Configure Dynamic VLAN Assignment with WLCs Based on ISE to Active Directory Group Map

Contents

Introduction

This document describes the concept of dynamic VLAN assignment.

Prerequisites

The document describes how to configure the wireless LAN controller (WLC) and Identity Services Engine (ISE) server in order to assign wireless LAN (WLAN) clients into a specific VLAN dynamically.

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs)
- Functional knowledge of an Authentication, Authorization, and Accounting (AAA) server such as an ISE
- Thorough knowledge of wireless networks and wireless security issues
- Functional and configurable knowledge of dynamic VLAN assignment
- Basic understanding of Microsoft Windows AD services, as well as a domain controller and DNS concepts
- Have basic knowledge of Control And Provisioning of Access Point protocol (CAPWAP)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5520 Series WLC that runs firmware release 8.8.111.0
- Cisco 4800 Series AP
- Native Windows supplicant and Anyconnect NAM
- Cisco Secure ISE version 2.3.0.298
- Microsoft Windows 2016 Server configured as a domain controller
- Cisco 3560-CX Series Switch that runs version 15.2(4)E1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Dynamic VLAN Assignment with RADIUS Server

In most WLAN systems, each WLAN has a static policy that applies to all clients associated with a Service Set Identifier (SSID), or WLAN in the controller terminology. Although powerful, this method has limitations because it requires clients to associate with different SSIDs in order to inherit different QoS and security policies.

Cisco WLAN solution addresses that limitation by the support of identity networking. This allows the network to advertise a single SSID but allows specific users to inherit different QoS, VLAN attributes, and/or security policies based on the user credential.

Dynamic VLAN assignment is one such feature that places a wireless user into a specific VLAN based on the credentials supplied by the user. This task to assign users to a specific VLAN is handled by a RADIUS authentication server, such as Cisco ISE. This can be used, for example, in order to allow the wireless host to remain on the same VLAN as it moves within a campus network.

The Cisco ISE server authenticates wireless users against one of several possible databases, which includes its internal database. For example:

- Internal DB
- Active Directory
- Generic Lightweight Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC)-compliant relational databases
- Rivest, Shamir, and Adelman (RSA) SecurID token servers
- RADIUS-compliant token servers

Cisco ISE Authentication Protocols and Supported External Identity Sources list the various authentication protocols supported by ISE internal and external databases.

This document focuses on authenticating wireless users that use Windows Active Directory external database.

After successful authentication, ISE retrieves the group information of that user from the Windows database and associates the user to the respective authorization profile.

When a client attempts to associate with a LAP registered with a controller, the LAP passes the credentials of the user to the WLC with the help of the respective EAP method.

WLC sends those credentials to ISE with the use of RADIUS protocol (encapsulating the EAP) and ISE passes the credentials of users to AD for validation with the help of the KERBEROS protocol.

AD validates the user credentials and upon successful authentication, informs the ISE.

Once the authentication is successful, the ISE server passes certain Internet Engineering Task Force (IETF) attributes to WLC. These RADIUS attributes decide the VLAN ID that must be assigned to the wireless client. The SSID (WLAN, in terms of WLC) of the client does not matter because the user is always assigned to this predetermined VLAN ID.

The RADIUS user attributes used for the VLAN ID assignment are:

- IETF 64 (Tunnel Type)â€”Set this to VLAN
- IETF 65 (Tunnel Medium Type)â€”Set this to 802
- IETF 81 (Tunnel Private Group ID)â€”Set this to VLAN ID

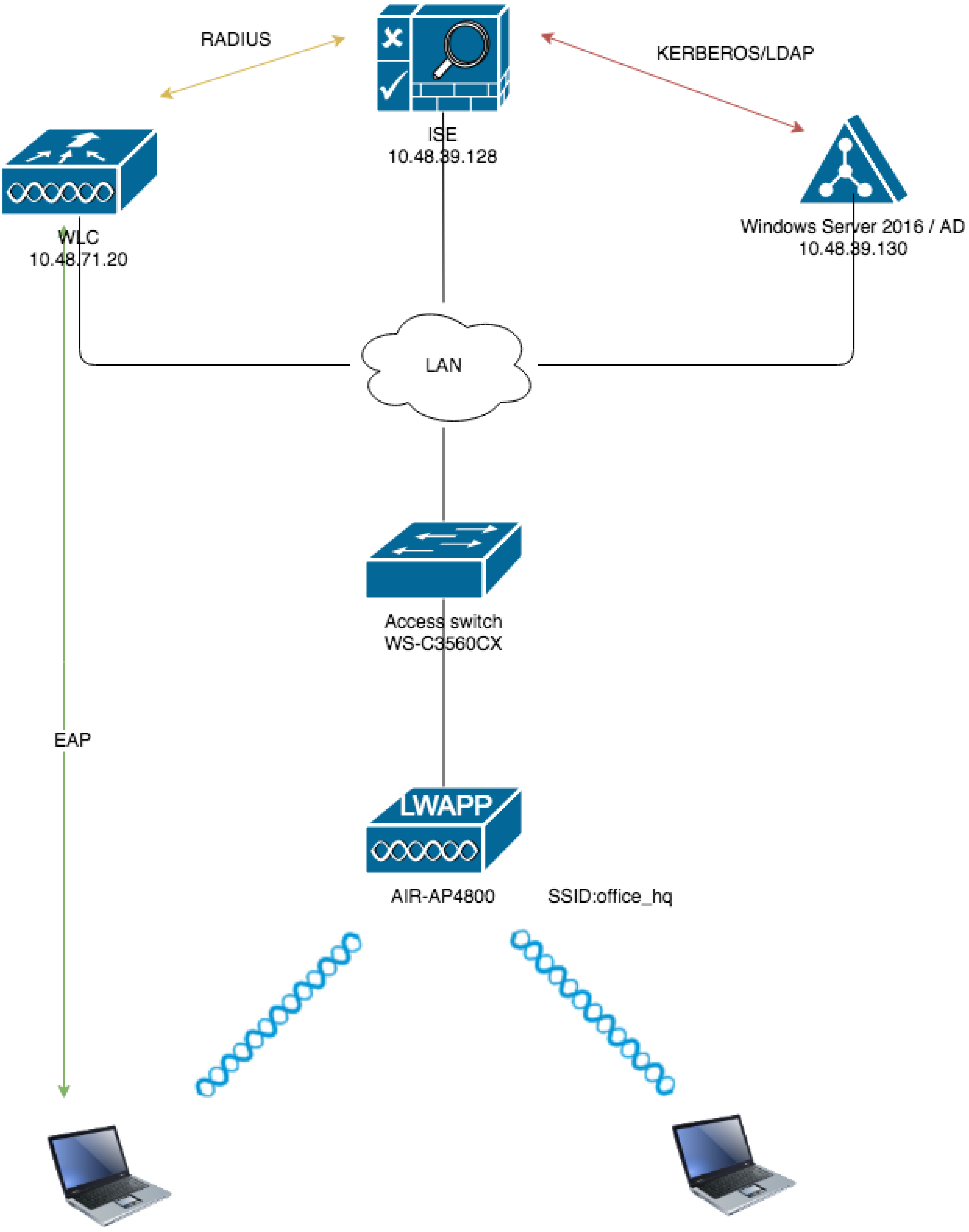
The VLAN ID is 12 bits and takes a value between 1 and 4094, inclusive. Because the Tunnel-Private-Group-ID is of type string, as defined in RFC2868 for use with IEEE 802.1X, the VLAN ID integer value is encoded as a string. When these tunnel attributes are sent, it is necessary to fill in the Tag field.

As noted in RFC 2868, section 3.1: the Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. Valid values for this field are 0x01 through 0x1F, inclusive. If the Tag field is unused, it must be zero (0x00). Refer to **RFC 2868** for more information on all RADIUS attributes.

Configure

This section provides the information needed to configure the described features in the document.

Network Diagram



Configurations

These are the configuration details of the components used in this diagram:

- The IP address of the ISE (RADIUS) server is 10.48.39.128.
- The Management and AP-manager Interface address of the WLC is 10.48.71.20.
- DHCP server resides in the LAN network and is configured for respective client pools; it is not shown

in the diagram.

- VLAN1477 and VLAN1478 are used throughout this configuration. Users from the **Marketing** department are configured in order to be placed into the VLAN1477 and users from the **HR** department are configured in order to be placed into VLAN1478 by the RADIUS server when both users connect to the same SSID â€• **office_hq**.

  VLAN1477: 192.168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1

- This document uses 802.1x with PEAP-mschapv2 as the security mechanism.

> **Note**: Cisco recommends that you use advanced authentication methods, such as EAP-FAST and EAP-TLS authentication, in order to secure the WLAN.

These assumptions are made before you perform this configuration:

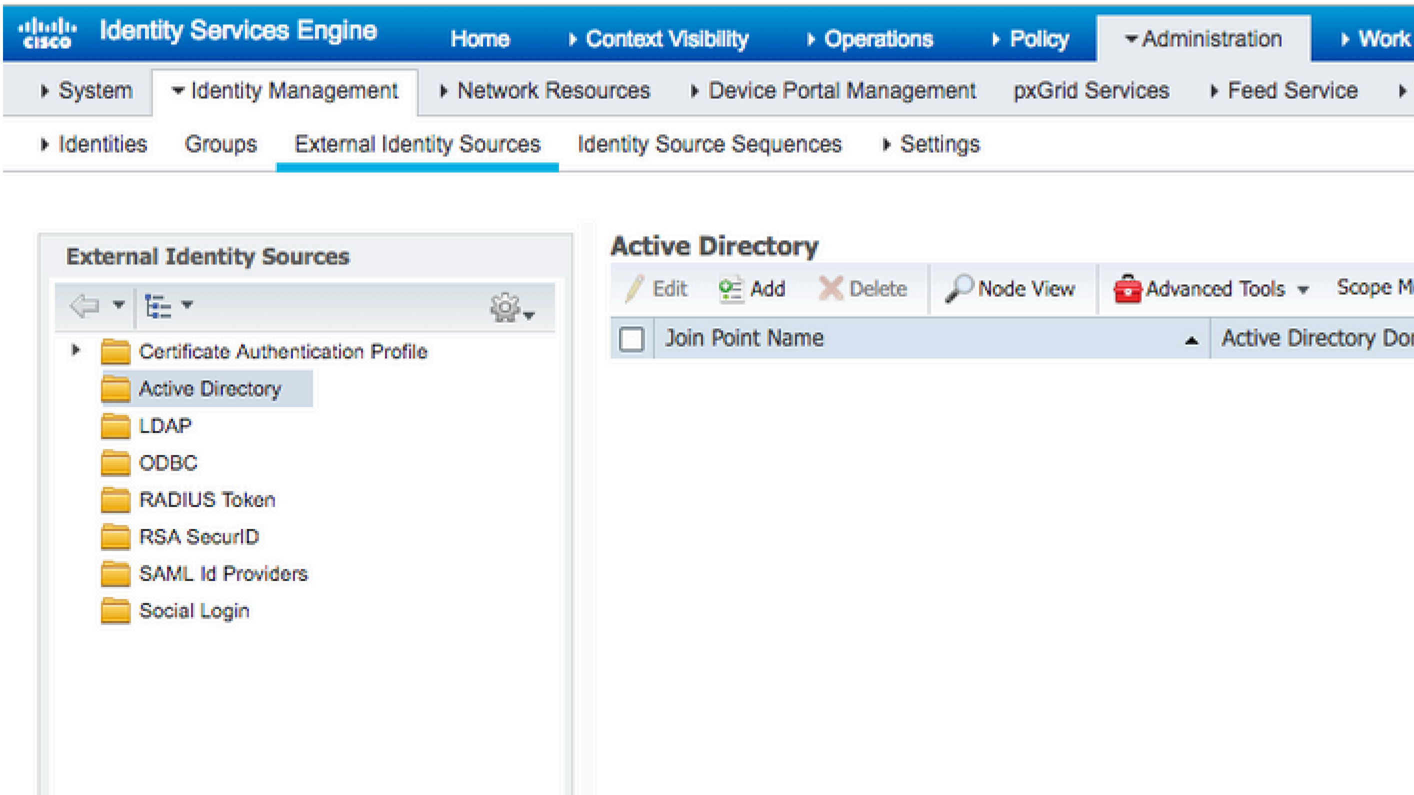
- The LAP is already registered with the WLC
- The DHCP server is assigned a DHCP scope
- Layer 3 connectivity exists between all devices in the network
- The document discusses the configuration required on the wireless side and assumes that the wired network is in place
- Respective users and groups are configured on AD

In order to accomplish dynamic VLAN assignment with WLCs based on ISE to AD group mapping, these steps must be performed:

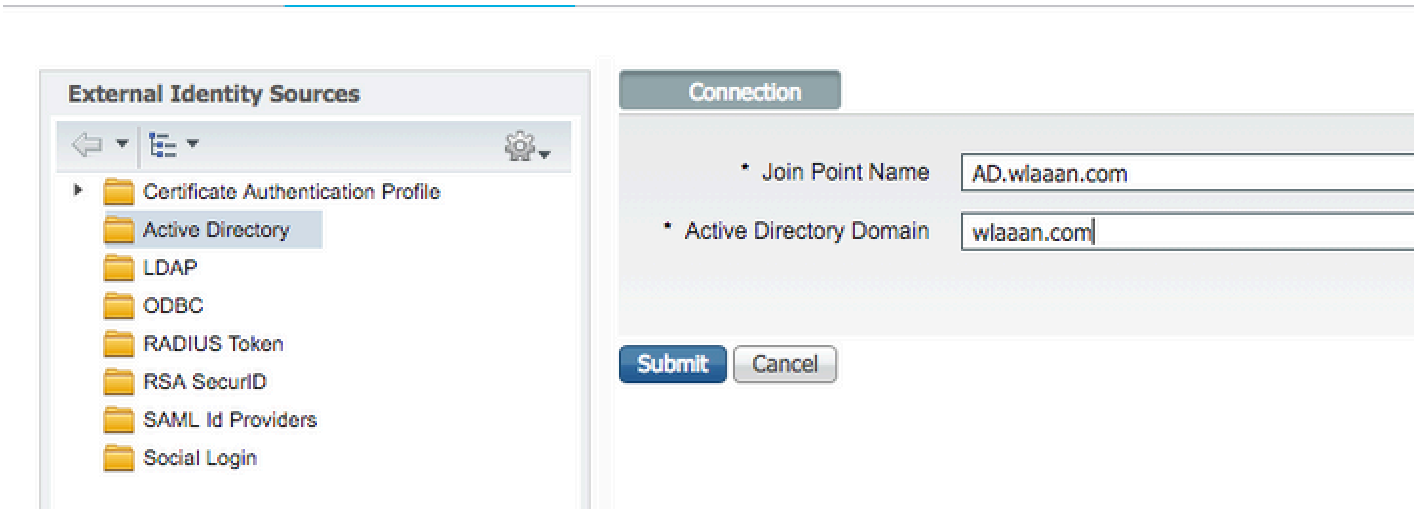
1. ISE to AD integration and configuration of authentication and authorization policies for users on ISE.
2. WLC configuration in order to support dot1x authentication and AAA override for SSID 'office_hq'.
3. End client supplicant configuration.

