使用基于ISE的WLC配置到Active Directory组映射的动态VLAN分配

目录

简介

本文档介绍动态VLAN分配的概念。

先决条件

本文档介绍如何配置无线LAN控制器(WLC)和身份服务引擎(ISE)服务器，以便动态地将无线LAN (WLAN)客户端分配到特定VLAN。

要求

Cisco 建议您了解以下主题：

- 无线局域网控制器(WLC)和轻量接入点(LAP)的基础知识
- 身份验证、授权和记帐(AAA)服务器（例如ISE）的功能知识
- 全面了解无线网络和无线安全问题
- 有关动态VLAN分配的功能和配置知识
- 基本了解Microsoft Windows AD服务以及域控制器和DNS概念
- 具备接入点协议(CAPWAP)控制和调配的基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行固件 8.8.111.0 版本的 Cisco 5520 系列 WLC
- Cisco 4800系列AP
- 本地Windows请求方和Anyconnect NAM
- 思科安全ISE版本2.3.0.298
- 配置为域控制器的 Microsoft Windows 2016 Server
- 运行版本15.2(4)E1的Cisco 3560-CX系列交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

使用 RADIUS 服务器执行动态 VLAN 分配

在大多数 WLAN 系统中，每个 WLAN 都有适用于与服务集标识符 (SSID) 关联的所有客户端的静态策略，即以控制器术语表示 WLAN。虽然此方法功能强大，但也具有局限性，这是因为，它要求客户端与不同的 SSID 相关联以便继承不同的 QoS 和安全策略。

思科WLAN解决方案通过支持身份网络解决了这一限制。 这允许网络通告单个SSID，但允许特定用户根据用户凭证继承不同的QoS、VLAN属性和/或安全策略。

动态 VLAN 分配便是一项这样的功能，它根据无线用户提供的凭证将该用户置于特定 VLAN 中。将用户分配到特定VLAN的任务由RADIUS身份验证服务器（例如Cisco ISE）处理。例如，为了让无线主机在园区网络中移动时保持同一个VLAN上，可以使用此选项。

思科ISE服务器根据多个可能的数据库（包括其内部数据库）之一对无线用户进行身份验证。例如：

- 内部数据库
- Active Directory
- 通用轻量目录访问协议 (LDAP)
- 与开放式数据库连接 (ODBC) 兼容的关系数据库
- Rivest、Shamir 和 Adelman (RSA) SecurID 令牌服务器
- 与 RADIUS 兼容的令牌服务器

Cisco ISE身份验证协议和支持的外部身份源列出了ISE内部和外部数据库支持的各种身份验证协议。

本文档重点介绍如何对使用Windows Active Directory外部数据库的无线用户进行身份验证。

身份验证成功后，ISE从Windows数据库中检索该用户的组信息，并将该用户关联到相应的授权配置文件。

当客户端尝试与注册到控制器的LAP关联时，LAP会在各自EAP方法的帮助下将用户的凭证传递到WLC。

WLC使用RADIUS协议（封装EAP）将这些凭证发送到ISE，ISE将用户的凭证传递到AD以在KERBEROS协议的帮助下进行验证。

AD验证用户凭证，并在身份验证成功后通知ISE。

身份验证成功后，ISE服务器会将某些Internet工程任务组(IETF)属性传递给WLC。这些RADIUS属性决定了必须分配给无线客户端的VLAN ID。客户端的 SSID（WLAN，从 WLC 的角度而言）并不重要，这是因为，会始终为用户分配此预先确定的 VLAN ID。

用于 VLAN ID 分配的 RADIUS 用户属性包括：

- IETF 64（隧道类型）—将此项设置为VLAN
- IETF 65（隧道介质类型）—将此值设置为802
- IETF 81（隧道专用组ID）—将此项设置为VLAN ID

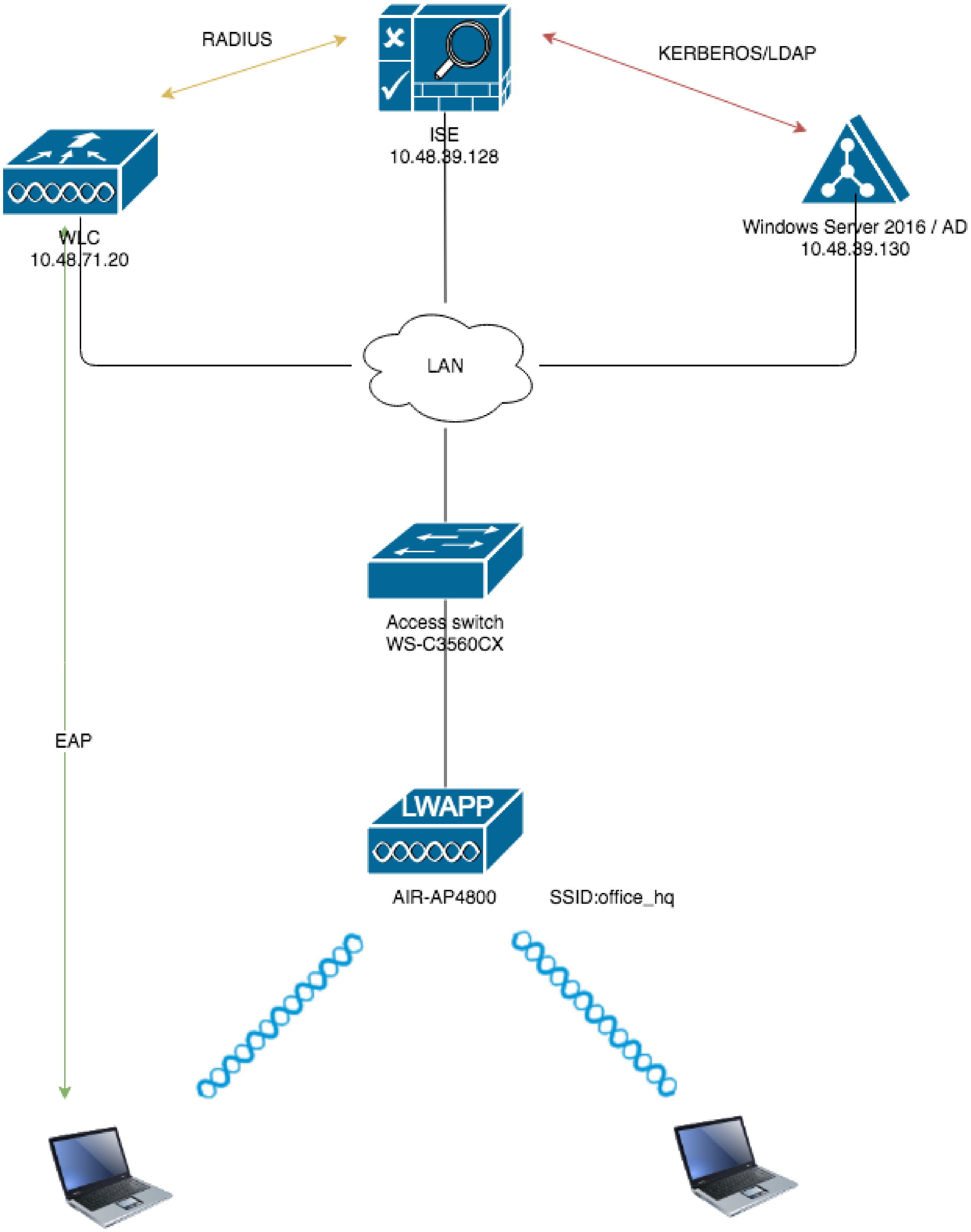
VLAN ID为12位，取值在1和4094（含）之间。由于Tunnel-Private- Group-ID属于字符串类型（如用于IEEE 802.1X的RFC2868中所定义），因此VLAN ID整数值被编码为字符串。当发送这些隧道属性时，需要填写 Tag 字段。

如RFC 2868第3.1部分中所述：“标记”字段的长度为一个二进制八位数，它用于提供在同一数据包中分组引用同一隧道属性的方法。此字段的有效值是 0x01 到 0x1F（包含 0x01 和 0x1F）。如果未使用 Tag 字段，则它一定为零 (0x00)。有关所有 RADIUS 属性的详细信息，请参阅 RFC 2868。

配置

本节提供配置文档中所述功能所需的信息。

网络图



配置

下面是此图中使用的组件的配置详细信息：

- ISE (RADIUS)服务器的IP地址是10.48.39.128。
- WLC的管理和AP管理器接口地址为10.48.71.20。
- DHCP服务器驻留在LAN网络中，并且针对各个客户端池进行了配置；如图所示。
- 此配置中使用VLAN1477和VLAN1478。营销部门的用户配置为置于VLAN1477中，HR 部门的用户配置为由RADIUS服务器置于VLAN1478中 当两个用户连接到同一个SSID时—office_hq.

  VLAN1477:192.168.77.0/24。网关：192.168.77.1 VLAN1478:192.168.78.0/24。网关：192.168.78.1
- 本文档使用带有PEAP-mschapv2的802.1x作为安全机制。

注意：Cisco建议您使用高级身份验证方法（例如EAP-FAST和EAP-TLS身份验证），以保护WLAN。

在执行此配置之前已做出以下假设：

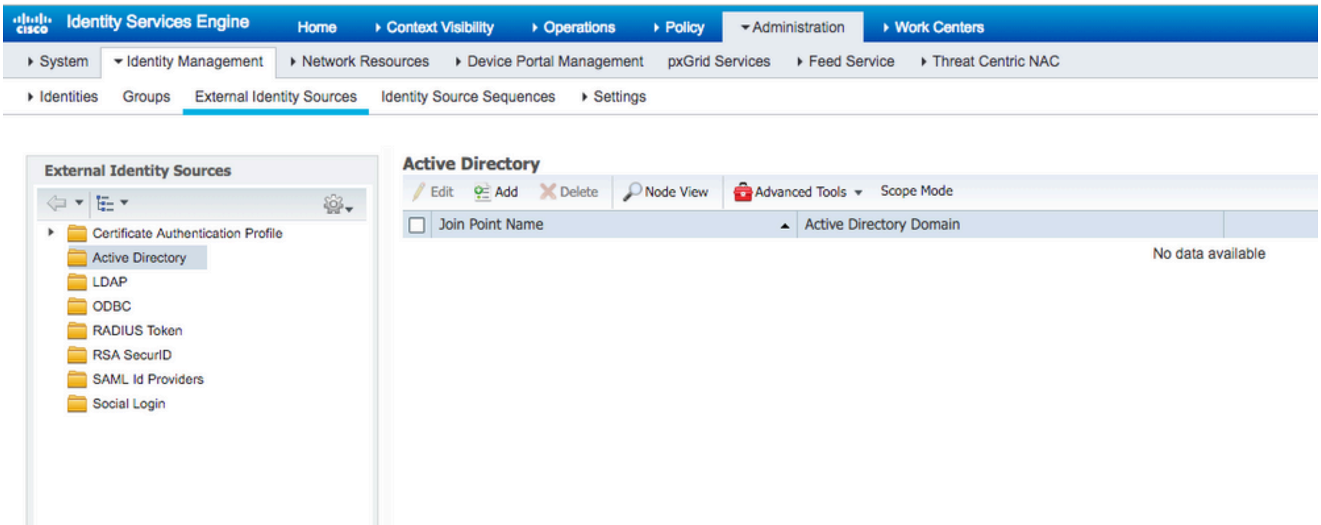
- LAP已注册到WLC
- DHCP服务器分配了一个DHCP作用域
- 网络中的所有设备之间存在第3层连接
- 本文档讨论在无线端所需的配置，并假设有线网络已部署到位
- 在AD上配置相应的用户和组

