

ISE 및 Catalyst 9800 Wireless LAN Controller로 동적 VLAN 할당 구성

목차

[소개](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[RADIUS 서버를 사용한 동적 VLAN 할당](#)

[구성](#)

[네트워크 다이어그램](#)

[구성 단계](#)

[Cisco ISE 컨피그레이션](#)

[1단계. Cisco ISE 서버에서 Catalyst WLC를 AAA 클라이언트로 구성](#)

[2단계. Cisco ISE에서 내부 사용자 구성](#)

[3단계. 동적 VLAN 할당에 사용되는 RADIUS\(IETF\) 특성을 구성합니다.](#)

[여러 VLAN에 대한 스위치 구성](#)

[Catalyst 9800 WLC 컨피그레이션](#)

[1단계. 인증 서버의 세부사항을 사용하여 WLC를 구성합니다.](#)

[2단계. VLAN 구성](#)

[3단계. WLAN\(SSID\) 구성](#)

[4단계. 정책 프로파일 구성](#)

[5단계. 정책 태그 구성](#)

[6단계. AP에 정책 태그 할당](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 동적 VLAN 할당의 개념 및 무선 클라이언트에 대해 이를 달성하기 위해 무선 LAN(WLAN)을 할당하도록 Catalyst 9800 WLC(wireless LAN controller) 및 Cisco ISE(Identity Service Engine)를 구성하는 방법에 대해 설명합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- WLC 및 LAP(Lightweight Access Point)에 대한 기본적인 지식을 얻으십시오.
- ISE와 같은 AAA 서버에 대한 기능 지식이 있어야 합니다.
- 무선 네트워크 및 무선 보안 문제에 대해 철저히 숙지하십시오.
- 동적 VLAN 할당에 대한 기능 지식이 있어야 합니다.
- CAPWAP(Control and Provisioning for Wireless Access Point)에 대한 기본적인 지식이 있어야

합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 16.12.4a를 실행하는 Cisco Catalyst 9800 WLC(Catalyst 9800-CL)
- 로컬 모드의 Cisco 2800 Series LAP.
- 기본 Windows 10 신청자.
- 버전 2.7을 실행하는 Cisco ISE(Identity Service Engine)
- 펌웨어 릴리스 16.9.6을 실행하는 Cisco 3850 시리즈 스위치입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

RADIUS 서버를 사용한 동적 VLAN 할당

대부분의 WLAN(Wireless Local Area Network) 시스템에서는 각 WLAN에 SSID(Service Set Identifier)와 연결된 모든 클라이언트에 적용되는 정적 정책이 있습니다. 강력하지만 이 방법은 여러 QoS 및 보안 정책을 상속하려면 클라이언트가 다른 SSID와 연결해야 하기 때문에 제한이 있습니다.

그러나 Cisco WLAN 솔루션은 ID 네트워킹을 지원합니다. 이를 통해 네트워크에서 단일 SSID를 광고하고 특정 사용자가 사용자 자격 증명을 기반으로 다른 QoS 또는 보안 정책을 상속받을 수 있습니다.

동적 VLAN 할당은 사용자가 제공한 자격 증명을 기반으로 무선 사용자를 특정 VLAN에 넣는 기능입니다. 특정 VLAN에 사용자를 할당하는 작업은 Cisco ISE와 같은 RADIUS 인증 서버에 의해 처리됩니다. 예를 들어, 이를 사용하여 무선 호스트가 캠퍼스 네트워크 내에서 이동하는 동일한 VLAN에 유지되도록 할 수 있습니다.

따라서 클라이언트가 컨트롤러에 등록된 LAP에 연결을 시도하면 WLC는 검증을 위해 사용자의 자격 증명을 RADIUS 서버에 전달합니다. 인증에 성공하면 RADIUS 서버는 특정 IETF(Internet Engineering Task Force) 특성을 사용자에게 전달합니다. 이러한 RADIUS 특성은 무선 클라이언트에 할당해야 하는 VLAN ID를 결정합니다. 사용자가 항상 이 미리 결정된 VLAN ID에 할당되므로 클라이언트의 SSID는 중요하지 않습니다.

VLAN ID 할당에 사용되는 RADIUS 사용자 특성은 다음과 같습니다.

