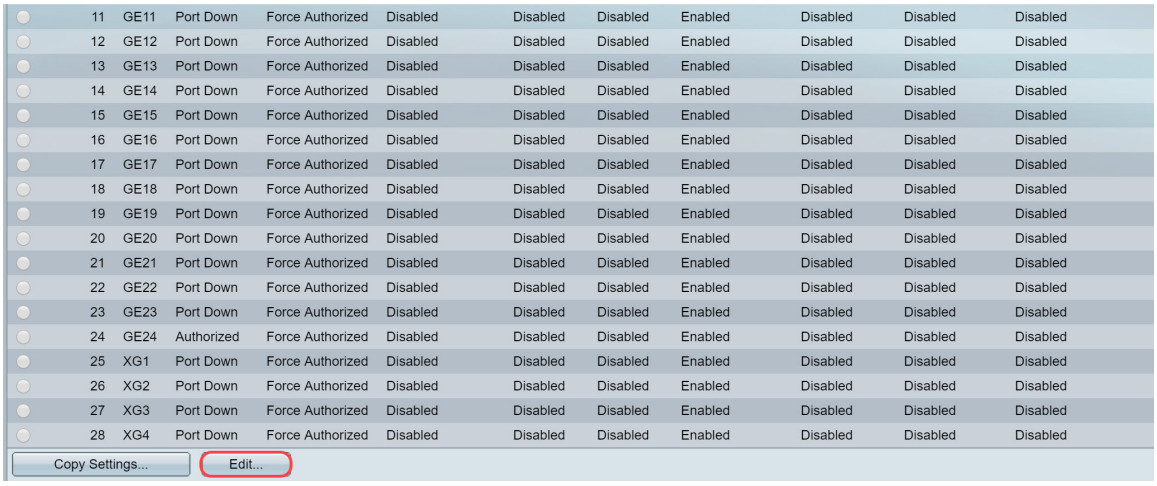


2단계. 포트 권한 부여를 구성할 포트를 선택합니다.

참고:스위치가 연결된 포트를 구성하지 마십시오.스위치는 신뢰할 수 있는 디바이스이므로 해당 포트를 *Forced Authorized로 유지합니다*.



3단계. 그런 다음 아래로 스크롤하여 **편집..**을 클릭합니다. 포트를 구성합니다.

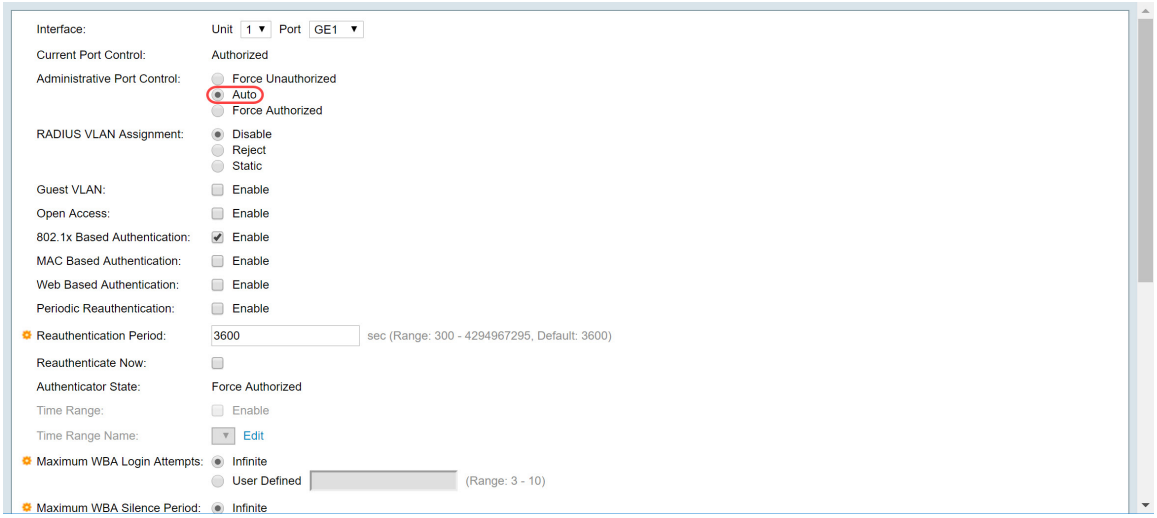


Edit *Port Authentication* 페이지에서 *Current Port Control* 필드는 현재 포트 권한 부여 상태를 표시합니다.상태가 *Authorized*인 경우, 포트가 인증되거나 Administrative Port *Control*이 Force Authorized *입니다*.반대로 상태가 *Unauthorized*(승인되지 않음)인 경우 포트가 인증되지 않거나 *Administrative Port Control(관리 포트 제어)*이 *Force Unauthorized(승인되지 않음)입니다*.인터페이스에서 서 플리 컨 트가 활성화 된 경우 현재 포트 제어는 서 플리 컨 트가 됩니다.