要完成基于ISE到AD组映射的WLC动态VLAN分配，必须执行以下步骤：

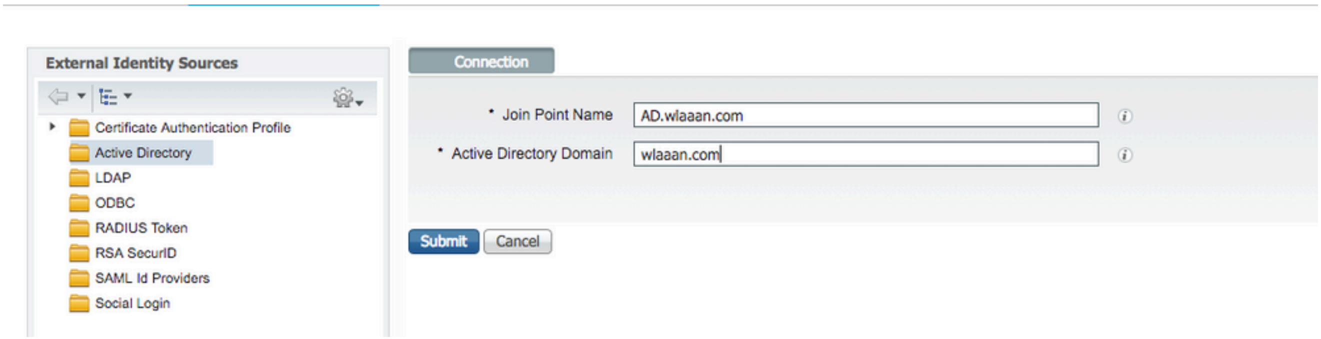
1. ISE到AD集成和配置ISE上用户的身份验证和授权策略。
2. WLC配置，以支持SSID 'office_hq'的dot1x身份验证和AAA覆盖。
3. 最终客户端请求方配置。

ISE到AD集成和配置ISE上用户的身份验证和授权策略

1. 使用admin帐户登录到ISE Web UI界面。
2. 导航到Administration > Identity management > External Identity Sources > Active directory。



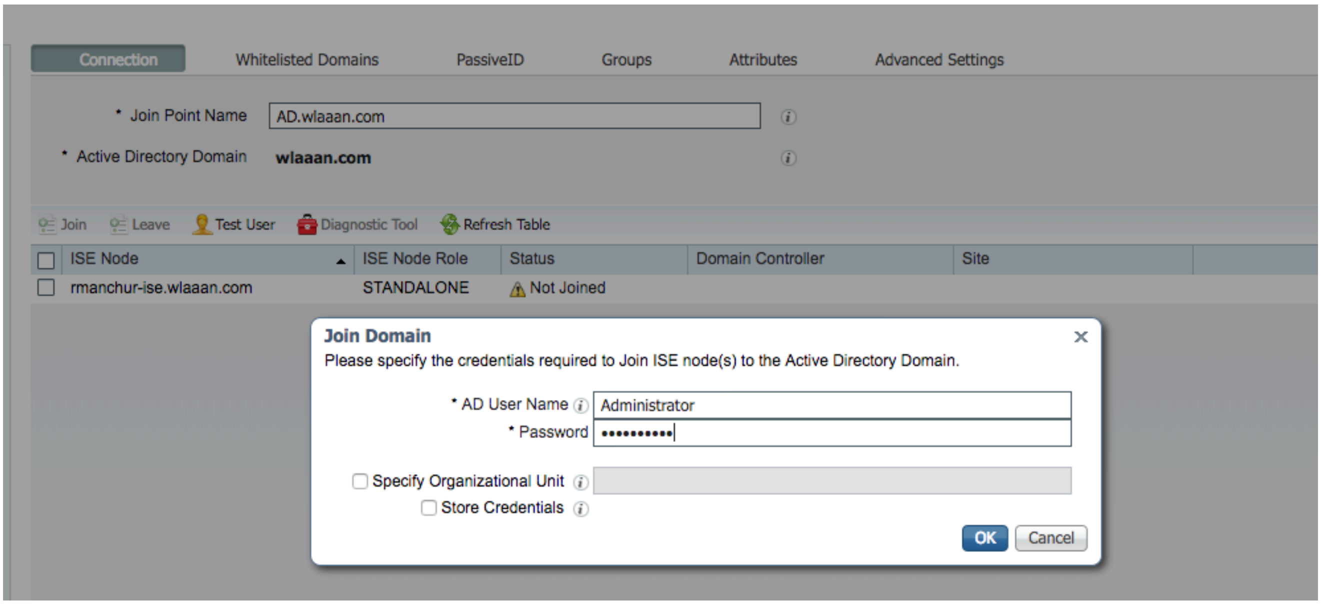
3. 单击Add，然后从Active Directory加入点名称设置输入域名和身份库名称。在本例中，ISE注册到域wlaaan.com，并且加入点指定为AD.wlaaan.com - ISE的本地重要名称。



* Join Point Name: AD.wlaaan.com

* Active Directory Domain: wlaaan.com

4. 按Submit下按钮后，将打开一个弹出窗口，询问您是否要立即将ISE加入AD。按Yes并提供具有管理员权限的Active Directory用户凭据，以将新主机添加到域中。



* Join Point Name: AD.wlaaan.com
* Active Directory Domain: wlaaan.com

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

Join Domain

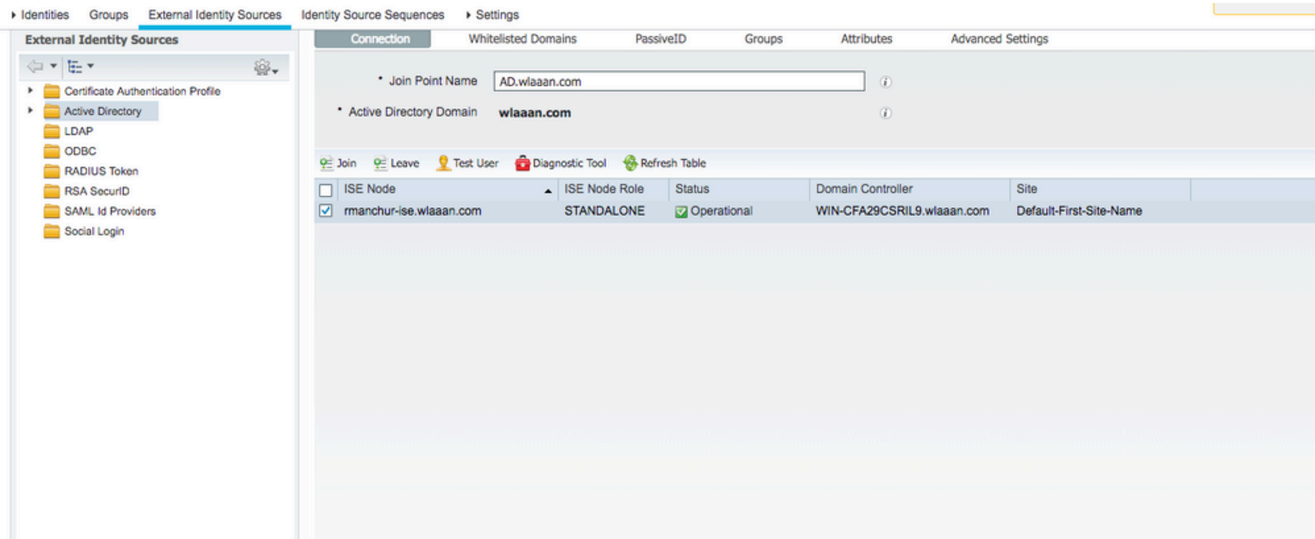
Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: Administrator
* Password: ••••••••••

□ Specify Organizational Unit

□ Store Credentials

5. 在此之后，您必须将ISE成功注册到AD。



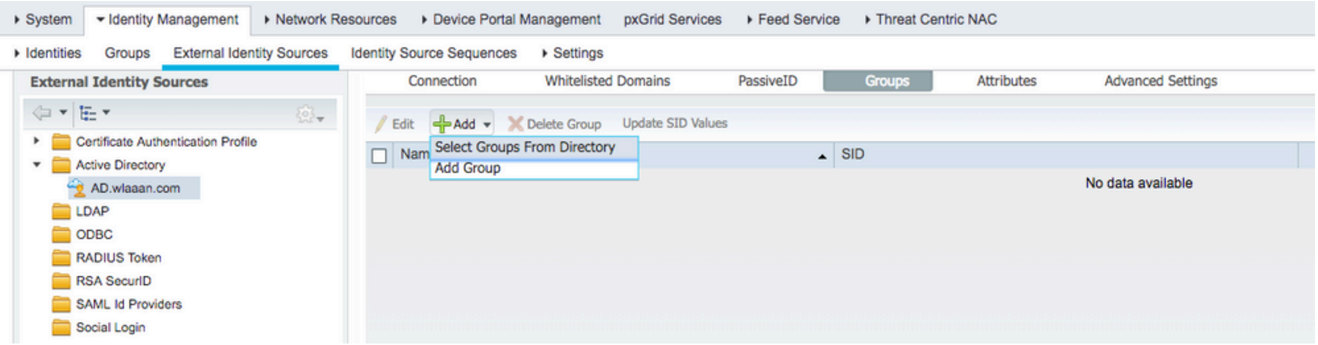
* Join Point Name: AD.wlaaan.com
* Active Directory Domain: wlaaan.com

□	ISE Node	ISE Node Role	Status	Domain Controller	Site
☑	rmanchur-ise.wlaaan.com	STANDALONE	✓ Operational	WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name