- IETF 64 (Tunnel Type) - VLAN으로 설정합니다.
- IETF 65(Tunnel Medium Type) - 802로 설정합니다.
- IETF 81(Tunnel Private Group ID) - VLAN ID로 설정합니다.

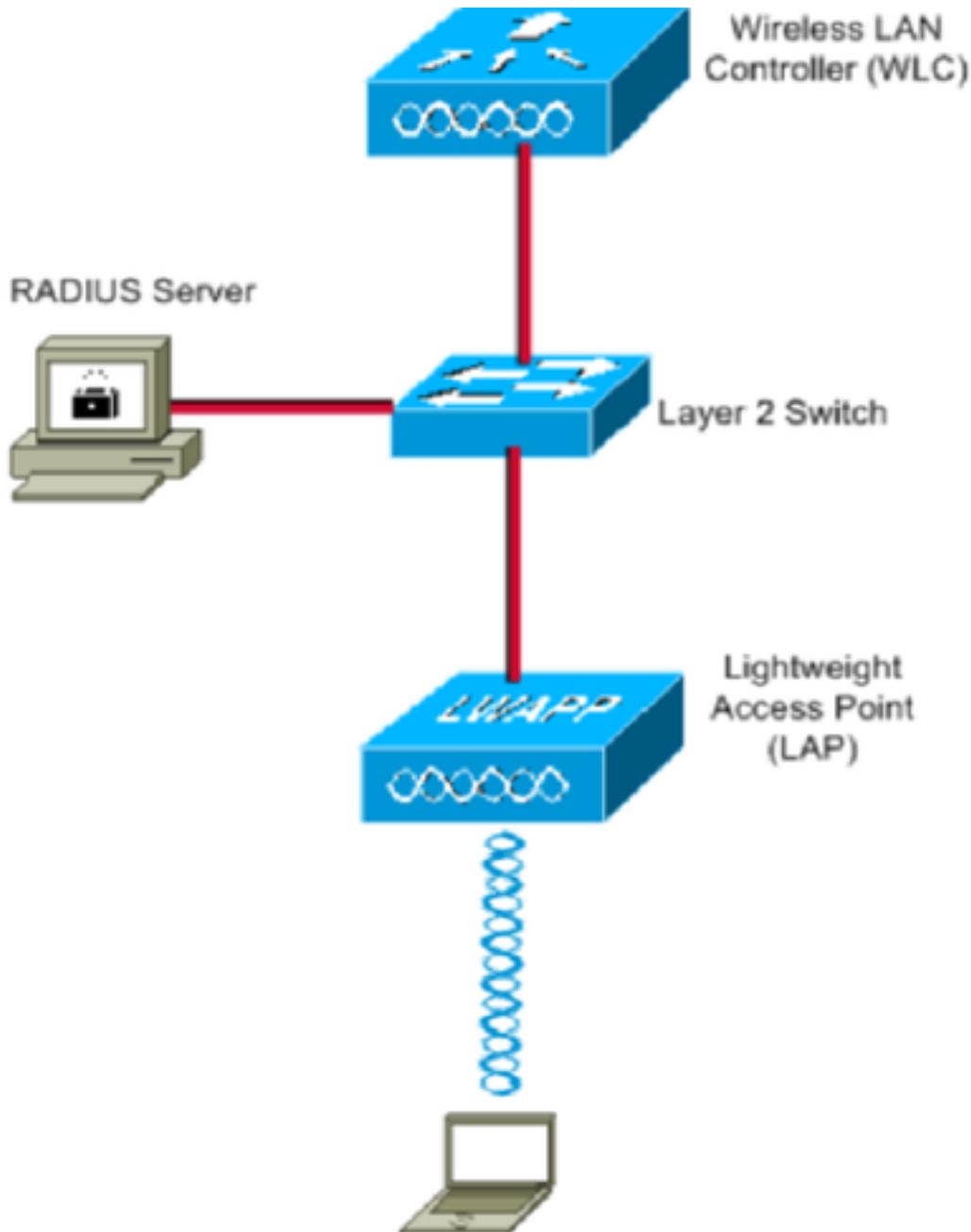
VLAN ID는 12비트이며 1과 4094 사이의 값을 포함합니다(포함). Tunnel-Private-Group-ID는 RFC2868에서 IEEE 802.1X와 함께 사용하기 위해 정의한 대로 문자열 유형이므로 VLAN ID 정수 값은 문자열로 인코딩됩니다. 이러한 터널 특성이 전송되면 Tag 필드에 이를 입력해야 합니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



다음은 이 다이어그램에서 사용되는 구성 요소의 구성 세부 정보입니다.