ISE to AD Integration and Configuration of Authentication and Authorization Policies for Users on ISE

1. Login to the ISE Web UI interface using an **admin** account.
2. Navigate to Administration > Identity management > External Identity Sources > Active directory.



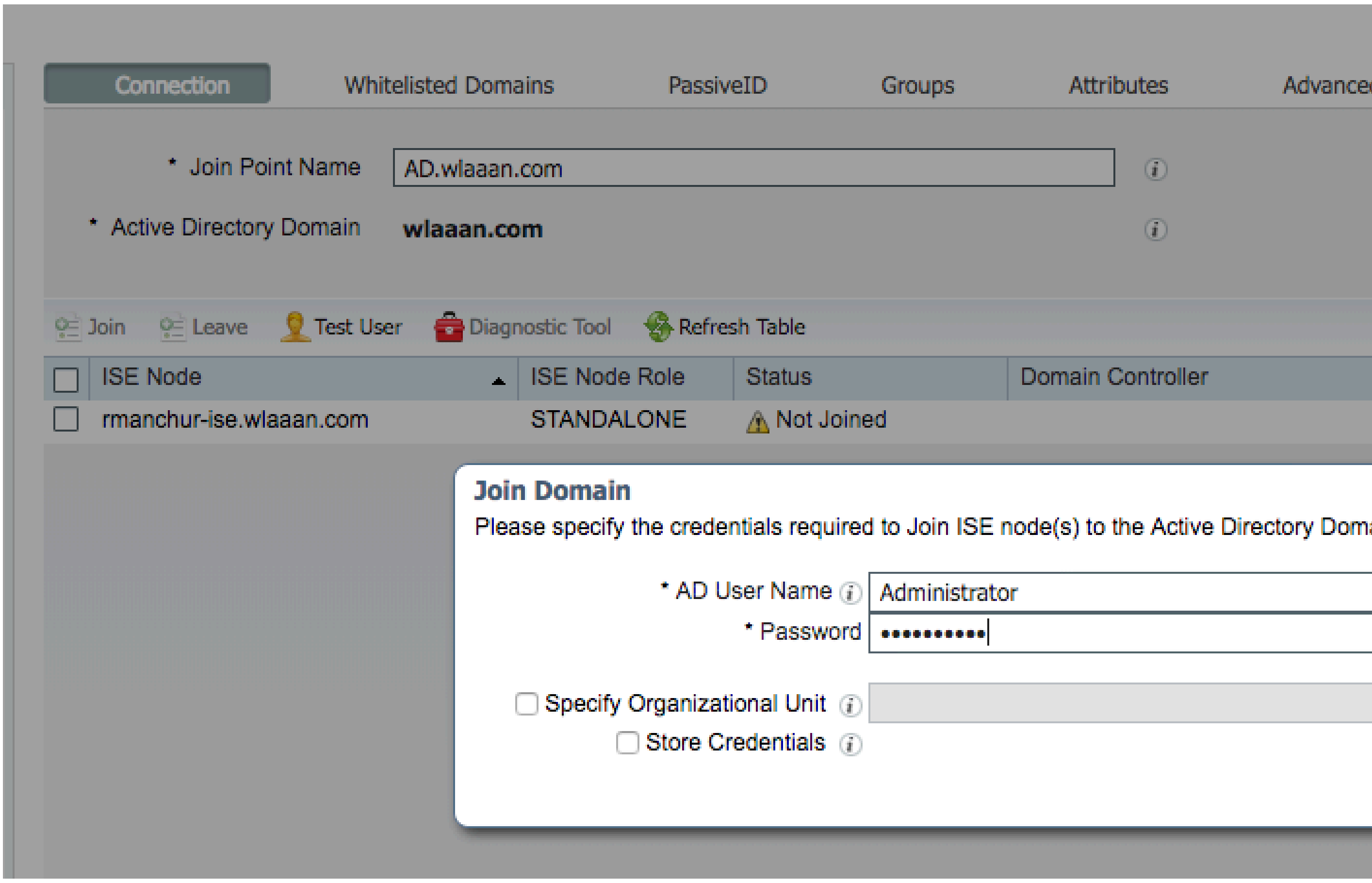
3. Click **Add** and enter the domain name and identity store name from the Active Directory Join Point Name settings. In the example, ISE is registered to the domain wlaaan.com and joinpoint is specified as AD.wlaaan.com - locally significant name to ISE.



* Join Point Name: AD.wlaaan.com

* Active Directory Domain: wlaaan.com

4. A pop-up window opens after Submit button is pressed that asks you if you want to join ISE to AD immediately. Press Yes and provide Active Directory user credentials with admin rights to add a new host to the domain.



Connection | Whitelisted Domains | PassiveID | Groups | Attributes | Advance

* Join Point Name: AD.wlaaan.com

* Active Directory Domain: **wlaaan.com**

Join | Leave | Test User | Diagnostic Tool | Refresh Table

□ ISE Node	ISE Node Role	Status	Domain Controller
□ rmanchur-ise.wlaaan.com	STANDALONE	⚠ Not Joined	

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Doma

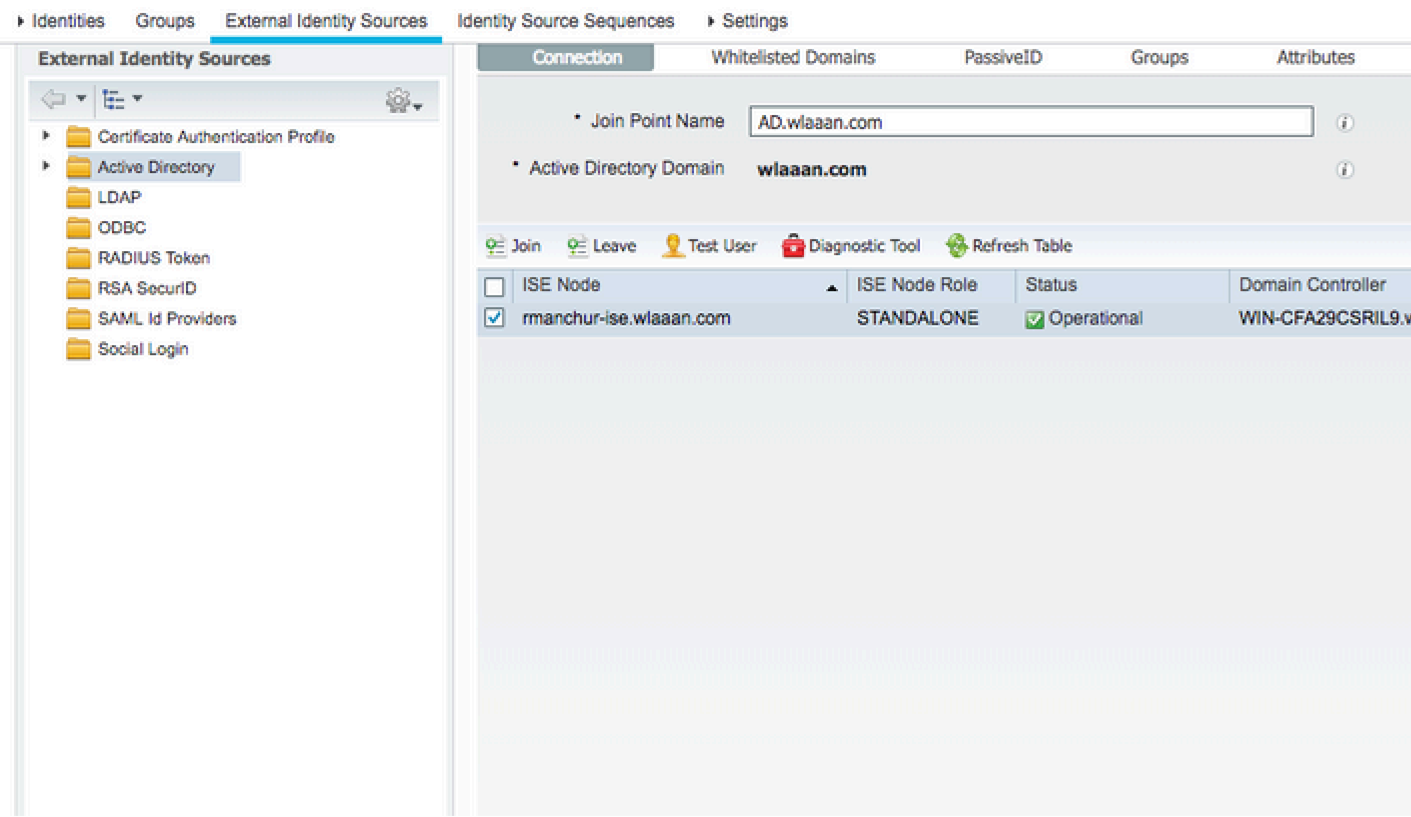
* AD User Name: Administrator

* Password: ••••••••••

□ Specify Organizational Unit

□ Store Credentials

5. After this point, you must have ISE successfully registered to AD.



Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Connection | Whitelisted Domains | PassiveID | Groups | Attributes

* Join Point Name: AD.wlaaan.com

* Active Directory Domain: **wlaaan.com**

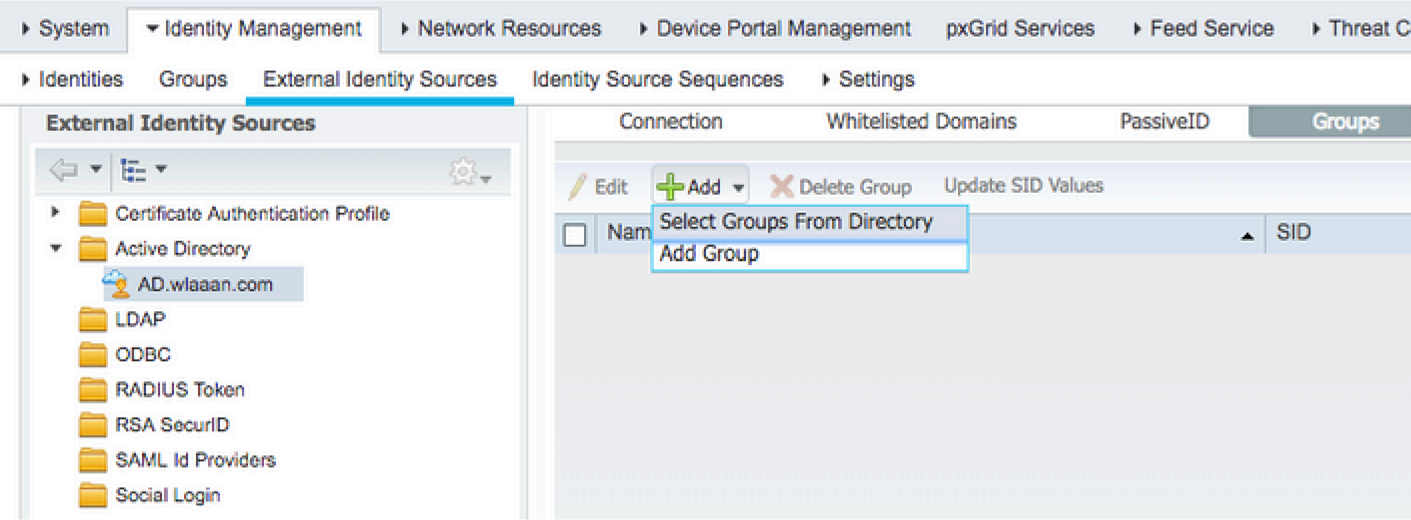
Join | Leave | Test User | Diagnostic Tool | Refresh Table

□ ISE Node	ISE Node Role	Status	Domain Controller
☑ rmanchur-ise.wlaaan.com	STANDALONE	☑ Operational	WIN-CFA29CSRIL9.v

