

스위치에서 원격 인증 RADIUS(Dial-In User Service) 서버 설정 구성

목표

RADIUS(Remote Authentication Dial-In User Service)는 네트워크 서비스를 연결 및 사용하는 사용자에게 중앙 집중식 AAA(Authentication, Authorization, and Accounting) 관리를 제공하는 네트워킹 프로토콜입니다. RADIUS 서버는 입력한 로그인 자격 증명을 통해 사용자의 ID를 확인하여 네트워크에 대한 액세스를 제어합니다. 예를 들어, 공용 Wi-Fi 네트워크는 대학 캠퍼스에 설치됩니다. 암호를 가진 학생만 이러한 네트워크에 액세스할 수 있습니다. RADIUS 서버는 사용자가 입력한 비밀번호를 확인하고 적절한 액세스를 허용하거나 거부합니다.

RADIUS 서버를 설정하면 클라이언트나 사용자가 네트워크에 액세스할 수 있도록 인증하기 전에 인증되므로 보안을 강화하는 데 유용합니다. RADIUS 서버는 서버 가용성, 재전송 및 시간 초과와 관련된 클라이언트 문제에 응답합니다. 또한 RADIUS 서버는 사용자 연결 요청을 처리하고, 사용자를 인증하며, 사용자에게 서비스를 제공하기 위해 필요한 구성 정보를 클라이언트에 보냅니다.

RADIUS 서버는 RADIUS 지원 디바이스로 구성된 네트워크를 중앙 집중식으로 제어하는 서버입니다. RADIUS 서버는 802.1X 또는 MAC(Media Access Control) 주소에 대한 전달 결정을 기반으로 합니다.

이 문서에서는 Sx350, SG350X 및 Sx550X Series 스위치에서 RADIUS 설정을 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

- SX350 시리즈
- SG350X 시리즈
- SX550X 시리즈

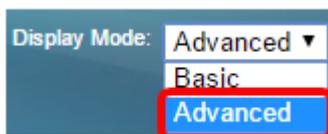
소프트웨어 버전

- 2.2.5.68

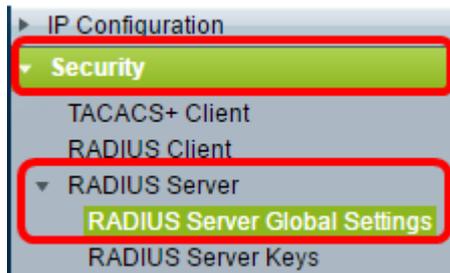
RADIUS 서버 설정 구성

RADIUS 서버 전역 설정 구성

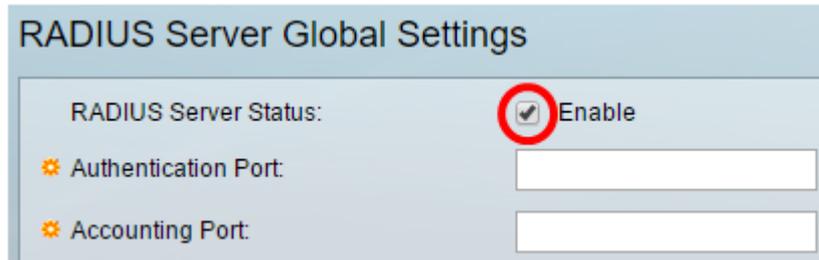
1단계. 스위치 웹 기반 유틸리티에 로그인하고 Display Mode 드롭다운 목록에서 Advanced를 선택합니다.