如果注册过程中有任何问题，可以使用Diagnostic Tool 来运行AD连接所需的测试。

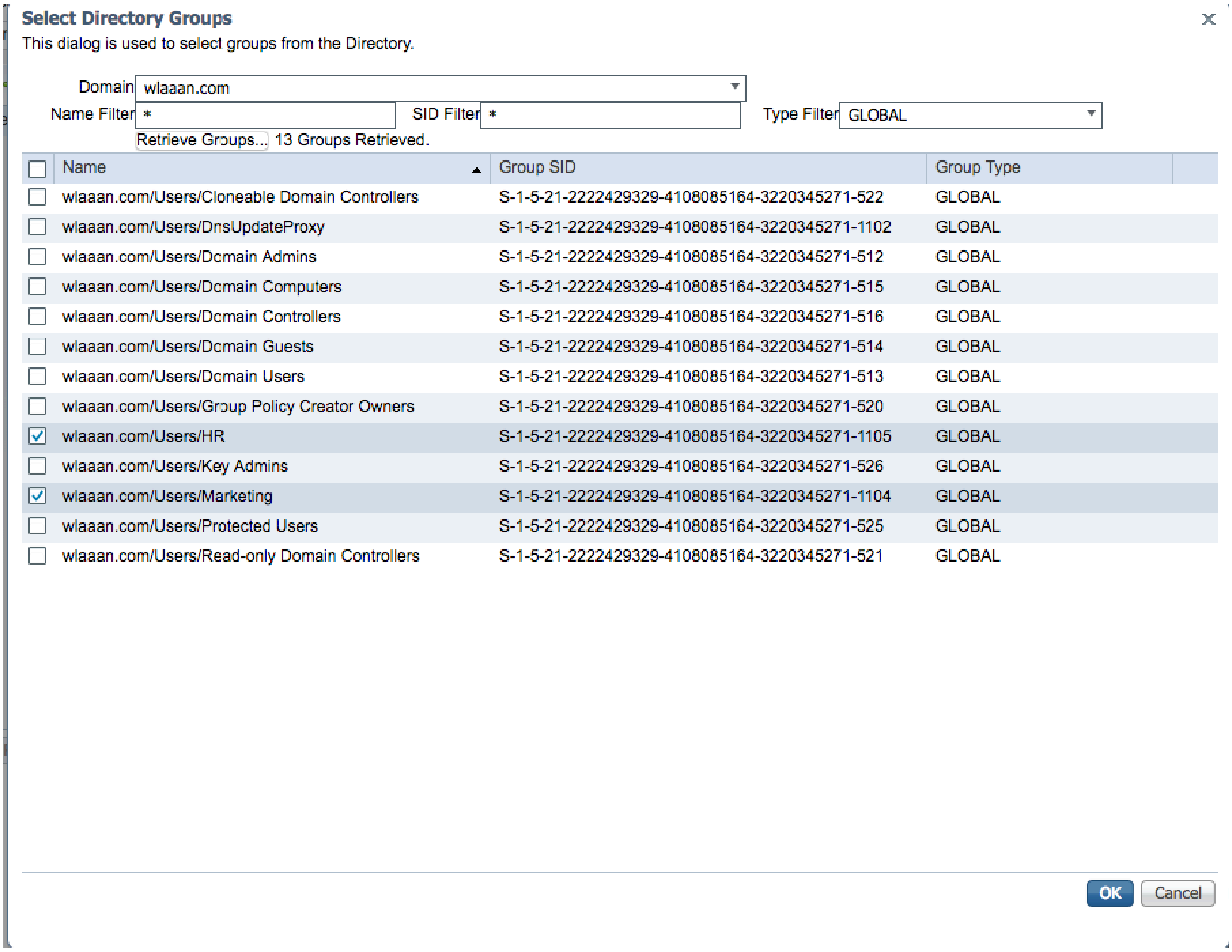
6. 您必须检索用于分配相应授权配置文件的活动目录组。导航到Administration > Identity management >
External Identity Sources > Active directory >

> Groups
，然后点击Add并选择Select Groups from Active Directory。



No data available

7. 将打开一个新的弹出窗口，您可以在其中指定过滤器以检索特定组或从AD检索所有组。从AD组列表中选择相应的组，然后按OK。



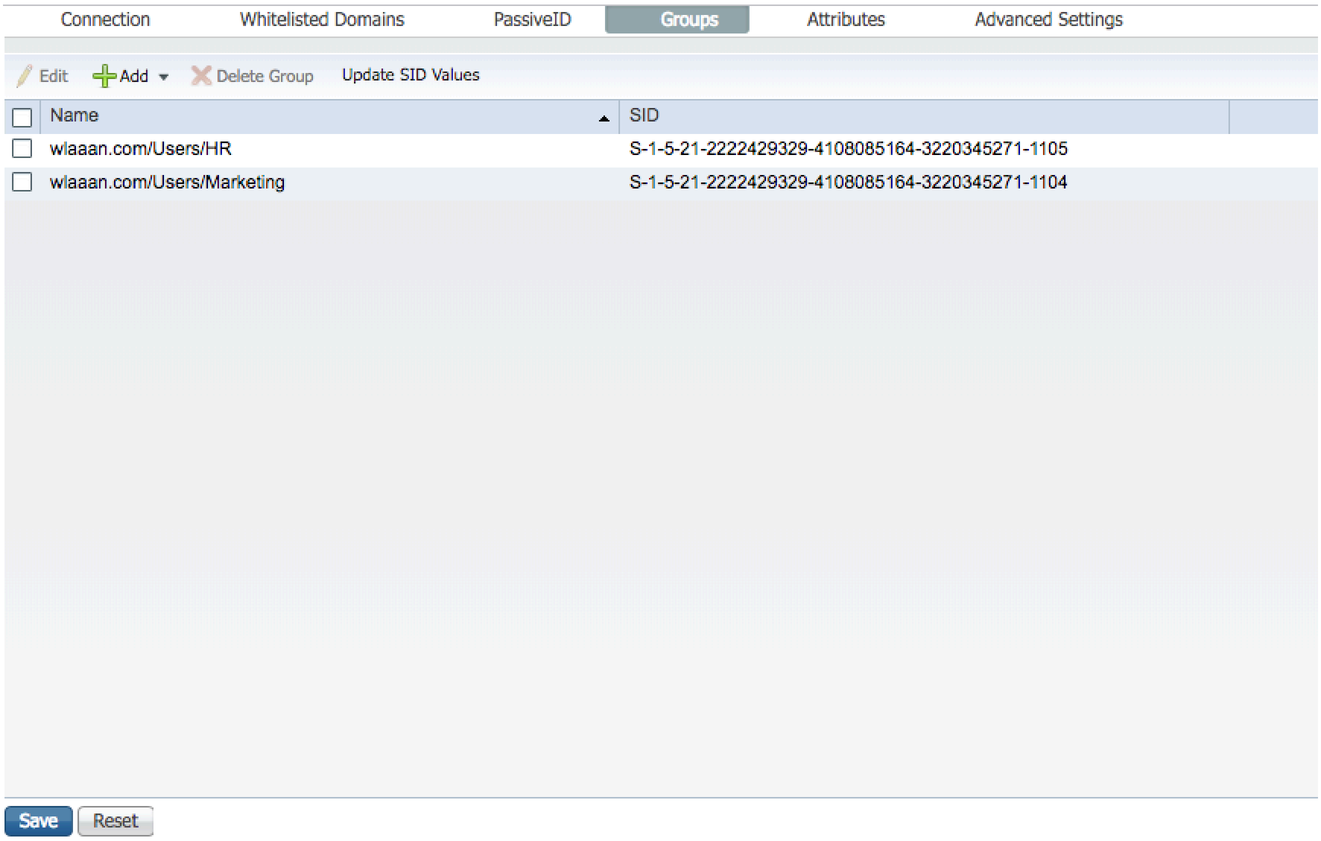
This dialog is used to select groups from the Directory.

Domain: wlaaan.com
Name Filter: *
SID Filter: *
Type Filter: GLOBAL

13 Groups Retrieved.

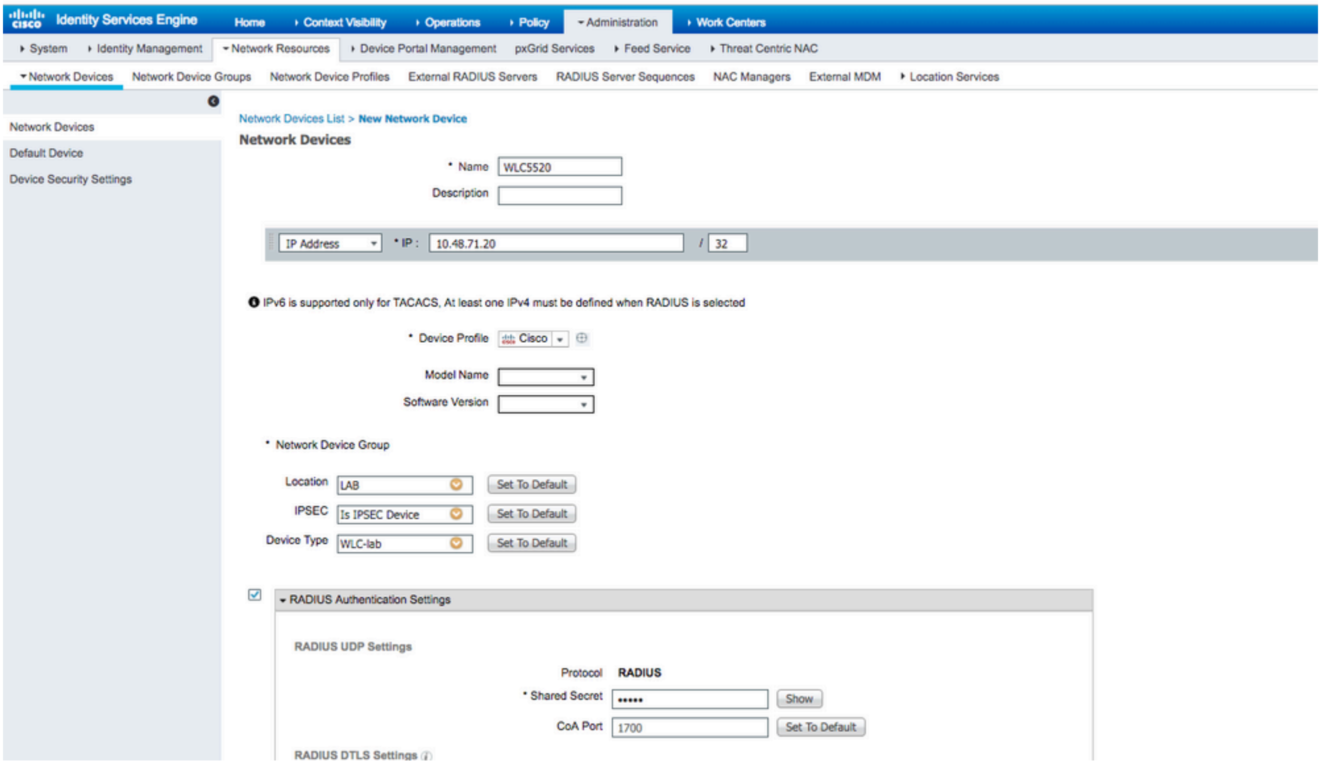
□	Name	Group SID	Group Type
□	wlaaan.com/Users/Cloneable Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-522	GLOBAL
□	wlaaan.com/Users/DnsUpdateProxy	S-1-5-21-2222429329-4108085164-3220345271-1102	GLOBAL
□	wlaaan.com/Users/Domain Admins	S-1-5-21-2222429329-4108085164-3220345271-512	GLOBAL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