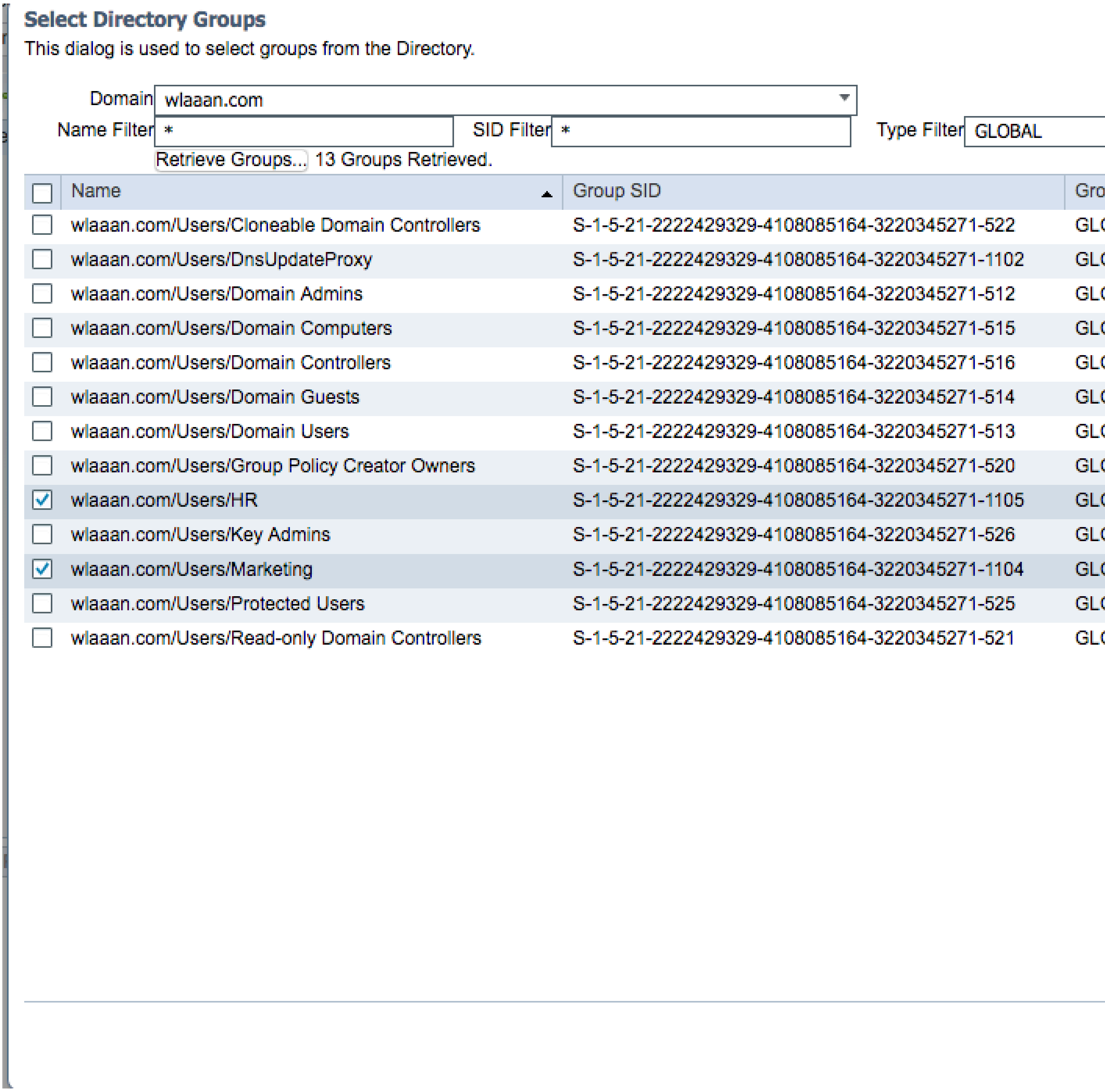
In case you have any issues with the registration process, you can use the Diagnostic Tool in order to run the tests required for AD connectivity.

6. You must retrieve groups for the active Directories that are used in order to assign respective

authorization profiles. Navigate to Administration > Identity management > External Identity Sources > Active directory > <Your AD> > Groups, then click Add and choose Select Groups from Active Directory.



7. A new pop-up window opens where you can either specify a filter in order to retrieve specific group(s) or retrieve all groups from AD.
   Choose the respective groups from the AD group list and press OK.



Select Directory Groups

This dialog is used to select groups from the Directory.

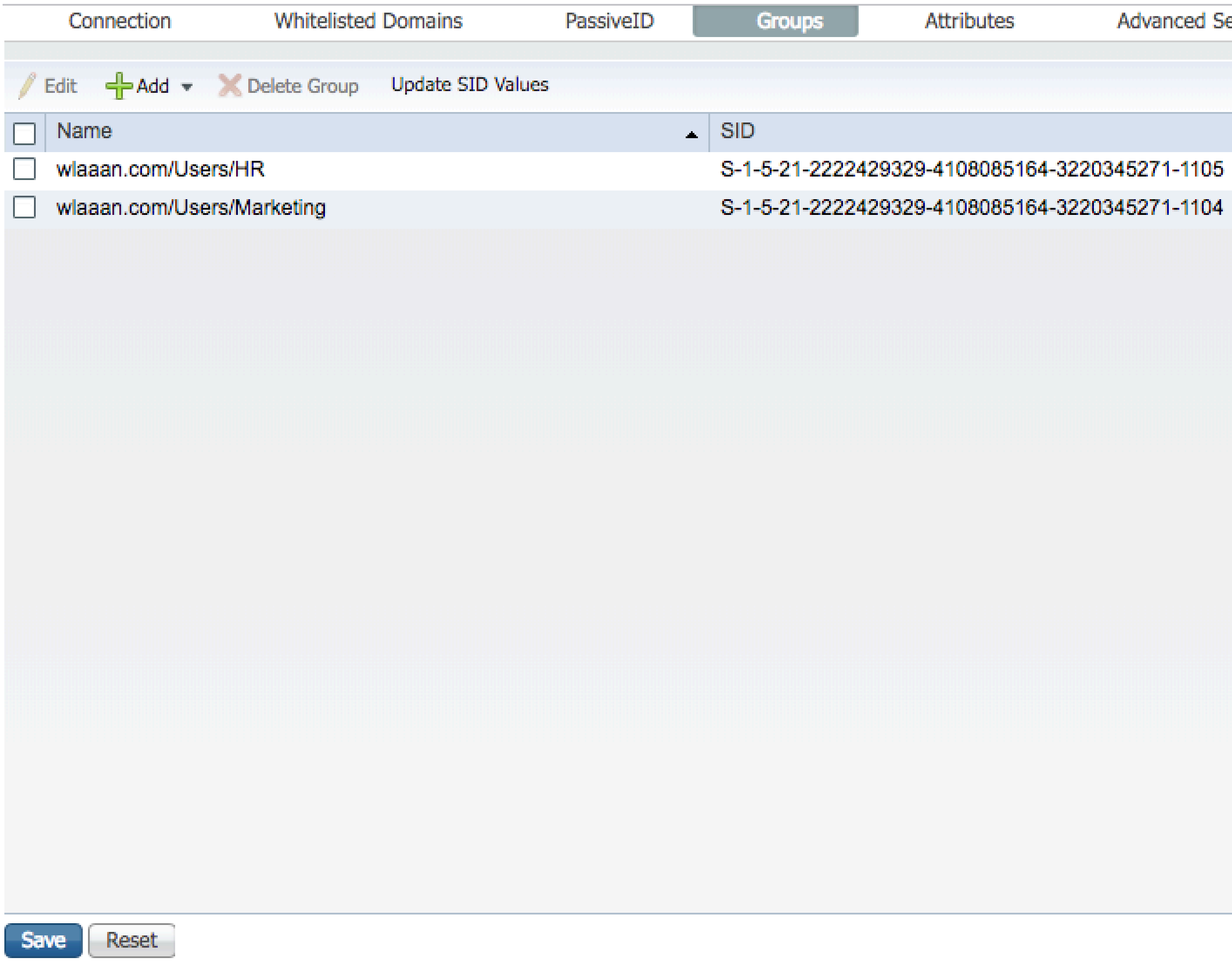
Domain wlaaan.com

Name Filter * SID Filter * Type Filter GLOBAL

Retrieve Groups... 13 Groups Retrieved.

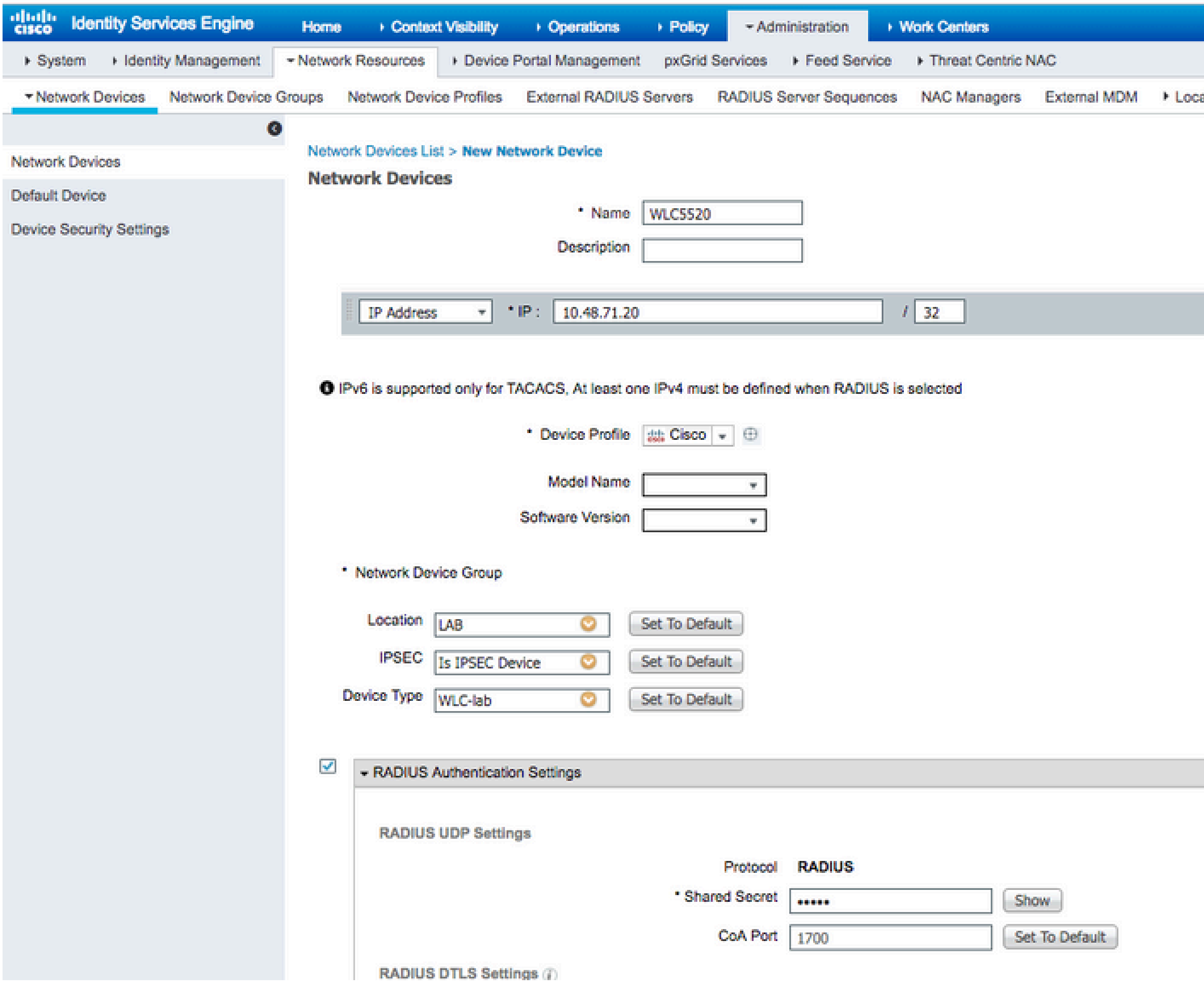
☐	Name	Group SID	Gro
☐	wlaaan.com/Users/Cloneable Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-522	GL
☐	wlaaan.com/Users/DnsUpdateProxy	S-1-5-21-2222429329-4108085164-3220345271-1102	GL
☐	wlaaan.com/Users/Domain Admins	S-1-5-21-2222429329-4108085164-3220345271-512	GL
☐	wlaaan.com/Users/Domain Computers	S-1-5-21-2222429329-4108085164-3220345271-515	GL
☐	wlaaan.com/Users/Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-516	GL
☐	wlaaan.com/Users/Domain Guests	S-1-5-21-2222429329-4108085164-3220345271-514	GL
☐	wlaaan.com/Users/Domain Users	S-1-5-21-2222429329-4108085164-3220345271-513	GL
☐	wlaaan.com/Users/Group Policy Creator Owners	S-1-5-21-2222429329-4108085164-3220345271-520	GL
☑	wlaaan.com/Users/HR	S-1-5-21-2222429329-4108085164-3220345271-1105	GL
☐	wlaaan.com/Users/Key Admins	S-1-5-21-2222429329-4108085164-3220345271-526	GL
☑	wlaaan.com/Users/Marketing	S-1-5-21-2222429329-4108085164-3220345271-1104	GL
☐	wlaaan.com/Users/Protected Users	S-1-5-21-2222429329-4108085164-3220345271-525	GL
☐	wlaaan.com/Users/Read-only Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-521	GL

8. Respective Groups are added to ISE and can be saved. Press Save.



□	Name	SID
□	wlaaan.com/Users/HR	S-1-5-21-2222429329-4108085164-3220345271-1105
□	wlaaan.com/Users/Marketing	S-1-5-21-2222429329-4108085164-3220345271-1104

9. Add WLC to the ISE Network device list - navigate to Administration > Network Resources > Network Devices and press Add.
   Complete configuration, by providing WLC management IP address and RADIUS shared secret between WLC and ISE.



