

مادختساب 9800 WLC ىل ع EAP-TLS نيوكت ISE Internal CA

تايوتحمل

قمدملا

[قيساس الابلطت ملما](#)

[قمدمختس ملما تانوك ملما](#)

[قيساس تامول عم](#)

[EAP-TLS ةقداصم قفدت](#)

[EAP-TLS قفدت ىف تاوطخ](#)

نيوكت ملما

[ةكبش لىل طىطخ تملما مسر ملما](#)

[تانىوك تملما](#)

[ISE نيوكت](#)

[ةكبش زاوج ةفاضا](#)

[ىلخ ادلا قداصم ملما عجز ملما نم ققحت ملما](#)

[ةقداصم ملما بولسا ةفاضا](#)

[ةداهش لىل ابق دىجت](#)

[ةداهش لخدم عاشنا](#)

[ىلخ اد مدختس م ةفاضا](#)

[RADIUS جهنو ISE ةداهش رىفوت لخدم نيوكت](#)

9800 WLC نيوكت

[9800 WLC ىل ISE مدخ ةفاضا](#)

[9800 WLC ىل ع مداوخ ةعومجم ةفاضا](#)

[9800 WLC ىل ع AAA قرط ةمئاق نيوكت](#)

[9800 WLC ىل ع ضىوف تملما قرط ةمئاق نيوكت](#)

[9800 WLC ىل ع جهن فىرعت فلم عاشنا](#)

[9800 WLC ىل ع WLAN ةكبش عاشنا](#)

[9800 WLC ىل ع جهن تملما فىرعت فلم عم WLAN ةطىرخ](#)

[9800 WLC ىل ع لوصول ةطقن ىل ا جهن تملما ةمالع ةمچرت](#)

[لامتك ادب \(WLC\) ةىكللس اللى ةىلحمل ةكبش لىل فى مچرت ملما رصنع نيوكت لىرغشت مئى دادع اللى](#)

[مدختس ملما ةداهش لىرغشت و عاشنا](#)

[Windows 10 لىرغشت ملما ماظن لمعمى زاوج ىل ع ةداهش لىل تىب ت](#)

[ةحصل ملما نم ققحت ملما](#)

[اهج الص او اعطخ اللى فاشكتسا](#)

[عجار ملما](#)

قمدملا

ةي وهلا تامدخ كرحم ل ق دصم ل عجرم ل امدخت ساب EAP-TLS ةق داصم دن تسم ل اذ ه فص ي
ن يمدخت س م ل ةق داصم ل

ةي ساس ال اابل طم ل

ةمدخت س م ل ا نوك م ل

ةيلال ةي دام ل ا نوك م ل ا وجرم ارب ل ا رادص ل ل ا دن تسم ل اذ ه ي ف ة دراو ل ا تامول عم ل ا دن تست

- 17.09.04a ضكري C9800-40-K9: ةيكل س ال ل م كحت ل ا ةدحو
- Cisco ISE: 4 ل ي غ ش ل ا دي ق 3 رادص ل ا احي حصت ج مان رب
- C9130AXI-D زارط ل ا: ل و ص و ل ا ة ط ق ن ج ذوم ن
- 9200-L-24P: ل و ح م ل ا

ةصاخ ةي لم عم ةئي ب ي ف ةدو ج و م ل ا ةزه ج ال ن م دن تسم ل اذ ه ي ف ة دراو ل ا تامول عم ل ا ءاش ن ا م ت
ت ن ا ك ا ذ ا (ي ض ا ر ت ف ا) ح و س م م ن ي و ك ت ب دن تسم ل اذ ه ي ف ةمدخت س م ل ا ةزه ج ال ا ع ي م ج ت ا د ب
ر م ا ي ال ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ل ا دي ق ك ت ك ب ش

ةي ساس ا تامول عم

ن ي م د خ ت س م ل ل ا ت ا د ا ه ش ر د ص ي ي ذ ل ا ا ه ب ص ا خ ل ا ق د ص م ل ا ع ج ر م ل ا ا ه ل ت ا س س و م ل ا م ط ع م
ء ا ش ن ا ل ه م ا د خ ت س ا ن ك م ي ج م د م ت ا د ا ه ش ع ج ر م ISE ن م ض ت ي . EAP-TLS ةق د ا ص م ل ن ي ي ئ ا ه ن ل ا
ا ل ي ت ل ا ت ا ه و ي ر ا ن ي س ل ا ي ف . EAP-TLS ةق د ا ص م ي ف ه م ا د خ ت س ا م ت ي ل ن ي م د خ ت س م ل ل ا ت ا د ا ه ش
ق د ص م ل ا ع ج ر م ل ا م ا د خ ت س ا ح ب ص ي ، ا ن ك م م ل م ا ك ل ا ق د ص م ل ا ع ج ر م ل ا م ا د خ ت س ا ا ه ي ف ن و ك ي
ا د ي ف م ا ر م ا م د خ ت س م ل ا ةق د ا ص م ل ISE ق د ص م ل ا

ةق د ا ص م ل ل ا ع ف ل ك ش ب ISE CA م ا د خ ت س ا ل ة ب و ل ط م ل ا ن ي و ك ت ل ا ت ا و ط خ دن تسم ل اذ ه ح ض و ي
EAP-TLS ةق د ا ص م ق ف د ت . ن ي ي ك ل س ال ل ا ن ي م د خ ت س م ل ا

EAP-TLS ةق د ا ص م ق ف د ت

Certificate (for server validation)
Client_key_exchange
Certificate_verify (to verify server trust)
Change_cipher_spec
TLS finished

10. نمضتي لوصول اي دحت RADIUS مداخل لسري، ليمعلا ةقداصم حاجن دنع:

Change_cipher_spec
Handshake finished message

11. RADIUS مداخل ةقداصم ل ةئجتلا نم ليمعلا ققحتي.

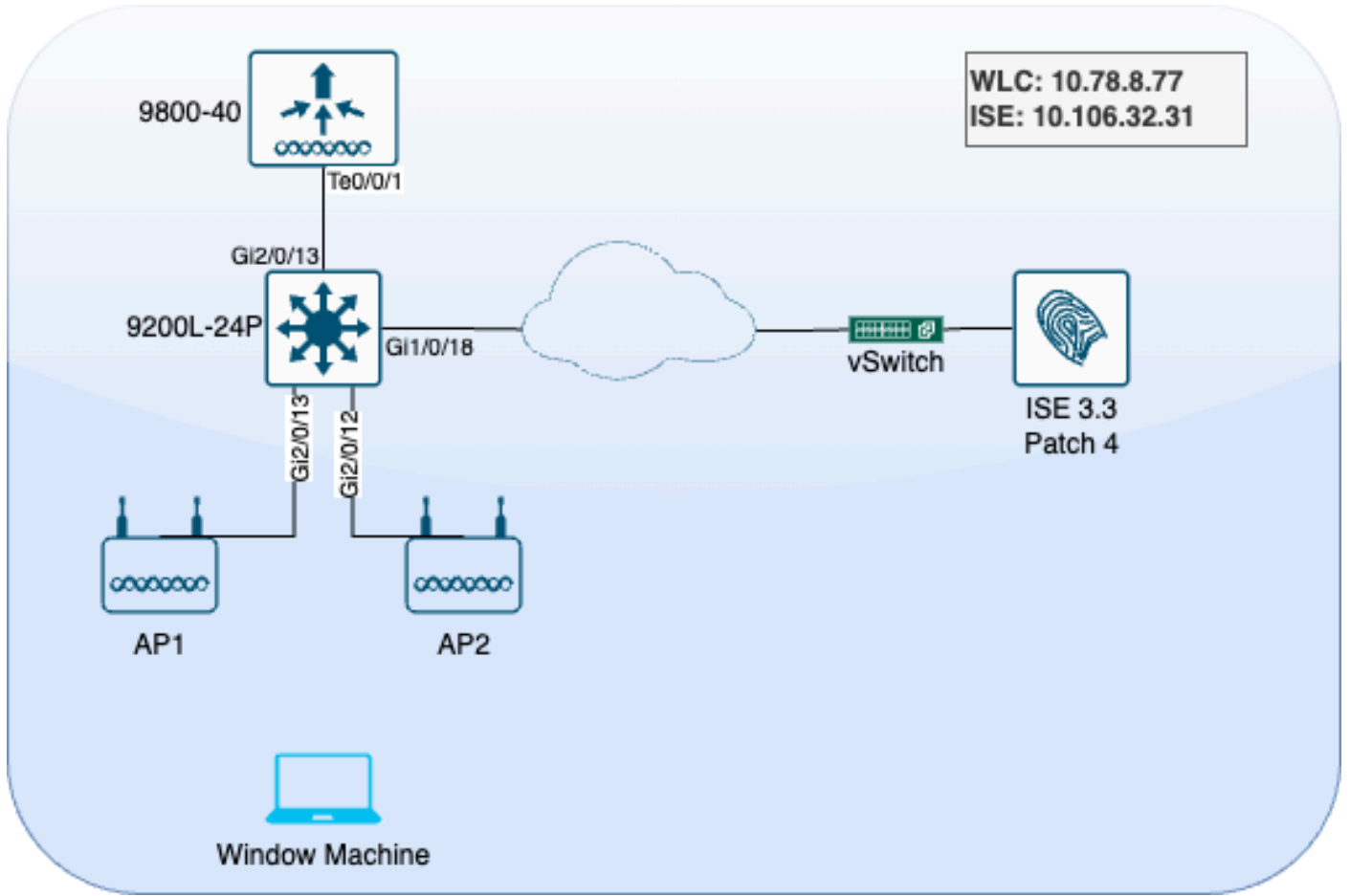
12. TLS ةحفاصم ءانثأ رسلا نم ايكيم انيد ديدج ريفشت حاتفم قاقتشا متي.