8. 相应的组会添加到ISE中并可保存。按 。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. 将WLC添加到ISE网络设备列表-导航到Administration > Network Resources > Network Devices，然后按Add。通过在WLC和ISE之间提供WLC管理IP地址和RADIUS共享密钥来完成配置。



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 Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type WLC-lab Set To Default

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

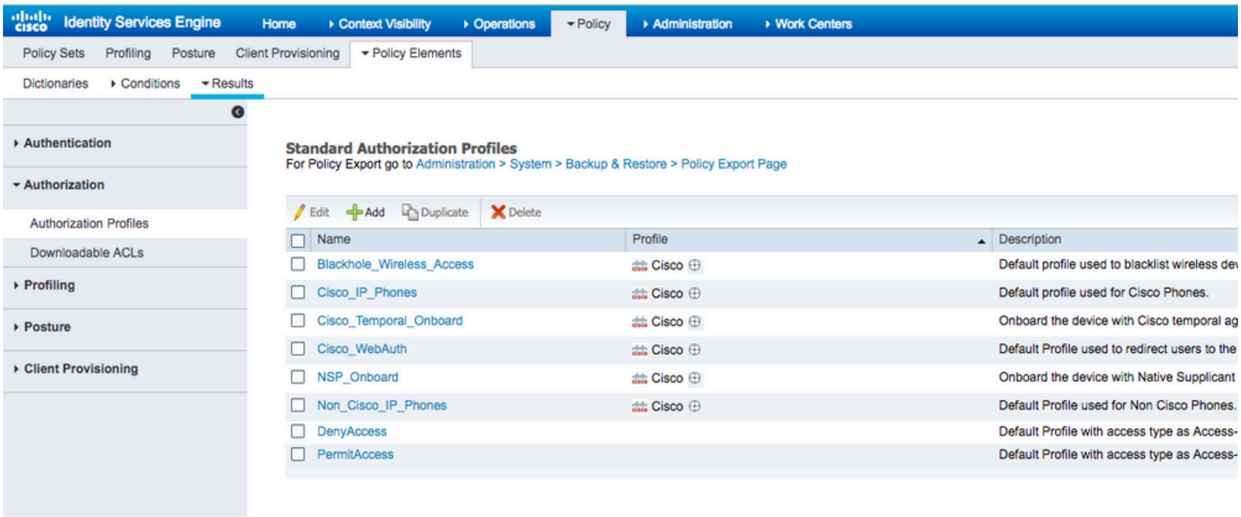
* Shared Secret ••••• Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

10. 现在，在您将ISE加入AD并将WLC添加到设备列表后，您可以开始为用户配置身份验证和授权策略。

- 创建授权配置文件，以将市场营销用户分配到VLAN1477，并将HR组用户分配到VLAN1478。
  导航到Policy > Policy Elements > Results > Authorization > Authorization profiles并单击Add按钮以创建新配置文件。

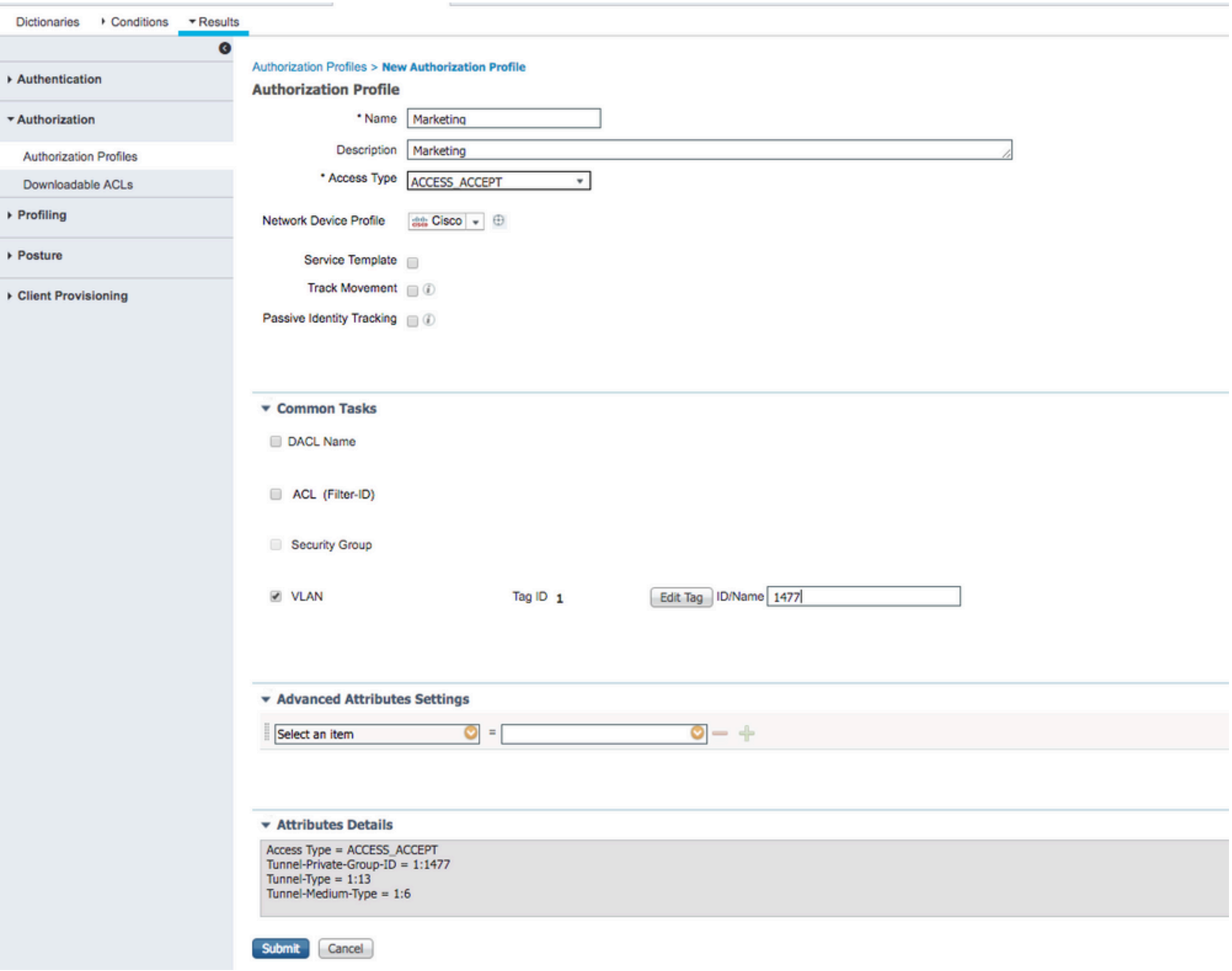


Standard Authorization Profiles

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

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless dev
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal ag
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the
NSP_Onboard	Cisco	Onboard the device with Native Supplicant
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-
PermitAccess		Default Profile with access type as Access-

- 使用相应组的VLAN信息完成授权配置文件配置；示例显示了Marketing组配置设置。



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   Edit Tag   ID/Name 1477

Advanced Attributes Settings

Select an item =

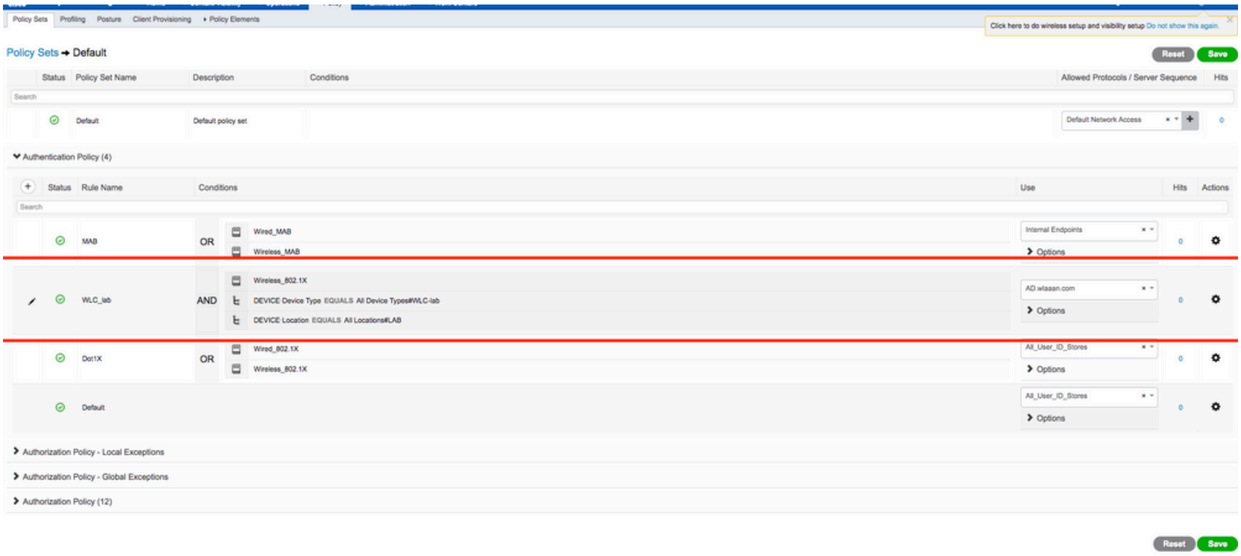
Attributes Details

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

必须为其他组执行类似配置，并且必须配置各自的VLAN标记属性。

- 配置授权配置文件后，您可以定义无线用户的身份验证策略。这可以通过配置Custom或修

改Default策略集来实现。在本示例中，Default策略集被修改。导航到Policy > Policy Sets > Default。默认情况下，对于dot1x身份验证类型，ISE将使用All_User_ID_Stores，尽管它使用当前默认设置，因为AD是All_User_ID_Stores的身份源列表的一部分，此示例对该相应LAB控制器使用更具体的规则WLC_lab，并使用AD作为身份验证的唯一源。



	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	✓	Default	Default policy set		Default Network Access	0

Authentication Policy (4)