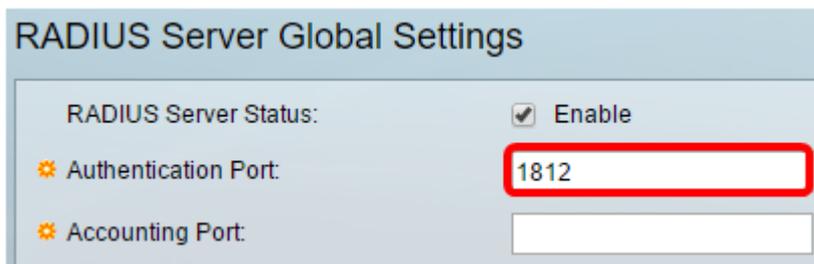
2단계. Security(보안) > RADIUS Server(RADIUS 서버) > RADIUS Server Global Settings(RADIUS 서버 전역 설정)를 선택합니다.



3단계. RADIUS Server Status(RADIUS 서버 상태)에 대해 Enable(활성화) 확인란을 선택합니다.



4단계. 인증 요청을 위해 RADIUS 서버 포트의 UDP(User Datagram Protocol) 포트 번호를 입력합니다.범위는 1~65535이고 기본값은 1812입니다.



5단계. 어카운팅 요청을 위해 RADIUS 서버 포트의 UDP 포트 번호를 입력합니다.범위는 1~65535이고 기본값은 1813입니다.



6단계. (선택 사항) RADIUS 어카운팅 이벤트에 대한 트랩을 생성하려면 Trap Settings(트랩 설정) 아래에서 RADIUS 어카운팅 트랩에 대해 Enable(활성화) 확인란을 선택합니다.



7단계. (선택 사항) 실패한 로그인에 대한 트랩을 생성하려면 RADIUS Authentication Failure Traps(RADIUS 인증 실패 트랩에 대한 Enable(활성화) 확인란을 선택합니다.

Trap Settings

RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Apply Cancel

8단계. (선택 사항) 성공한 로그인에 대한 트랩을 생성하려면 RADIUS Authentication Success Traps(RADIUS 인증 성공 트랩에 대한 **Enable(활성화)** 확인란을 선택합니다.

Trap Settings

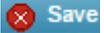
RADIUS Accounting Traps: Enable

RADIUS Authentication Failure Traps: Enable

RADIUS Authentication Success Traps: Enable

Apply Cancel

9단계. **적용**을 클릭합니다.

10단계.  아이콘은 구성이 성공적으로 저장되었음을 나타냅니다. 컨피그레이션을 영구적으로 저장하려면 File Operations(파일 작업) 페이지로 이동하거나 페이지 상단의  아이콘을 클릭합니다. 그렇지 않으면 **닫기**를 클릭합니다.

RADIUS 서버 키 구성

1단계. RADIUS Server(RADIUS 서버) 아래에서 **RADIUS Server Keys(RADIUS 서버 키)**를 선택합니다.

▼ Security

- TACACS+ Client
- RADIUS Client
- ▼ RADIUS Server
 - RADIUS Server Global Settings
 - RADIUS Server Keys**

2단계. (선택 사항) 필요한 경우 기본 RADIUS 키를 입력합니다. Default Key(기본 키)에 입력한 값은 기본 키를 사용하도록 구성된 모든 서버(Add RADIUS Server(RADIUS 서버 추가) 페이지에서)에 적용됩니다.

RADIUS Server Keys

Default Key: Keep existing default key

Encrypted

Plaintext (0/128 characters used)

MD5 Digest: bed128365216c019988915ed3add75fb

Apply Cancel

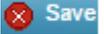
Default Key(기본 키) - 디바이스와 RADIUS 클라이언트 간의 인증 및 암호화에 사용할 기본 키 문자열을 선택합니다. 옵션은 다음과 같습니다.

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

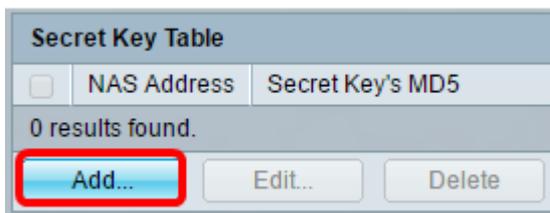
MD5 Digest(MD5 다이제스트) - 사용자가 입력한 비밀번호의 MD5 다이제스트를 표시합니다.

