

تایوت حمل

مدقم

ةيسيس، ألا تابل طت ملأ

تابع طتملا

مدختن ملائکہ

تاج الطص الـ

**RADIUS مداخل عم VLAN چک شل یکی مانیدلا نیی عتلای**

نیوکرک

## ةكبش للى طاختل امسيللا

تائیوکتلا

ISE ایلے نبی مدت سے ملک ضریوف تھا اور وہ داصل ملکا تھا اسی سر، ڈیکھتے تو جنم AD ایلے

AAA، SSID 'office\_hg'، مودم WLC بنيوكت، واجتلاع، داشر، ملا dot1x معدل.

## قصص لامباقع

## اھالص او عاطخآل ا فاش کتسا

ةمدقم

نیعت کریم موهفم ۃقیث و اذه فصی

## ةي س اس، ألا تابل طتملا

تالیف طتملہ

Cisco یا سیکسوس نوکت ناؤب فرعم کیدل نوکت اوملاب عیض لاتلا ڈیل:

- ةيكلساللا (WLCs) ةيلحملاءكبشلا يف مكحتلاتاحوب ةيساسأ ةفرعم عضولا يف لوصولا طاقنو Lightweight (LAPs)
  - ISE لثم (AAA) ةبساحملاءضيوفتلاءقداصملامداخل ةيفيظولا ةفرعملاء
  - يكلساللا نامألا تالكشم و ةيكلساللا تاكبشلاب ةقيقد ةفرعم
  - ةيكيماني دللا VLAN ةكبشنويتعتل نيوكتلل ةلباق ةيفيظو ةفرعم
  - لاجملاب مكحتلاراحوال ةفاضلاب Microsoft Windows AD، تامدخل ئيساسألا مهفلاب

میهافم و DNS

- دادم إل او مكحتلا ثيچ نم (CAPWAP) لوصول اطقن لوكوتورب ئيساساً فرع مهيدل

## ةمدختسملا تانوكملا

ئيلاتلا ئيداملا تانوكملا وجماربللا تارادصا ئىل دنتسملا اذه يف ئدراوللا تامولعملما دنتس

- Cisco 5520 Series WLC 8.8.111.0 رادص إل ، تباشلا جمانربلا لغشي يذلا
- cisco 4800 sery AP
- Windows AnyConnect NAM ويلىص ئالا بل اط
- Cisco Secure ISE 2.3.0.298 رادص إل
- Microsoft Windows 2016 Server نيوكت مت لاجملاب مكحت ئدحوك
- Cisco 3560-CX 15.2(4)E1 رادص إل لغشي يذلا

ئصالخ ئيلمعم ئيپ يف ئدوجوملا ئزهجألا نم دنتسملا اذه يف ئدراوللا تامولعملما عاشن مت تناك اذا . (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ئمدختسملا ئزهجألا عيمج تأدب رمأ يأ لمحتملا ريثأتلل كمهف نم داكتف ، ليغشتلا ديق كتكتبش.

## تاحالطصا

[تاحالطصا لوح تامولعملما نم ديزم ىلع لوصحلل ئينقتلا Cisco تاحيملت تاحالطصا عجرات دنتسملا](#)

## RADIUS مداخ عم VLAN ۋە كېشل يكيماني دلا نيءيعتل

عالمعلا عيمج ىلع قبطنن ئتباث ئس اي س WLAN ۋە كېش لكل نوكى ، ئامظنان مطعم يف مغرلا ىلعو . مكحتلا ئدح وتاحالطصم يف WLAN وأ (SSID) ئمدخللا ئعومجم فرع مب ني طبترملما ب نارتقا ال ئالمعلا نم بلطتت اهنأل دويق اهل ئقيرطلا هذه نأ ال ، ئلاعف اهنأ نم فلتخملا ناما ال جهنو (QoS) ئمدخللا ئدوج ئثارول ئفلىخ.

حمسى اذهو . ئي وهلا تاكبش مع د ئطساوب ددحت ييتلا Cisco نم WLAN تاكبش لولج نيءوانع ئدوج ئيروت ب نيددح نيمدختسملا حمسى هنكلو دحاو SSID فرع نع نالع إلاب ئاكبش لل دامتغا تانايىب ئىل دنتسملا ناما ال تاس اي س وأ VLAN تامس و ئفلىخ ئاملا (QoS) ئمدخللا مدختسملا.

ئاكبش يف يكلىسال مدختسم عضت ييتلا تازىملا كلت دحأ و ئيكيماني دلا VLAN نيءيعت ئممهملا هذه ئجل اعم ممت . مدختسملا اهمدق ييتلا دامتغا تانايىب ىلع ئانب ئنيعم RADIUS ، Cisco ISE . ئاقبلا يكلىساللا فيض ملل حامس ل ، لاثملا ليبس ىلع ، اذه مادختس ئاكمىي ئاكبش ىلع ئاقبلا يف يكلىساللا مداخ ئاسف ئانثا اهسفن VLAN .

دعاؤق نيب نم ئدحاو تانايىب ئدعاق لباقم نيءيكلساللا نيمدختسملا Cisco ISE مداخ ق داصي

لابتملا ليبس ىلع .ةيلخادلا هتانايip ٰدعاق نم ضت ،ةلمتحم ٰددمتم تانايip

- ةيلخاد تانايip ٰدعاق
- طشنلا ليلدلا
- ليلدلا ىلإ لوصولل في فخل ماعلا لوكتوربلا (LDAP)
- ٰحوت فمل تانايibla ٰدعاق لاصتا عم ٰقف اوتم ةي طابترا تانايip دعائق (ODBC)
- نم ٰزيممل SecureID و Rivest Shamir و Adelman (RSA) مداو خ
- عم ٰقف اوتمل زيممل زمرلا مداو خ RADIUS

تالوكوتورب فلت خ ٰقمع دمل ةيج راخلا ةي وهلا رداصم Cisco ISE ٰقداصم تالوكوتورب درست .ةيج راخلاو ةيلخادلا ٰدعائق طساوب ٰقمع دمل ةقداصمل

ٰدعاق نوم دختس ي نيدلا نيكلساللا نيم دختس مل ةقداصم ىلع دنتسملا اذه زكري .ةيج راخلا Windows Active Directory تانايip

ٰدعاق نم مدختس مل كلذب ةصالخا ٰعومجم مل اتما ولع ةجيءو ،ٰقداصمل حاجن دعب .صالخا لي وختلا في رعت فلمب مدختس مل طبريو Windows تانايip

،مكحت ٰدحو عم ٰلجم Lightweight عضولا يف لوصو ٰطقن عم نرتقي نأ لي معلا لواحي امدنع رصنع ىلإ مدختس مل دامتعا تانايip ررمت Lightweight عضولا يف لوصولا ٰطقن ناف بولسأب ةصالخا تامي لمعتل امادختس اب (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا EAP .ةلصلأا يذ

EAP نم ضت ي يذلا (RADIUS) لوكتورب مادختسا اب ISE ىلإ هذه دامتعالا تانايip WLC لسرت لوكتورب ٰدعاس مب ققحتلل AD ىلإ نيم دختس مل دامتعا تانايip Kerberos .ررمي و

مالعاب موقعي ،ٰقداصمل حاجن دنع و مدختس مل دامتعا تانايip ٰحص نم ققحتلاب AD موقعي ISE .