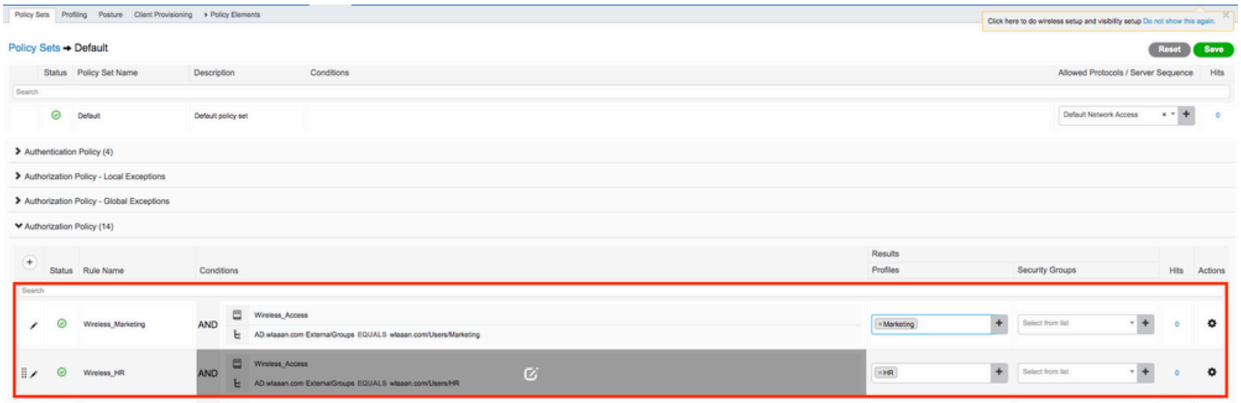
	Status	Rule Name	Conditions		Use	Hits	Actions
	✓	MAB	OR	Wired_MAB Wireless_MAB	Internal Endpoints Options	0	⚙
	✓	WLC_lab	AND	Wireless_802.1X DEVICE Device Type EQUALS All Device Types#WLC-lab DEVICE Location EQUALS All Locations#LAB	AD.wlaaan.com Options	0	⚙
	✓	Dot1X	OR	Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	0	⚙
	✓	Default			All_User_ID_Stores Options	0	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (12)

- 现在，您必须为根据组成员身份分配相应授权配置文件的用户创建授权策略。导航到Authorization policy部分并创建策略以完成此要求。



	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	✓	Default	Default policy set		Default Network Access	0

Authentication Policy (4)

Authorization Policy - Local Exceptions

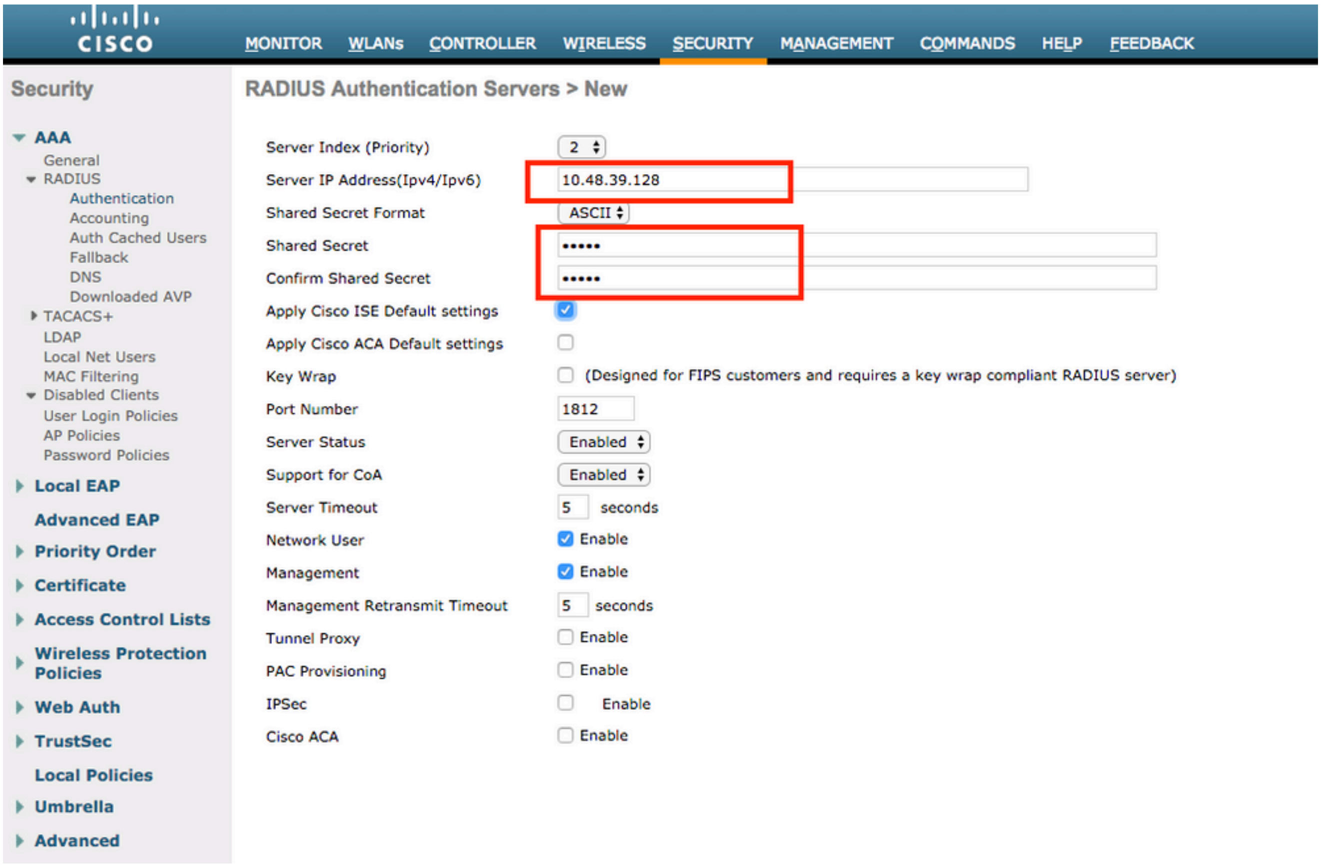
Authorization Policy - Global Exceptions

Authorization Policy (14)

	Status	Rule Name	Conditions		Results Profiles	Security Groups	Hits	Actions
	✓	Wireless_Marketing	AND	Wireless_Access AD.wlaaan.com ExternalGroups EQUALS wlaaan.com/Users/Marketing	Marketing	Select from list	0	⚙
	✓	Wireless_HR	AND	Wireless_Access AD.wlaaan.com ExternalGroups EQUALS wlaaan.com/Users/HR	HR	Select from list	0	⚙

支持SSID 'office_hq'的dot1x身份验证和AAA覆盖的WLC配置

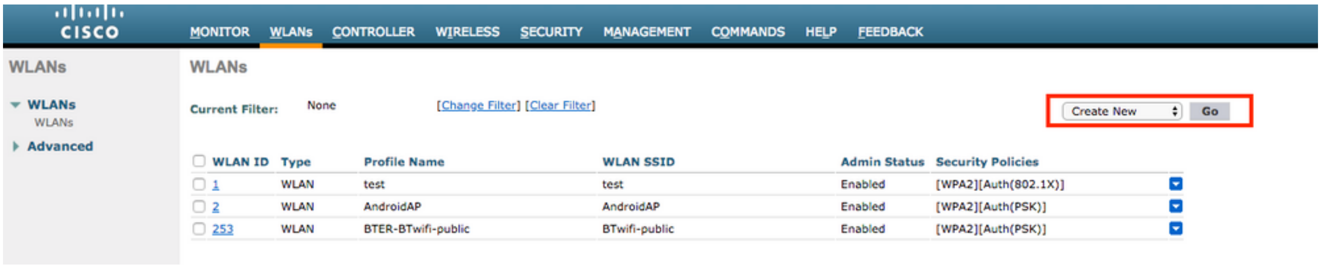
1. 将ISE配置为WLC上的RADIUS身份验证服务器。导航到Web UI界面中的Security > AAA > RADIUS > Authentication部分，并提供ISE IP地址和共享密钥信息。



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 key wrap compliant RADIUS server)
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

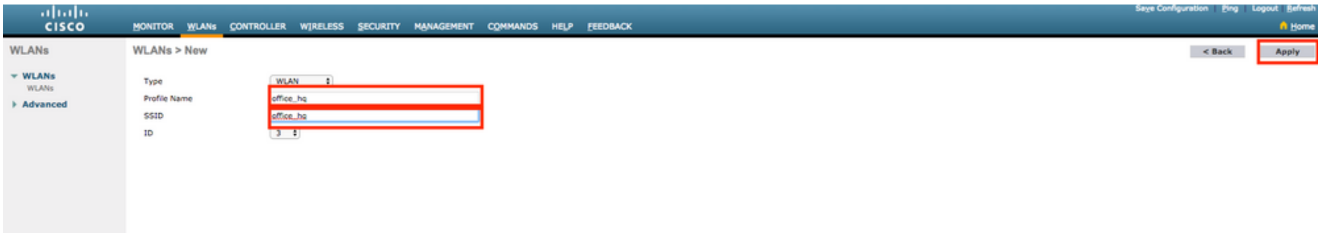
2. 在WLC上的WLANs部分下配置SSIDoffice_hq；此示例使用WPA2/AES+dot1x和AAA覆盖配置SSID。已为WLAN选择接口Dummy，因为仍会通过RADIUS分配正确的VLAN。必须在WLC上创建此虚拟接口并给予IP地址，但IP地址不必是有效的，而且上行链路交换机中无法创建放置该虚拟接口的VLAN，因此如果没有分配VLAN，客户端将无法访问任何位置。