13. سمتم لمللا ىلا م ث قداصم ل ىلا مداخل نم EAP-SUCCESS ةلاسر لسرت.

14. ةكبشلا ىلا لوصول EAP-TLS ني كمت مت يذلا يكلساللا ليمعلا عيطتسي.
نآلا ةيكلساللا

نيوكتلا

ةكبشلا ل يطيختلا مسرلا



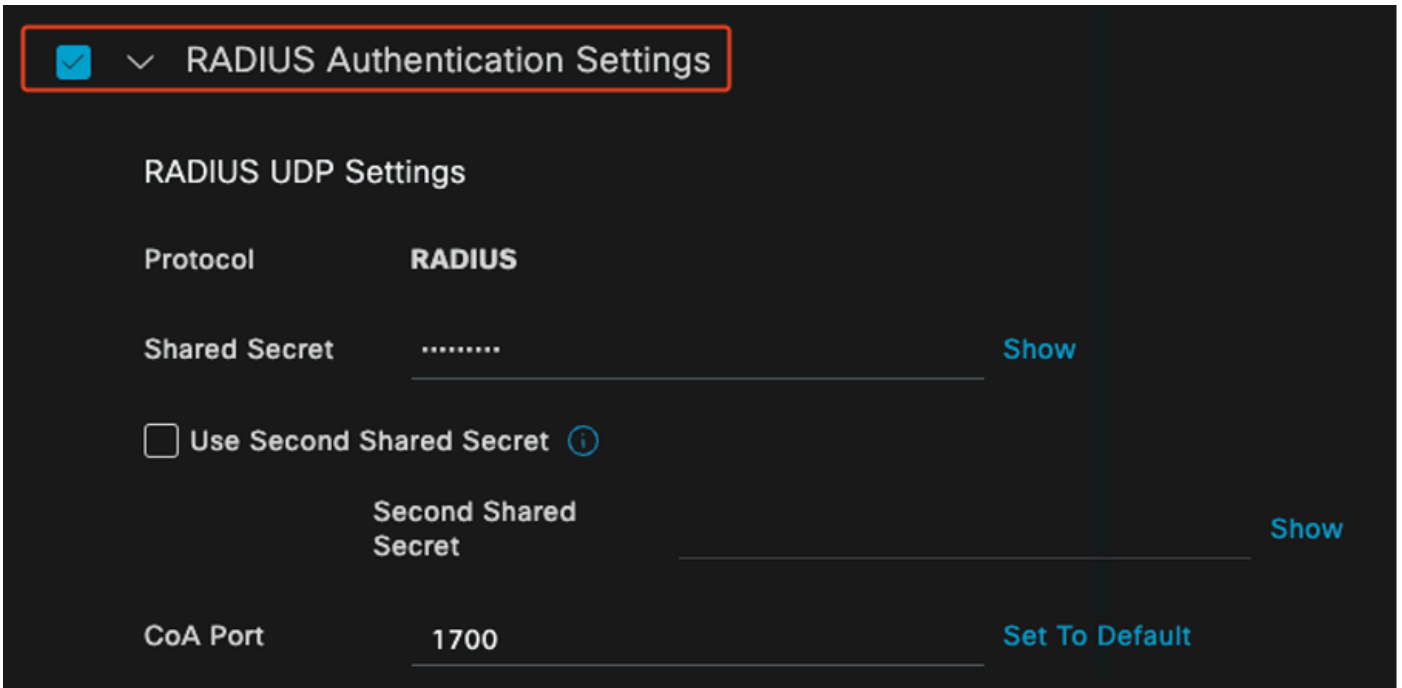
لماعم لاي جولو بوط

تاني وكتال

نينا وكتال و ISE: نينا وكتال ب موقن، مسقلا اذه في

ISE نينا وكتال

مسقلا اذه في ةشاش تاطقل ةوطخ لك بحاصت. ISE مداخل نينا وكتال تاوطخ يلي ام في
يئرمل هي جوتال ريفوتل

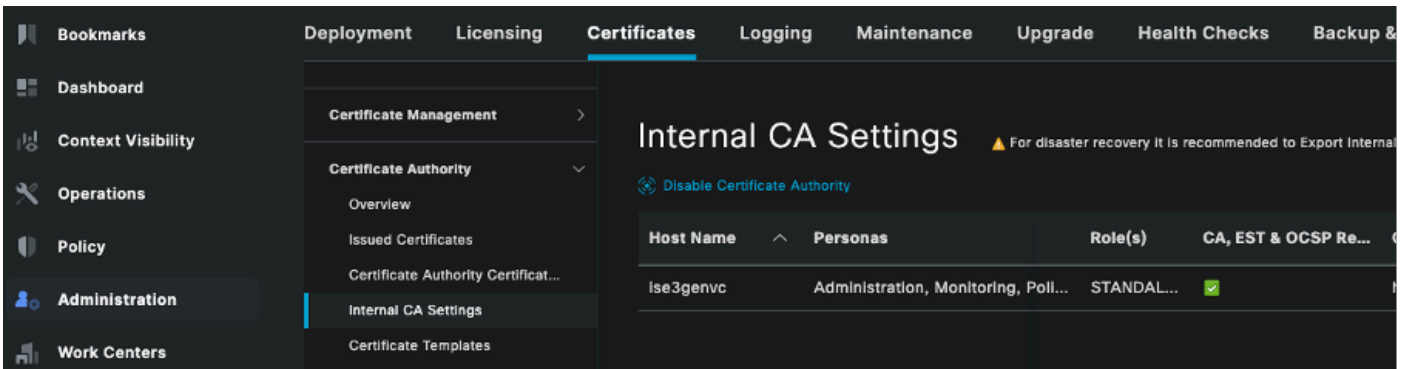


ةكېش زاھج ةفاضإ

ي لخادلل ق دصملا عجرملا نم ققحتلا

ةي لاتلا تاوطخلل مدختسأ ، (CA) ي لخادلل ق دصملا عجرملا تادادعإ نم ققحتلل

1. ق دصملا عجرملا تادادعإ > ق دصملا عجرملا > تاداهشلا > ماظنلا > ةرادإلا يلى لقتنا . ي لخادلل
2. ي لخادلل ق دصملا عجرملا طيشنت ديكأتل ق دصملا عجرملا دومع نيكمت نم دكأت .



ي لخادلل ق دصملا عجرملا نم ققحتلا

ة ق داصملا بولسأ ةفاضإ

ص صخم ةي وه لس لس لس ةفاضإ . ةي وهلا رصم تال س لس ت > ةي وهلا ةرادإ > ةرادإ يلى لقتنا
لخدللا يلى لوخدلا ليحست رصم ي ف مكحتلل

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

Identity Source Sequences List > Allow_EMP_Cert

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	<input type="text" value="Internal Users"/>
Guest Users	
All_AD_Join_Points	

> < < >

ةقد اصملا بولسأ

ةداهشلا بللق ديدحت

ةيولاتلا تاوطلال مدختسأ، ةداهش بللق ديدحتل

تاداهشلا بللق > قدصملا عجرملا > تاداهشلا > ماظنلا > ةرادإلا لىل لقتنا 1. ةوطلال

ديدج ةداهش بللق ءاشنإل ةفاضل+ ةنوقيا قوف رقنا 2. ةوطلال

2.1 بللق ل ل ISE مداخل يلحم ديرف مساريفوت

2.2 لىل \$UserName\$ (CN) ءئاشنلا مسالا نييعت نم دكأت

2.3 MAC ناونع ىل ع (SAN) عوضوم لل لىدبلا مسالا نىي عت نم ققحت 2.3.

2.4 ISE Internal CA لىل SCEP RA فىرعت فلم نىي عت 2.4.

2.5 لىم عملا ةقداصم نىكمتب مق ، عسوملا حاتفملا مادختسا مسق ي 2.5.

Field	Value
* Name	EAP_Authentication_Certificate_Template
Description	This template will be used to issue certificates for EAP Authentication
Subject	
Common Name (CN)	\$UserName\$
Organizational Unit (OU)	Example unit
Organization (O)	Company name
City (L)	City
State (ST)	State
Country (C)	US
Subject Alternative Name (SAN)	MAC Address
Key Type	RSA
Key Size	2048
* SCEP RA Profile	ISE Internal CA
Valid Period	730 Day(s) (Valid Range 1 - 3652)
Extended Key Usage	<input checked="" type="checkbox"/> Client Authentication <input type="checkbox"/> Server Authentication

ةداهشلا بلق

ةداهش لخدم عاشنإ

ةداهشلا تاوطخلا مدختسا ، لىم عملا ةداهش عاشنإل ةداهش لخدم عاشنإل

ةداهشلا مېدقت > ةزهجال لخدم ةرادإ > ةرادإل لىل لقتنا 1. ةوطخلا

ةدېدج لخدم ةحفص دادعإل عاشنإ قوف رقنا 2. ةوطخلا

ةلوهسب هيلع فرعتلل لخدملل دىرف مسارى فوتب مق 3. ةوطخلا

3.1. 8443 لىل اذه نىي عت ؛ هيلع ةبوابلا لمعتل ذفنملا مقرر تخأ.