Network Devices

* Name: WLC5520

Description:

IP Address * IP : 10.48.71.20 / 32

IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: LAB

IPSEC: Is IPSEC Device

Device Type: WLC-lab

☑ RADIUS Authentication Settings

RADIUS UDP Settings

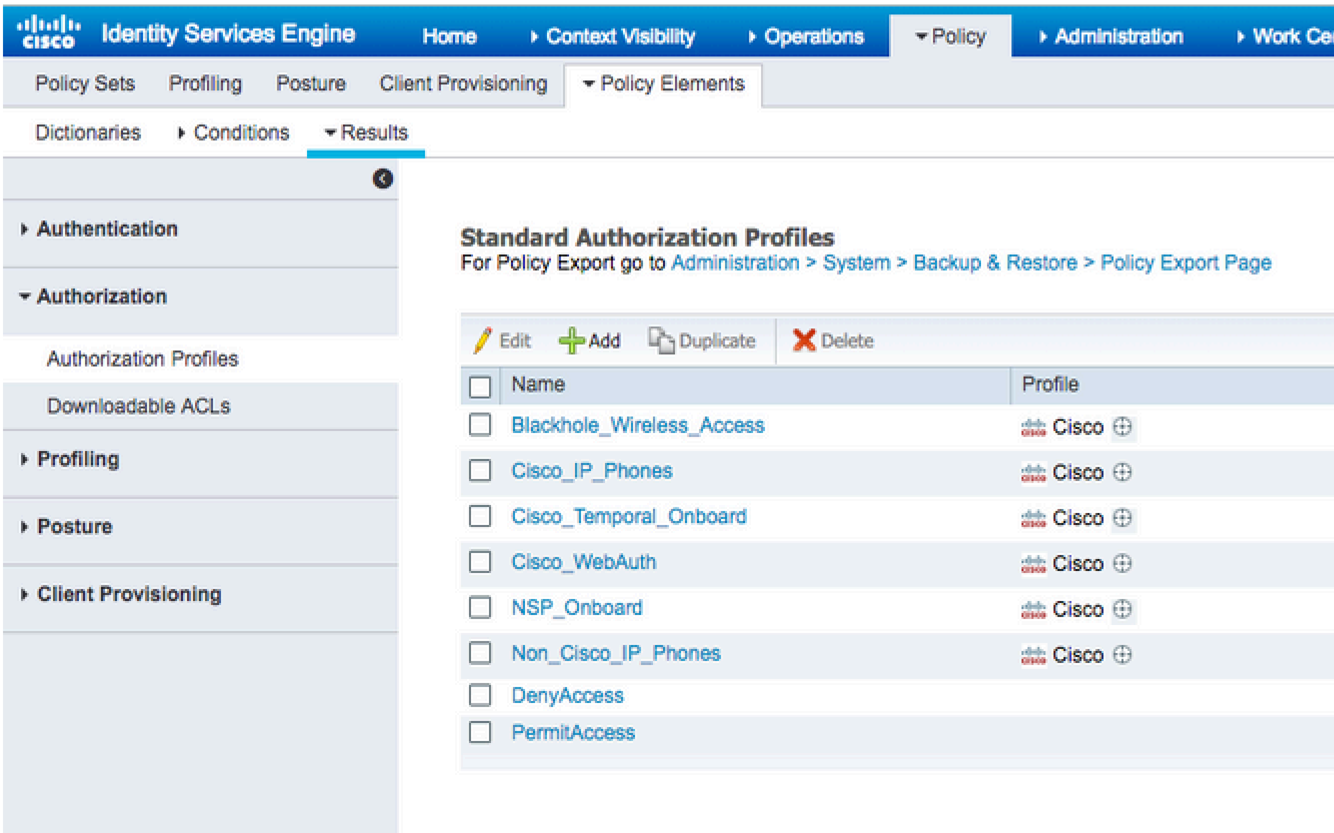
Protocol: RADIUS

* Shared Secret: •••••

CoA Port: 1700

RADIUS DTLS Settings

10. Now after you joined ISE to AD and added the WLC to the device list, you can start the configuration of authentication and authorization policies for users.
    - Create an authorization profile in order to assign users from **Marketing** to **VLAN1477** and from the **HR** group to **VLAN1478**.
      Navigate to Policy > Policy Elements > Results > Authorization > Authorization profiles and click the Add button in order to create a new profile.

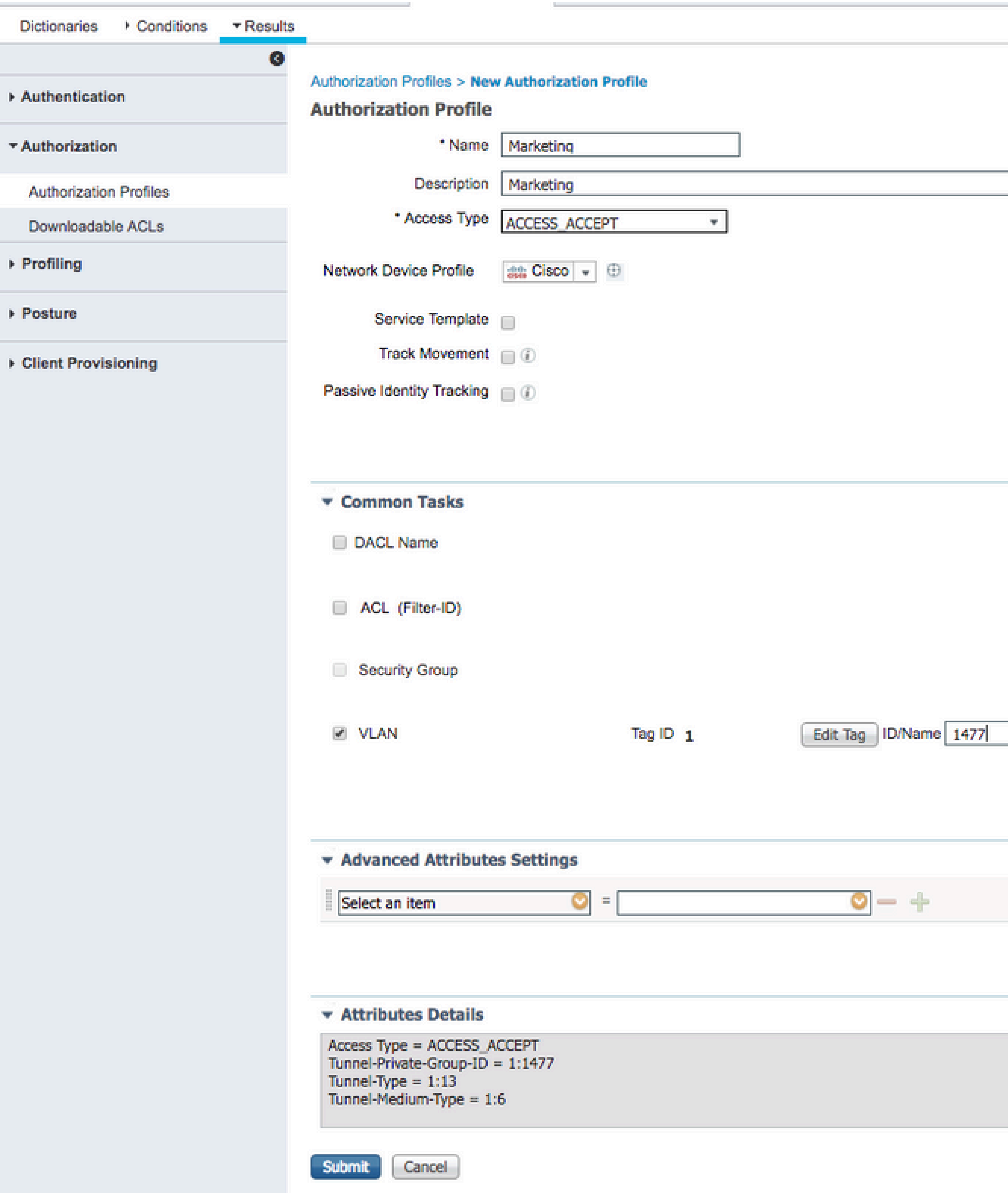


Standard Authorization Profiles

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Name	Profile
□	Blackhole_Wireless_Access	Cisco ⊕
□	Cisco_IP_Phones	Cisco ⊕
□	Cisco_Temporal_Onboard	Cisco ⊕
□	Cisco_WebAuth	Cisco ⊕
□	NSP_Onboard	Cisco ⊕
□	Non_Cisco_IP_Phones	Cisco ⊕
□	DenyAccess	
□	PermitAccess	

- Complete the authorization profile configuration with VLAN information for the respective group; the example shows Marketing group configuration settings.



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name: Marketing

Description: Marketing

* 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 ID/Name 1477

Advanced Attributes Settings

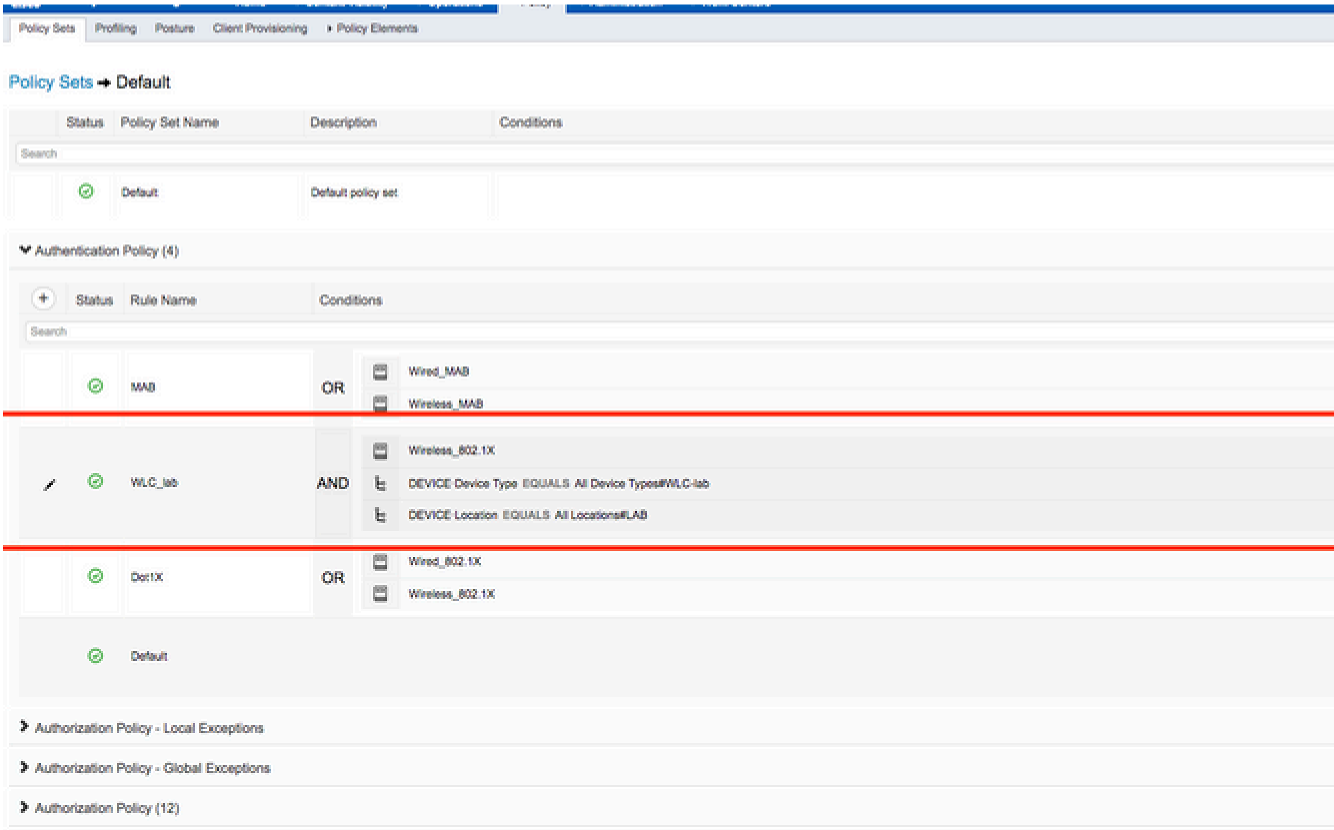
Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:1477
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Similar configuration must be done for other groups and respective VLAN tag attributes must be configured.

- After authorization profiles are configured, you can define authentication policies for wireless users. This can be done either by configuring Custom or modifying the Default Policy set. In this example, the Default policy set is modified. Navigate to Policy > Policy Sets > Default. By default for dot1x authentication type, ISE is going to use All_User_ID_Stores, although it works even with current default settings since **AD** is part of the identity source list of All_User_ID_Stores, this example uses a more specific rule WLC_lab for that respective LAB controller and uses **AD** as the only source for authentication.



Policy Sets → Default

Status	Policy Set Name	Description	Conditions
✓	Default	Default policy set	

Authentication Policy (4)

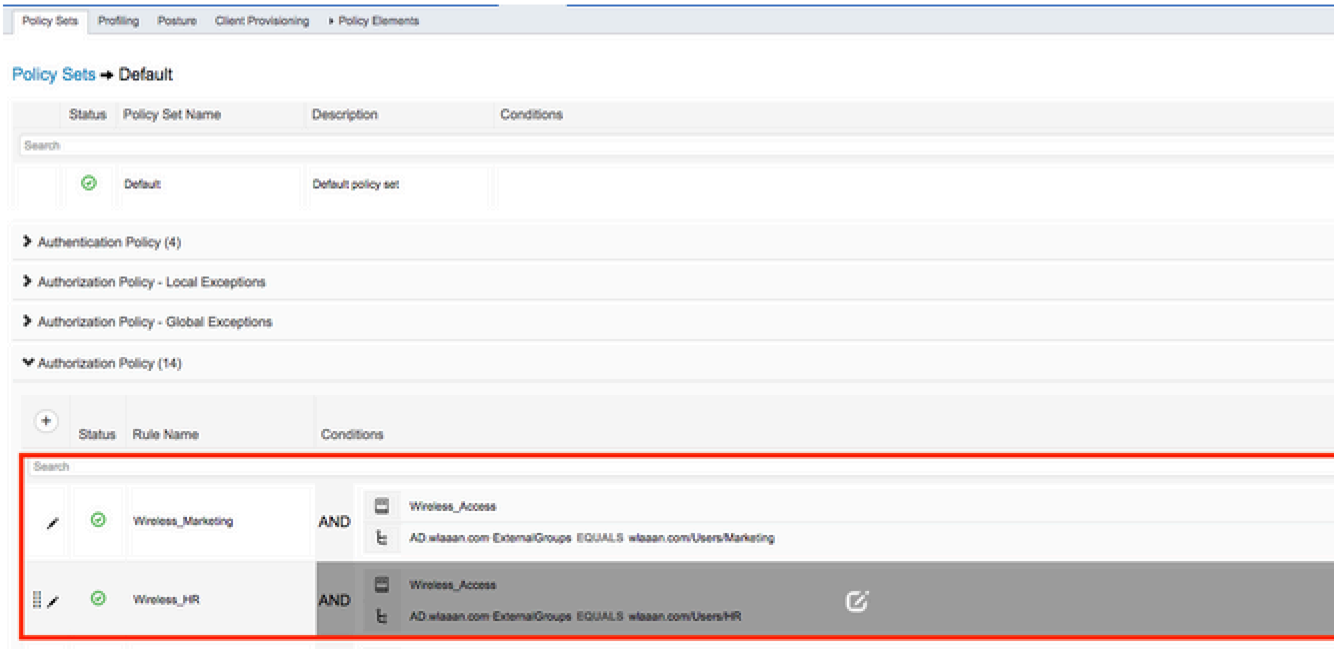
Status	Rule Name	Conditions
✓	MAB	OR Wired_MAB Wireless_MAB
✓	WLC_lab	AND Wireless_802.1X DEVICE·Device Type EQUALS All Device Types#WLC-lab DEVICE·Location EQUALS All Locations#LAB
✓	Dot1X	OR Wired_802.1X Wireless_802.1X
✓	Default	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (12)

- Now you must create authorization policies for users that assign respective authorization profiles based on group membership. Navigate to Authorization policy section and create policies in order to accomplish that requirement.