تنرتن إلأ ئس دنه لمع قرفل ئنيعم تامس ريرمب ISE مداخ موقعي ،ٰقداصمل حاجن درجمب هذه RADIUS تامس ددحت (WLC) .ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع ىلإ (IETF) ب قلعتي امي ف WLAN (SSID) مهي ال .يكلساللا لي مععل هنيري عت بجي يذلا VLAN فرع م .اقبسم ددح مل امئاد مدختس مل نيري عت مت ي هنأ ليمعل VLAN (WLC)

ي ه VLAN فرع نيري عتل ٰمدختس مل RADIUS مدختس مل تامس :

- IETF 64 ىلإ اذه تتبث—(قفنلا عون) VLAN
- IETF 65 ىلإ اذه نيري عت—(قفنلل طسوتم عون) 802
- IETF 81 ىلإ اذه تتبث—(صالخا قفنلا ٰعومجم فرع) VLAN id

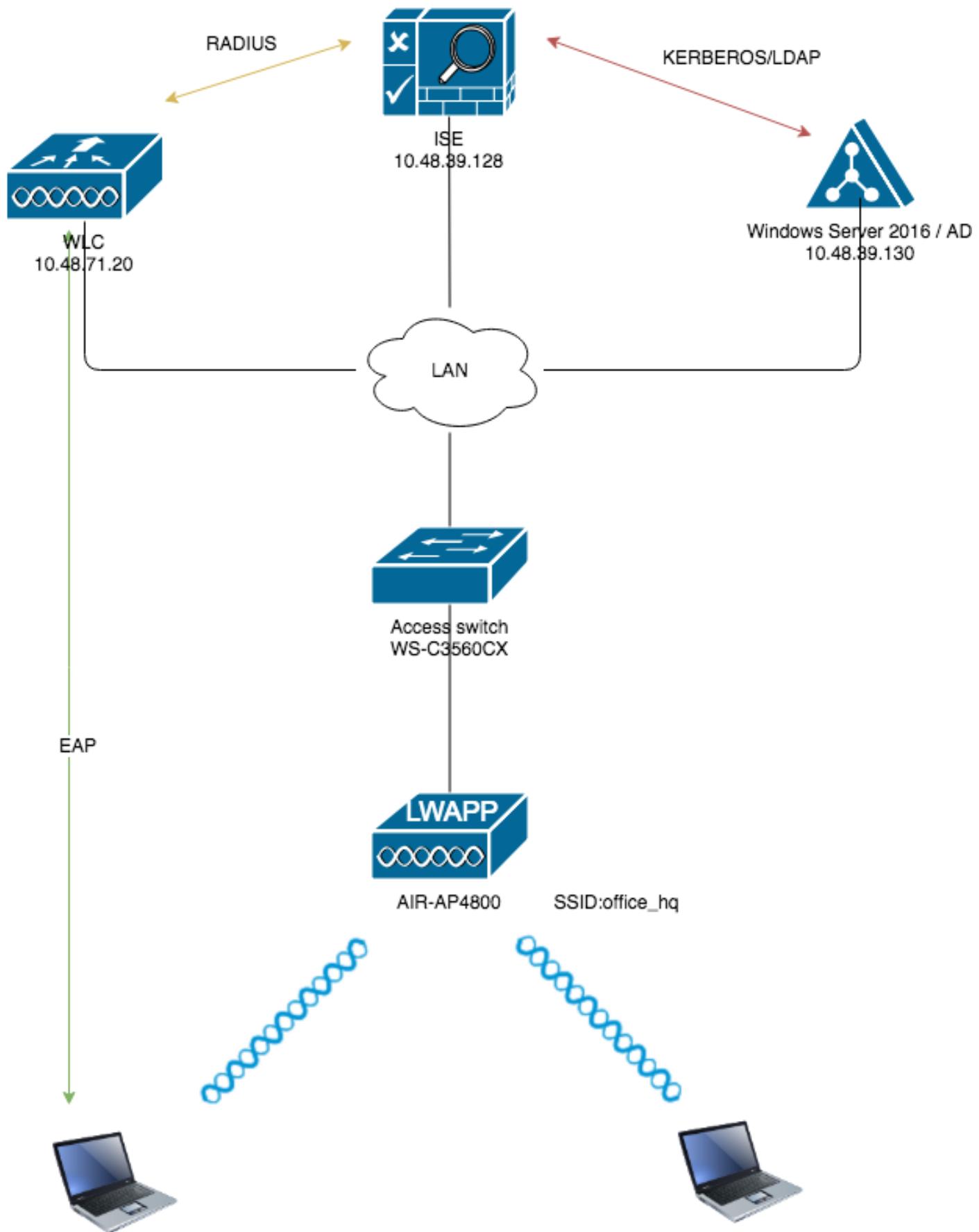
Tunnel-Private- نأ .ةلماش ،4094 و 1 نيب ٰقميق ذخأي و تب ٰدحو 12 وه VLAN مت ي ، IEEE 802.1X عوم مادختسا الل RFC2868 يف ددح م وه امك ،ةلس لس عونلا نم وه ،هذ قفنلا تامس لاسرا مت ي امدنع .ةلس لس VLAN فرع مل حيحصل ددعلا ٰقميق ريفشت ،زييمتل اماع لقح يف ألمت نأ يرورضلا نمف .

لوطب دحاو ينامث ماظن نع ةرابع ةماليعلا لقح: 3.1: مسقلا، [RFC 2868](#) يف ةراشإلا تمت امك سفن ىلا ريشت يتلا ةمزحلا سفن يف تامسلأا عيمجتل ةليسو ريفوت هب دصقيو ريع ةماليعلا لقح ناك اذا .ةلماش، 0x01 ىتح 0x1F، يه لقحلا اذهل ةحلالصلما ميقلأا .قفنلا لوح تامولعملانم ديزم ىلع لوصحلل [RFC 2868](#) عجار.(0x00) رفص نوكبي نأ بجي، مدخلتسنم تامس عيمج RADIUS.

## نيوكتلا

دنتسملا يف ةحضوملا تازيملا نيوكتل ةمزاللا تامولعملامسقلا اذه رفوي.