3.2. لخدملا اذهل لىل ISE عممتسي يتلا تاهجاولا دح.

3.3. ةيضا رتفا لخدم تاداهش ةومجمك تاداهشلا ةومجم ةمالع دح.

م دختسمل ةيوهلا نزم لس لس تىل ريشي يذلا ، ةقداصل بولس أ دىحت 3-4
لخدملا اذى لىل لوخدلا لىجست ةقداصل

ىل ع . ةبوابلا لىل لوصولا اهئاضأل نكمي يتلا ةدمتعمل تاعومجملا نيمضت 3-5
لىل نومتنى نوم دختسمل ناك اذا نىفظوملا نىم دختسمل ةومجم دح ، لاثملا لىبس
ةومجملا هذى .

3.6. تاداهشلا ريفوت تاداعل نمض اهب حومسمل تاداهشلا بل اوق دىحتب مق .

The screenshot shows a web application interface for 'Certificate Provisioning'. The top navigation bar includes 'Blocked List', 'BYOD', 'Certificate Provisioning' (highlighted), and 'Client Provisioning'. A left sidebar contains menu items: 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (highlighted), 'Work Centers', and 'Interactive Features'. The main content area is titled 'Portals Settings and Customization' and contains the following fields and sections:

- Portal Name:** EMP CERTIFICATE PORTAL
- Description:** (empty field)
- Language File:** (dropdown menu)
- Portal test URL:** (blue text link)
- Portal Behavior and Flow Settings:** (underlined section)
- Portal Page Customization:** (section)

Portal & Page Settings

Portal Settings

HTTPS port:*

1

8443

(8000 - 8999)

Allowed Interfaces:*

2

For PSNs Using Physical Interfaces

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3
- Gigabit Ethernet 4
- Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured

- Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: *

3

Default Portal Certificate Group

Configure certificates at:

[Administration > System > Certificates > System Certificates](#)

Authentication method: *

4

Certificate_Request_Sequence

Configure authentication methods at:

[Administration > Identity Management > Identity Source Sequences](#)

Configure authorized groups

User account with Super admin privilege or ERS admin privilege will have access to the portal

Available

Q

- ALL_ACCOUNTS (default)
- GROUP_ACCOUNTS (default)
- OWN_ACCOUNTS (default)

Chosen

Employee

Choose all

Clear all

Fully qualified domain name (FQDN):

> Login Page Settings

> Acceptable Use Policy (AUP) Page Settings

> Post-Login Banner Page Settings

> Change Password Settings

∨ Certificate Portal Settings

Certificate Templates: * EAP_Authentication_Certificate_Template × ∨

ةداهشلا لخدم نيوكت

ةباوبلا رابتخال URL ناونع قوف رقنلاب ةباوبلا رابتخال كنكمي ،دادعإلا اذه لامتك ا درجمبو .لخدملا ةحفص ارجإلا اذه حتفي .

Portals Settings and Customization

Portal Name:

EMP CERTIFICATE PORTAL

Description:

Language File ∨

Portal test URL

رابتخال لخدم ةحفصل URL ناونع

https://10.106.32.31:8443/certprovportal/PortalSetup.action?portal=45aea9cb-29c8-4f73-98bb-63543bba423a

CISCO Certificate Provisioning Portal

Sign On
Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

Username:
emp

Password:

Sign On

لخدملة حفس

يلخاد مدختسم ةفاضل

ةللالا تاوطخلا مدختسأ، صيخرتلا لخدم ربع ةقداصلل مدختسم عاشنإل:

1. نيمدختسمل > تايوهال > ةيوهال ةرادإ > ةرادإل إلل لقتنا.
2. ماظنل إلل مدختسم ةفاضل رايلخال قوف رقنا.
3. مق، لاثملا ليلبس إلل مدختسمل اهليل يمتنل يتلل مدختسمل ةيوه تاعومجم دح. نيفظوملا ةعومجم إلل مدختسمل نييعتب

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

Network Access Users

Edit + Add Change Status Import Export Delete Duplicate

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	emp					Employee	

يلخاد مدختسم ةفاضل

RADIUS جهنو ISE ةداهش ريفوت لخدم نيوكت

ISE جهن تاعومجم نيوكتب موقن، نآل. ISE ةداهش ريفوت لخدم دادعإ قباسل مسقلا يطغ مدختسمل ةقداصلل حامسلل RADIUS.

1. ISE RADIUS جهن تاعومجم نيوكت.
2. تاسايلل تاعومجم > ةسايلل إلل لقتنا.
3. ةديدج جهن ةعومجم عاشنإل (+) عمجال ةمالع قوف رقنا.

نيمدختسمل ةقداصلل ةمصم ةطيسب تاسايس ةعومجم دادعإ مق، لاثملا اذه يف مهتاداهش مادختساب.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	EMP Wireless 802.1x Auth		AND Wireless_802.1X Airespace-Airespace-Wlan-Id EQUALS 17	Default Network Access	0		

تاسايس ةعوم جم

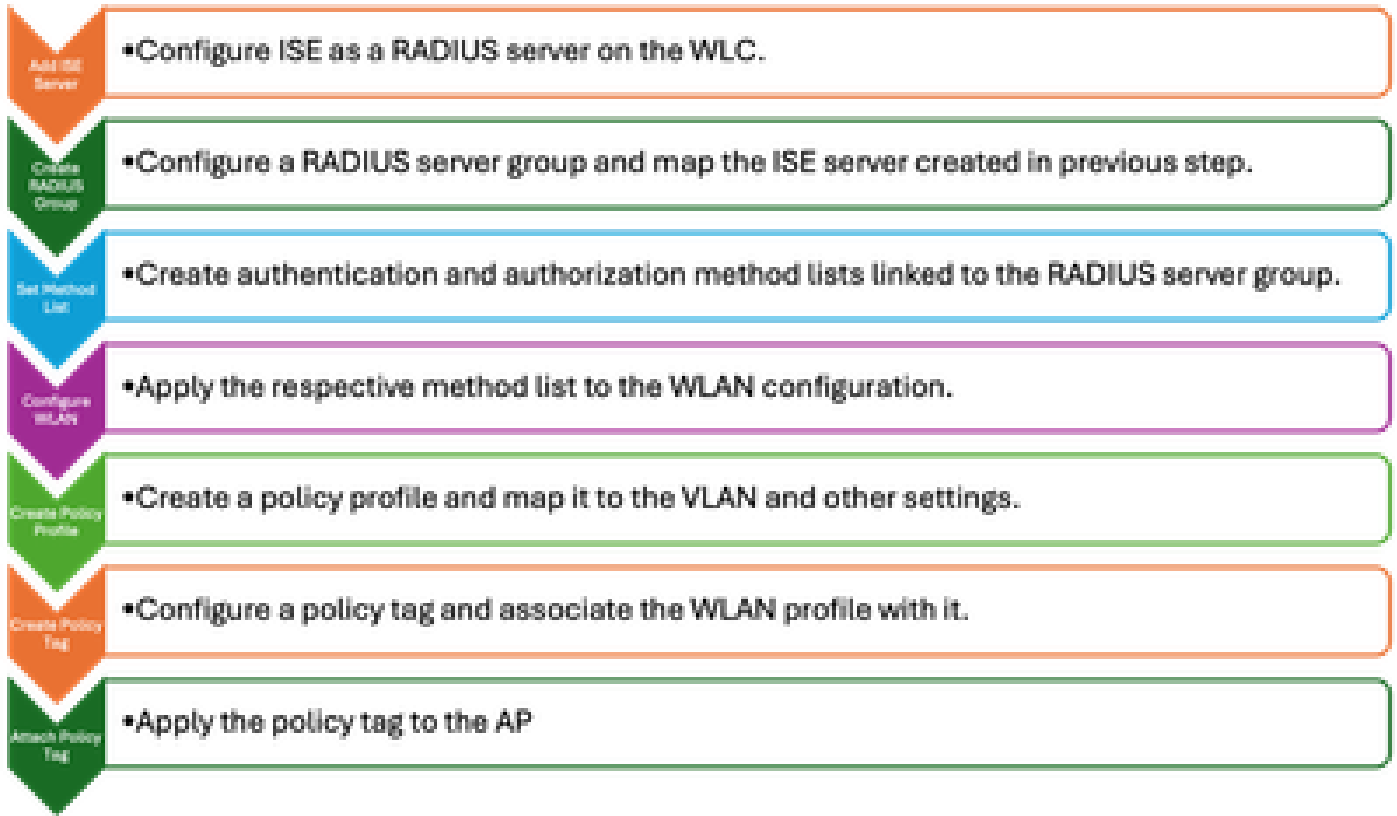
Status	Rule Name	Conditions	Use	Hits	Actions
●	Allow Certificate Authentication	EAP-TLS	Allow_EMP_Cert	0	Options
●	Default		DenyAccess	0	Options

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Authz Employee	EAP-TLS	PermisAccess	Employees	0	
●	Default		DenyAccess	Select from list	0	

ضيوف تال او ةقدا صملا تاسايس ضرعت جهن ةعوم جم

9800 WLC نيوكت

(WLC) ةيكل سلالا ةيكل حملا ةكبش لاي ف مكحتلا ةدحوب ةصاخلا نيوكتلا تاوطخ يلاي امي ف
 يئرمللا هيحوتلا ريفوتل مسقلا اذه ي ف ةشاش تاقل لب ةوطخ لك قافرا متي. 9800 زارط



WLC نيوكت تاوخط

إدخال ISE إلى WLC 9800

1. من أجل إعداد WLC (9800) كسيرفر راديوس (RADIUS) على WLC، يجب إعداد ISE كسيرفر راديوس على WLC.
2. من أجل إعداد ISE كسيرفر راديوس على WLC، يجب إعداد ISE كسيرفر راديوس على WLC.
3. من أجل إعداد ISE كسيرفر راديوس على WLC، يجب إعداد ISE كسيرفر راديوس على WLC.