- Cisco ISE (RADIUS) 서버의 IP 주소는 10.10.1.24 입니다.
- WLC의 관리 인터페이스 주소는 10.10.1.17입니다.
- 컨트롤러의 내부 DHCP 서버는 무선 클라이언트에 IP 주소를 할당하는 데 사용됩니다.
- 이 문서에서는 PEAP가 포함된 802.1x를 보안 메커니즘으로 사용합니다.
- VLAN102는 이 컨피그레이션 전체에서 사용됩니다. 사용자 이름 jonathga-102는 RADIUS 서버에 의해 VLAN102에 배치되도록 구성됩니다.

구성 단계

이 컨피그레이션은 다음 세 가지 범주로 구분됩니다.

- Cisco ISE 구성.
- 여러 VLAN에 대한 스위치를 구성합니다.
- Catalyst 9800 WLC 구성.

Cisco ISE 컨피그레이션

이 구성에는 다음 단계가 필요합니다.

- Cisco ISE 서버에서 Catalyst WLC를 AAA 클라이언트로 구성합니다.
- Cisco ISE에서 내부 사용자를 구성합니다.
- Cisco ISE에서 동적 VLAN 할당에 사용되는 RADIUS(IETF) 특성을 구성합니다.

1단계. Cisco ISE 서버에서 Catalyst WLC를 AAA 클라이언트로 구성

이 절차에서는 WLC가 사용자 자격 증명을 ISE에 전달할 수 있도록 ISE 서버에 AAA 클라이언트로 WLC를 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. ISE GUI에서 **Administration > Network Resources > Network Devices** 선택 **Add**.
2. 이미지에 표시된 대로 WLC와 ISE 간의 WLC 관리 IP 주소 및 RADIUS 공유 암호로 컨피그레이션을 완료합니다.

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MD

Network Devices List > **New Network Device**

Network Devices

* Name (highlighted)

Description

IP Address / (highlighted)

* Device Profile (highlighted)

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol (highlighted)

* Shared Secret (highlighted)

Use Second Shared Secret

CoA Port

2단계. Cisco ISE에서 내부 사용자 구성

이 절차에서는 Cisco ISE의 내부 사용자 데이터베이스에 사용자를 추가하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. ISE GUI에서 **Administration > Identity Management > Identities** 선택 **Add**.
2. 이미지에 표시된 대로 사용자 이름, 비밀번호 및 사용자 그룹으로 컨피그레이션을 완료합니다

The screenshot shows the 'New Network Access User' configuration page in the Cisco ISE GUI. The navigation path is: Administration > Identity Management > Identities > Network Access Users List > New Network Access User. The configuration fields are as follows:

- Network Access User:**
 - * Name: jonathga-102
 - Status: Enabled
 - Email: (empty)
- Passwords:**
 - Password Type: Internal Users
 - * Login Password: (masked) [Generate Password]
 - Re-Enter Password: (masked) [Generate Password]
 - Enable Password: (masked) [Generate Password]
- User Information:**
 - First Name: (empty)
 - Last Name: (empty)
- Account Options:**
 - Description: (empty)
 - Change password on next login:
- Account Disable Policy:**
 - Disable account if date exceeds: 2021-05-18 (yyyy-mm-dd)
- User Groups:**
 - VLAN102 (selected)

Buttons: Submit, Cancel

3단계. 동적 VLAN 할당에 사용되는 RADIUS(IETF) 특성을 구성합니다.

