

# Sx500 Series Stackable Switch의 802.1x 속성 구성

## 목표

IEEE 802.1x는 클라이언트와 서버 간의 액세스 제어를 용이하게 하는 표준입니다. LAN을 통해 클라이언트에 서비스를 제공하거나 스위치 포트에 연결된 클라이언트를 이 경우 RADIUS(Remote Authentication Dial-In User Service)를 실행하는 인증 서버에서 인증해야 합니다. 802.1x 포트 기반 인증을 활성화하려면 스위치에서 802.1x를 전역적으로 활성화해야 합니다.

802.1x를 완전히 구성하려면 다음 컨피그레이션을 수행해야 합니다.

1. VLAN을 생성하고 [여기](#)를 클릭합니다.
2. VLAN에 포트를 할당하고 위에서 언급한 문서를 계속합니다. CLI에서 구성하려면 [여기](#)를 클릭합니다.
3. 포트 인증을 구성하려면 [여기](#)를 클릭합니다.

이 문서에서는 인증 및 게스트 VLAN 속성을 포함하는 802.1x 속성을 구성하는 방법에 대해 설명합니다. 기타 구성에 대해서는 위의 문서를 참조하십시오. 게스트 VLAN은 802.1x 또는 MAC 기반 인증을 통해 가입 디바이스 또는 포트를 인증하고 인증하지 않아도 되는 서비스에 대한 액세스를 제공합니다.

## 적용 가능한 디바이스

·SX500 Series Stackable Switch

## 소프트웨어 버전

•1.3.0.62

## 802.1x 속성에서 포트 기반 인증 및 게스트 VLAN 활성화

1단계. 웹 구성 유틸리티에 로그인하여 보안 > 802.1X > 등록 정보를 선택합니다. 등록 정보 페이지가 열립니다.

2단계. 포트 기반 802.1x 인증을 활성화하려면 Enable in Port-Based Authentication 필드를 선택합니다.

3단계. Authentication Method(인증 방법) 필드에서 원하는 라디오 버튼을 클릭합니다 .RADIUS 서버는 클라이언트 인증을 수행합니다.이 서버는 사용자의 인증 여부를 확인하고 클라이언트가 LAN 및 기타 스위치 서비스에 액세스할 수 있는지 여부를 스위치에 알립니다 .스위치는 프록시 역할을 하며 서버는 클라이언트에 투명합니다.

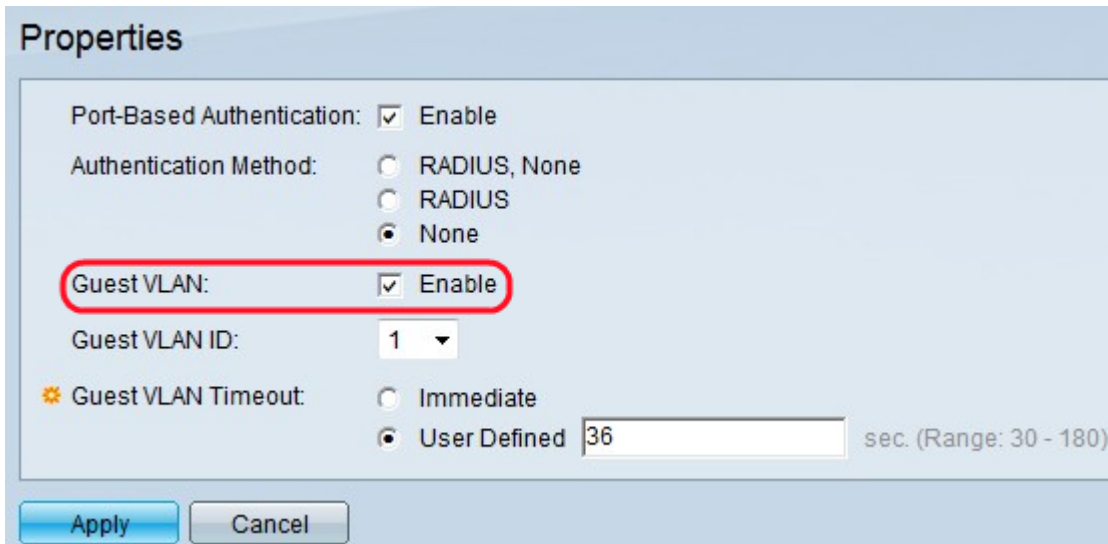
·RADIUS, None — RADIUS 서버의 도움으로 먼저 포트 인증을 수행합니다.서버가 다운된

경우와 같이 서버에서 응답이 없는 경우 인증이 수행되지 않고 세션이 허용됩니다. 서버를 사용할 수 있고 사용자 자격 증명이 올바르지 않으면 액세스가 거부되고 세션이 종료됩니다.

·RADIUS — RADIUS 서버를 기반으로 포트 인증을 수행합니다. 인증이 수행되지 않으면 세션이 종료됩니다.

·없음 — 사용자를 인증하지 않고 세션을 허용합니다.

4단계. (선택 사항) Enable(활성화)을 선택하여 Guest VLAN(게스트 VLAN) 필드에서 권한이 없는 포트에 대한 게스트 VLAN의 사용을 활성화합니다. 게스트 VLAN이 활성화된 경우, 모든 권한이 없는 포트는 게스트 VLAN ID 필드에서 선택한 VLAN에 자동으로 조인합니다. 포트가 나중에 인증되면 게스트 VLAN에서 제거됩니다.