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add Delete

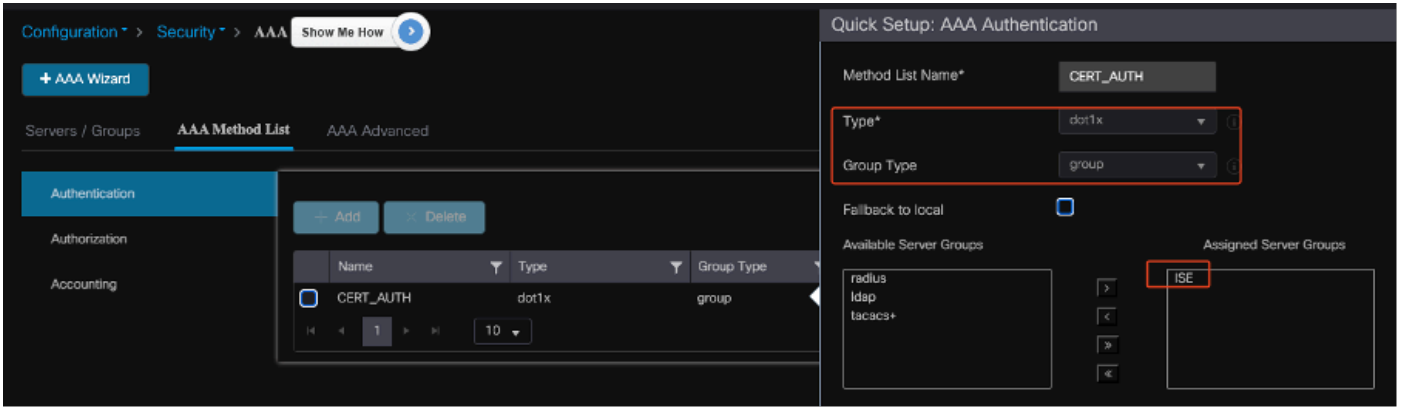
RADIUS

TACACS+

LDAP

Create AAA Radius Server

Name*	ISE3	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	10.106.32.31	CoA Server Key Type	Clear Text
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ
Key Type	Clear Text	Confirm CoA Server Key
Key* ⓘ	Automate Tester	<input type="checkbox"/>
Confirm Key*		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

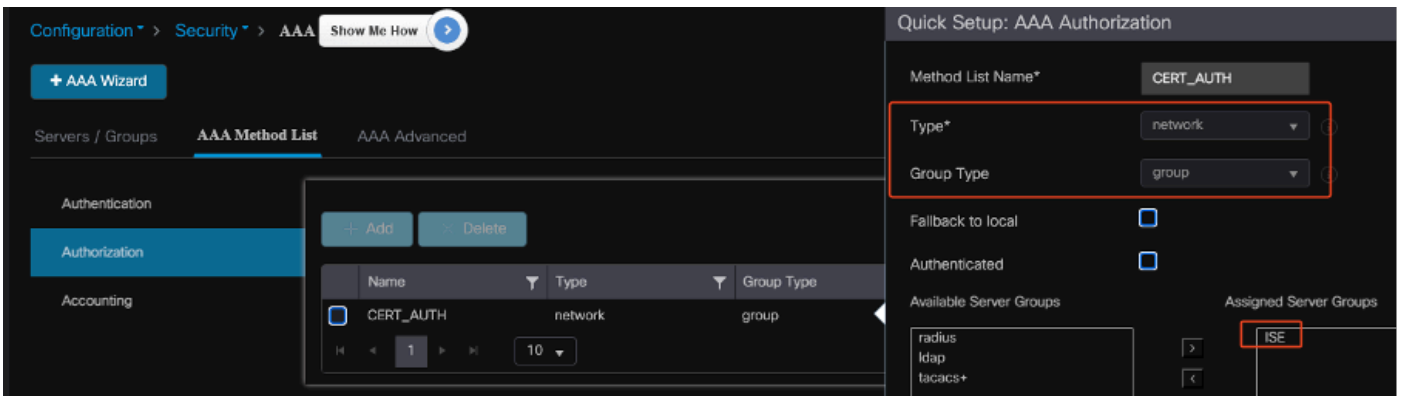


قداصلملا قرط مئاوق عاشنا

9800 WLC ىلع ضيوفتلا قرط ةمئاوق نيوك

ةيلا تال تاوطخلا مدختسا، ليوختلا قرط ةمئاوق دادعإل:

1. AAA قرط ةمئاوق مسق لخاد ضيوفتلا بيوبتلا ةمالع ىلإ لقتنا.
2. ةديج ليوخت قرط ةمئاوق عاشنا ةفاضل قوف رقنا.
3. عونك ةكبشلا رتخأ.
4. ةومجم عونك ةومجم ددح.
5. مداوخ ةومجمك ISE مداوخ ةومجم نيومتب مق.