이 절차에서는 무선 사용자에게 대한 권한 부여 프로파일 및 인증 정책을 생성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. ISE GUI에서 Policy > Policy Elements > Results > Authorization > Authorization profiles 선택 Add 새 프로파일을 생성합니다.
2. 각 그룹에 대한 VLAN 정보로 권한 부여 프로파일 컨피그레이션을 완료합니다. 이 그림에서는 jonathga-VLAN-102 그룹 구성 설정.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Authorization Profiles > jonathga-VLAN-102

Authorization Profile

* Name: jonathga-VLAN-102

Description: Dynamic-Vlan-Assignment

Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template:

Track Movement:

Passive Identity Tracking:

Common Tasks

DACL Name

ACL (Filter-ID)

Security Group

VLAN Tag ID 1 Edit Tag ID/Name 102

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
 Tunnel-Private-Group-ID = 1:102
 Tunnel-Type = 1:13
 Tunnel-Medium-Type = 1:6

Save Reset

권한 부여 프로파일을 구성한 후 무선 사용자에게 대한 인증 정책을 생성해야 합니다. 새 Custom 정책 또는 수정 Default 정책 설정 이 예에서는 사용자 지정 프로필이 생성됩니다.

3. 다음으로 이동 Policy > Policy Sets 선택 Add 이미지에 표시된 대로 새 정책을 생성하려면

이제 그룹 멤버십에 따라 각 권한 부여 프로파일을 할당하려면 사용자에게 대한 권한 부여 정책을 생성해야 합니다.

5. 열기 Authorization policy 섹션 및 정책을 생성하여 이미지에 표시된 대로 해당 요구 사항을 달성합니다.

여러 VLAN에 대한 스위치 구성

스위치를 통해 여러 VLAN을 허용하려면 컨트롤러에 연결된 스위치 포트를 구성하려면 다음 명령을 실행해야 합니다.

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

참고: 기본적으로 대부분의 스위치는 트렁크 포트를 통해 해당 스위치에 생성된 모든 VLAN을 허용합니다. 유선 네트워크가 스위치에 연결된 경우 이 동일한 컨피그레이션을 유선 네트워크에 연결하는 스위치 포트에 적용할 수 있습니다. 이렇게 하면 유무선 네트워크의 동일한 VLAN 간에 통신이 가능합니다.

Catalyst 9800 WLC 컨피그레이션

이 구성에는 다음 단계가 필요합니다.

- 인증 서버의 세부사항으로 WLC를 구성합니다.
- VLAN을 구성합니다.
- WLAN(SSID)을 구성합니다.
- 정책 프로필을 구성합니다.
- 정책 태그를 구성합니다.
- AP에 정책 태그를 할당합니다.

1단계. 인증 서버의 세부사항을 사용하여 WLC를 구성합니다.

클라이언트를 인증하기 위해 RADIUS 서버와 통신할 수 있도록 WLC를 구성해야 합니다.

다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 **Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add** 이미지에 표시된 대로 RADIUS 서버 정보를 입력합니다.

The screenshot shows the Cisco WLC GUI for 'Authentication Authorization and Accounting'. The 'Servers / Groups' tab is active, and the 'RADIUS' server type is selected. The 'Create AAA Radius Server' dialog is open, with the following fields highlighted in red:

- Name*: Cisco-ISE
- Server Address*: 10.10.1.24
- Key*: [Redacted]
- Confirm Key*: [Redacted]

Other fields in the dialog include:

- PAC Key:
- Key Type: Clear Text
- Auth Port: 1812
- Acct Port: 1813
- Server Timeout (seconds): 1-1000
- Retry Count: 0-100
- Support for CoA: ENABLED
- CoA Server Key Type: Clear Text
- CoA Server Key: [Empty]
- Confirm CoA Server Key: [Empty]
- Automate Tester:

At the bottom of the dialog, the 'Apply to Device' button is highlighted in red.

2. RADIUS 서버를 RADIUS 그룹에 추가하려면 **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add** 이미지에 표시된 대로

Create AAA Radius Server Group

Name*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance DISABLED

Source Interface VLAN ID

Available Servers: server-2019

Assigned Servers: Cisco-ISE

3. 인증 방법 목록을 생성하려면 **Configuration > Security > AAA > AAA Method List > Authentication > + Add** 이미지에 표시된 대로

Authentication Authorization and Accounting

Servers / Groups

General

Authorization

Name

Quick Setup: AAA Authentication

Method List Name* ISE-SERVER

Type* dot1x ⓘ

Group Type group ⓘ

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- radgrp_SykesLab
- server2019
- tacacgrp_SykesLab

Assigned Server Groups

- ISE-SERVER

Cancel Apply to Device

2단계. VLAN 구성

이 절차에서는 Catalyst 9800 WLC에서 VLAN을 구성하는 방법에 대해 설명합니다. 이 문서의 앞부분에서 설명한 대로 RADIUS 서버의 Tunnel-Private-Group ID 특성에 지정된 VLAN ID도 WLC에 있어야 합니다.