WLANs

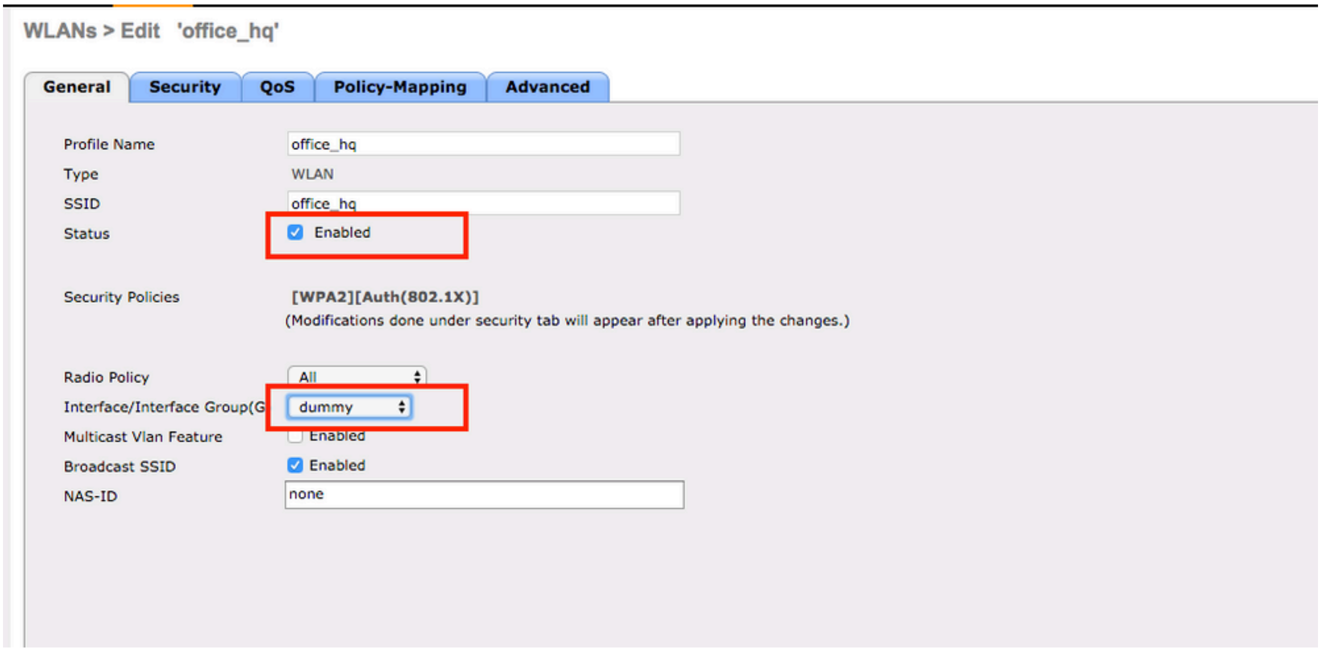
Current Filter: None [Change Filter] [Clear Filter]

☐ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☐ 1	WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]
☐ 2	WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]
☐ 253	WLAN	BTER-BTwifi-public	BTwifi-public	Enabled	[WPA2][Auth(PSK)]



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.)

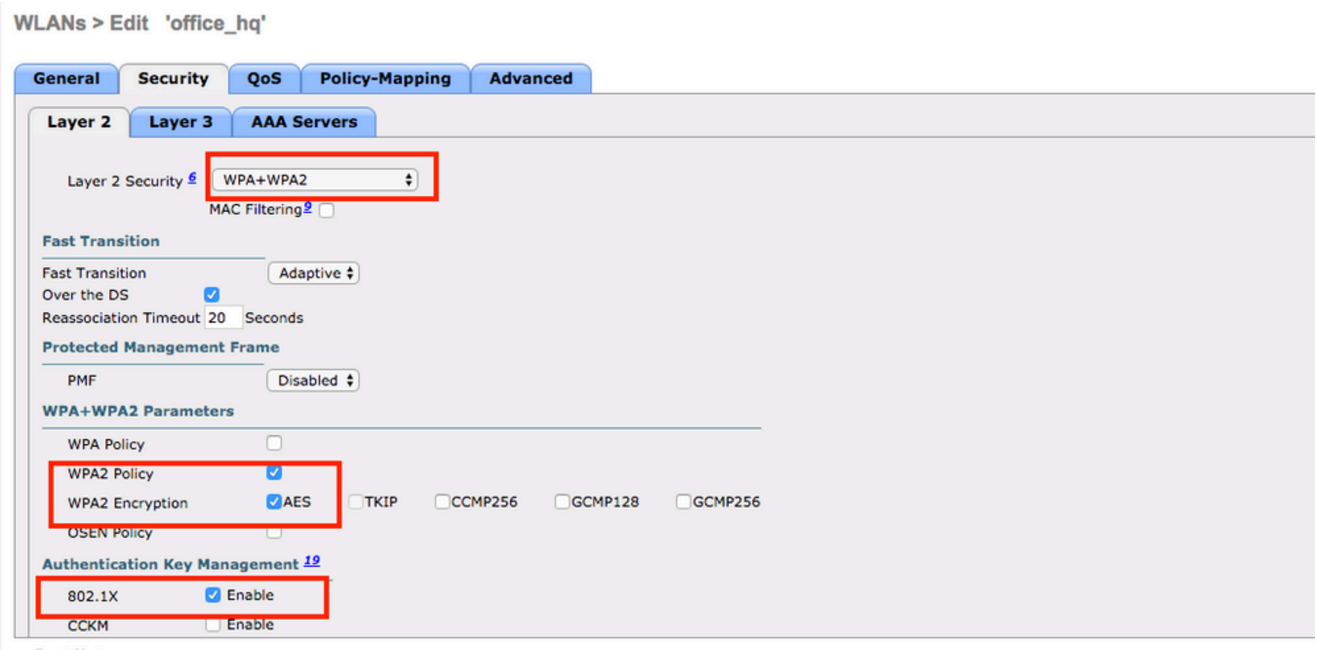
Radio Policy All

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 ☑

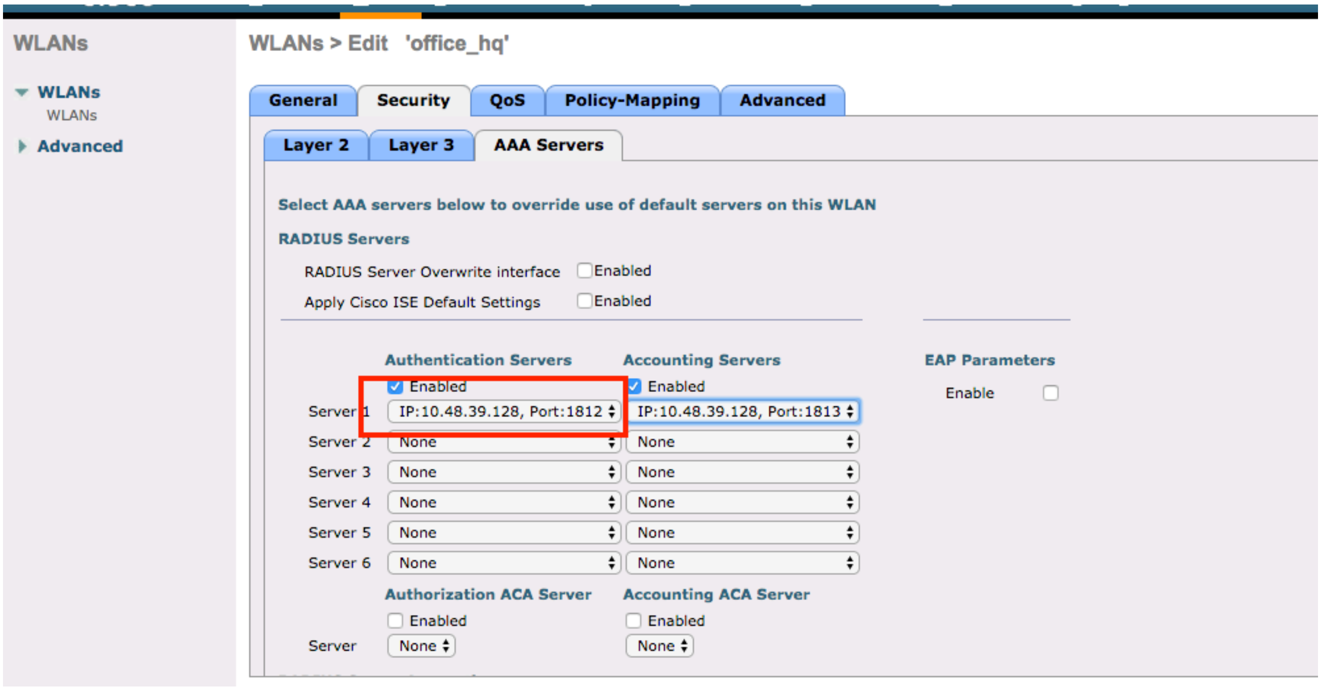
WPA2 Encryption ☑AES □TKIP □CCMP256 □GCMP128 □GCMP256

OSEN Policy □

Authentication Key Management [19]

802.1X ☑ Enable

CCKM □ Enable



WLANs > Edit 'office_hq'

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

RADIUS Servers

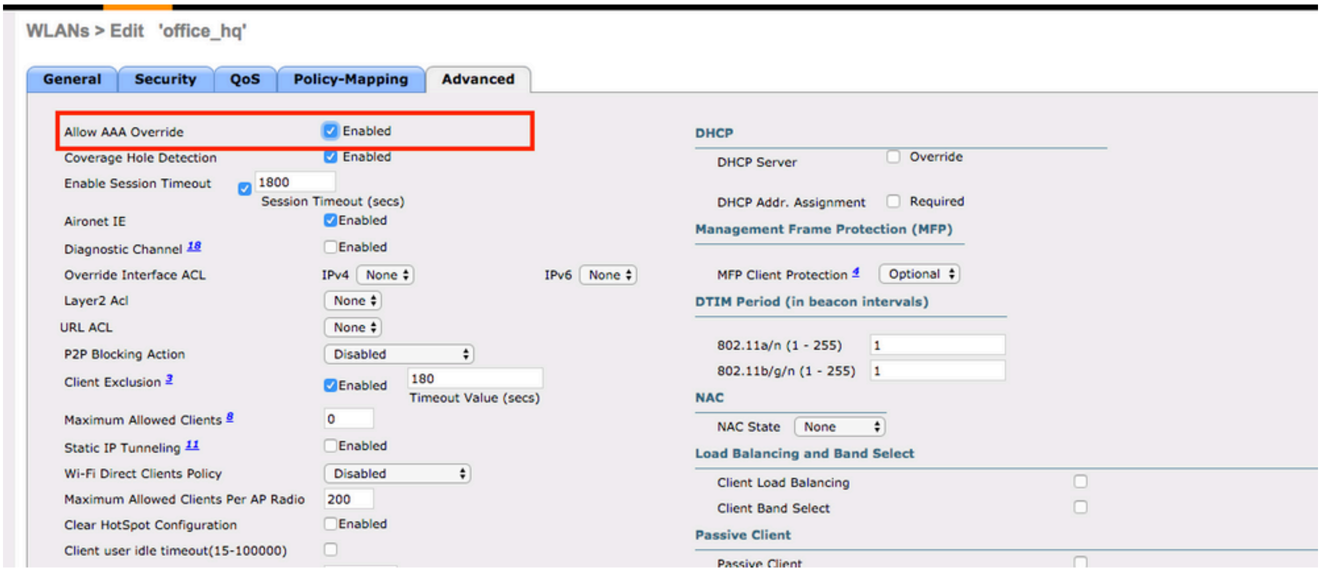
RADIUS Server Overwrite interface □Enabled