참고: 이 예에서는 Default Key(기본 키) 아래의 Keep existing default key(기존 기본 키 유지)가 선택됩니다.

3단계. 적용을 클릭합니다.

4단계.  아이콘은 구성이 성공적으로 저장되었음을 나타냅니다. 컨피그레이션을 영구적으로 저장하려면 File Operations(파일 작업) 페이지로 이동하거나 페이지 상단의  Save 아이콘을 클릭합니다.

5단계. (선택 사항) Secret Key Table(비밀 키 테이블) 영역에서 **Add(추가)** 버튼을 클릭하여 비밀 키를 추가합니다.



6단계. NAS의 IP 주소 또는 RADIUS 클라이언트를 포함하는 스위치를 *NAS Address* 필드에 입력합니다.

참고: 아래 이미지에서 192.168.1.118은 IP 주소의 예로 사용됩니다.

7단계. 원하는 비밀 키를 선택합니다.

참고: 아래 이미지에서 Plaintext를 예로 선택합니다.

옵션은 다음과 같습니다.

- 기본 키 사용 — 지정된 서버의 경우 디바이스는 기존 기본 키 문자열을 사용하여 RADIUS 클라이언트를 인증하려고 시도합니다.
- 암호화 — MD5를 사용하여 통신을 암호화하려면 암호화된 형식으로 키를 입력합니다.
- 일반 텍스트 — 일반 텍스트 모드에서 키 문자열을 입력합니다. 최대 128자를 입력할 수 있습니다.

8단계. 적용을 클릭합니다.

9단계.  아이콘은 구성이 성공적으로 저장되었음을 나타냅니다. 컨피그레이션을 영구적으로 저장하려면 File Operations(파일 작업) 페이지로 이동하거나 페이지 상단의  Save 아이콘을 클릭합니다. 그렇지 않으면 닫기를 클릭합니다.

RADIUS 서버 그룹 구성

RADIUS 서버 그룹은 디바이스를 RADIUS 서버로 사용할 사용자 그룹입니다. 그룹을 설정하려면 아래 지침을 따르십시오.

1단계. RADIUS Server(RADIUS 서버) 아래에서 **RADIUS Server Groups(RADIUS 서버 그룹)**를 선택합니다.



2단계. RADIUS Server Group(RADIUS 서버 그룹) 테이블 아래의 Add(추가) 버튼을 클릭합니다.



3단계. 팝업 창에서 *Group Name* 필드에 그룹 이름을 입력합니다. 최대 32자를 입력할 수 있습니다.

참고: 아래 이미지에서 GroupA1은 예제로 사용됩니다.

* Group Name: (7/32 characters used)
 * Privilege Level: (Range: 1 - 15, Default: 1)
 Time Range: Enable
 Time Range Name:

4단계. 그룹에 지정할 권한 레벨을 입력합니다. 권한 레벨은 생성한 각 그룹에 할당할 액세스 레벨을 결정합니다. 레벨을 1~15에서 설정할 수 있습니다. 기본값은 1입니다.

참고: 이 예에서는 7이 사용됩니다.

* Group Name: (7/32 characters used)
 * Privilege Level: (Range: 1 - 15, Default: 1)
 Time Range: Enable
 Time Range Name:

- 1 (읽기 전용 CLI 액세스) — 그룹의 사용자는 GUI에 액세스할 수 없으며 디바이스 컨피그레이션을 변경하지 않는 CLI 명령에만 액세스할 수 있습니다.
- 7 (읽기/제한된 쓰기 CLI 액세스) — 그룹의 사용자는 GUI에 액세스할 수 없으며 디바이스 컨피그레이션을 변경하는 일부 CLI 명령에만 액세스할 수 있습니다. 자세한 내용은 [CLI 참조 가이드](#)를 참조하십시오.
- 15 (읽기/쓰기 관리 액세스) — 그룹의 사용자가 GUI에 액세스할 수 있으며 디바이스를 구성할 수 있습니다.