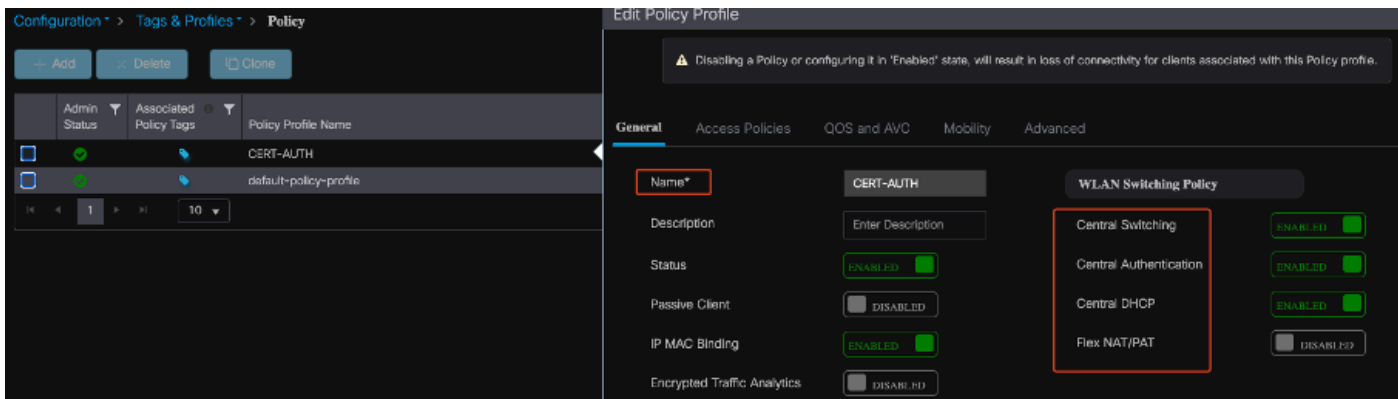


ليوختلا قرط ةمئاوق ةفاضل

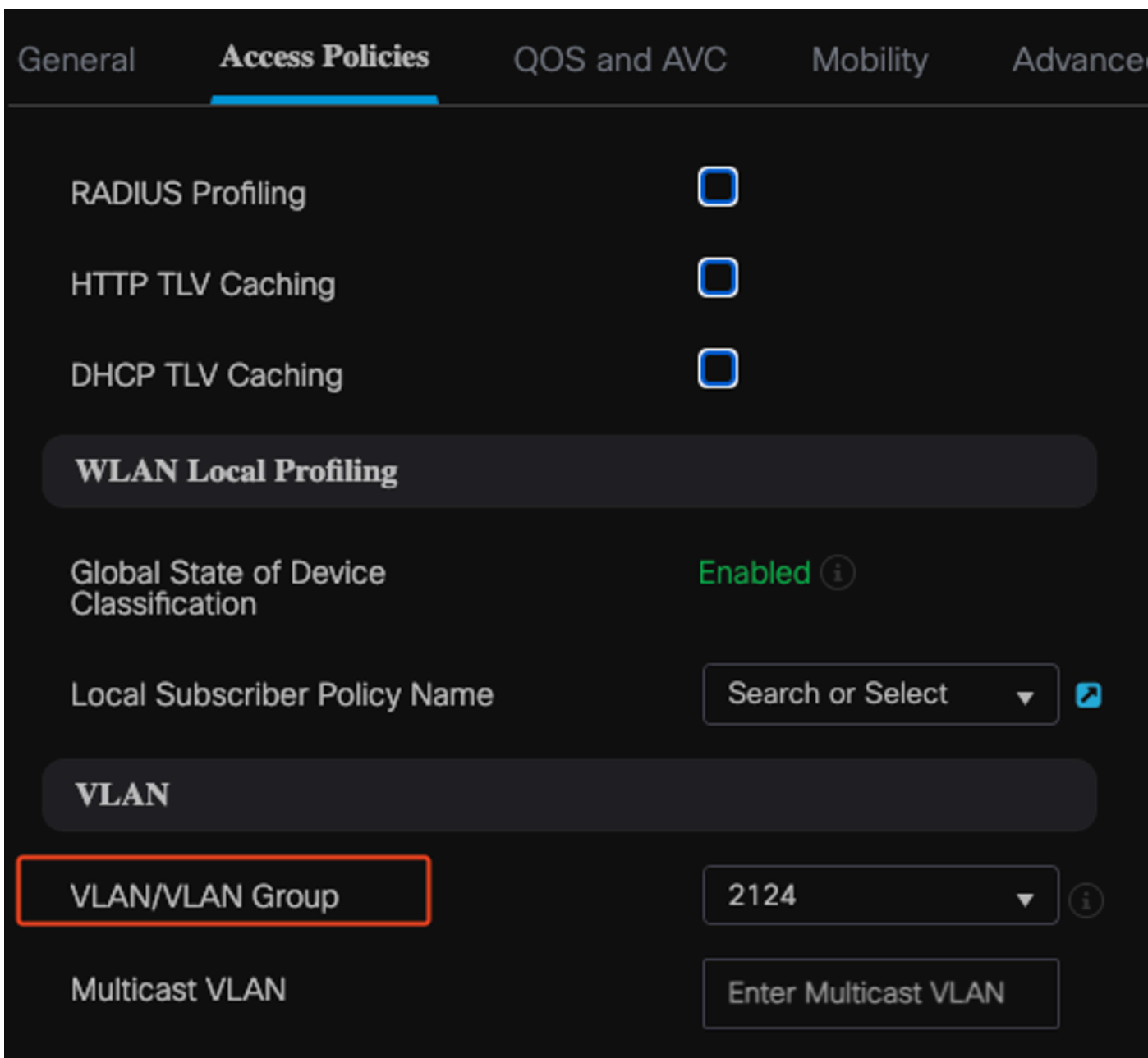
9800 WLC ىلع جهن فيرعت فلم عاشنا

جهن فيرعت فلم عاشنا يف رمتسا، RADIUS ةومجم نيوك لامتك عم:

1. ةسايسلا > فيرعتلا تافلومو تامالعال > نيوكتلا ىلإ لقتنا.
2. ديجهن فيرعت فلم عاشنا ةفاضل قوف رقنا.
3. ايزكرم عيش لك نوكي، لاثملا اذه يف. جهنلا فيرعت فلم ةبسانملا تاملعل رتخأ. ليملعلا ةصاخلا VLAN ةكبشك ربتخملا ةصاخلا VLAN ةكبش مادختسا متي.



ةسايسال فيرعت فلم نيوكت



ةسايسال طي طخت لى VLAN

بيوبتال عمالع في AAA زواجت راىخ نيكمتم نم دكأت، RADIUS ضيوفت نيوكت دنع في مكحتال ءءول ءاءعإل اءءءمسي. ءسايسال فيرعت فلم ءاءءعإب ءصإل ءمءقءم

ىل ع RADIUS لى ءءنءس م ل لى وءءل ءاساى س قى بءءب ءى ك ل س ال ل ءى ل ءم ل ء ءب ش ل ل ءزء ء ل او نى مءءءس م ل ل

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

WLAN Timeout

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

Guest LAN Session Timeout

DHCP

IPv4 DHCP Required

DHCP Server IP Address

Show more >>>

AAA Policy

Allow AAA Override

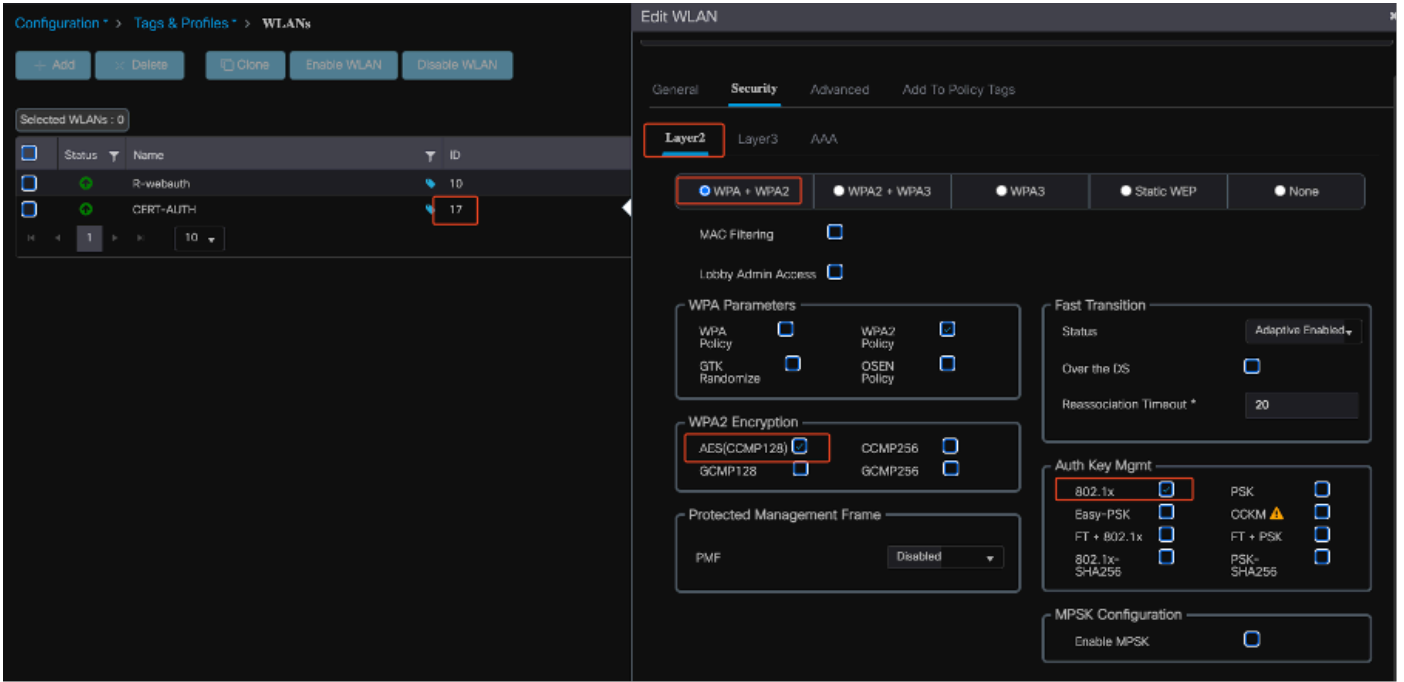
AAA زءءء

WLC 9800 لى ع WLAN ء ءب ش ءءش ن ل

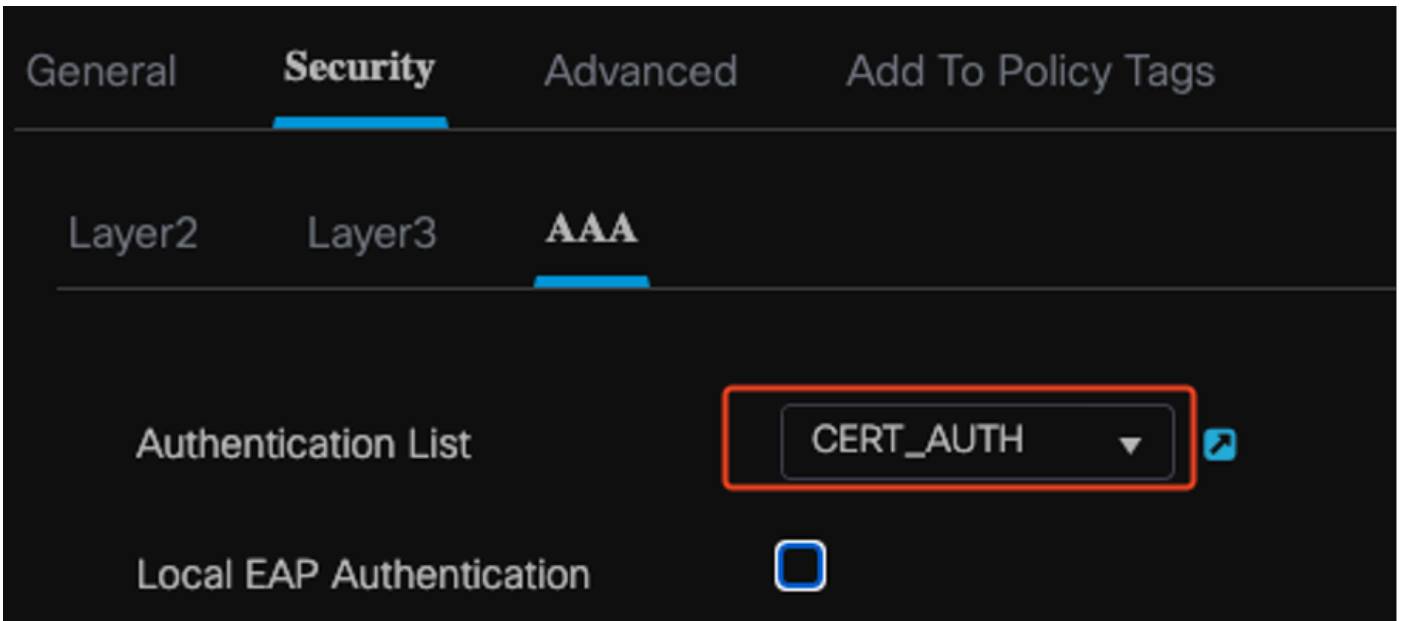
ءى ل ل ء ل ء اوءء ل مءءءس ء ، 802.1x ءق ءاص م ب ءءىء ء WLAN ء ءب ش ءاءء ل