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

EAP Parameters

Enable □



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 □ Override

DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

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

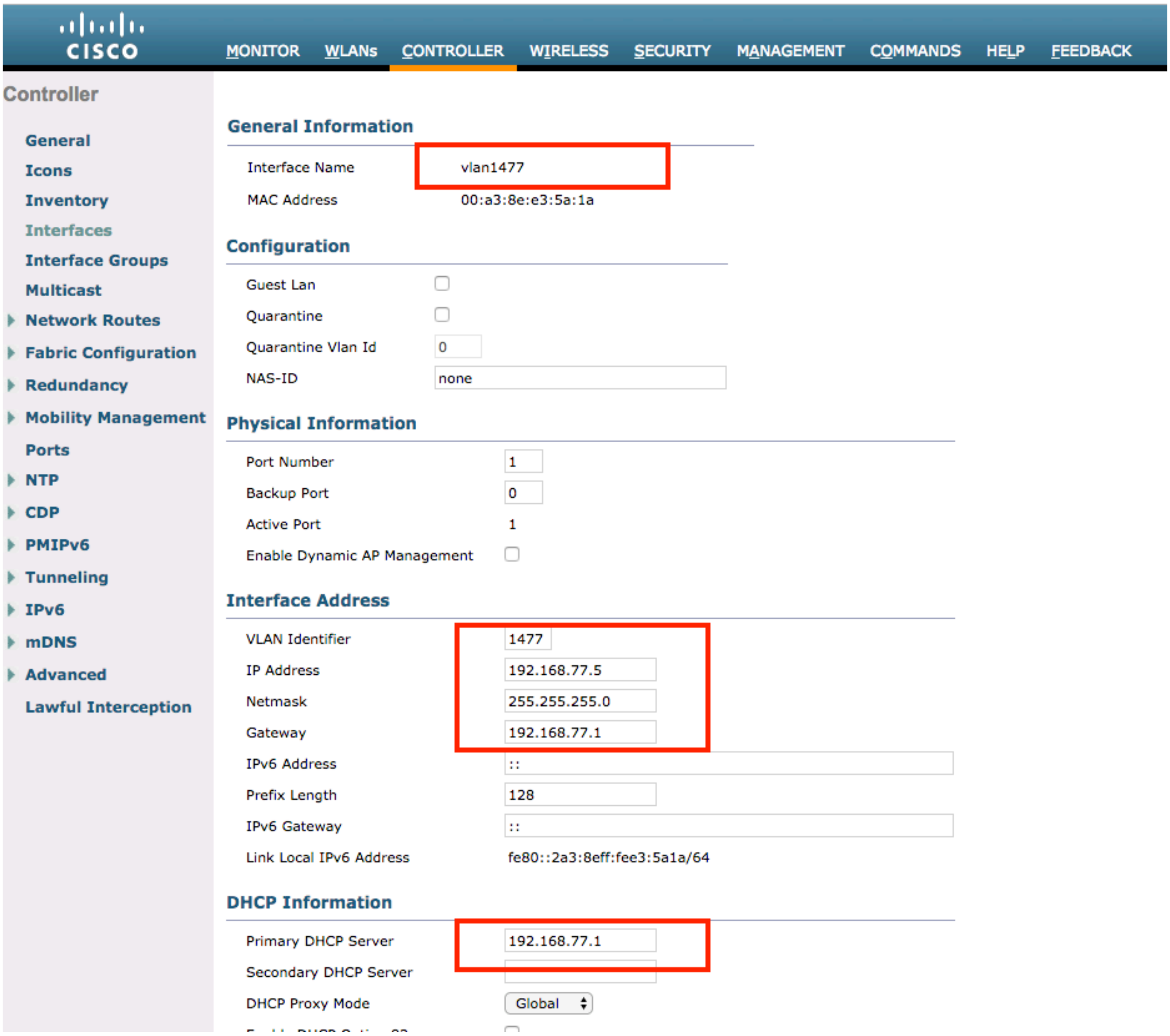
Client Load Balancing □

Client Band Select □

Passive Client

Passive Client □

3. 您还必须在WLC上创建用户VLAN的动态接口。导航至Controller > InterfacesUI菜单。如果WLC在该VLAN中具有动态接口，则它只能执行通过AAA收到的VLAN分配。



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

Enable DHCP Option 82 □

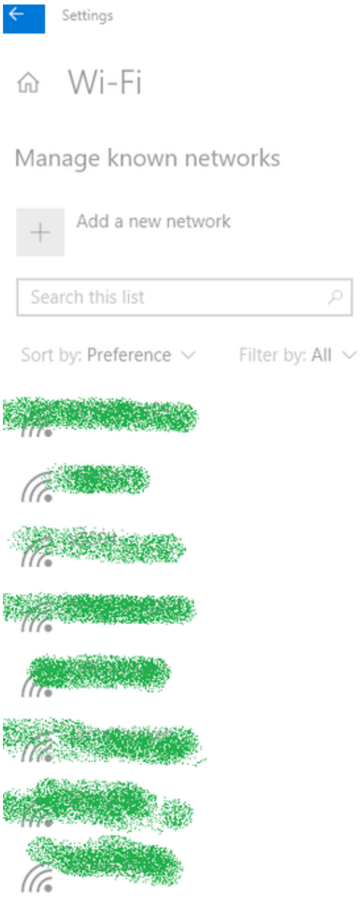
验证

使用Windows 10本地请求方和Anyconnect NAM测试连接。

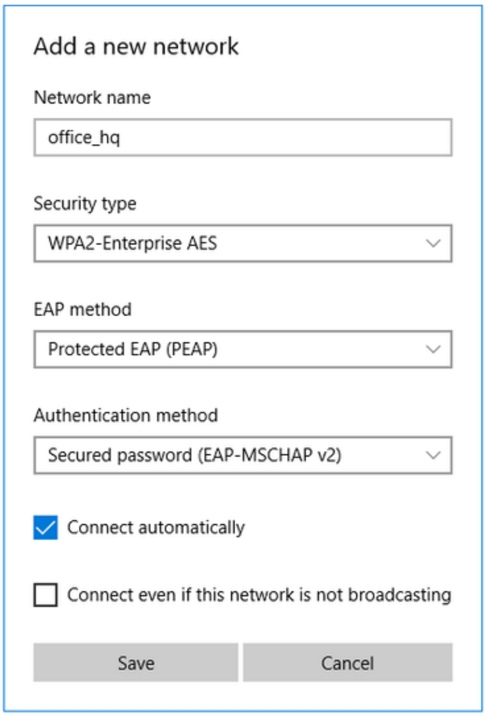
由于您使用的是EAP-PEAP身份验证且ISE使用自签名证书(SSC)，您必须同意证书警告或禁用证书验证。在企业环境中，必须在ISE上使用签名和受信任证书，并确保最终用户设备在“受信任CA”(Trusted CA)列表下安装了相应的根证书。

测试与Windows 10和本地请求方的连接：

1. 打开Network & Internet settings > Wi-Fi > Manage known networks并通过按Add new network钮创建新的网络配置文件；填写所需信息。



[redacted]



Add a new network

Network name: office_hq

Security type: WPA2-Enterprise AES

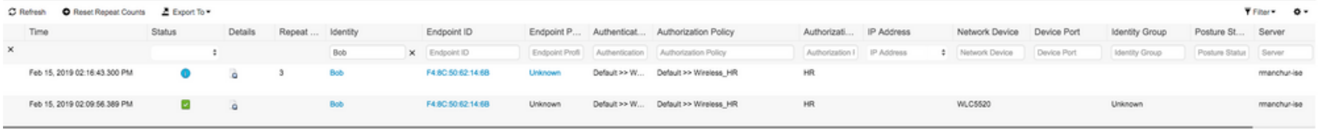
EAP method: Protected EAP (PEAP)

Authentication method: Secured password (EAP-MSCHAP v2)

☑ Connect automatically

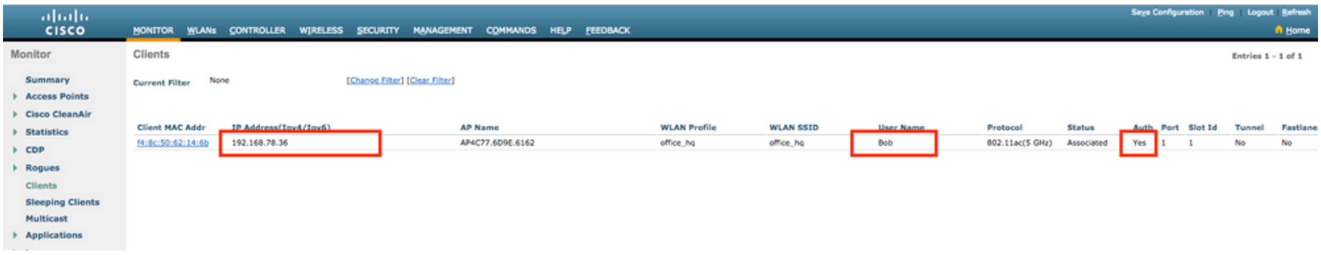
☐ Connect even if this network is not broadcasting

2. 检查ISE上的身份验证日志并确保为用户选择了正确的配置文件。



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture St...	Server
				Bob											
Feb 15, 2019 02:16:43.300 PM	●		3	Bob	F4:8C:50:62:14:6B	Unknown	Default >> W...	Default >> Wireless_HR	HR						rmanchur-ise
Feb 15, 2019 02:09:56.389 PM	✓			Bob	F4:8C:50:62:14:6B	Unknown	Default >> W...	Default >> Wireless_HR	HR		WLC5520		Unknown		rmanchur-ise

3. 检查WLC上的客户端条目，确保它已分配到正确的VLAN并处于RUN状态。



Clients

Current Filter None [Change Filter] [Clear Filter]

Entries 1 - 1 of 1

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel	Fastlane
f4:8c:50:62:14:6b	192.168.78.36	AP4C77.6D9E.6162	office_hq	office_hq	Bob	802.11ac(5 GHz)	Associated	Yes	1	1	No	No