Policy Sets → Default

Status	Policy Set Name	Description	Conditions
✓	Default	Default policy set	

Authentication Policy (4)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

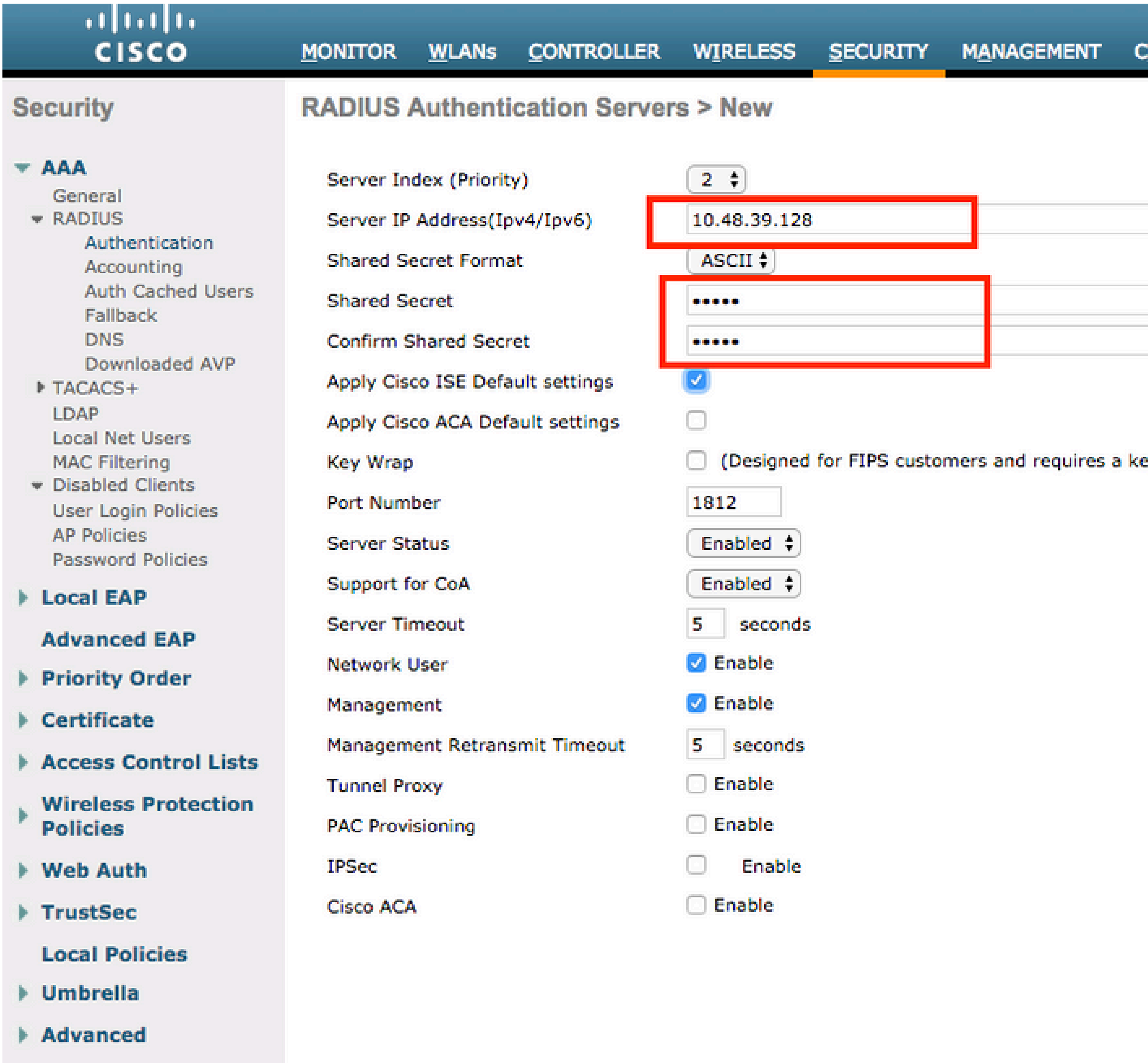
Authorization Policy (14)

Status	Rule Name	Conditions
✓	Wireless_Marketing	AND Wireless_Access AD·wlaaan.com·ExternalGroups EQUALS wlaaan.com/Users/Marketing
✓	Wireless_HR	AND Wireless_Access AD·wlaaan.com·ExternalGroups EQUALS wlaaan.com/Users/HR

WLC Configuration to Support dot1x Authentication and AAA Override for SSID 'office_hq'

1. Configure ISE as a RADIUS authentication server on WLC. Navigate to Security > AAA > RADIUS > Authentication section in the web UI interface and provide the ISE IP address and shared secret

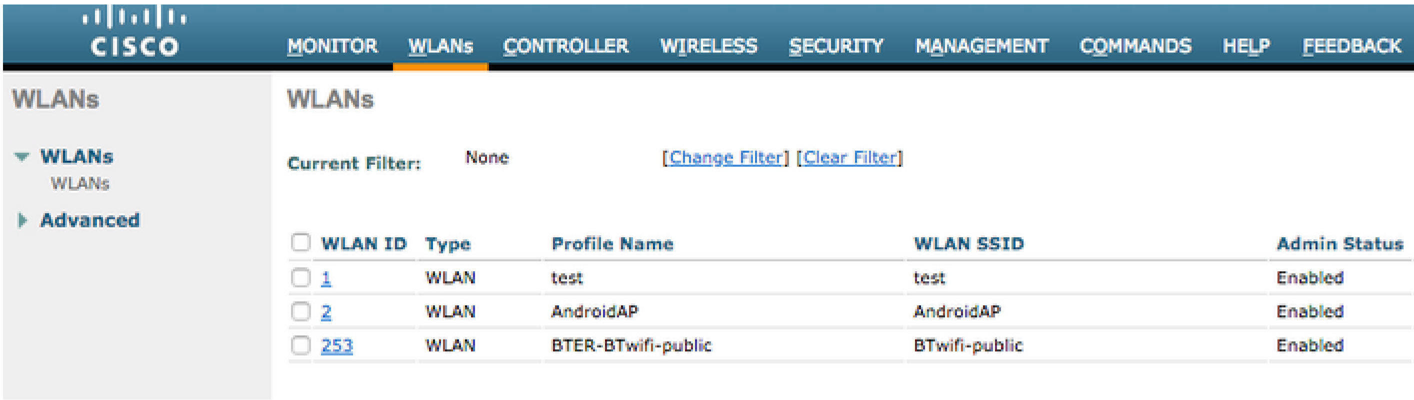
information.



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IP Address(Ipv4/Ipv6)	10.48.39.128
Shared Secret Format	ASCII
Shared Secret	•••••
Confirm Shared Secret	•••••
Apply Cisco ISE Default settings	☑
Apply Cisco ACA Default settings	□
Key Wrap	□ (Designed for FIPS customers and requires a ke
Port Number	1812
Server Status	Enabled
Support for CoA	Enabled
Server Timeout	5 seconds
Network User	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	□ Enable
PAC Provisioning	□ Enable
IPSec	□ Enable
Cisco ACA	□ Enable

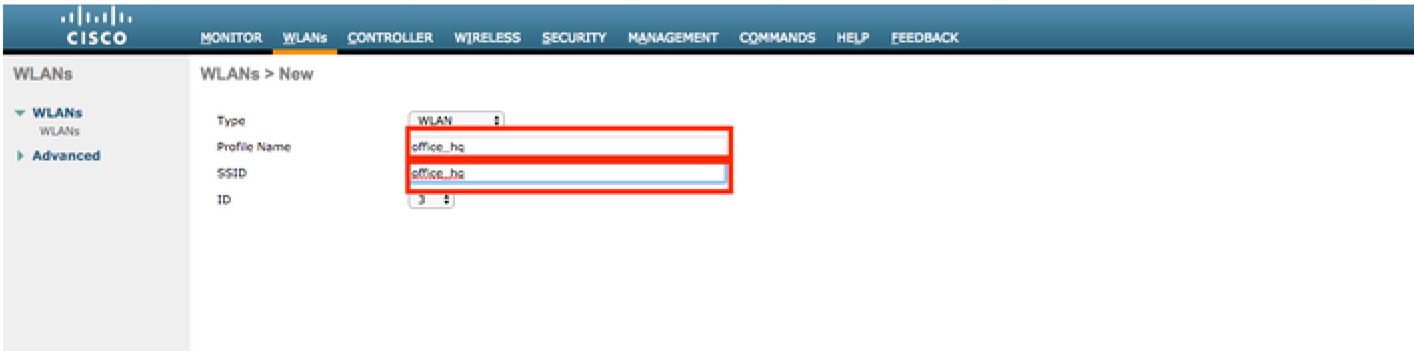
2. Configure SSID office_hq under the WLANs section on the WLC; this example configures SSID with WPA2/AES+dot1x and AAA override. Interface Dummy is chosen for the WLAN since the proper VLAN is assigned via RADIUS anyway. This dummy interface must be created on the WLC and given an IP address, but the IP address does not have to be valid and the VLAN in which it is put can not be created in the uplink switch so that if no VLAN is being assigned, the client cannot go anywhere.



WLANs

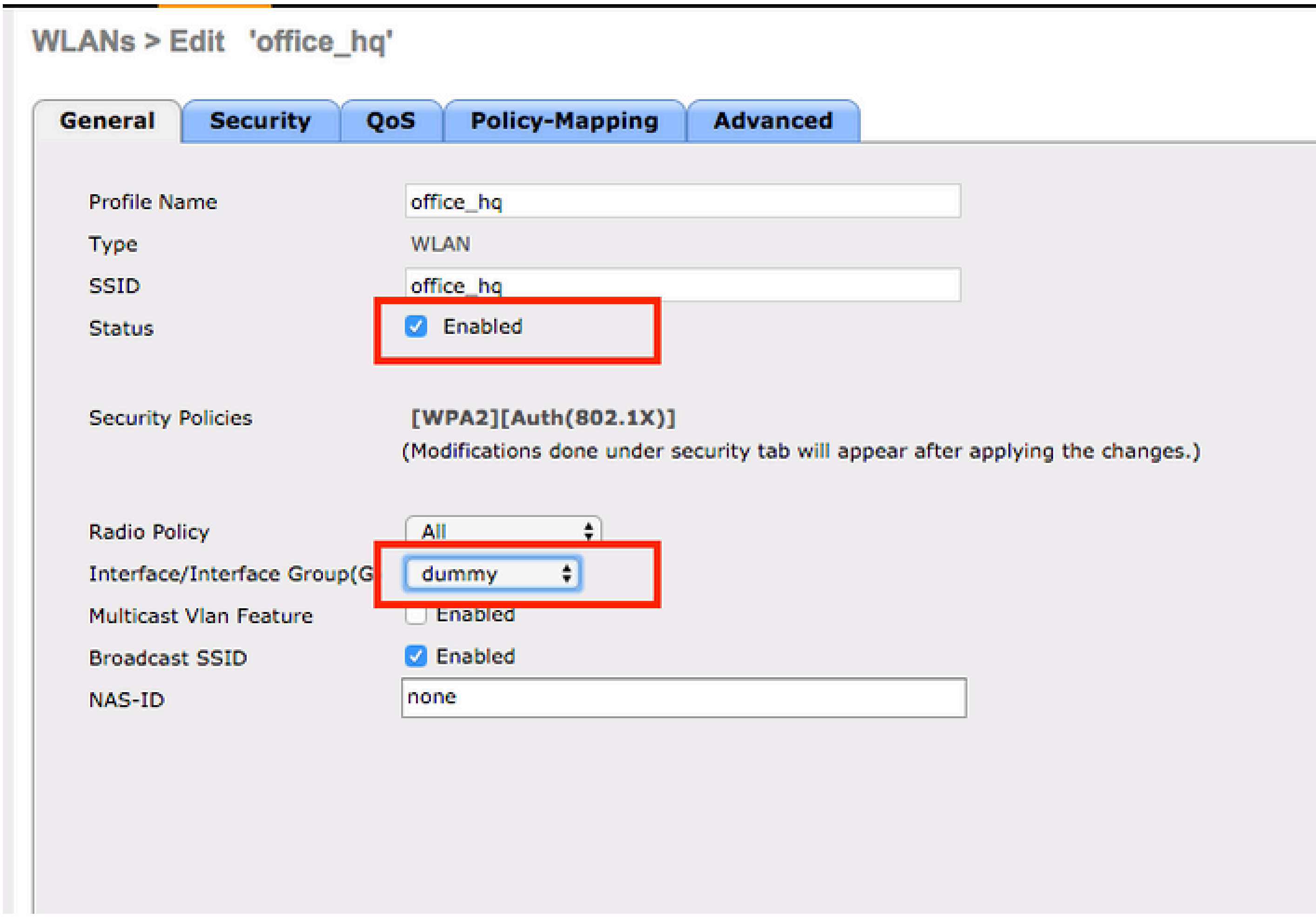
Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status
□ 1	WLAN	test	test	Enabled
□ 2	WLAN	AndroidAP	AndroidAP	Enabled
□ 253	WLAN	BTER-BTwifi-public	BTwifi-public	Enabled