1. WLAN ءءءب ش > فى رءء ل ءءءل م وءءءل ء ل > نى وءءل ل لى ل ل ءءن ل
2. ءءىء ء WLAN ء ءب ش ءءش ن ل ءءءل ءءل رءن ل

3. 802.1x ةقداصم نيكم تب مقو 2 ةقبطال ةقداصم تادادع إدح



WLAN فيرعت فلم نيوكت

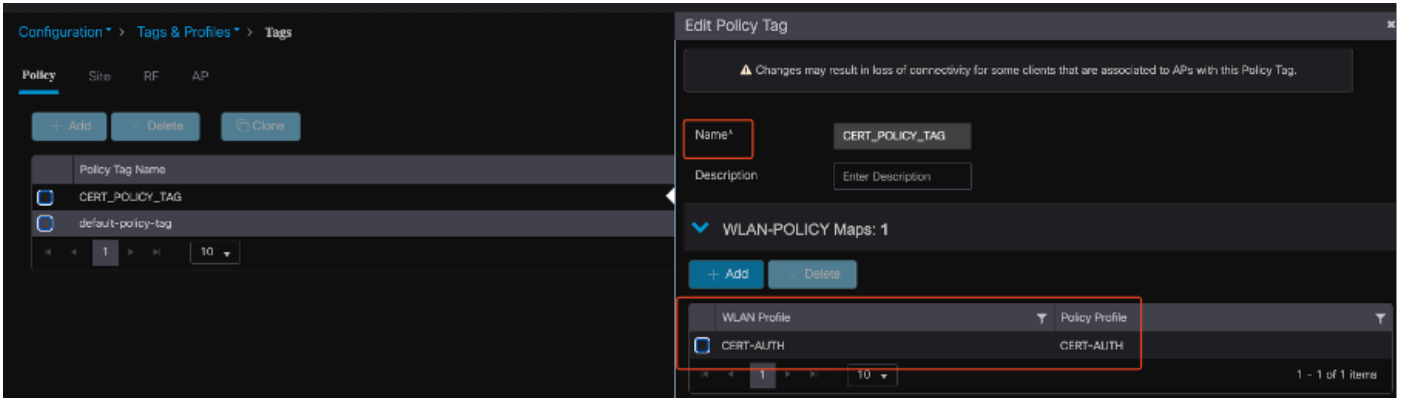


قرطال ةمئاق ةطيخ إىل WLAN فيرعت فلم

9800 WLC إىل جهنللا فيرعت فلم عم WLAN ةطيخ

ةيلا تاولخال مدختسأ ،ةسايس فيرعت فلمب كب ةصاخلا WLAN ةكبش نارقإل

1. زييمت تامالع > فيرعت تافلومو زييمت تامالع > نيوكتلا إىل لقتنا.
2. ةديج زييمت ةمالع ةفاضل ةفاضل قوف رقنا.
3. فيرعت فلم إىل اثيرح هؤاشنإ مت يذلا WLAN نييعتب مق ،WLAN-policy مسق ي ف بسانملا ةسايسلا.

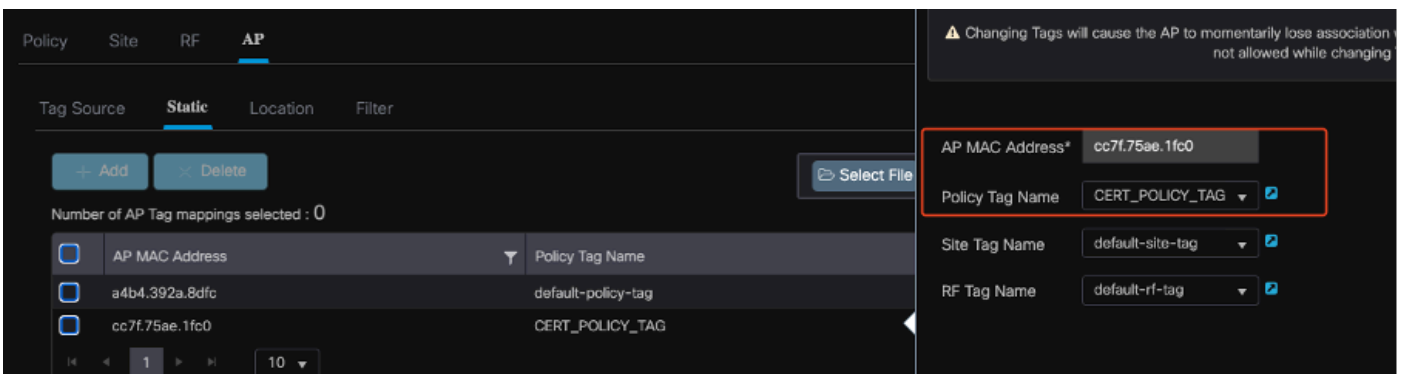


ةساي سلا ةمالع نيوكت

9800 WLC لوصول ةطقن ل جهنلا ةمالع ةمچرت

ةة لال تاوطخل لمكأ (AP) لوصول ةطقن ل جهنلا ةمالع نيعةتل:

1. AP > زيمت تامالع > تافي صوت و زيمت تامالع > نيوكتل ل ل لقتنا.
2. لوصول ةطقن نيوكت نمض "يكي تاتاس ل نكاس" مسقلا ل ل لقتنا.
3. اهنوكت ديرت يتل ةدحمل لوصول ةطقن ل رقنا.
4. ةدحمل لوصول ةطقن ل اهئاشناب تمق يتل جهنلا ةمالع نيعةتب مق.



لوصول ةطقن ةمالع نيعةت

(WLC) ةيكل سلال ةي ل حمل ةكبش ل ل ي ف مكحتل ل رصنع نيوكت ليغشت متي دادعلا لامتك دب

```

aaa group server radius ISE
  server name ISE3
  ip radius source-interface Vlan2124
aaa authentication dot1x CERT_AUTH group ISE
aaa authorization network CERT_AUTH group ISE
aaa server radius dynamic-author
  client 10.106.32.31 server-key Cisco!123
!

```

```

wireless profile policy CERT-AUTH
aaa-override
ipv4 dhcp required
vlan 2124
no shutdown

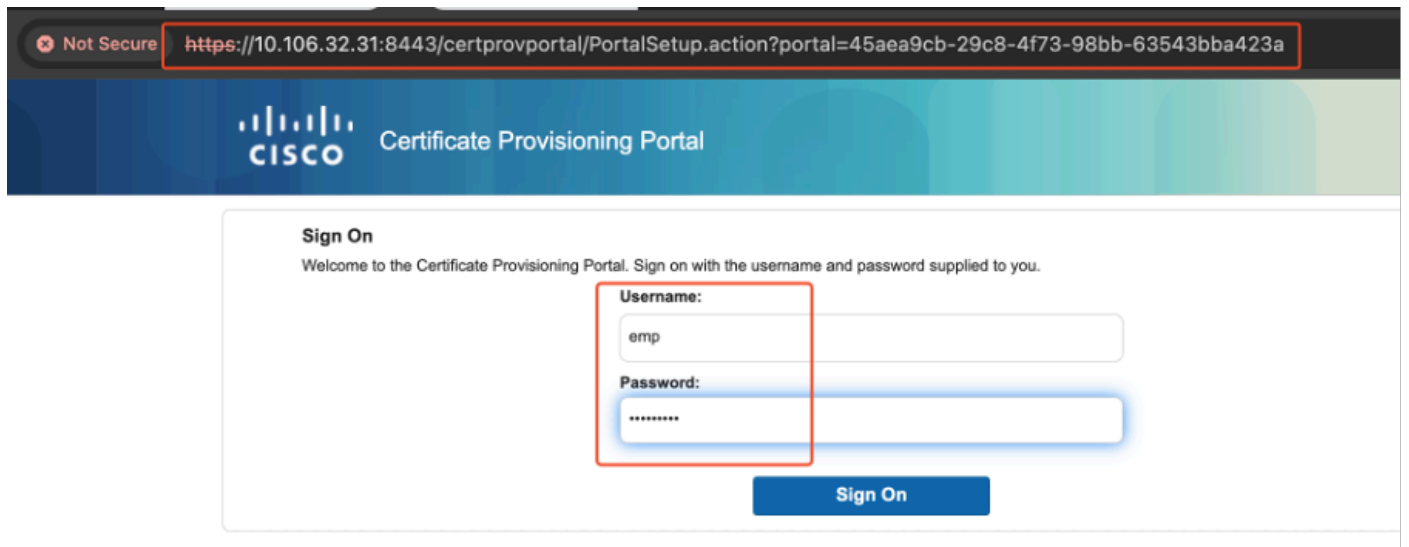
```

```
wlan CERT-AUTH policy CERT-AUTH
wlan CERT-AUTH 17 CERT-AUTH
security dot1x authentication-list CERT_AUTH
no shutdown
!
wireless tag policy CERT_POLICY_TAG
wlan CERT-AUTH policy CERT-AUTH
```

مدخست سمل ل ةداهش ليزنت و عاشن

ةي لالتا تاوطلال عبتا ،مدخست سمل ةداهش ليزنت و عاشن

1. اق بس م هدادع مت يذلا ةداهش ل لخدم ي ل مدخست سمل ل لوخد ليجست ب مق .