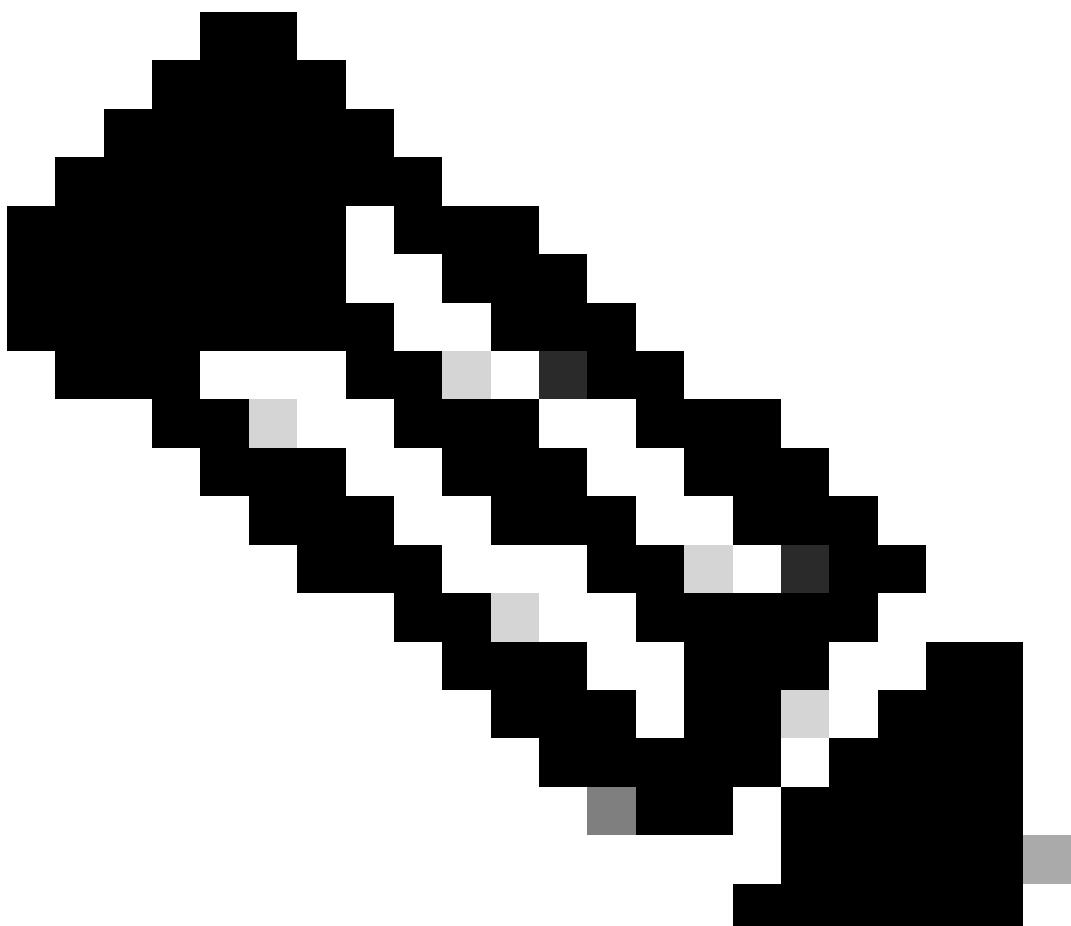
## ةكبشلل يطيطختلا مسرا



تاني وكتلا

ططخمل اذه يف ۋەمدىخىسىمىلا تانوكمىلا نىوكت ليصافت يە ذە:

- ناوونع IP مداخلاً ISE (RADIUS) 10.48.39.128.
  - ئيلحملا ئكبسلا يف مكحتلار ئدحوب ئصالخا AP-Manager و ئرادىلار ئهجاناونع (WLC) 10.48.71.20.
  - متى الو ئيلباقملار ئالىمجلات ئامجتلەنۈيوكتىمىتى LAN ئكبس يف DHCP مداخ دجاوتى ططخملار ئيف هضرۇم.
  - نىوكتىمىتى .نىوكتلار اذە رېب VLAN1478 ئكبس و VLAN1477 ئكبس مادختسى متى نىوكتىمىتى و VLAN1477 ئكبس يف مەعۇضولجىنەم قىيىوستىلا مىسق نەم نىيمدختىسىملا مداخ ئەتساوب VLAN1478 ئكبس يف مەعۇضولجىنەم HR مىسق نەم نىيمدختىسىملا سەفنەب نىيمدختىسىملا الىك لىصتى امدىنەع SSID — office\_hq.
- VLAN1477: 192.168.77.0/24. اپلار 192.168.77.1. VLAN1478: 192.168.78.0/24. اپلار 192.168.78.1
- ناماً ئيلآك 802.1xPEAP-mschapv2 دنتسىمىلا اذە مىدختسى.
- 



EAP-FAST و Cisco اپلار مادختسى ئوقداشىم لىثم، ئەمدقتىمىلا ئوقداشىملا قرط مادختسى Cisco يىصوت ئەظحالىم

---

EAP-TLS، WLAN نيمأتل ۋە كېش.

نېوكتىلا اذه ذىفنت لبىق تاپسا ارتفالا ھۇزۇمۇتى:

- اپلەپ لەپ لەپ لەپ لەپ

- مەدەنلەپ DHCP قاپان نېيىعت مەت

- ئەكپشلى يەن ئەزىزىلەپ عىمەج نېب 3 ئەقپەطلى لەصتا دەچۈمى

- ئەكپشلى نأ ضرۇتفىو يېكلىساللا بەناجلا ئىلۇ بولطمەلە نېوكتىلا دەنتسەملە شەقانىي اھۇضۇم يەن ئېكلىساللا

- ئىلۇ ئەصاخلا تاپسا وەجمەلەو نېمەدختسەملە نېوكت مەت

ئەكپشلى يەن مەكھىتىلا مەئاوق مادختساب ئېكىيەمانىدىلە VLAN ئەكپش نېيىعت زاجنا لەجأ نەم ھەذە ذىفنت بەجي، AD، IEEE نېيىعت ئىلە اداھاتسە (WLCs) ئېكلىساللا ئەيلەحملە: تاوطخۇلما

ئىلۇ نېمەدختسەملەل ضىوفتىلەو ئەقادىصەلە تاسايسىن نېوكت و AD ئىلە IEEE.

2. مەعەنەن ئەنلەپ زواجتەوەx AAA ل SSID 'office\_hq'.

3. يەنلەپ سەمتىلەن نېوكت.

ئىلۇ نېمەدختسەملەل ضىوفتىلەو ئەقادىصەلە تاسايسىن ئەئىھەت و جەنم د ئىلە AD ئىلە IEEE

1. لەفۆرم بەسەح مادختساب IEEE Web UI ئەجاو ئىلە لۇخىلە لېجىست.

2. Administration > Identity management > External Identity Sources > Active directory.

The screenshot shows the Cisco ISE web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC, Identities, Groups, External Identity Sources (which is currently selected), Identity Source Sequences, and Settings.

The main content area is titled "External Identity Sources". On the left, a tree view lists various authentication profiles: Certificate Authentication Profile, Active Directory (selected), LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The "Active Directory" node under "Certificate Authentication Profile" is highlighted.