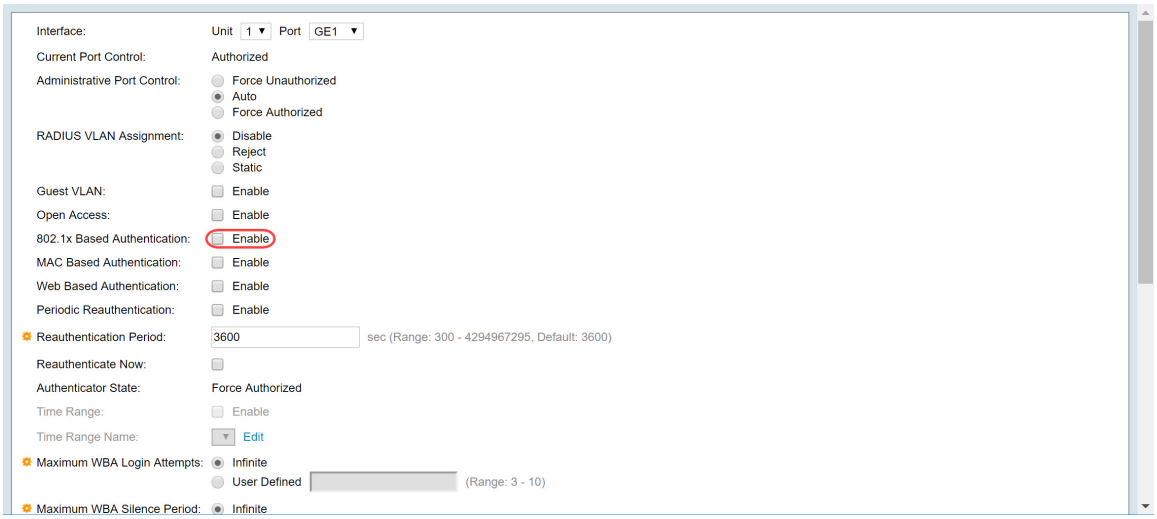
4단계. 관리 포트 권한 부여 상태를 선택합니다.포트를 **자동**으로 **구성합니다**.사용 가능한 옵션은 다음과 같습니다.

- Forced Unauthorized(강제 승인됨) — 인터페이스를 무단 상태로 전환하여 인터페이스 액세스를 거부합니다.디바이스는 인터페이스를 통해 클라이언트에 인증 서비스를 제공하지 않습니다.
- Auto — 디바이스에서 포트 기반 인증 및 권한 부여를 활성화합니다.이 인터페이스는 디바이스와 클라이언트 간의 인증 교환을 기반으로 권한 있는 또는 권한 없는 상태 간에 이동합니다.
- Forced Authorized(강제 권한 부여) - 인증 없이 인터페이스를 인증합니다.