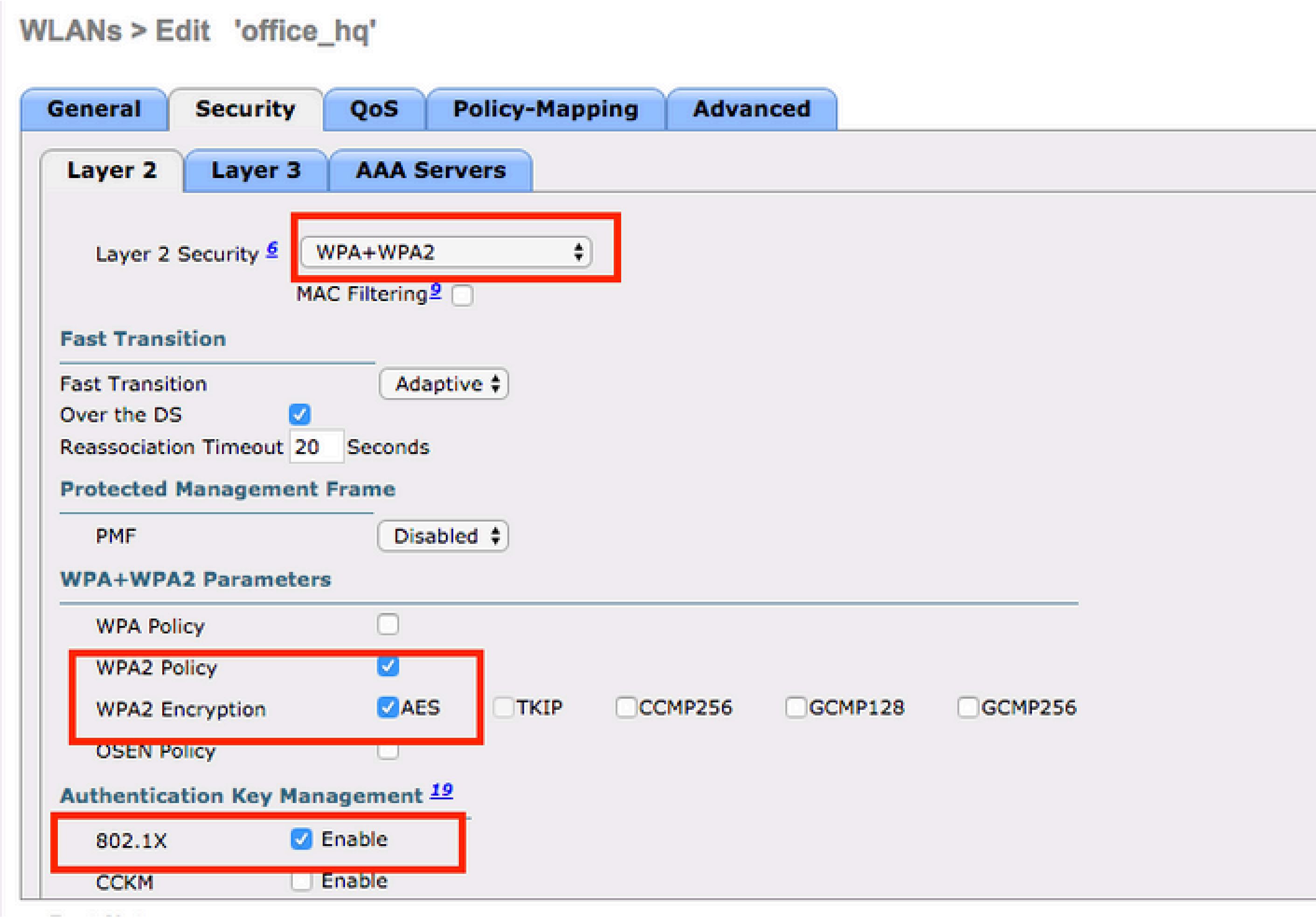
WLANs > New

Type	WLAN
Profile Name	office_hq
SSID	office_hq
ID	3



WLANs > Edit 'office_hq'

Profile Name	office_hq
Type	WLAN
SSID	office_hq
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G	dummy
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none



WLANs > Edit 'office_hq'

Layer 2 Security[6] WPA+WPA2

MAC Filtering[9] □

Fast Transition

Fast Transition Adaptive

Over the DS ☑

Reassociation Timeout 20 Seconds

Protected Management Frame

PMF Disabled

WPA+WPA2 Parameters

WPA Policy □

WPA2 Policy ☑

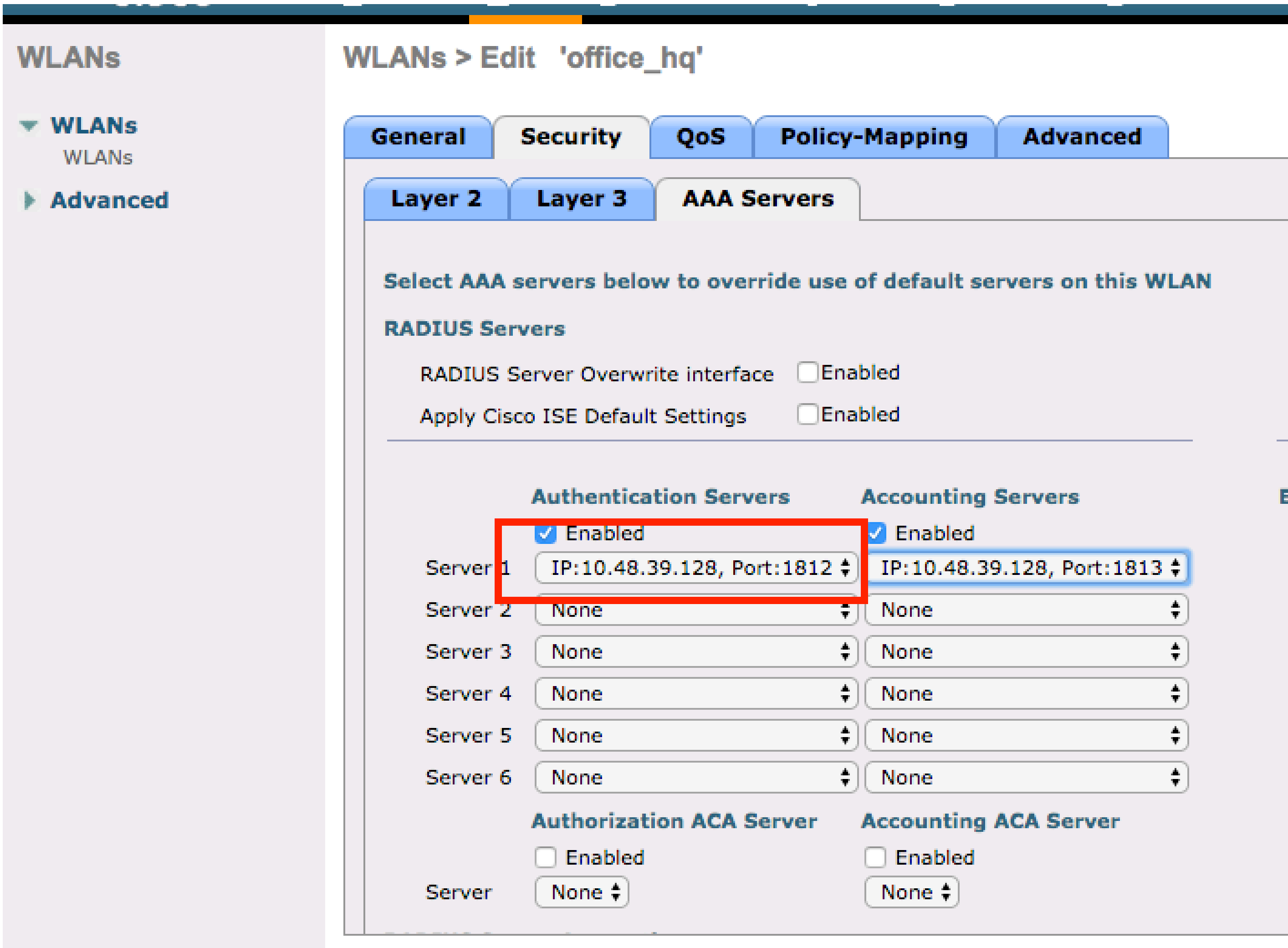
WPA2 Encryption ☑AES □TKIP □CCMP256 □GCMP128 □GCMP256

OSEN Policy □

Authentication Key Management[19]

802.1X ☑ Enable

CCKM □ Enable



WLANs

- WLANs
  - WLANs
- Advanced

WLANs > Edit 'office_hq'

General | Security | QoS | Policy-Mapping | Advanced
Layer 2 | Layer 3 | AAA Servers

Select AAA servers below to override use of default servers on this WLAN

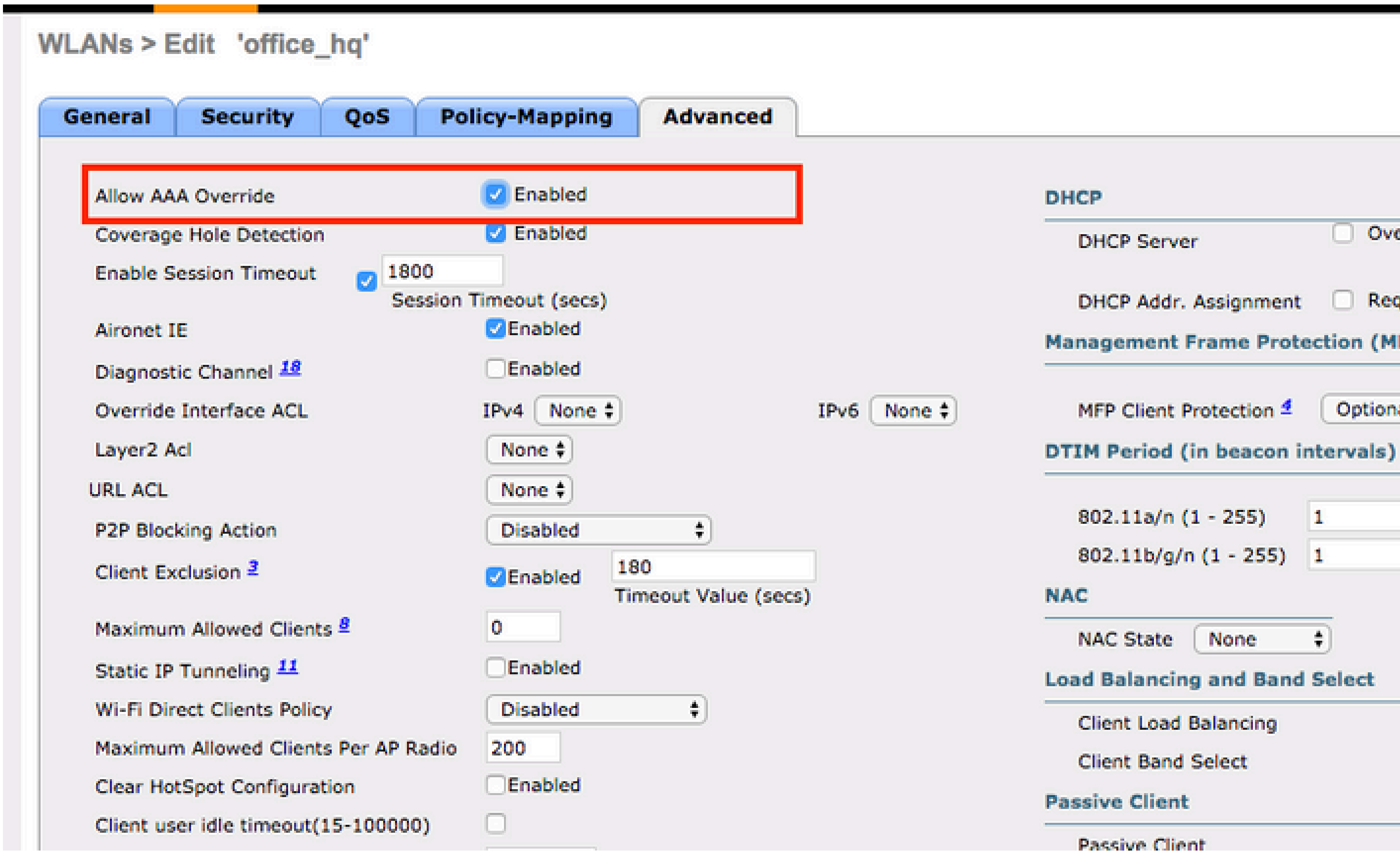
RADIUS Servers

RADIUS Server Overwrite interface □Enabled

Apply Cisco ISE Default Settings □Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.48.39.128, Port:1812	IP:10.48.39.128, Port:1813
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

	Authorization ACA Server	Accounting ACA Server
	□ Enabled	□ Enabled
Server	None	None



WLANs > Edit 'office_hq'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑Enabled

Diagnostic Channel 18 □Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion 3 ☑Enabled 180 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling 11 □Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

Clear HotSpot Configuration □Enabled

Client user idle timeout(15-100000) □

DHCP

DHCP Server □ Ove

DHCP Addr. Assignment □ Req

Management Frame Protection (MI

MFP Client Protection 4 Option

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

Load Balancing and Band Select

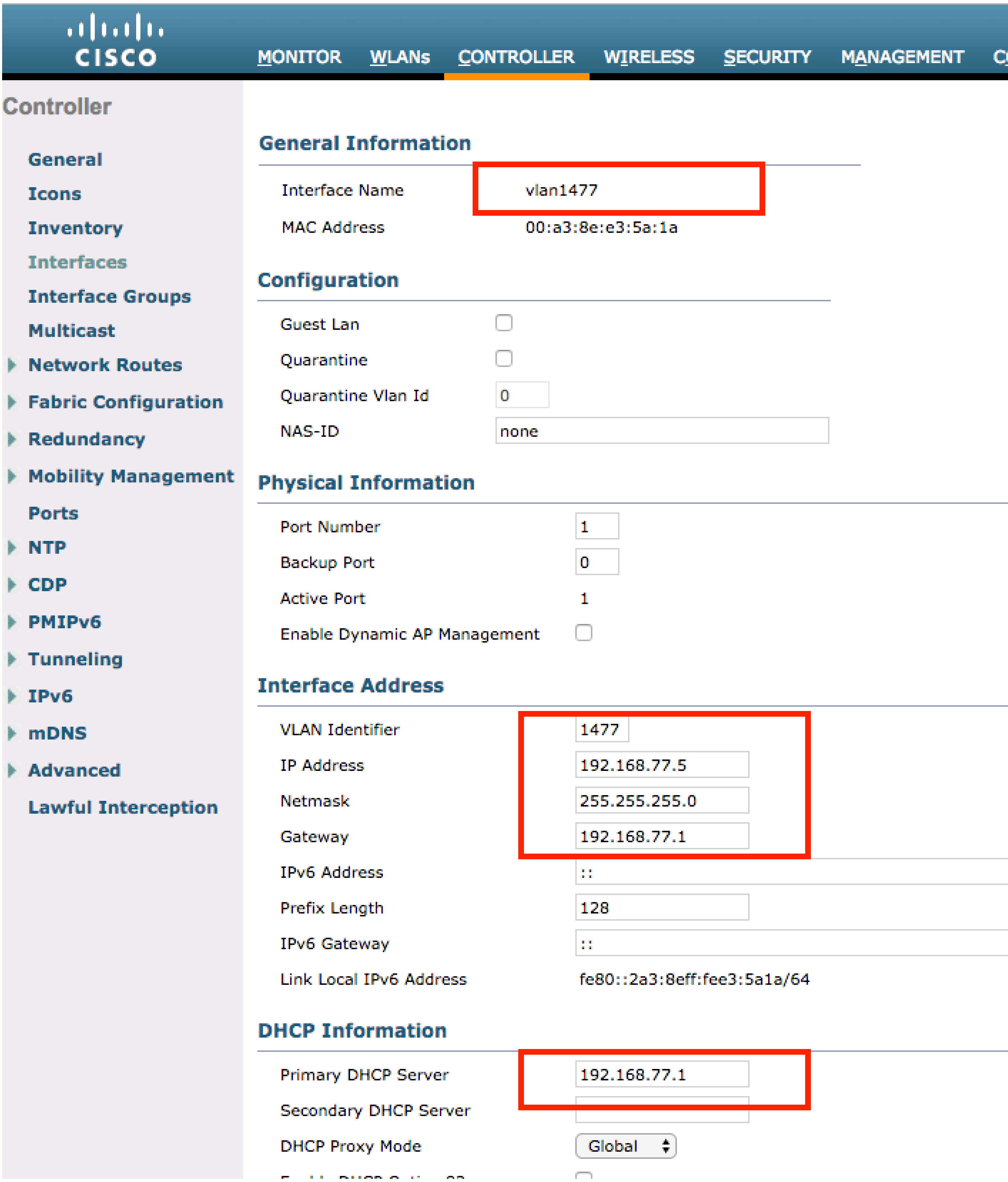
Client Load Balancing

Client Band Select

Passive Client

Passive Client

3. You must also create dynamic interfaces on the WLC for user VLANs. Navigate to Controller > Interfaces UI menu. The WLC can only honor the VLAN assignment received via AAA if it has a dynamic interface in that VLAN.