이 예에서는 사용자 jonathga-102가 Tunnel-Private-Group ID of 102 (VLAN =102) RADIUS 서버에 있습니다

1. 다음으로 이동 **Configuration > Layer2 > VLAN > VLAN > + Add** 이미지에 표시된 대로

Search Menu Items

- Dashboard
- Monitoring
- Configuration**
- Administration
- Troubleshooting

VLAN

SVI **VLAN** VLAN Group

+ Add × Delete

	VLAN ID	Name
<input type="checkbox"/>	1	defau
<input type="checkbox"/>	100	VLAN
<input type="checkbox"/>	210	VLAN
<input type="checkbox"/>	2602	VLAN

2. 이미지에 표시된 대로 필요한 정보를 입력합니다.

Create VLAN

Create a single VLAN

VLAN ID*

102

Name

State

ACTVATED

IGMP Snooping

DISABLED

ARP Broadcast

DISABLED

Port Members

Search

Available (2)

Gi1



Gi2



Associated (0)

No Associated Members

Create a range of VLANs

VLAN Range*

- (Ex:5-7)

Cancel

Apply to Device

참고: 이름을 지정하지 않으면 VLAN에 VLANXXXX라는 이름이 자동으로 할당됩니다. 여기서 XXXX는 VLAN ID입니다.

필요한 모든 VLAN에 대해 1단계와 2단계를 반복합니다. 단계를 완료하면 3단계로 진행할 수 있습니다.

3. 데이터 인터페이스에서 VLAN이 허용되는지 확인합니다. 포트 채널이 사용 중인 경우 다음 위치로 이동합니다. **Configuration > Interface > Logical > PortChannel name > General**. 구성된 것으로 표시되는 경우 **Allowed VLAN = All** 구성을 완료했습니다. Cisco의 **Allowed VLAN = VLANs IDs**를 클릭하고 필요한 VLAN을 추가하고 그 후 **Update & Apply to Device**. 사용 중인 포트 채널이 없는 경우 **Configuration > Interface > Ethernet > Interface Name > General**. 구성된 것으로 표시되는 경우 **Allowed VLAN = All** 구성을 완료했습니다. Cisco의 **Allowed VLAN = VLANs IDs**를 클릭하고 필요한 VLAN을 추가하고 그 후 **Update & Apply to Device**.

이 이미지는 All 또는 특정 VLAN ID를 사용하는 경우 인터페이스 설정과 관련된 컨피그레이션을 보여줍니다.

General

Advanced

Interface

GigabitEthernet3

Description

(1-200 Characters)