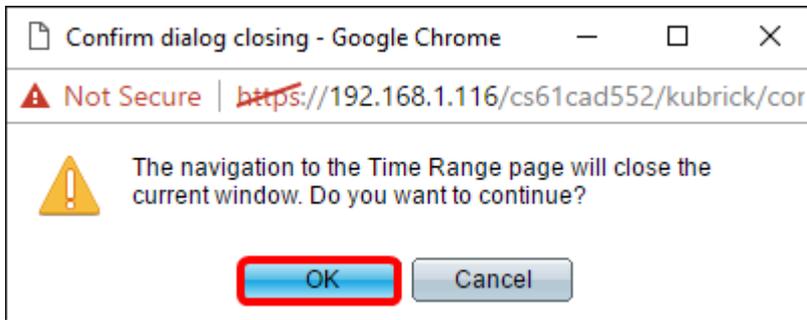
5단계. (선택 사항) 이 그룹에 대해 시간 범위를 적용하려면 시간 범위에 대해 사용 확인란을 선택합니다. 그렇지 않으면 [15단계로 건너뛰십시오](#).

* Group Name: (7/32 characters used)
 * Privilege Level: (Range: 1 - 15, Default: 1)
 Time Range: Enable

6단계. 시간 범위 이름 옆에 있는 **Edit**(수정) 링크를 클릭하여 시간 설정을 구성합니다.

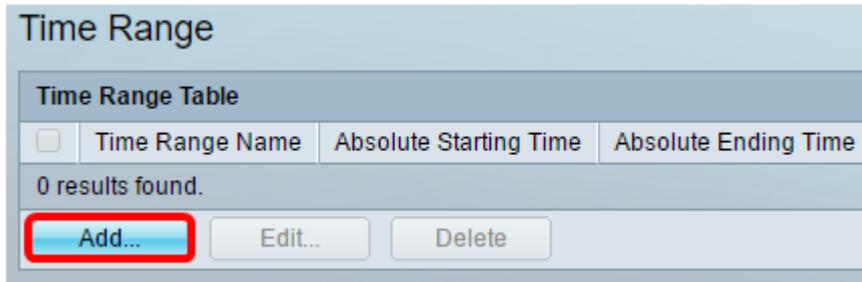
* Group Name: (7/32 characters used)
 * Privilege Level: (Range: 1 - 15, Default: 1)
 Time Range: Enable
 Time Range Name:

7단계. Time Range(시간 범위) 설정을 계속 진행할 수 있도록 현재 창이 닫혀 있음을 알리는 팝업 창이 나타납니다. 확인을 클릭합니다.



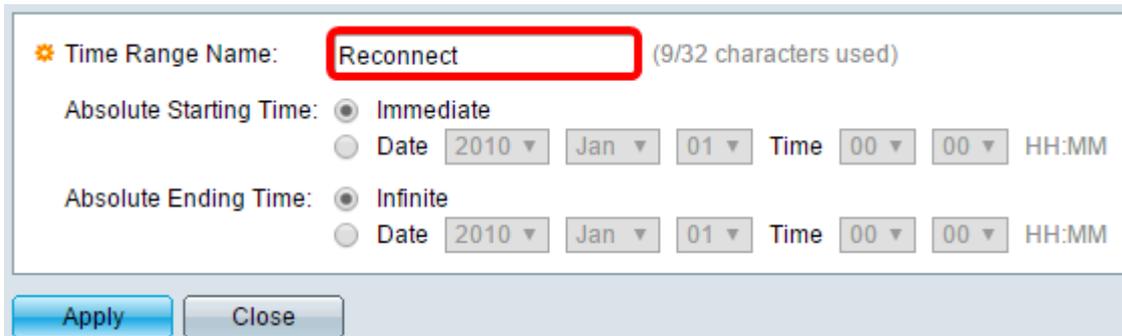
그러면 Time Range(시간 범위) 페이지로 이동합니다.