General Information

Interface Name	vlan1477
MAC Address	00:a3:8e:e3:5a:1a

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0
NAS-ID	none

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	1477
IP Address	192.168.77.5
Netmask	255.255.255.0
Gateway	192.168.77.1
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::2a3:8eff:fee3:5a1a/64

DHCP Information

Primary DHCP Server	192.168.77.1
Secondary DHCP Server	
DHCP Proxy Mode	Global

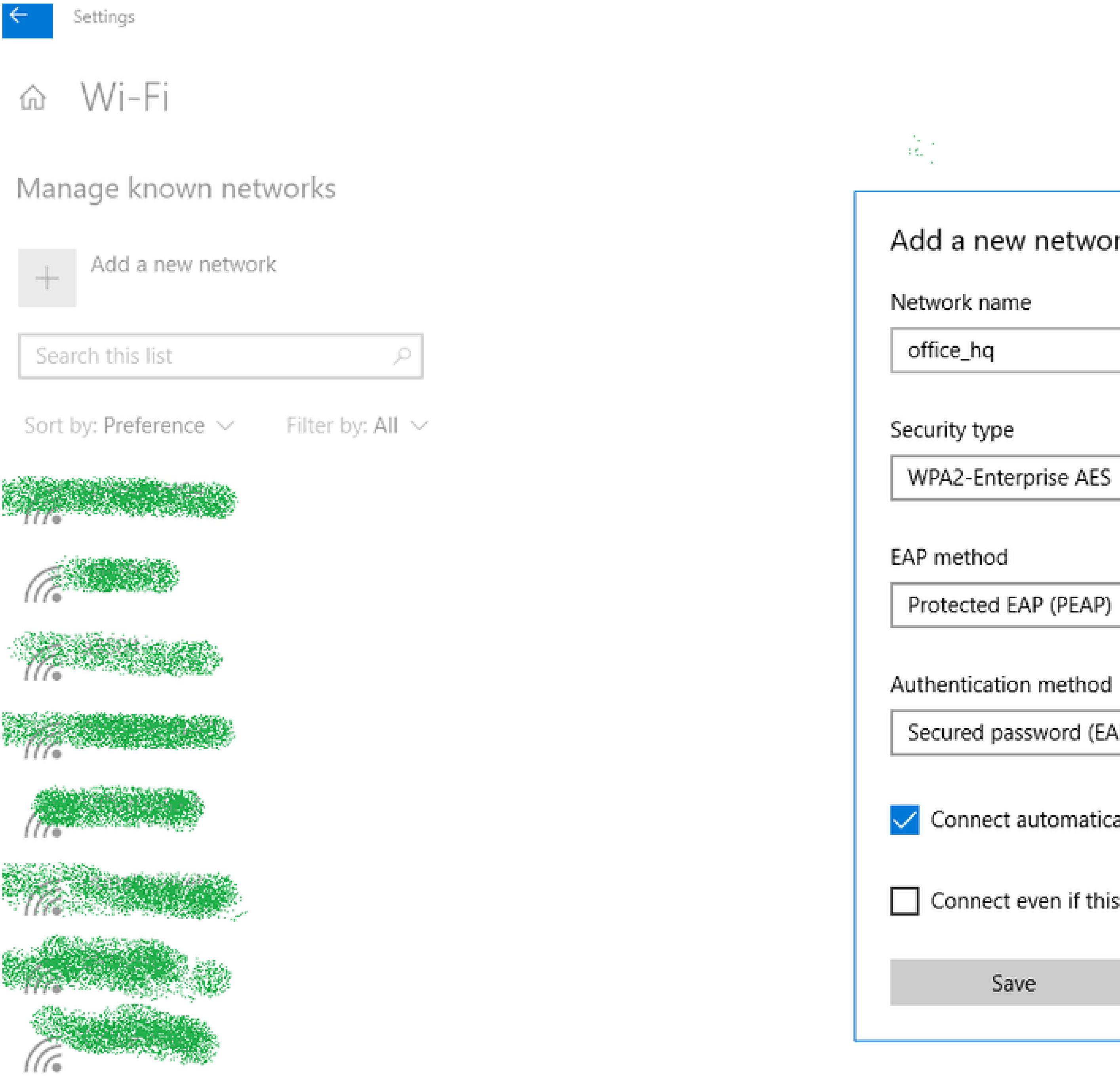
Verify

Use the Windows 10 native supplicant and Anyconnect NAM in order to test connections.

Since you are using EAP-PEAP authentication and ISE is using a Self-Signed Certificate (SSC), you must agree to a certificate warning or disable certificate validation. In a corporate environment, you must use a signed and trusted certificate on ISE and ensure that the end-user devices have the appropriate root certificate installed under the Trusted CA list.

Test connection with Windows 10 and native supplicant:

1. Open Network & Internet settings > Wi-Fi > Manage known networks and create a new network profile by pressing the Add new network button;fill in the required information.



[redacted]

Add a new networ

Network name: office_hq

Security type: WPA2-Enterprise AES

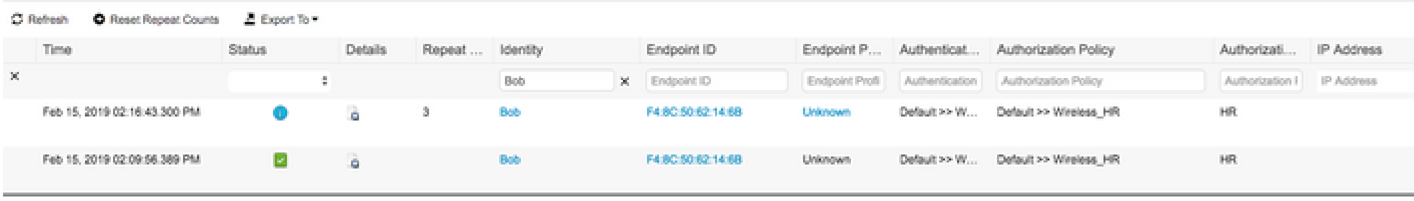
EAP method: Protected EAP (PEAP)

Authentication method: Secured password (EA

☑ Connect automatica

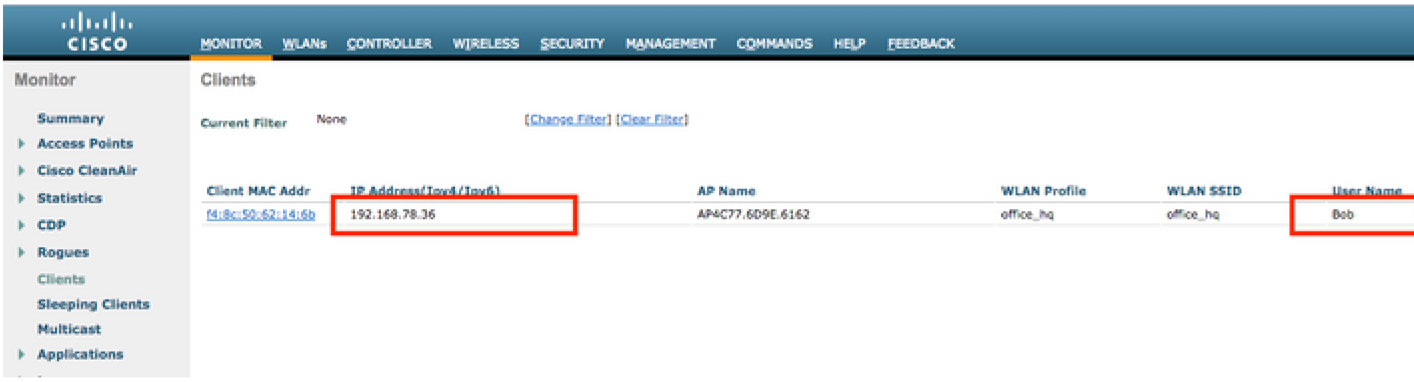
□ Connect even if this

2. Check the authentication log on ISE and ensure the right profile is selected for the user.



	Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address
×					Bob ×	Endpoint ID	Endpoint Profi	Authentication	Authorization Policy	Authorization I	IP Address
	Feb 15, 2019 02:16:43.300 PM	●		3	Bob	F4:8C:50:62:14:6B	Unknown	Default >> W...	Default >> Wireless_HR	HR	
	Feb 15, 2019 02:09:56.389 PM	✓			Bob	F4:8C:50:62:14:6B	Unknown	Default >> W...	Default >> Wireless_HR	HR	

3. Check client entry on WLC and ensure it is assigned to the right VLAN and is in the **RUN** state.



Clients

Current Filter None [Change Filter] [Clear Filter]

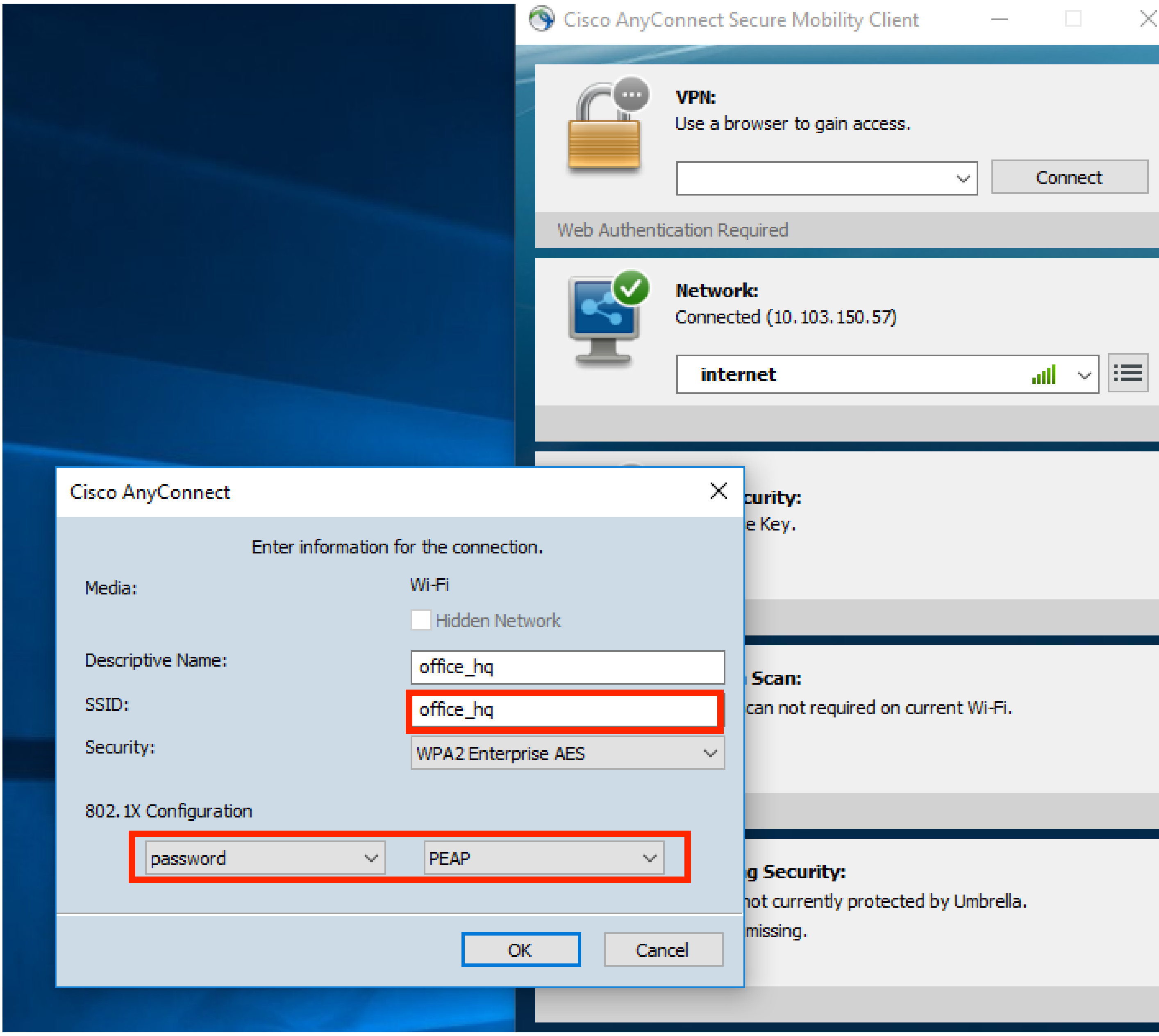
Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name
f4:8c:50:62:14:6b	192.168.78.36	AP4C77.6D9E.6162	office_hq	office_hq	Bob

4. From the **WLC CLI**, the client status can be checked with the show client dertails <mac-address>:

```
show client detail f4:8c:50:62:14:6b
Client MAC Address............................... f4:8c:50:62:14:6b
Client Username ................................. Bob
Client Webauth Username ......................... N/A
Hostname: .......................................
Device Type: .................................... Intel-Device
AP MAC Address................................... 70:69:5a:51:4e:c0
AP Name.......................................... AP4C77.6D9E.6162
AP radio slot Id................................. 1
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Bob
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 242 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.78.36
Gateway Address.................................. 192.168.78.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
EAP Type......................................... PEAP
Interface........................................ vlan1478
VLAN............................................. 1478
Quarantine VLAN.................................. 0
Access VLAN...................................... 1478
```

Test connection with Windows 10 and Anyconnect NAM:

1. Choose the SSID from the available SSIDs list and the respective EAP authentication type (in this example PEAP) and the inner authentication form.