ةداهش ل لخدم ي ل لوصول

2. ةداهش ل عاشن ةحفص كلذ دع ب ISE مدقي . (AUP) لوبق م ل مادختس ال ةسايس لوبق .
3. (ةداهش عيقوت بلط نودب) ةدرفم ةداهش عاشن ددح .

Certificate Provisioning

I want to: *

Generate a single certificate (without a certificate...) 1

Common Name (CN): *

emp 2

MAC Address: *

242f.d0da.a563 3

Choose Certificate Template: *

EAP_Authentication_Certificate_Template 4

Description:

Certificate Download Format: *

PKCS12 format, including certificate chain (...) 5

Certificate Password: *

Enter password to download and view/install the certificate

Confirm Password: *

Generate

Reset

ةداهشلا ءاشنإ

ةةمازللا لوقحلا هذة لامتكأ نم دكأت ،ةداهشلا ريفوت لخدم ربع ةداهش ءاشنإل

- ةداهش يف ءاشنلا مسالا لوقح يف ةمدقملا ةميقللا ةقداصلما مداخ مدختسي :نإ يس (ذلا) مدختسملما مسالا لخدأ ،"ءاشنلا مسالا" لوقح يف .ام مدختسم ةقداصلم ليمعلا (ةداهشلا ريفوت لخدم ىلإ لوخدلا ليجستل هتمدختسأ
- ةفلتخم ميقتب ربحمسي X.509 قحلم وه MAC: Subject Alternative Names (SAN) ناونع عاونع لوقح يف ،طقاتلابو .طقف MAC ناونع 2.0 رادصلا ، Cisco ISE معدي .نامأ ةداهشب SAN/MAC.
 - عجرملا اهمدختسي يتلا لوقحلا نم ةومجم ةداهشلا بلالقي دحتي :ةداهشلا بلالقي لثم لوقح مادختسإ متي .ةداهش رادصاوام بلطةحص نم ققحتلا دنع قدصملا مسالا CN قباطي نأ بجي) بلطلا ءحص نم ققحتلل (CN) ءاشنلا مسالا رادصا ءانثأ قدصملا عجرملا لبق نم ىرخألا لوقحلا مدختست .(مدختسملما

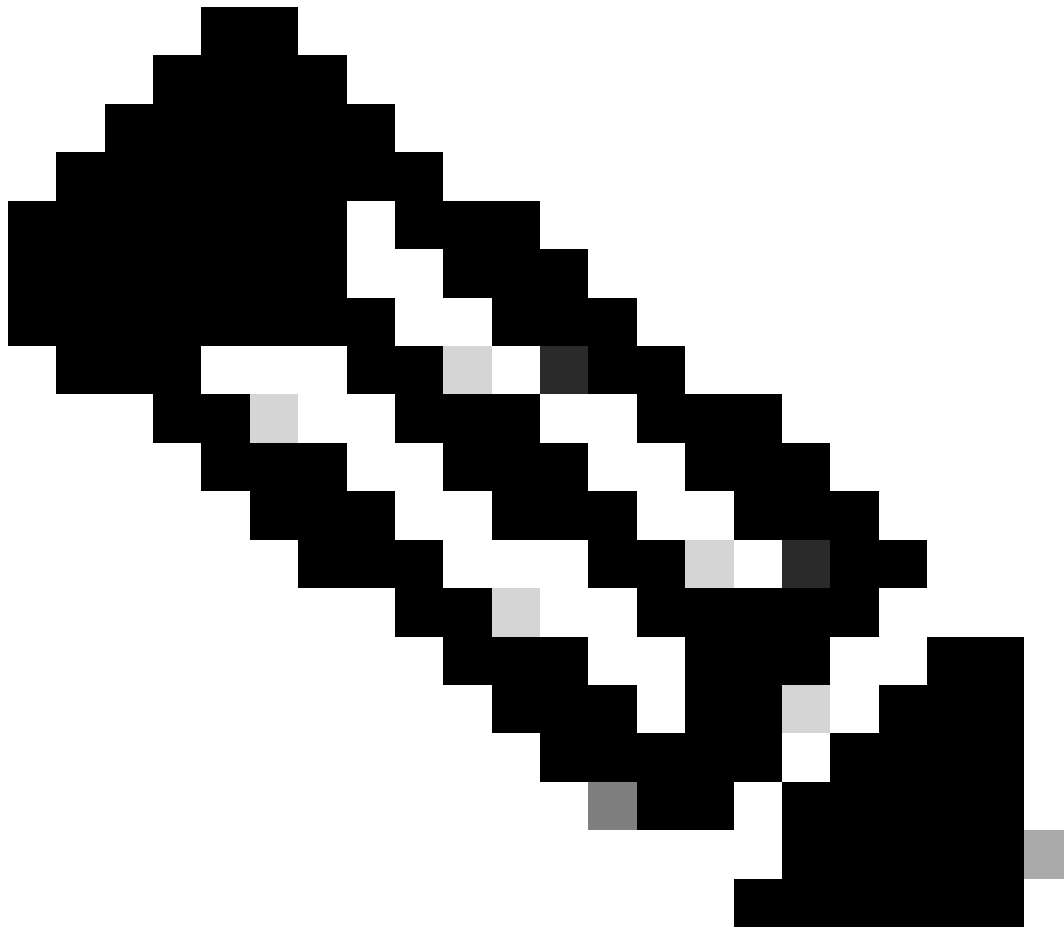
ةداهشلا

- ريفوت كيلع بجي .كتداهش نيماتل صيخرت رورم ةملك ىل اجاتحت :ةداهشلا رورم ةملك زاهجلا ىلع ةداهشلا داريتساو ةداهشلا تايتوحم ضرعل ةداهشلا رورم ةملك
- ةيلاللا دعاوقلا عم كب ةصاخلا رورملا ةملك قفاوتت نا بجي
- مقرو دحاو ريغص فرحو لقالا ىلع دحاو يلالهتسا فرح ىلع رورملا ةملك يوتحت نا بجي دحاو
 - افرح 15 و 8 نيب رورملا ةملك لوط حوارتي نا بجي
 - ا ب حومسلا فرحالا نمضتت a-z، a-z، 0-9، _، #