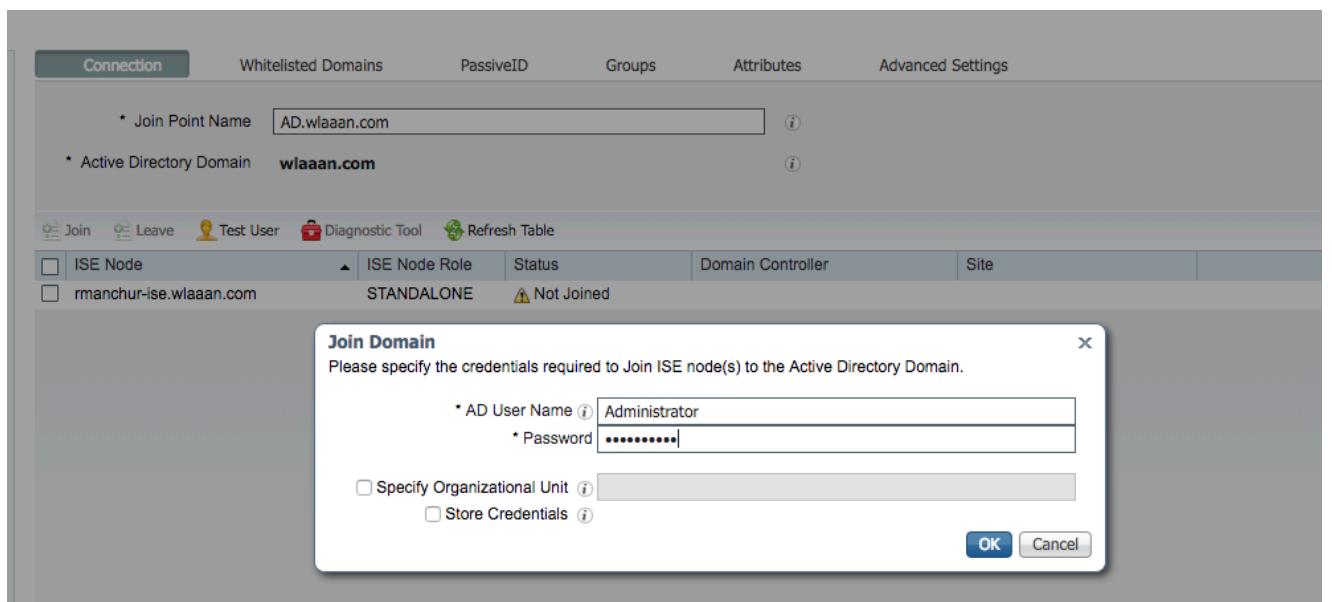
To the right, a separate window titled "Active Directory" shows a list of "Join Point Name" and "Active Directory Domain". A message at the bottom right states "No data available".

3. مامضىنالا ئەطقن مەسەا "تادادعە نەم ئىوهەلە نزەم مەسەو لاجىلە مەسەلخ داؤ ئەفاضى قوف رقنى. ئەطقن دىدەت مەتىو wlaaan.com لاجىلە يەن IEEE لېجىست مەتى، لاثمەلە يەن Active Directory".

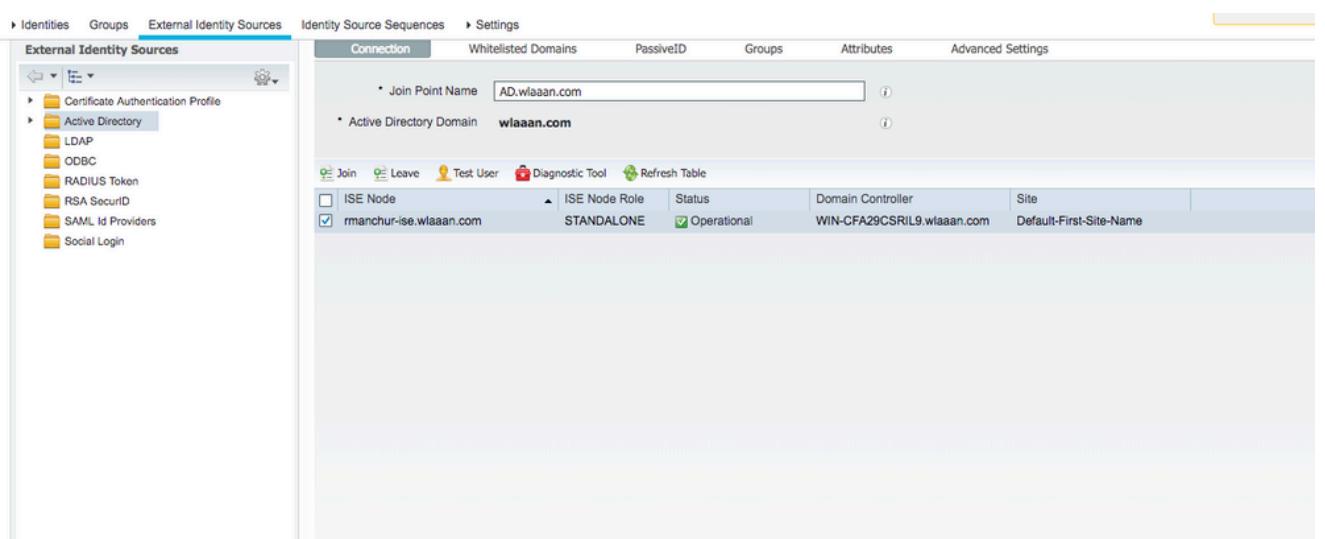
AD.wlaaan.com-ك لەصتا AD.wlaaan.com-ك لەلەجەم مەاه مەسەا IEEE.



4. AD ىلإ ISE مرضنت نأ ديرت تنك اذى كلأسى رز طغض Submit دع بـ ققثبنم ڈفان حتفى. ۋەپاسىنلا لوقسىملا قوقج عم دامتىع Active Directory مىدختىمىم دامتىع Yes طغضىرا. ارۇف لاجىملا ىلإ دىدج فىيضم.



5. يف حاجنب لجىسم ISE كىدل نوكىي نأ بجي، ۋەطقنلا ھذه دع بـ AD.



مادختىسى كىنكمىي، ليجىستلا ۋېلىمۇ يف كىدل لكاشم يأ دوجو ۋەلاح يف Diagnostic Tool in order to اتسال ئېبولىملا تارابتىخالا تىرىپ كر AD.

في رعت تافلم ندي عتل اهم ادختس ا متي يتلا ظطش نلا لئال دل ا تاع ومجم دادرتس ا بجي  
Administration > Identity management > External Identity Sources > Active directory >

## > Groups

، اخراجی قواف رقنا مث ، Select Groups from Active Directory.

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

▶ Identities Groups External Identity Sources Identity Source Sequences ▶ Settings

**External Identity Sources**

Connection	Whitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings
<p>Edit <span style="color: green;">+ Add</span> <span style="color: red;">Delete Group</span> Update SID Values</p> <p>Select Groups From Directory</p> <p>Add Group</p> <p>No data available</p>					

Active Directory  
AD.wlaan.com

LDAP

ODBC

RADIUS Token

RSA SecurID

SAML Id Providers

Social Login

7. ئەعومۇجىم دادرتسال ئېفصىت لىماع دىدحت كنكمىي ثىح ئەدىج ئەقىشىنم ئەذفان حەتفت.  
نۇم تاڭۇمۇجىملا ئېمچ دادرتسا وأ ئەنىيۇم (تاڭۇمۇجىم) AD.  
طغىچىسى او AD ئەعومۇجىم ئەمىئاق نۇم ئېنۇملىكلا تاڭۇمۇجىملا رىتىخا OK.