8단계. Time Range Table(시간 범위 테이블)에서 Add(추가) 버튼을 클릭합니다.

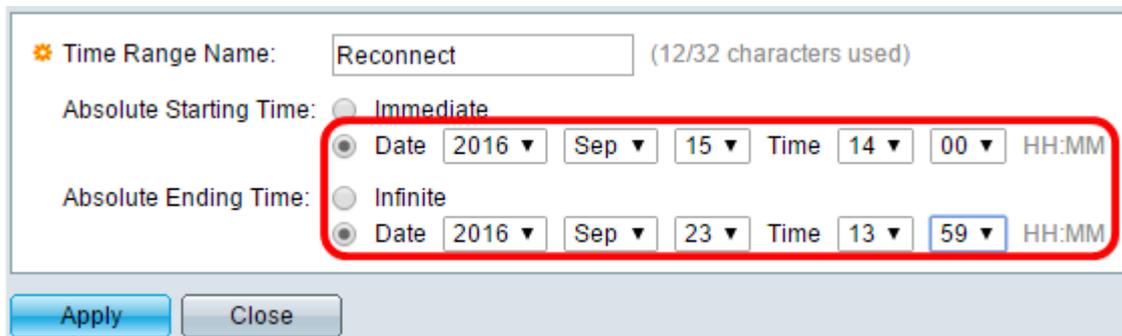


9단계. 시간 범위 이름 필드에 시간 범위의 이름을 입력합니다.

참고:아래 이미지에서 Reconnect(다시 연결)가 예로 사용됩니다.



10단계. 라디오 버튼을 클릭하여 원하는 절대 시작 및 종료 시간을 선택합니다.



- 절대 시작 시간 — 시작 시간을 정의하려면 다음 중에서 선택합니다.
- 즉시 — 시간 범위를 즉시 시작하려면 이 옵션을 선택합니다.
- 날짜, 시간 — 시간 범위가 시작되는 날짜와 시간을 지정하려면 이 옵션을 선택합니다.
- 절대 종료 시간 — 시작 시간을 정의하려면 다음 중에서 선택합니다.
- Infinite — 시간 범위가 끝나지 않도록 하려면 이 옵션을 선택합니다.
- 날짜, 시간 — 시간 범위가 끝나는 날짜와 시간을 지정하려면 이 옵션을 선택합니다.

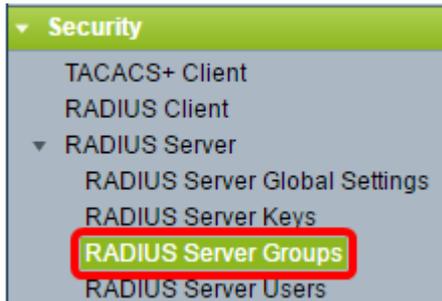
참고:이 예에서는 날짜 및 시간을 선택합니다.

11단계. 적용을 클릭합니다.

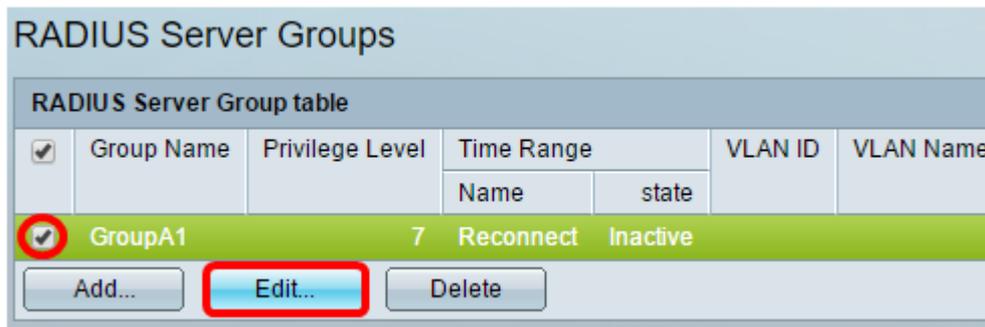
12단계.  아이콘은 구성이 성공적으로 저장되었음을 나타냅니다.컨피그레이션을 영구적으로 저장하려면 File Operations(파일 작업) 페이지로 이동하거나 페이지 상단의  Save 아이콘을 클릭합니다.그렇지 않으면 닫기를 클릭합니다.