The screenshot shows a 'Properties' dialog box with the following settings:

- Port-Based Authentication:  Enable
- Authentication Method:  RADIUS, None;  RADIUS;  None
- Guest VLAN:  Enable
- Guest VLAN ID: 1 (dropdown menu)
- Guest VLAN Timeout:  Immediate;  User Defined 36 sec. (Range: 30 - 180)

Buttons: Apply, Cancel

MAC 인증 모드를 사용하려면 먼저 게스트 VLAN 모드를 구성해야 합니다. 802.1x 프레임워크를 사용하면 디바이스(신청자)가 연결된 원격 디바이스(인증자)에서 포트 액세스를 요청할 수 있습니다. 포트 액세스를 요청하는 서플리컨트가 인증되고 권한 있는 경우에만 데이터를 포트에 보낼 수 있습니다. 그렇지 않으면 인증자는 데이터가 게스트 VLAN 및/또는 인증되지 않은 VLAN으로 전송되지 않는 한 신청자 데이터를 폐기합니다.

**참고:** 게스트 VLAN이 구성된 경우 다음과 같은 특성을 가진 고정 VLAN입니다.

- 기존 고정 VLAN에서 수동으로 정의해야 합니다.
- Guest-VLAN이 활성화된 무단 디바이스 또는 디바이스 포트에서만 자동으로 사용할 수 있습니다.
- 포트가 Guest-VLAN-enabled인 경우, 포트가 인증되지 않은 경우 스위치는 자동으로 포트를 게스트 VLAN의 태그 없는 멤버로 추가하고, 포트의 첫 번째 서플리컨트가 인증될 때 게스트 VLAN에서 포트를 제거합니다.
- 게스트 VLAN은 음성 VLAN 및 인증되지 않은 VLAN으로 사용할 수 없습니다.

**시간 절약:** 게스트 VLAN이 비활성화된 경우 7단계로 건너뛩니다.

5단계. Guest VLAN ID 드롭다운 목록의 VLAN 목록에서 게스트 VLAN ID를 선택합니다.

Properties

Port-Based Authentication:  Enable

Authentication Method:  RADIUS, None  
 RADIUS  
 None

Guest VLAN:  Enable

Guest VLAN ID: **1**

Guest VLAN Timeout:  Immediate  
 User Defined  sec. (Range: 30 - 180)

Apply Cancel

6단계. Guest VLAN Timeout(게스트 VLAN 시간 초과) 필드에서 원하는 라디오 버튼을 클릭합니다.사용 가능한 옵션은 다음과 같습니다.

- Immediate — 게스트 VLAN은 10초 후 만료됩니다.
- 사용자 정의 — 사용자 정의 필드에 기간을 수동으로 입력합니다.

**참고:**링크 업 후, 소프트웨어에서 802.1x 신청자를 탐지하지 않거나 포트 인증에 실패한 경우 게스트 VLAN 시간 초과 기간이 만료된 후에만 포트가 게스트 VLAN에 추가됩니다.포트가 Authorized(권한 있음)에서 Not Authorized(권한 없음)로 변경되면 게스트 VLAN Timeout(게스트 VLAN 시간 제한) 기간이 만료된 후에만 포트가 게스트 VLAN에 추가됩니다.VLAN Authentication Table(VLAN 인증 테이블)은 모든 VLAN을 표시하고 인증 활성화 여부를 표시합니다.

7단계. 적용을 클릭하여 설정을 저장합니다.

## 인증되지 않은 VLAN 컨피그레이션

802.1x가 활성화되면 게스트 VLAN 또는 인증되지 않은 VLAN의 일부가 아닌 한, 인증되지 않은 포트 또는 디바이스는 VLAN에 액세스할 수 없습니다.포트를 VLAN에 포트 페이지를 사용하여 VLAN에 수동으로 추가해야 합니다.

1단계. 웹 구성 유틸리티에 로그인하여 [보안] > [802.1X] > [속성]을 선택합니다. [속성] 페이지가 열립니다.

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
<input checked="" type="radio"/>	2	VLAN 2	Enabled
<input type="radio"/>	3	VLAN 3	Enabled
Edit..			

2단계. 페이지를 아래로 스크롤하여 VLAN Authentication Table(VLAN 인증 테이블)로 이동하고, 인증을 비활성화할 VLAN의 라디오 버튼을 클릭한 다음 Edit(수정)를 클릭합니다.Edit VLAN Authentication(VLAN 인증 수정) 페이지가 열립니다.

VLAN ID: 2 ▼

VLAN Name: VLAN 2

Authentication:  Enable

Apply Close

3단계. (선택 사항) VLAN ID 드롭다운 목록에서 VLAN ID를 선택합니다.

VLAN ID: 2 ▼

VLAN Name: VLAN 2

Authentication:  Enable

Apply Close

4단계. **Enable(활성화)**을 선택 취소하여 인증을 비활성화하고 VLAN을 인증되지 않은 VLAN으로 만듭니다.

5단계. **적용**을 클릭하여 설정을 적용합니다.VLAN 인증 테이블이 변경됩니다.

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
<input checked="" type="radio"/>	2	VLAN 2	Disabled
<input type="radio"/>	3	VLAN 3	Enabled

Edit..