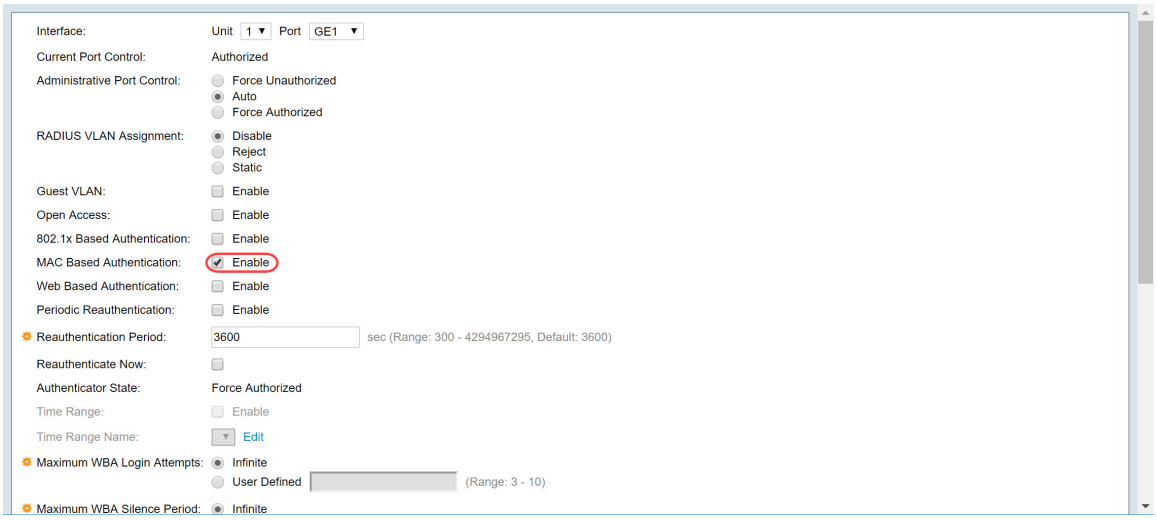
참고: *Forced Authorized*(강제 권한 부여)가 기본값입니다.



5단계. *802.1X 기반 인증* 필드에서 802.1X를 인증으로 사용하지 않으므로 활성화 확인란의 선택을 취소합니다.기본값 *802.1x 기반 인증*이 활성화됩니다.



6단계. 서 플리 컨 트 MAC 주소를 기반으로 포트 인증을 활성화 하려면 *MAC 기반 인증*에 대해 활성화 확인란을 선택합니다.8개의 MAC 기반 인증만 포트에서 사용할 수 있습니다.



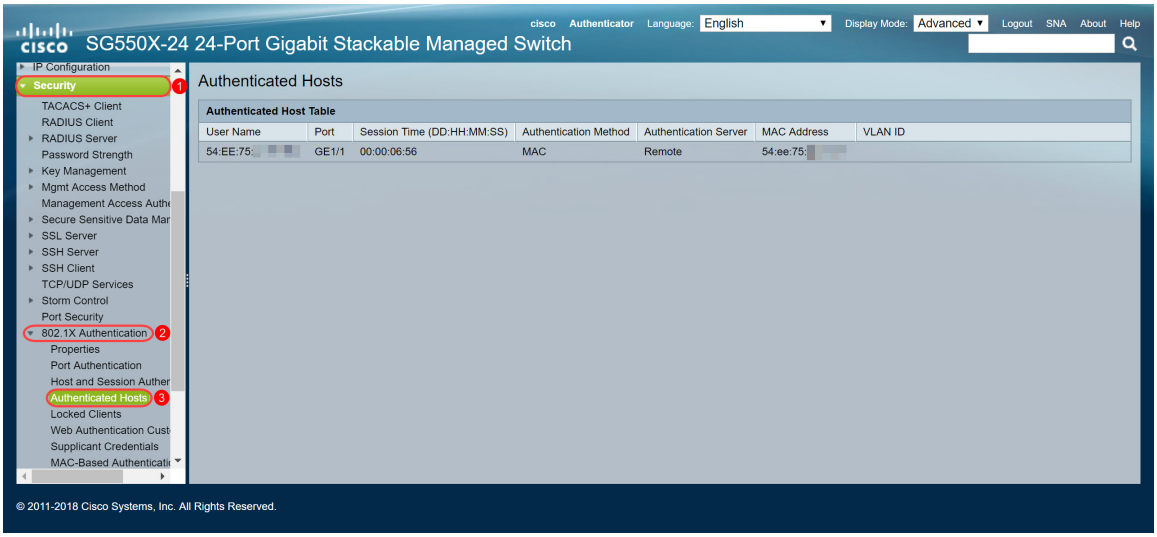
7단계. **적용**을 클릭하여 변경 사항을 저장합니다.

컨피그레이션을 저장하려면 화면 상단의 **Save**(저장) 버튼을 누릅니다.