Admin Status

UP 

Port Fast

disable ▼

Enable Layer 3 Address

DISABLED

Switchport Mode

trunk ▼

Allowed Vlan

All Vlan IDs

Native Vlan

▼

General

Advanced

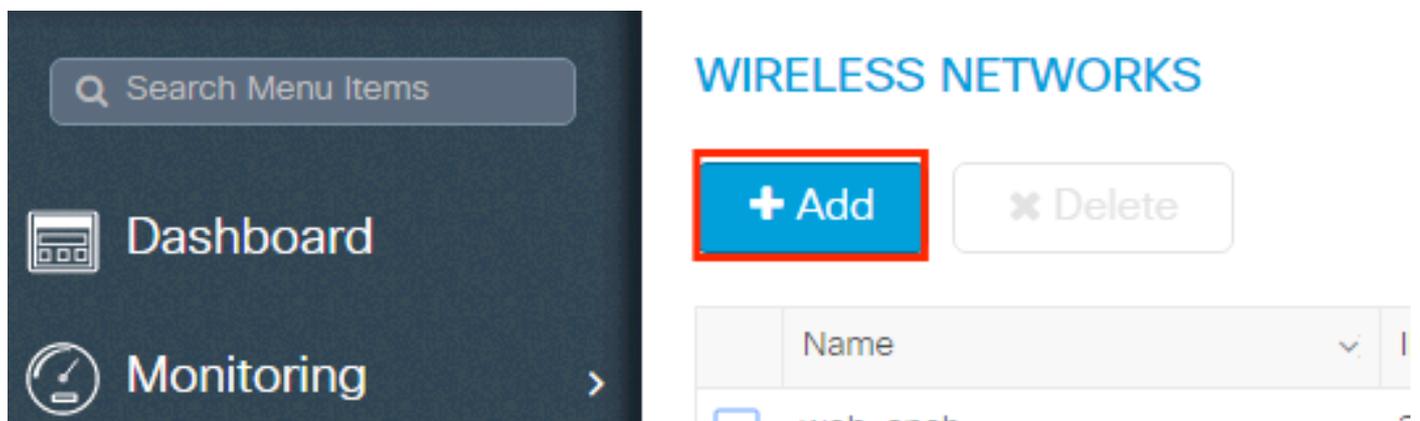
Interface	GigabitEthernet1	
Description	<input type="text"/>	(1-200 Characters)
Speed	<input type="text" value="1000"/>	
Admin Status	<input type="button" value="UP"/>	
Enable Layer 3 Address	<input type="checkbox"/> DISABLED	
Switchport Mode	<input type="text" value="trunk"/>	
Allowed Vlan	<input type="radio"/> All <input checked="" type="radio"/> Vlan IDs	
Vlan IDs	<input type="text" value="551,102,105"/>	(e.g. 1,2,4,6-10)
Native Vlan	<input type="text" value="551"/>	

3단계. WLAN(SSID) 구성

이 절차에서는 WLC에서 WLAN을 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. WLAN을 생성하려면 다음으로 이동 **Configuration > Wireless > WLANs > + Add** 이미지에 표시된 대로 필요에 따라 네트워크를 구성합니다.



2. 이미지에 표시된 대로 WLAN 정보를 입력합니다.

Add WLAN ✕

General Security Advanced

Profile Name*	Dinamyc-VLAN	Radio Policy	All ▼
SSID*	Dinamyc-VLAN	Broadcast SSID	ENABLED <input checked="" type="checkbox"/>
WLAN ID*	6		
Status	ENABLED <input checked="" type="checkbox"/>		

↶ Cancel

📄 Apply to Device

3. 다음으로 이동 Security 필요한 보안 방법을 선택합니다. 이 경우 이미지에 표시된 대로 WPA2 + 802.1x를 선택합니다.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	WPA + WPA2 ▼	Fast Transition	Adaptive Enab... ▼
MAC Filtering	<input type="checkbox"/>	Over the DS	<input checked="" type="checkbox"/>
Protected Management Frame		Reassociation Timeout	20
PMF	Disabled ▼		
WPA Parameters			
WPA Policy	<input type="checkbox"/>		

↶ Cancel 📄 Save & Apply to Device

Add WLAN

PMF Disabled

WPA Parameters

WPA Policy

WPA2 Policy

WPA2 Encryption

AES(CCMP128)

CCMP256

GCMP128

GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

발신 **Security > AAA** 탭에서 3단계에서 생성한 인증 방법을 선택합니다. **Configure the WLC with the Details of the Authentication Server** 이미지에 표시된 섹션:

Add WLAN

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List ISE-SERVER ⓘ

Local EAP Authentication

Cancel Apply to Device

4단계. 정책 프로파일 구성

이 절차에서는 WLC에서 정책 프로필을 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. 다음으로 이동 **Configuration > Tags & Profiles > Policy Profile** 그리고 **default-policy-profile** 이미지에 표시

된 대로 새 이미지를 만듭니다.

Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Policy Profile

+ Add Delete

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

1 10 items per page

Edit Policy Profile

General Access Policies QOS and AVC Mobility Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name* default-policy-profile

Description default policy profile

Status **ENABLED**

Passive Client DISABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT 2-65519

WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

2. 에서 **Access Policies** 탭은 무선 클라이언트가 이 WLAN에 연결할 때 기본적으로 할당되는 VLAN을 이미지에 표시된 대로 할당합니다.