그러면 메인 페이지로 이동합니다.

13단계. RADIUS Server(RADIUS 서버) 아래에서 RADIUS Server Groups(RADIUS 서버 그룹)를 다시 클릭합니다.

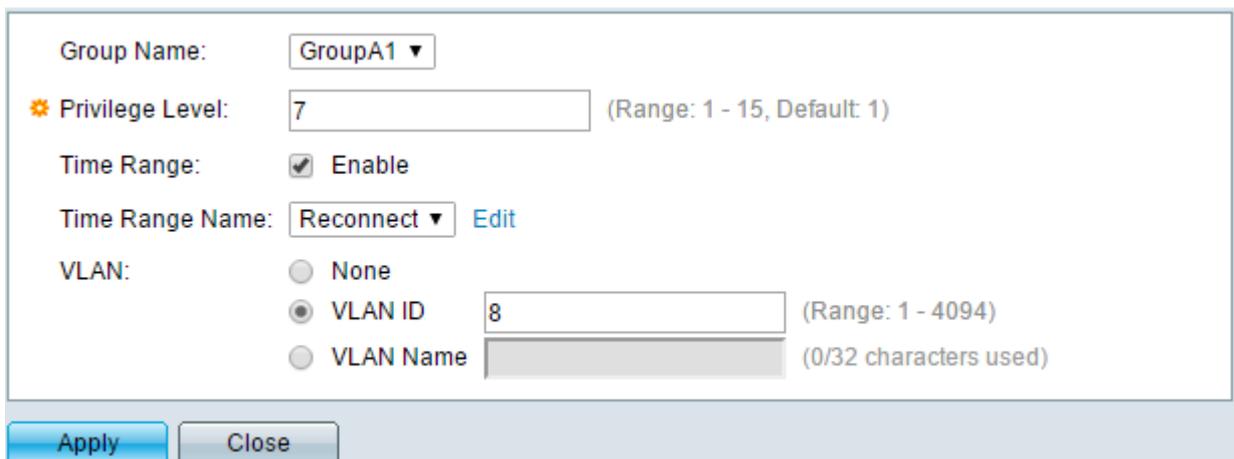


14단계. 새로 생성된 그룹이 이제 RADIUS 서버 그룹 테이블 아래에 표시됩니다.그룹 이름 옆의 상자를 선택한 다음 편집을 클릭합니다.



15단계(선택 사항) 그룹의 VLAN을 선택합니다.옵션은 다음과 같습니다.

- 없음 — 지정된 VLAN이 없습니다.
- VLAN ID — VLAN ID를 지정합니다.
- VLAN 이름 — VLAN 이름을 지정합니다.



A screenshot of the configuration form for a RADIUS Server Group. The 'Group Name' is set to 'GroupA1'. The 'Privilege Level' is set to '7' (Range: 1 - 15, Default: 1). The 'Time Range' is set to 'Enable'. The 'Time Range Name' is set to 'Reconnect' (with an 'Edit' link). The 'VLAN' section has three options: 'None', 'VLAN ID' (selected, with a value of '8' and Range: 1 - 4094), and 'VLAN Name' (with a note '(0/32 characters used)'). At the bottom are 'Apply' and 'Close' buttons.