**Select Directory Groups**

This dialog is used to select groups from the Directory.

Domain		wlaaan.com		
Name Filter		*	SID Filter	
			Type Filter	
Retrieve Groups... 13 Groups Retrieved.				
<input type="checkbox"/>	Name	Group SID	Group Type	
<input type="checkbox"/>	wlaaan.com/Users/Cloneable Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-522	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/DnsUpdateProxy	S-1-5-21-2222429329-4108085164-3220345271-1102	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Domain Admins	S-1-5-21-2222429329-4108085164-3220345271-512	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Domain Computers	S-1-5-21-2222429329-4108085164-3220345271-515	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-516	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Domain Guests	S-1-5-21-2222429329-4108085164-3220345271-514	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Domain Users	S-1-5-21-2222429329-4108085164-3220345271-513	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Group Policy Creator Owners	S-1-5-21-2222429329-4108085164-3220345271-520	GLOBAL	
<input checked="" type="checkbox"/>	wlaaan.com/Users/HR	S-1-5-21-2222429329-4108085164-3220345271-1105	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Key Admins	S-1-5-21-2222429329-4108085164-3220345271-526	GLOBAL	
<input checked="" type="checkbox"/>	wlaaan.com/Users/Marketing	S-1-5-21-2222429329-4108085164-3220345271-1104	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Protected Users	S-1-5-21-2222429329-4108085164-3220345271-525	GLOBAL	
<input type="checkbox"/>	wlaaan.com/Users/Read-only Domain Controllers	S-1-5-21-2222429329-4108085164-3220345271-521	GLOBAL	

Save. اهظفح نكمي وISE ىلا ئىنعملا تاعومجملا ئفاضا متن.

Connection Whitelisted Domains PassiveID Groups Attributes Advanced Settings

Edit Add Delete Group Update SID Values

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

**Save** **Reset**

9. ایلی لقتنا - ISE ڈکبش زاہج ڈمئاق ایلی WLC ڈفاصن اور طغض ایڈد Devices Add.
- و WLC نیب کرتشملا RADIUS رسو WLC و رادل IP ناونع ریفوت لالخ نم، لمک نیوکت ISE.

Identity Services Engine Administration > Network Resources > Network Devices

Network Devices List > New Network Device

Network Devices

- Name: WLC5520
- Description:
- IP Address: 10.48.71.20 / 32
- 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

10. ةيلح ملا ةكبشلا يف مكحتلا رصنه ةفاض او AD ئلإ ISE ئلإ كمامضنا دعب نآلأ  
ةقداصملاتاسايس نيوكت عدب كنكمي ،ةزهجألا ةممئاق ئلإ (WLC) ةيكليساللا  
نيمدختسممل ضيوفتل او.

- ئلإ قيوستلا نم نيمدختسملا نيعتل ضيوفت فيرعت فلم عاشناب مق VLAN1477 HR ئلإ عومجم نمو VLAN1478.
- **قفوف رقناو** ئلإ لقتنا Policy > Policy Elements > Results > Authorization > Authorization profiles  
ديدج صيصخت فلم عاشنالل Add رزلا.

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices.
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal authentication.
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the web authentication page.
NSP_Onboard	Cisco	Onboard the device with Native Suplicant.
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Deny.
PermitAccess		Default Profile with access type as Access-Permit.

- **وعومجممل VLAN** ةكبش تامولعم مادختساب ليوختلا فيرعت فلم نيوكت لمكأ .  
وعومجممل نيوكت تادادعMarketing اثمل احضوي ؛ةينعملما.

Dictionaries > Conditions > Results

**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

Submit Cancel

وەم الاع تامس نیوکت بجی و ئىخالا تاوعومجم لىلثامم نیوکت ئارج ابجي  
وەلباقاملا.

- وەق دااصملاباس اياس ديدحت كنكمي، ليوختلا تافيصوت نیوکت دعب  
وەعومجم نیوکت لالخ نم اما كلذب مايقلابا نكمي. نېيكلساللا نيمدختسمىلل  
ئيضاارتفالا جەنللا ۋەعومجم لىدعت مەت، لاثملابا اذه يەف اھلىدىدعت واجەنلابا  
مەدختسىي، وەق دااصملابا عونلادot1x ايضاارتفالا Policy > Policy Sets > Default.  
ئيلاحلابا ئيضاارتفالا تادادعىلا عم يىتح لمعى ھەنأ نم مغىرلا ىلۇع،  
لاثملابا اذه مەدختسىي، All\_User\_ID\_Stores، ۋەل ئيواھلا رەصم ۋەمىئاق نم عزج وە AD ناڭ ارظن  
رەصمك AD مەدختسىي و ئىنعملا مەكحەتلابا ۋەل WLC\_lab دىدەت رىڭڭا ۋەدعاق  
وەق دااصملابا دىچو.

- نوييعتب نوموقي نيذلا نيمدخلتسملل ليوخت تاسايس عاشننا نآلاكيلع بجي  
لى لقتنان. ةعومجملا ئيوضع لى ادانتسا ةصالخ ليوخت فيرعت تافلم  
Authorization بلطتملا اذه قيقحت لجأ نم تاسايس عاشناب مقو مسقل policy.

WLC ل AAA ج SSID 'office\_hq' زواجتو dot1x وفقااصم معدل نيوكت

1. ئيلإ لقتنان RADIUS مدادخك WLC. ئيلإ لقتنان RADIUS > AAA > RADIUS > Security > AAA > RADIUS > Authentication ISE IP او مولعمل اوناع رفوبىولا مدخلتسا مهجاو يف مسق  
ةيرسلاتا كرتشملا.

**CISCO**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

## Security

### RADIUS Authentication Servers > New

**AAA**

- General
- RADIUS
  - Authentication
  - Accounting
  - Auth Cached Users
  - Fallback
  - DNS
  - Downloaded AVP
- TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
- Disabled Clients
  - User Login Policies
  - AP Policies
  - Password Policies

**Local EAP**

**Advanced EAP**

**Priority Order**

**Certificate**

**Access Control Lists**

**Wireless Protection Policies**

**Web Auth**

**TrustSec**

**Local Policies**

**Umbrella**

**Advanced**

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	<input checked="" type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (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	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

WLANs		WLANs					
WLANs		WLANs					
Current Filter: None		<a href="#">[Change Filter]</a> <a href="#">[Clear Filter]</a>			<a href="#">Create New</a> <a href="#">Go</a>		
<a href="#">WLANs</a>		WLANs					
WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies		
1	WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
253	WLAN	BTER-BTwifi-public	BTwifi-public	Enabled	[WPA2][Auth(PSK)]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