Edit Policy Profile

General **Access Policies** QOS and AVC Mobility Advanced

WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

VLAN

VLAN/VLAN Group

Multicast VLAN

WLAN ACL

IPv4 ACL

IPv6 ACL

URL Filters

Pre Auth

Post Auth

참고: 제공된 예에서는 인증 성공 시 무선 클라이언트를 특정 VLAN에 할당하는 RADIUS 서버의 작업입니다. 따라서 정책 프로파일에 구성된 VLAN이 블랙홀 VLAN일 수 있으며, RADIUS 서버는 이 매핑을 재정의하고, RADIUS 서버의 사용자 Tunnel-Group-Private-ID 필드 아래에 지정된 VLAN에 해당 WLAN을 통해 들어오는 사용자를 할당합니다.

- 에서 **Advance** 탭에서 **Allow AAA Override** RADIUS 서버가 이미지에 표시된 대로 적절한 VLAN에 클라이언트를 배치하는 데 필요한 특성을 반환할 때 WLC 컨피그레이션을 재정의하려면 확인란을 선택합니다.

Edit Policy Profile

General Access Policies QOS and AVC Mobility **Advanced**

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

NAC State

Policy Name

Fabric Profile Search or Select

Umbrella Parameter Map Not Configured

mDNS Service Policy default-mdns-service [Clear](#)

WLAN Flex Policy

VLAN Central Switching

Split MAC ACL Search or Select

Air Time Fairness Policies

2.4 GHz Policy Search or Select

5 GHz Policy Search or Select

Cancel Update & Apply to Device

5단계. 정책 태그 구성

이 절차에서는 WLC에서 정책 태그를 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

1. 다음으로 이동 **Configuration > Tags & Profiles > Tags > Policy** 이미지에 표시된 대로 새 항목을 추가합니다.

Search Menu Items

Dashboard Monitoring > Configuration > Administration > Troubleshooting

Manage Tags

Policy Site RF AP

+ Add Delete

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

10 items per page

2. Policy Tag에 이름을 추가하고 +Add, 이미지에 표시된 대로

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

3. 이미지에 표시된 대로 WLAN 프로파일을 원하는 정책 프로필에 연결합니다.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
◀ 0 ▶ 10 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

Add Policy Tag



Name*

Dynamic-VLAN

Description

Enter Description

WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> Dinamyc-VLAN	default-policy-profile

10 items per page 1 - 1 of 1 items

RLAN-POLICY Maps: 0

Cancel

Apply to Device

6단계. AP에 정책 태그 할당

이 절차에서는 WLC에서 정책 태그를 구성하는 방법에 대해 설명합니다.

다음 단계를 완료하십시오.

- 다음으로 이동 **Configuration > Wireless > Access Points > AP Name > General Tags** 관련 정책 태그를 할당한 다음 **Update & Apply to Device** 이미지에 표시된 대로

Edit AP

General Interfaces High Availability Inventory ICap Advanced

General		Version	
AP Name*	AP2802I-B-K9	Primary Software Version	16.12.4.31
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	10b3.d677.a8c0	Predownloaded Version	N/A
Ethernet MAC	084f.a9a2.8ed4	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Local	IOS Version	16.12.4.31
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8	DHCP IPv4 Address	10.10.102.101
CleanAir NSI Key		Static IP (IPv4/IPv6)	<input type="checkbox"/>
Tags		Time Statistics	
Policy	Dynamic-VLAN	Up Time	0 days 0 hrs 4 mins 52 secs
Site	default-site-tag	Controller Association Latency	1 min 36 secs

Cancel Update & Apply to Device

주의: AP의 정책 태그가 변경되면 WLC와의 연결이 끊기고 다시 조인됩니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

Windows 10 및 네이티브 서플리컨트를 연결 테스트 합니다. 사용자 이름 및 암호를 입력 하면 ISE의 VLAN에 매핑 된 사용자의 정보를 입력 합니다.

이전 예에서 RADIUS 서버에 지정된 대로 jonathga-102가 VLAN102에 할당되어 있습니다. 다음 예에서는 이 사용자 이름을 사용하여 인증을 수신하고 RADIUS 서버에서 VLAN에 할당합니다.

인증이 완료되면 전송된 RADIUS 특성에 따라 클라이언트가 적절한 VLAN에 할당되었는지 확인해야 합니다. 이 작업을 수행하려면 다음 단계를 완료하십시오.

1. 컨트롤러 GUI에서 **Monitoring > Wireless > Clients > Select the client MAC address > General > Security**

Information 이미지에 표시된 대로 VLAN 필드를 찾습니다.