Cisco AnyConnect Secure Mobility Client

VPN:
Use a browser to gain access.

Web Authentication Required

Network:
Connected (10.103.150.57)

internet

curity:
e Key.

Scan:
can not required on current Wi-Fi.

g Security:
not currently protected by Umbrella.
missing.

Cisco AnyConnect

Enter information for the connection.

Media: Wi-Fi

□ Hidden Network

Descriptive Name: office_hq

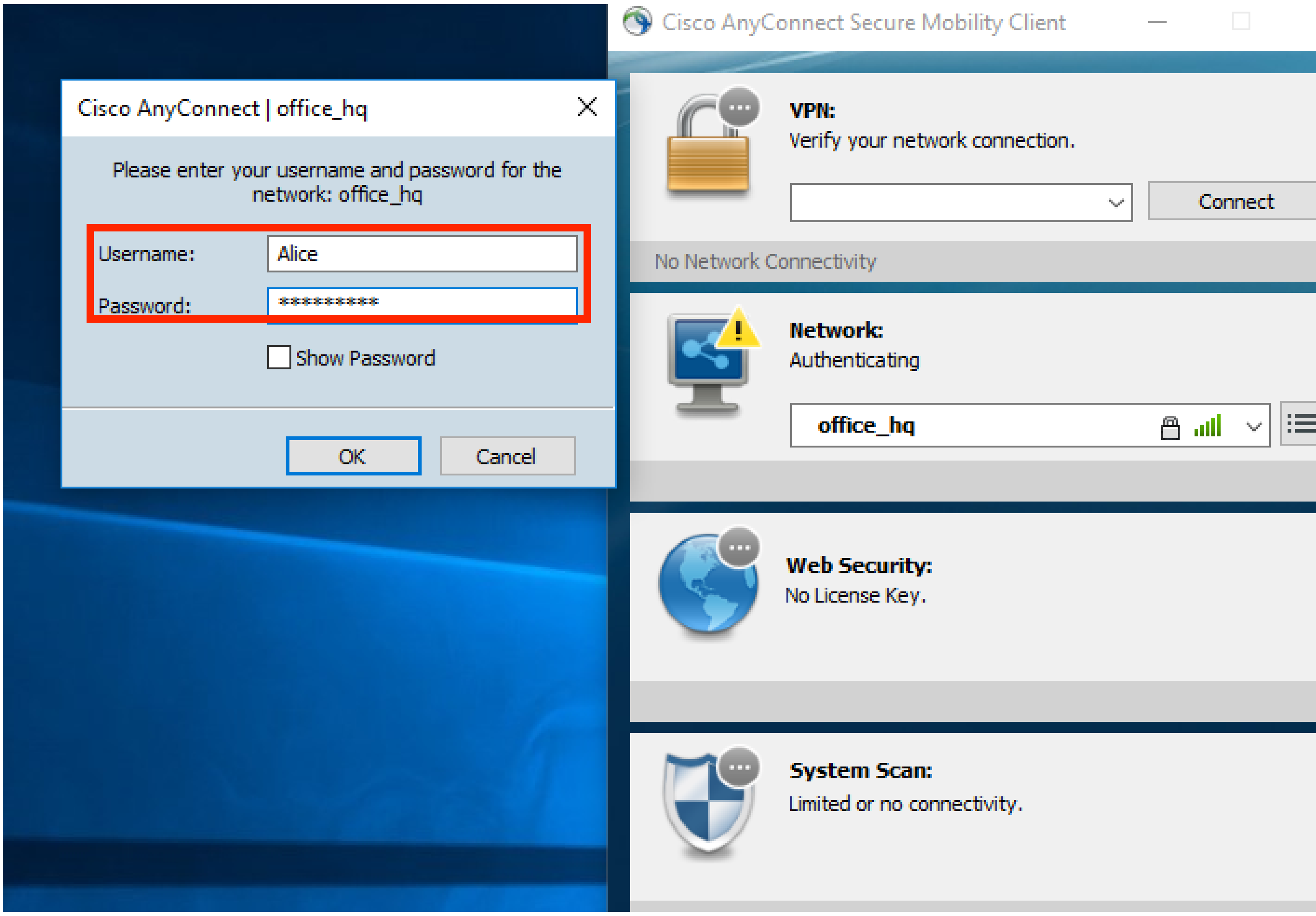
SSID: office_hq

Security: WPA2 Enterprise AES

802.1X Configuration

password PEAP

2. Provide username and password for user authentication.



Cisco AnyConnect | office_hq

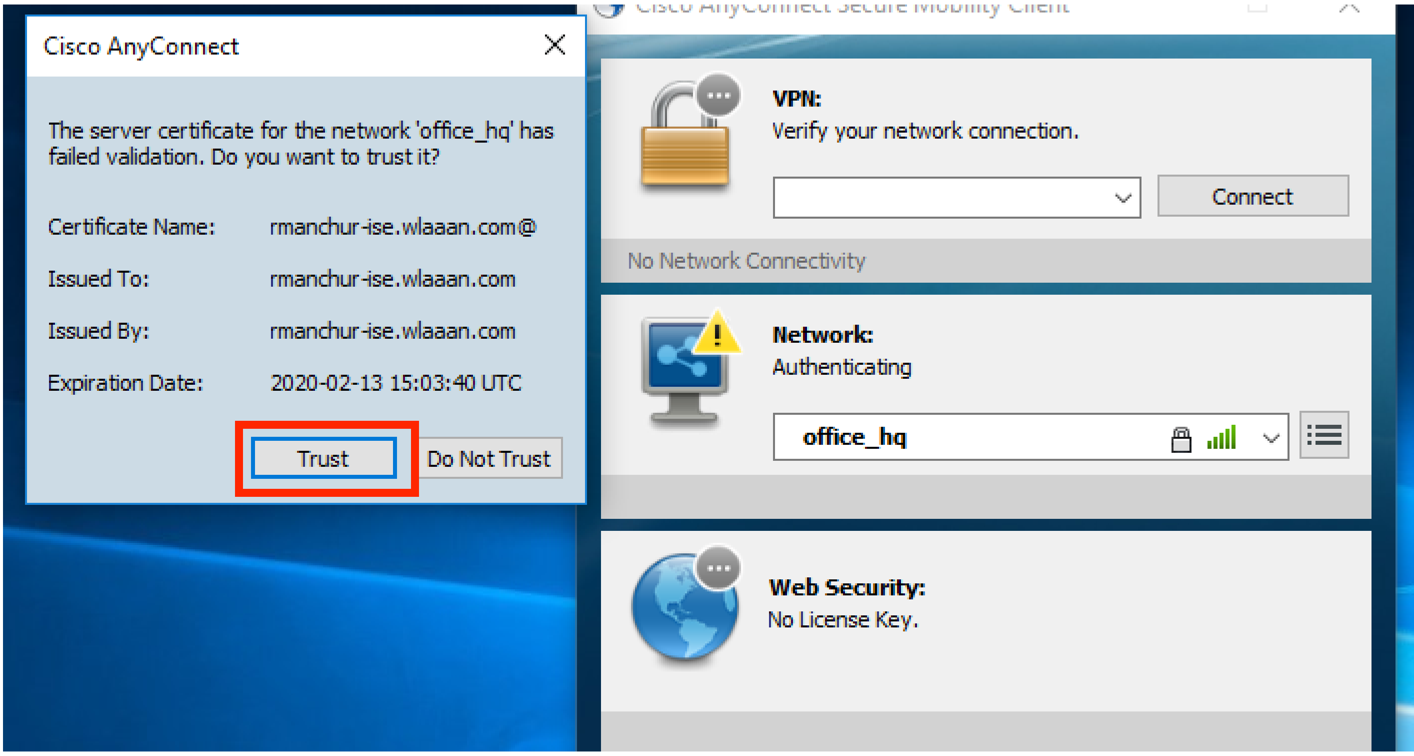
Please enter your username and password for the network: office_hq

Username: Alice

Password: **********

□ Show Password

3. Since ISE is sending an SSC to the client, you must manually choose to trust the certificate (in the production environment it is highly recommended to install the trusted certificate on ISE).



Cisco AnyConnect

The server certificate for the network 'office_hq' has failed validation. Do you want to trust it?

Certificate Name: rmanchur-ise.wlaaan.com@

Issued To: rmanchur-ise.wlaaan.com

Issued By: rmanchur-ise.wlaaan.com

Expiration Date: 2020-02-13 15:03:40 UTC

Cisco AnyConnect Secure Mobility Client

VPN:
Verify your network connection.

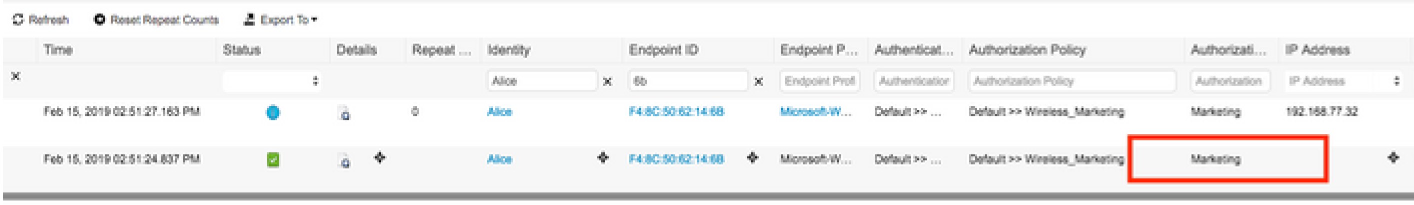
No Network Connectivity

Network:
Authenticating

office_hq

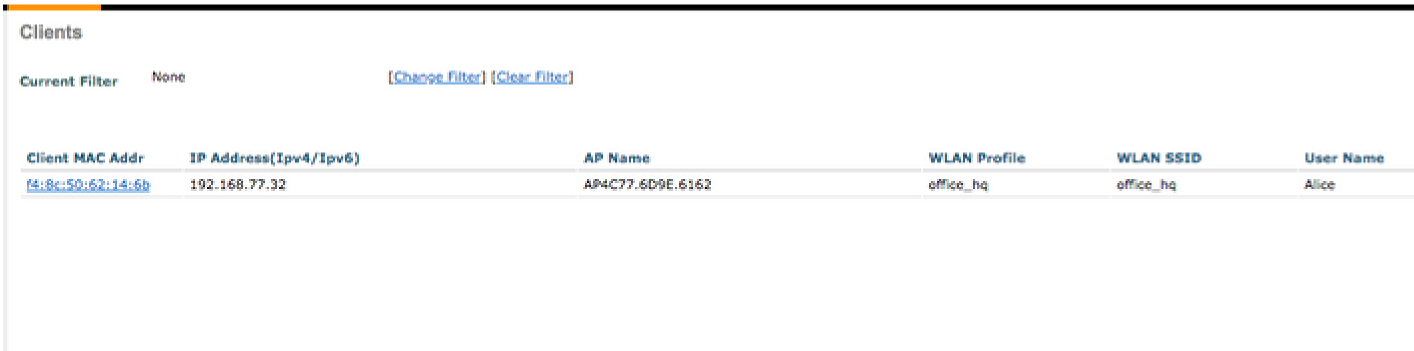
Web Security:
No License Key.

4. Check authentication logs on ISE and ensure the right authorization profile is selected for the user.



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address
				Alice	6b	Endpoint Prof	Authentication	Authorization Policy	Authorization	IP Address
Feb 15, 2019 02:51:27.163 PM	●		0	Alice	F4:8C:50:62:14:6B	Microsoft-W...	Default >> ...	Default >> Wireless_Marketing	Marketing	192.168.77.32
Feb 15, 2019 02:51:24.837 PM	✓			Alice	F4:8C:50:62:14:6B	Microsoft-W...	Default >> ...	Default >> Wireless_Marketing	Marketing	

5. Check client entry on the WLC and ensure it is assigned to the right VLAN and is in the **RUN** state.



Clients

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name
f4:8c:50:62:14:6b	192.168.77.32	AP4C77.6D9E.6162	office_hq	office_hq	Alice

6. From the **WLC CLI**, the client status can be checked with the show client dertails <mac-address>:

```
Client MAC Address............................... f4:8c:50:62:14:6b
Client Username ................................. Alice
Client Webauth Username ......................... N/A
Hostname: .......................................
Device Type: .................................... Intel-Device
AP MAC Address................................... 70:69:5a:51:4e:c0
AP Name.......................................... AP4C77.6D9E.6162
AP radio slot Id................................. 1
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

Troubleshoot

1. Use the `test aaa radius username <user> password <password> wlan-id <id>` in order to test the RADIUS connection between WLC and ISE and the `test aaa show radius` in order to show the results.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id........................................ 2
  ApGroup Name................................... none

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  Called-Station-Id               00-00-00-00-00-00:AndroidAP
  Calling-Station-Id              00-11-22-33-44-55
  Nas-Port                        0x00000001 (1)
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743



test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id........................................ 2
  ApGroup Name................................... none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)



(Cisco Controller) >
```

2. Use the debug client <mac-address> in order to troubleshoot wireless client connectivity issues.
3. Use the debug aaa all enable in order to troubleshoot authentication and authorization issues on the WLC.

> **Note**: Use this command only with the debug mac addr in order to limit the output based on the MAC address for which debugging is done.

4. Refer to ISE live logs and session logs in order to identify problems authentication failures and AD communication issues.