WLANs > New

Type	<input type="text" value="WLAN"/>
Profile Name	<input type="text" value="office_hq"/>
SSID	<input type="text" value="office_hq"/>
ID	<input type="text" value="3"/>

[Back](#) [Apply](#)

## WLANS &gt; Edit 'office\_hq'

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

Profile Name	office_hq
Type	WLAN
SSID	office_hq
Status	<input checked="" type="checkbox"/> 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	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

## WLANS &gt; Edit 'office\_hq'

**General** **Security** **QoS** **Policy-Mapping** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security	WPA+WPA2
MAC Filtering	<input type="checkbox"/>
<b>Fast Transition</b>	
Fast Transition	Adaptive
Over the DS	<input checked="" type="checkbox"/>
Reassociation Timeout	20 Seconds
<b>Protected Management Frame</b>	
PMF	Disabled
<b>WPA+WPA2 Parameters</b>	
WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES
TKIP	<input type="checkbox"/>
CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>
GCMP256	<input type="checkbox"/>
<b>OSEN Policy</b>	
<b>Authentication Key Management</b>	
802.1X	<input checked="" type="checkbox"/> Enable
CCKM	<input type="checkbox"/> Enable

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		EAP Parameters
<input checked="" type="checkbox"/> Enabled	IP:10.48.39.128, Port:1812	<input checked="" type="checkbox"/> Enabled	IP:10.48.39.128, Port:1813	Enable <input type="checkbox"/>
Server 1	None	Server 2	None	
Server 3	None	Server 4	None	
Server 5	None	Server 6	None	
Server 6	None			
<b>Authorization ACA Server</b>		<b>Accounting ACA Server</b>		
<input type="checkbox"/> Enabled		<input type="checkbox"/> Enabled		
Server None		Server None		

WLANS > Edit 'office\_hq'

**General**

- Allow AAA Override  Enabled
- Coverage Hole Detection  Enabled
- Enable Session Timeout  1800 Session Timeout (secs)
- Aironet IE  Enabled
- Diagnostic Channel [10](#)  Enabled
- Override Interface ACL IPv4  None IPv6  None
- Layer2 Acl  None
- URL ACL  None
- P2P Blocking Action  Disabled
- Client Exclusion [2](#)  Enabled 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 [1](#)  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. **Controller > VLANs.** لمعتسمل WLC لىل ع يكرح نرافق تقلخ اضيأ يغبني تنأ. **نأ AAA** رباع ملتسي VLAN تدهم طقف عي طتسى WLC لىا. مدخلتسمل الة هجاو و قمىاق Interfaces VLAN نأ يف يكرح نرافق وە ىقلتى.

**Controller**

**General**

**Icons**

**Inventory**

**Interfaces**

**Interface Groups**

**Multicast**

▶ **Network Routes**

▶ **Fabric Configuration**

▶ **Redundancy**

▶ **Mobility Management**

**Ports**

▶ **NTP**

▶ **CDP**

▶ **PMIPv6**

▶ **Tunneling**

▶ **IPv6**

▶ **mDNS**

▶ **Advanced**

**Lawful Interception**

**General Information**

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

**Configuration**

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

**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

## ةحصـلـا نـم قـقـحتـلـا

رابط خال AnyConnect NAM و Windows 10 ليغشتلا ماظنل ةيلصلأا ئبلاطملا مدخلتساً تالاصتالا.

نأ بجي ،(SSC) اي تاذ عقوم ةداهش مدخلتسي EAP-PEAP ئق داصم مدخلتست كنأ امب كيلع بجي ،تاكرشلا ئي بيف . ةداهشلا نم قبحتللا لي طمعت وأ ةداهش ريدحت ئلע قفافت ئلע يئاهنلا مدخلتسملأا ۆزهجاً لوصح نامض وISE يف اهب قووثوم و عقوم ةداهش مدخلتسا اهب قووثوملا CA ۆرمىاق نامض ئتبثمللا ئبسانمللا رذجلما ئداهشلا

يصل ألا بـ Windows 10 ليغشتل ماظنباً لاصتاً رابتخاً

- دي دج ئىكبس فى يرغت فلم ئاشناب مقولا تامولعملار ئېبعتب مقولا زىل ئىل عرضلاب Add new network.

The screenshot shows the Windows Settings interface under 'Wi-Fi'. It displays a list of known networks, each represented by a green icon and a blurred name. Below the list are buttons for 'Add a new network' and a search bar. To the right, a modal window titled 'Add a new network' is open, containing fields for 'Network name' (set to 'office\_hq'), 'Security type' (set to 'WPA2-Enterprise AES'), 'EAP method' (set to 'Protected EAP (PEAP)'), and 'Authentication method' (set to 'Secured password (EAP-MSCHAP v2)'). There are also two checkboxes: 'Connect automatically' (checked) and 'Connect even if this network is not broadcasting' (unchecked). At the bottom of the modal are 'Save' and 'Cancel' buttons.

حیحصلاء فیرعتلار فلم دیدحت نم دکأت و ISE لود دنوع قدادصملا لجس نم ققحت. مدخلتسملل.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorizatio...	IP Address	Network Device	Device Port	Identity Group	Posture St...	Server
Feb 15, 2019 02:16:43 300 PM	<span style="color: blue;">●</span>	Q	3	Bob	F4:8C:50:62:14:6B	Unknown	Default >> W...	Default >> Wireless_HR	HR					manchu-ise	
Feb 15, 2019 02:09:56 389 PM	<span style="color: green;">■</span>	Q		Bob	F4:8C:50:62:14:6B	Unknown	Default >> W...	Default >> Wireless_HR	HR	WLC5520			Unknown	manchu-ise	

3. ئيكلساللا ئيلحملار ئاكبىشلار يف مكحتلار رصىنۈلىك لىمعلار لاخدا نم ققحت. لىغشتلار ئالاح يف هنأ نموىنمىلار VLAN ئاكبىشلەرنىيەت نم دکأت و.

The screenshot shows the Cisco WLC Client Monitor interface. On the left, there's a navigation menu with options like MONITOR, WLANs, CONTROLLER, WIRED, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The main area displays a table of clients. The table has columns for Client MAC Addr (highlighted with a red box), IP Address (highlighted with a red box), AP Name, WLAN Profile, WLAN SSID, User Name (highlighted with a red box), Protocol, Status, Auth. Port, Slot Id, Tunnel, and Fastlane. The table shows one entry: Client MAC Addr F4:8C:50:62:14:6B, IP Address 192.168.78.36, AP Name AP4C77.609E.6162, WLAN Profile office\_hq, WLAN SSID office\_hq, User Name Bob, Protocol 802.11ac(5 GHz), Status Associated, Auth. Port 1, Slot Id 1, Tunnel No, and Fastlane No. At the top right, there are links for 'Save Configuration', 'Ping', 'Logout', and 'Refresh'.