The screenshot shows the Cisco Catalyst GUI for monitoring wireless clients. On the left, a list of clients is shown with one client selected (MAC: b88a.6010.3c60, IP: 10.10.102.121). On the right, the 'Client' configuration page is open, with the 'Security Information' sub-tab selected. Under the 'Server Policies' section, the 'VLAN' field is set to '102'. Other fields include 'VLAN Name' (VLAN0102) and 'VLAN' (102).

이 창에서 RADIUS 서버에 구성된 RADIUS 특성에 따라 이 클라이언트가 VLAN102에 할당되었는지 확인할 수 있습니다. CLI에서 `show wireless client summary detail` 이미지에 표시된 것과 동일한 정보를 보려면

```
Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address      SSID      AP Name      State      IP Address      Device-type      VLAN
BSSID           Auth Method Created      Connected      Protocol Channel Width SGI NSS Rate CAP Username
-----
00:00:00:10:3c:60 Dinamyc-VLAN AIR-AP2802I-A-R9 Run 10.10.105.200 Intel-Device 105
00:00:00:44:40:00 [802.1X] 05 06 11n(2.4) 1 20/20 Y/Y 1/1 24.0 E jonathga-105

Catalyst-C9800-CL#show wireless client summary detail
Number of Clients: 1

MAC Address      SSID      AP Name      State      IP Address      Device-type      VLAN
BSSID           Auth Method Created      Connected      Protocol Channel Width SGI NSS Rate CAP Username
-----
00:00:00:10:3c:60 Dinamyc-VLAN AIR-AP2802I-A-R9 Run 10.10.102.121 Intel-Device 102
00:00:00:44:40:00 [802.1X] 54 55 11n(2.4) 1 20/20 Y/Y 1/1 m5 E jonathga-102
```

2. 이(가) **Radioactive traces** RADIUS 특성을 WLC로 성공적으로 전송하도록 합니다. 이렇게 하려면 다음 단계를 수행하십시오. 컨트롤러 GUI에서 **Troubleshooting > Radioactive Trace > +Add**. 무선 클라이언트의 Mac 주소를 입력합니다. 선택 **Start**. 클라이언트를 WLAN에 연결합니다. 다음으로 이동 **Stop > Generate > Choose 10 minutes > Apply to Device > Select the trace file to download the log**.

추적 출력의 이 부분은 RADIUS 특성의 성공적인 전송을 보장합니다.

```
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Received from id
1812/60 10.10.1.24:0, Access-Accept, len 352
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: authenticator e5 5e
58 fa da 0a c7 55 - 53 55 7d 43 97 5a 8b 17
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: User-Name
[1] 13 "jonathga-102"
```

```

2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: State
[24] 40 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Class
[25] 54 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Type
[64] 6 VLAN [13]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Medium-Type
[65] 6 ALL_802 [6]
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Message
[79] 6 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Message-
Authenticator[80] 18 ...
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): 01:
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: Tunnel-Private-
Group-Id[81] 6 "102"
2021/03/21 22:22:45.236 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: EAP-Key-Name
[102] 67 *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Send-Key
[16] 52 *
2021/03/21 22:22:45.237 {wncd_x_R0-0}{1}: [radius] [25253]: (info): RADIUS: MS-MPPE-Recv-Key
[17] 52 *
2021/03/21 22:22:45.238 {wncd_x_R0-0}{1}: [eap-auth] [25253]: (info): SUCCESS for EAP method
name: PEAP on handle 0x0C000008

2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: username 0 "jonathga-102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: class 0 43 41 43 53 3a 33 33 30 32 30 41 30 41 30 30 30 30 30 33 35 35 36
45 32 32 31 36 42 3a 49 53 45 2d 32 2f 33 39 33 33 36 36 38 37 32 2f 31 31 32 36 34 30 ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: tunnel-type 1 13 [vlan] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute :
tunnel-medium-type 1 6 [ALL_802] ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
:tunnel-private-group-id 1 "102" ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [aaa-attr-inf] [25253]: (info): [ Applied attribute
: timeout 0 1800 (0x708) ]
2021/03/21 22:22:46.700 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [25253]: (info):
[0000.0000.0000:unknown] AAA override is enabled under policy profile

```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [최종 사용자 가이드](#)