참고:이 예에서는 VLAN ID 8이 사용됩니다.

16단계. 적용을 누릅니다.

17단계.  아이콘은 구성이 성공적으로 저장되었음을 나타냅니다.컨피그레이션을 영구적으로 저장하려면 File Operations(파일 작업) 페이지로 이동하거나 페이지 상단의  아이콘을 클릭합니다.그렇지 않으면 닫기를 클릭합니다.

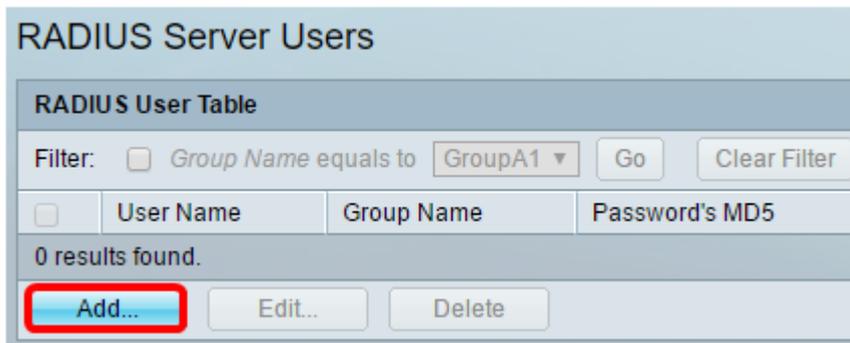
RADIUS 서버 사용자 구성

이전에 생성한 그룹에 사용자를 추가하려면

1단계. RADIUS Server(RADIUS 서버) 아래에서 **RADIUS Server Users(RADIUS 서버 사용자)**를 클릭합니다.

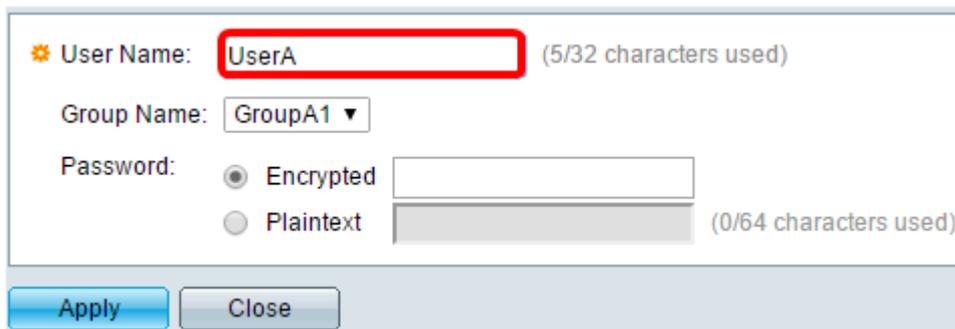


2단계. RADIUS User Table(RADIUS 사용자 테이블)에서 Add(추가) 버튼을 클릭합니다.



3단계. 사용자 이름 필드에 사용자 이름을 입력합니다.

참고:이 예제에서는 UserA가 사용됩니다.



4단계. Group Name(그룹 이름) 드롭다운 목록에서 사용자가 속한 그룹을 선택합니다.

5단계. Password(비밀번호) 영역에서 라디오 버튼을 클릭합니다.

6단계. 기본 비밀번호를 입력합니다.

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

참고: 이 예에서는 일반 텍스트가 선택됩니다.

6단계. 적용을 클릭합니다.

7단계.  아이콘은 구성이 성공적으로 저장되었음을 나타냅니다. 컨피그레이션을 영구적으로 저장하려면 File Operations(파일 작업) 페이지로 이동하거나 페이지 상단의  Save 아이콘을 클릭합니다. 그렇지 않으면 닫기를 클릭합니다.

이제 스위치에서 RADIUS 서버 설정을 구성했어야 합니다.

(c) 2016 Cisco Systems, Inc. 모든 권한은 당사에 있습니다.