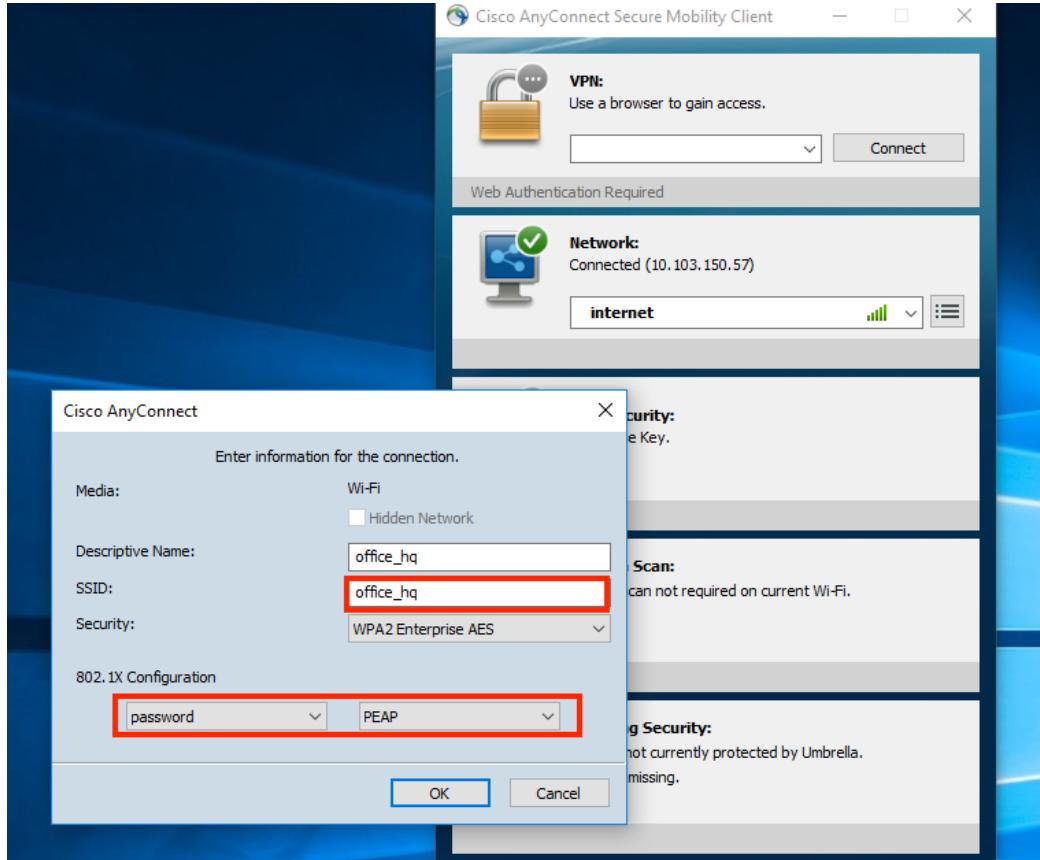
4. ئيكلساللا ئيلحملار ئاكبىشلار يف مكحتلار رصىنۈلىك (CLI) رم او رطس ئادختساپ لىمعلار ئالاح نم ققحتلار نكمىي:

```
show client detail f4:8c:50:62:14:6b
Client MAC Address..... f4:8c:50:62:14:6b
```

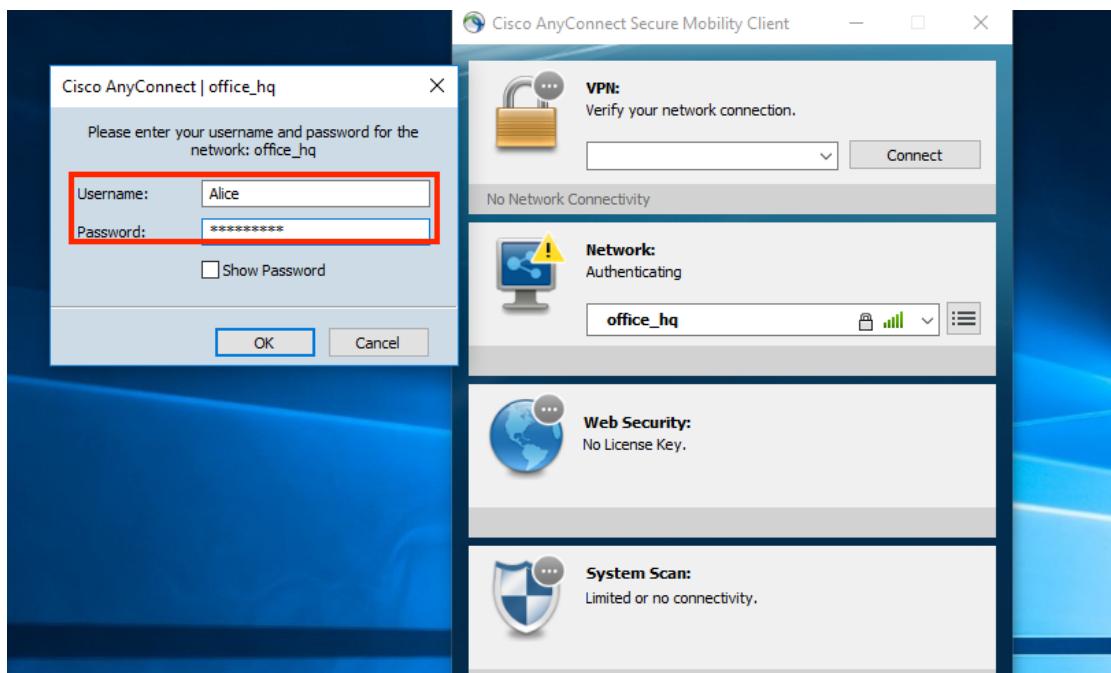
Client Username .....	Bob
Client Webauth Username .....	N/A
Hostname: .....	
Device Type: .....	Intel-Device
AP MAC Address.....	70:69:5a:51:4e:c0
AP Name.....	AP4C77.6D9E.6162
AP radio slot Id.....	1
Client State.....	Associated
User Authenticated by .....	RADIUS Server
Client User Group.....	Bob
Client 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

## Windows 10 و AnyConnect NAM: رابتخا لاصتالا ب

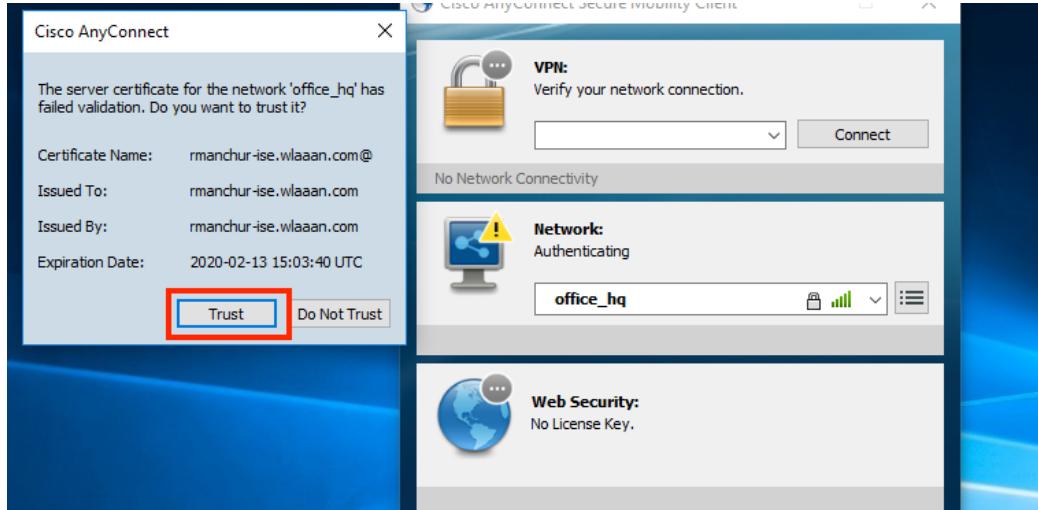
1. (ف) يف) اذه اذه ملأ اثلا (PEAP) ملأ اثلا (EAP) عونو وحاتملا ملأ SSID ةممي اق نم رتختا.