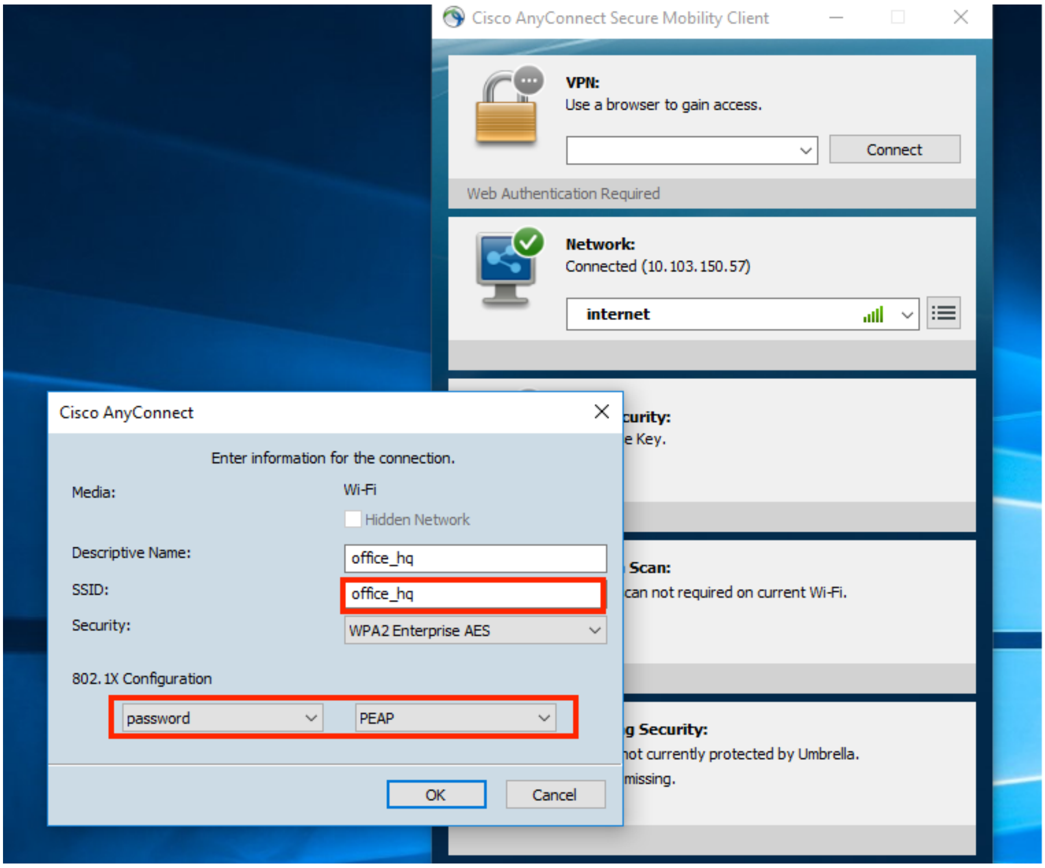
4. 从WLC CLI，可使用show client dertails
命令检查客户端状态：

```
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
```

测试与Windows 10和Anyconnect NAM的连接：

1. 从available SSIDs列表和相应的EAP身份验证类型（在本示例PEAP中）以及内部身份验证表单中选择SSID。



Cisco AnyConnect Secure Mobility Client
VPN:
Use a browser to gain access.
Connect
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
OK
Cancel

Enter information for the connection.

Media: Wi-Fi

□ Hidden Network

Descriptive Name: office_hq

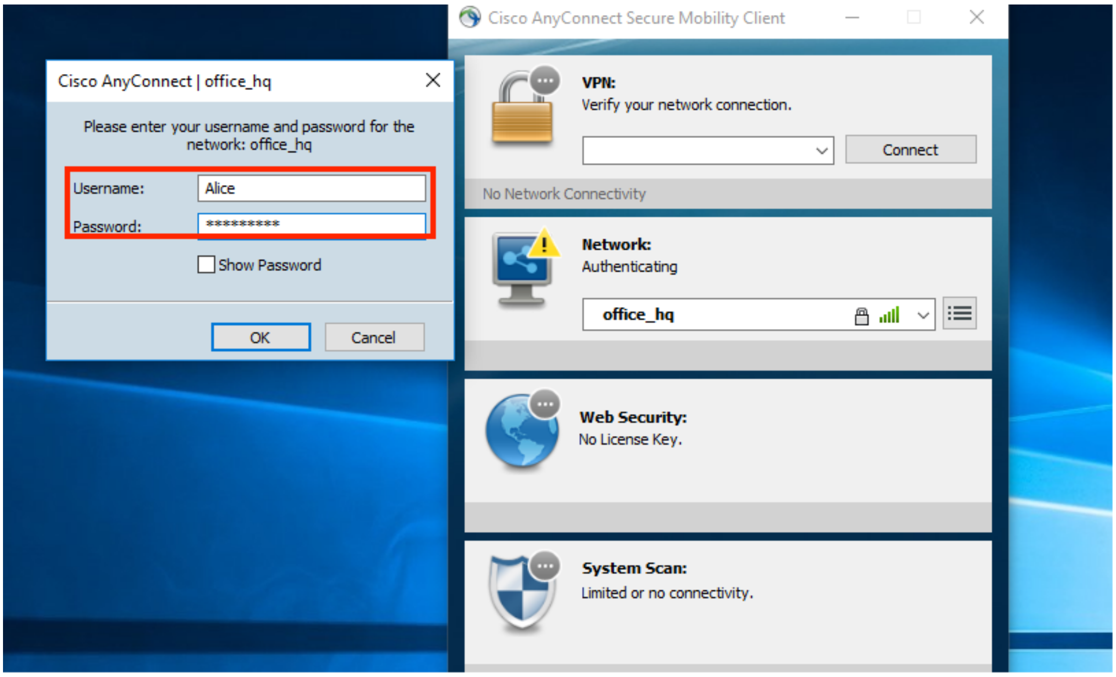
SSID: office_hq

Security: WPA2 Enterprise AES

802.1X Configuration

password PEAP

2. 提供用于用户身份验证的用户名和密码。



Cisco AnyConnect | office_hq

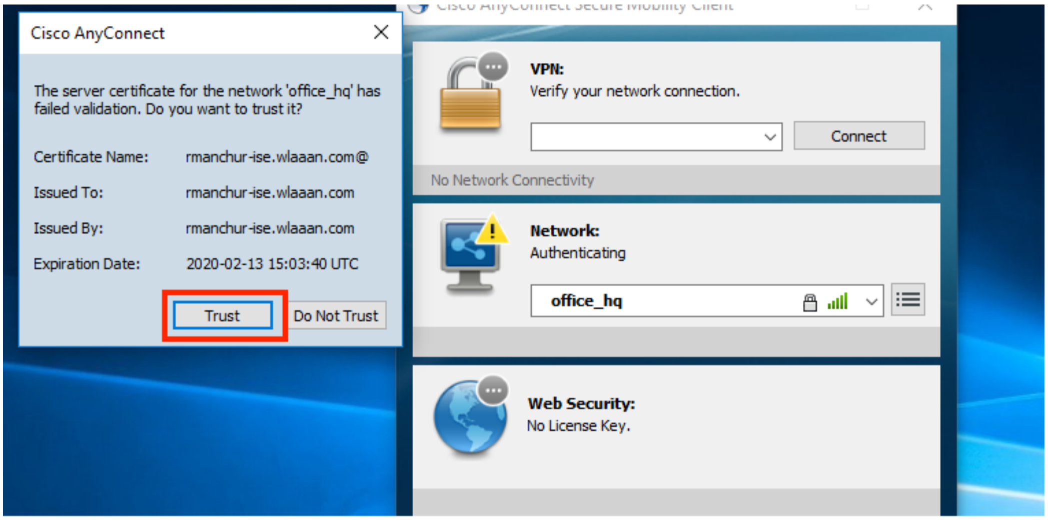
Please enter your username and password for the network: office_hq

Username: Alice

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

□ Show Password

3. 由于ISE正在向客户端发送SSC，您必须手动选择信任证书（在生产环境中，强烈建议在ISE上安装受信任证书）。



Cisco AnyConnect

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

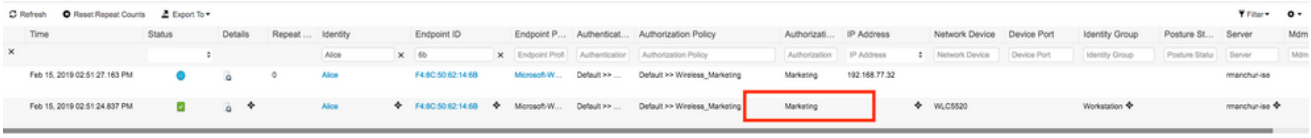
Certificate Name: rmanchur-ise.wlaaan.com@

Issued To: rmanchur-ise.wlaaan.com

Issued By: rmanchur-ise.wlaaan.com

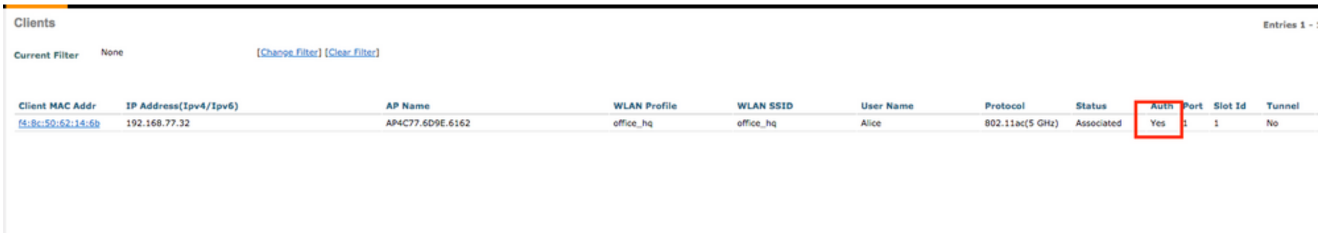
Expiration Date: 2020-02-13 15:03:40 UTC

4. 检查ISE上的身份验证日志并确保为用户选择了正确的授权配置文件。



Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizati...	IP Address	Network Device	Device Port	Identity Group	Posture St...	Server	Mdm
				Alice	6b	Endpoint Profi	Authentication	Authorization Policy	Authorization	IP Address	Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
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					rmanchur-ise	
Feb 15, 2019 02:51:24.837 PM	✓			Alice	F4:8C:50:62:14:6B	Microsoft-W...	Default >> ...	Default >> Wireless_Marketing	Marketing		WLC5520		Workstation		rmanchur-ise	

5. 检查WLC上的客户端条目，确保它已分配到正确的VLAN并处于RUN状态。



Clients

Entries 1 - :

Current Filter None [Change Filter] [Clear Filter]

Client MAC Addr	IP Address(Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel
f4:8c:50:62:14:6b	192.168.77.32	AP4C77.6D9E.6162	office_hq	office_hq	Alice	802.11ac(5 GHz)	Associated	Yes	1	1	No

6. 从WLC CLI，可使用show client dertails 命令检查客户端状态：

```
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
```

故障排除

1. 使用test aaa radius username

password

wlan-id

可测试WLC和ISE之间的RADIUS连接，使用test aaa show radius可显示结果。

```
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. 使用debug client 排除无线客户端连接问题。
3. 使用debug aaa all enable对WLC上的身份验证和授权问题进行故障排除。

注意：请仅对debug mac addr使用此命令，以便根据完成调试的MAC地址限制输出。

4. 请参阅ISE实时日志和会话日志，以确定身份验证失败和AD通信问题。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。