결론

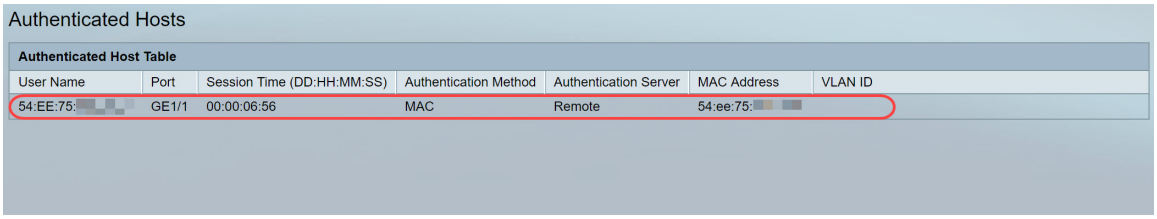
이제 스위치에서 MAC 기반 인증을 성공적으로 구성했습니다.MAC 기반 인증이 작동하는지 확인하려면 아래 단계를 수행하십시오.

1단계. Security(**보안**) **> 802.1X Authentication(802.1X 인증) > Authenticated Hosts(인증된 호스트)로 이동하여** 인증된 사용자에 대한 세부 정보를 확인합니다.

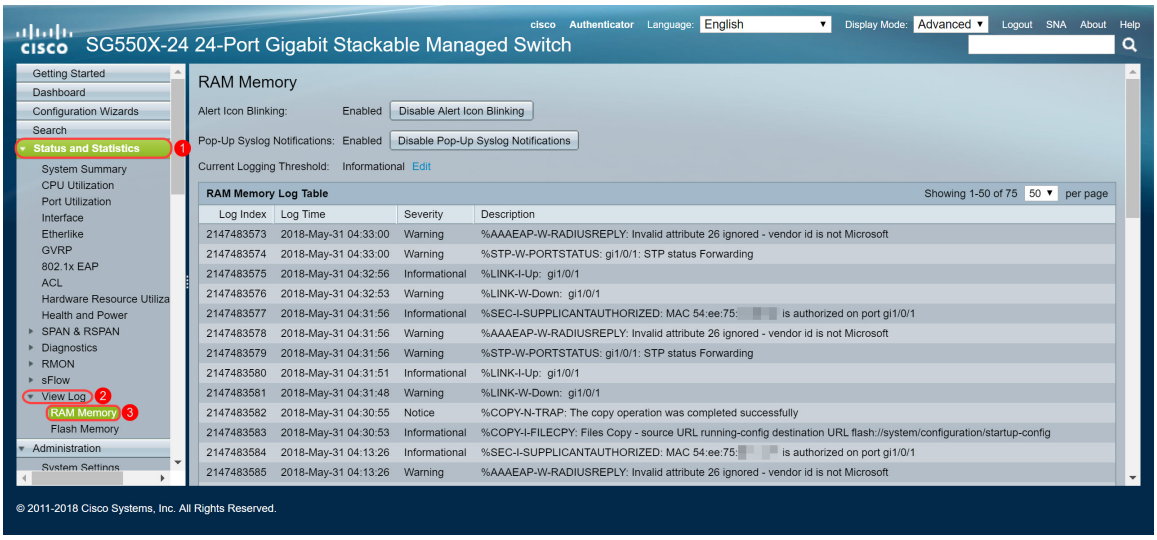


2단계. 이 예에서는 Authenticated *Host* Table(인증된 호스트 테이블)에서 이더넷 MAC 주소가 인증되었음을 확인할 수 있습니다.다음 필드는 다음과 같이 정의됩니다.

- 사용자 이름 — 각 포트에서 인증된 신청자 이름.
- Port — 포트의 번호입니다.
- 세션 시간(DD:HH:MM:SS) — 신청자가 포트에서 인증 및 권한 부여된 액세스 권한을 받은 시간입니다.
- 인증 방법 — 마지막 세션이 인증된 방법입니다.
- Authenticated Server(인증된 서버) - RADIUS 서버.
- MAC 주소 — 신청자 MAC 주소를 표시합니다.
- VLAN ID — 포트의 VLAN.



3단계. (선택 사항) **Status and Statistics > View Log > RAM Memory로 이동합니다**.RAM *Memory* 페이지에는 RAM(캐시)에 저장된 모든 메시지가 시간순으로 표시됩니다.항목은 *Log Settings* 페이지의 컨피그레이션에 따라 RAM 로그에 저장됩니다.



4단계. *RAM Memory Log Table(RAM 메모리 로그 테이블)*에서 MAC 주소가 포트 gi1/0/1에서 인증되었음을 알리는 정보 로그 메시지가 표시됩니다.

참고:MAC 주소의 일부가 흐리게 표시됩니다.

이 문서의 비디오 버전 보기...

[여기를 클릭하여 Cisco의 다른 기술 대화를 확인하십시오.]