2. مدخلة سملة اقصاد مل رورمل اقملا و مدخلة سملة امسا ريفوتب مق.



3. ةداهشل ايف ةقثل ا راي ت خا كيلع بجي ف ، لي مع ل اى ل ا اس راب موق ي SSC نأ ا ل ا رظن ن و . اى ل ع اه ب ق و ث و مل ا ةداهشل ا ت ي ب ث ت ب ة د ش ب ي ص و ي ج ا ت ن إ ل ا ة ئ ي ب ي ف ) ا ي و د ي (ISE).



4. حيحصل ليوختلاري فيرعت فلم ديكأتو ISE ىلع ئقاداصملاتالجس نم ققحت مدخلتسملل.

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
Feb 15, 2019 02:51:27.163 PM	Connected	0	Alice	F4:8C:50:62:14:6b	Microsoft W...	Default >>	Default >> Wireless_Marketing	Marketing	Marketing	192.168.77.32					rmanchur-ise	
Feb 15, 2019 02:51:24.837 PM	Connected	0	Alice	F4:8C:50:62:14:6b	Microsoft W...	Default >>	Default >> Wireless_Marketing	Marketing	Marketing		WLC6520		Workstation		rmanchur-ise	

5. ئيكلساللا ئيلحملاركبسلىا يف مكحتلارصنع ىلع لماعلا لاخدا نم ققحت لىغشتلا ئلاح يف هنأنموئنميلا VLAN ئكبسلىا ئيييعت نم ديكأتو.

Clients															Entries 1 - 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. ئيكلساللا ئيلحملاركبسلىا يف مكحتلارصنع (CLI) رماوا رطس ئهجاونم ادختساب لماعلا ئلاح نم ققحتلا نكمي show client details :

```

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..... wlan1477
VLAN..... 1477

```

## اهالص او ءاطخألا فاشكتسا

1. تلمعتسا in order test aaa radius username

password

wlan-id

جئاتنلا تضرع to IJ RADIUS و WLC نيب ليصوت ISEtest aaa show radiusin order to تربتختا.

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

Radius Test Request

Wlan-id.....	2
ApGroup Name.....	none
 Attributes	
-----	
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)

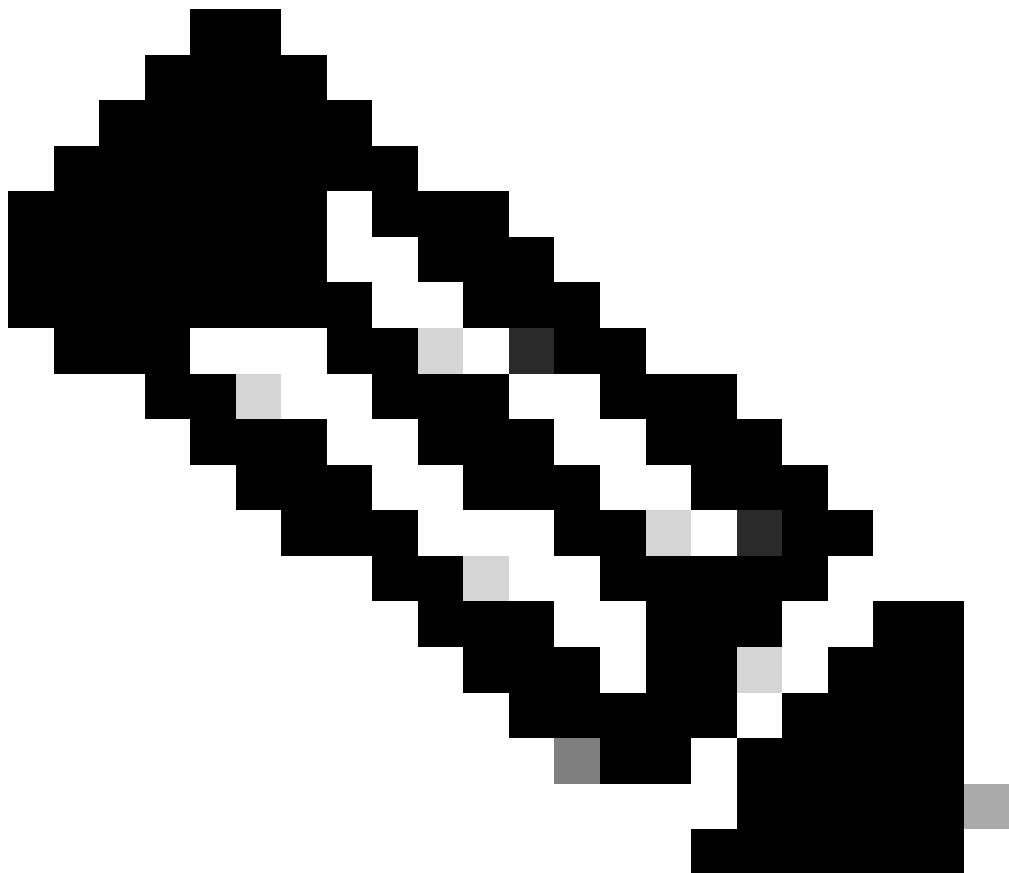
(Cisco Controller) >

2. لـ debug client تلمعتسا

رادصـا ئـيلـوصـوم نـوبـز يـكـلـسـالـتـيـرـحـتـ.

ىـلـعـاـحـالـصـاـوـضـيـوـفـتـلـاـوـقـدـاصـمـلـاـعـاطـخـأـفـاشـكـتـسـالـرـمـأـلـمـدـخـتـسـأـ.

ـعـكـبـشـلـاـيـفـمـكـحـتـلـاـرـصـنـعـ (WLC).



نانونع ىلإ ادانتسا جارخإلا ديدجتلى debug mac addr طقف رمألا اذه مدخلتسا: ظحالم  
5. عاطخألا حي حصت متى يذلا MAC.

- 
4. لشف تالاح لكاشم ديدجتل تاسلجلالا تالجس و ئرشابملالا ISE تالجس ىلإ عجرات  
تالاصتى لكاشم و ئقدادصملالا AD.

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).