ةداهشلا ليزنتو عاشنال عاشنال دح ،لوقحلا لك ةئبعت درجمب

Windows لىغشلالا ماظن ب لمعي زاهج ىلع ةداهشلا تيبتت 10

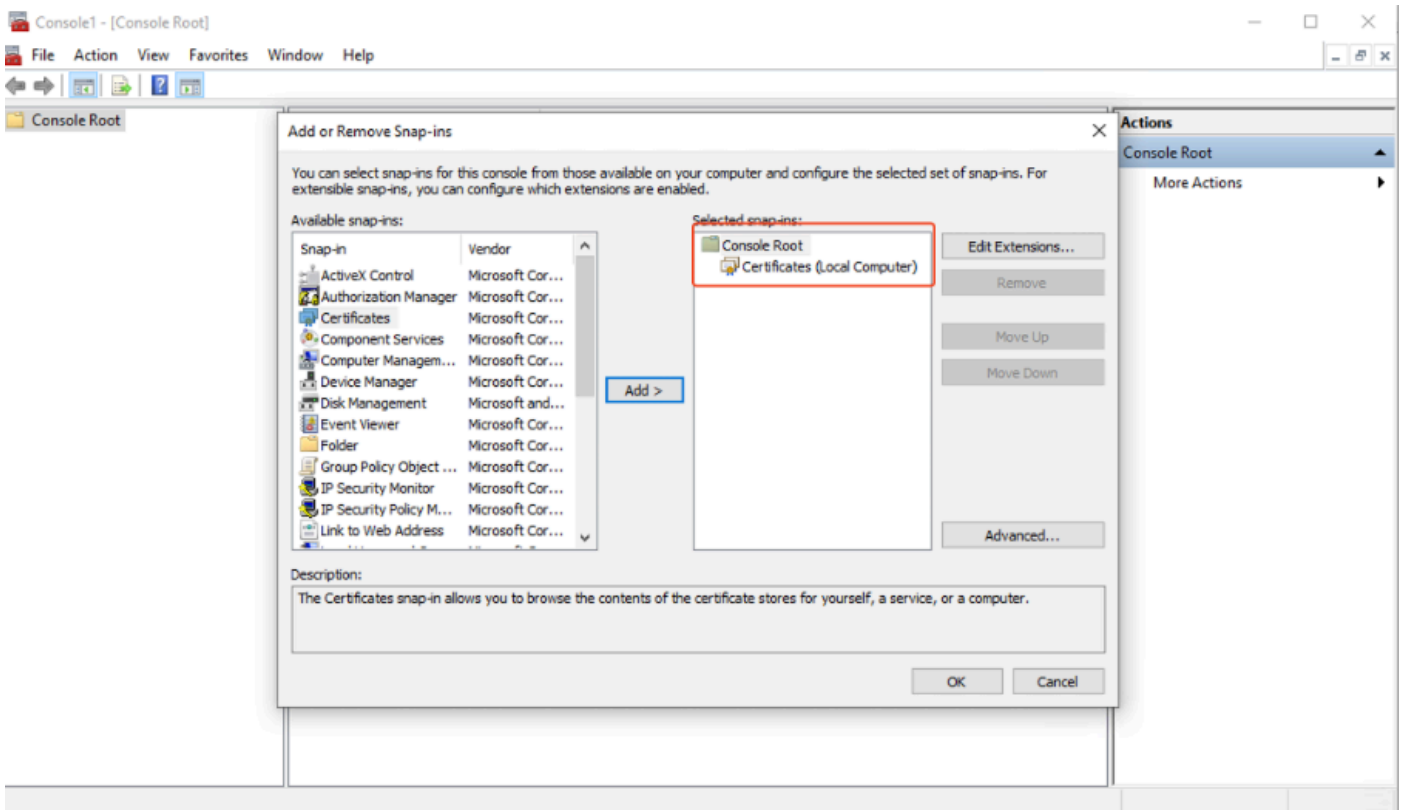
ل ةيرادللا مكحتلا ةدحوحتفا ، Windows 10 لىغشلالا ماظن ب لمعي زاهج ىلع ةداهش تيبتتلا ةيلاللا تاوطللا مادختساب (MMC) Microsoft



ةراشتساب حصني اذل Windows دادعإ ىلع ءانب تاميعلتلا هذه فلتخت دق: ءظحالم ءدحم ليصافت ىلع لوصحلل Microsoft قوائو

1. ليغشت مٲ ءب ىلع رقنا .
2. Microsoft ءتف مٲي .ل.اخدإل ءاتفم طغضاو "ليغشت" ءبرمل ي ف mmc بتك .
3. ءداهشلل ءيفاضإل ءادلأ ءفاضإ .
4. ءيفاضإ ءادلأ/ءلازا/ءفاضإ > فلم ىل لقتنا .
5. ءفاضإ رقناو ءاداهش رتأ مٲ ، ءفاضإ دء .
6. ءاهن قوف رقناو ، يءلم رءوي بمكلا مٲ ، رءوي بمكلا باسء دء .

يءلم رءوي بمكلا ىلع ءاداهشل ءرادإ ءاوطءل هذه كل ءءت



مءءء MMC ل Windows ءءو

ءداهشل ءاريتسا 1. ءوطءل

1.1. ءمءاقلا ي ءارج قوف رقنا .

1.2. ءاريتسا دء مٲ ، مءملا ءفاك ىل لقتنا .

1.3. هءيءءو ءزاءء ىلع نءءملا ءاداهشل فلم ءقوم ءيءءءل ءابلل اءملا ربع مءءء .



← Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\admin\Desktop\emp-2025-01-06_08-30-59\emp_C4-E9-0

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX, .P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Next

Cancel

ةداهشلا داريئسإ

ءاشنإ دنع اهئأشنأ يئلا رورملا ةملك لاخذإ كنم بلطي ،ةداهشلا داريئسإ ةيئلمع ءانثأ
ةداهشلا داريئسإ نم نكمتت يتح ةقذب هذه رورملا ةملك لاخذإ نم دكأت .لخدملا ىلع ةداهشلا
ءاغنب كزاهج ىلع اهئيبثتو

← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

Display Password

Import options:

- Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
- Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
- Protect private key using virtualized-based security(Non-exportable)
- Include all extended properties.

Next Cancel

ةداهشلا رورم ةملك لاخدا

ةبسانملا تادلجملا ىلإ تاداهشلا لقن 2. ةوطخل

2.1. > (ىلحم رتوي بمك) تاداهشلا ىلإ لقتناو Microsoft (MMC) نم ةرادإل مكحت ةدحوحتفا .
ىصخش دلجم

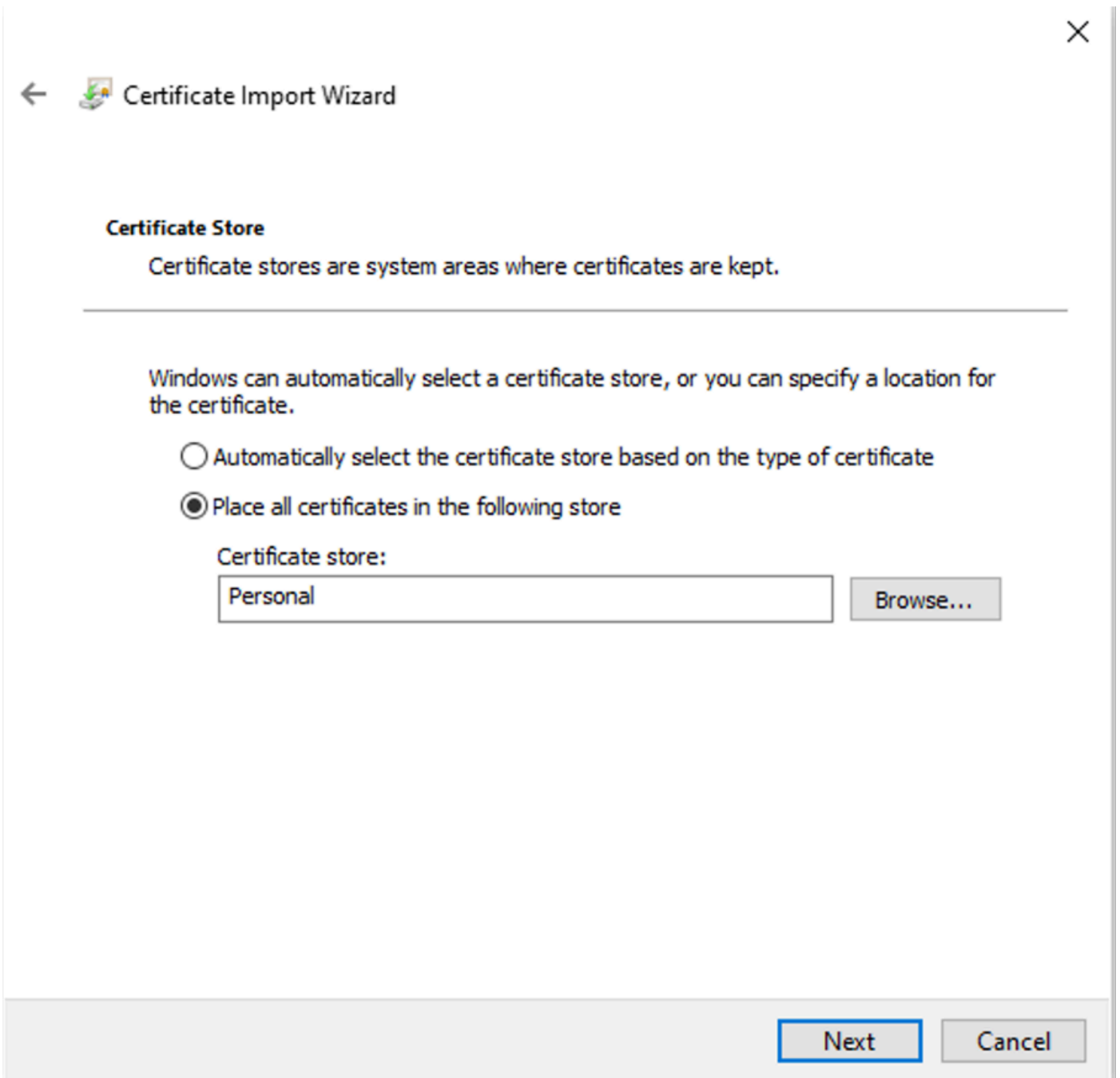
ق دصملا عجرملا وأ رذجلال ق دصملا عجرملا لثم) اهعاونأ ديدحتو تاداهشلا ةعجارم 2-2.
(ىصخشلا وأ طيسولا).

2.3. بسانملا نزملا ىلإ ةداهش لك لقن:

اهيف قوئوملا رذجلال ةداهش عجارم ىلإ لاقتنالا: رذجلال ق دصملا عجرملا تاداهش 2-4.

ةطسوتملا قي دصتلا تاطلس ىلإ لاقتنالا: ةطيسولا CA تاداهش 2-5.

ي.صخشلل دلجملا يف كرتأ :ة.صخشلل تاداهشلل -2-6



ي.صخشلل دلجملا يف تاداهشلل نيزخت

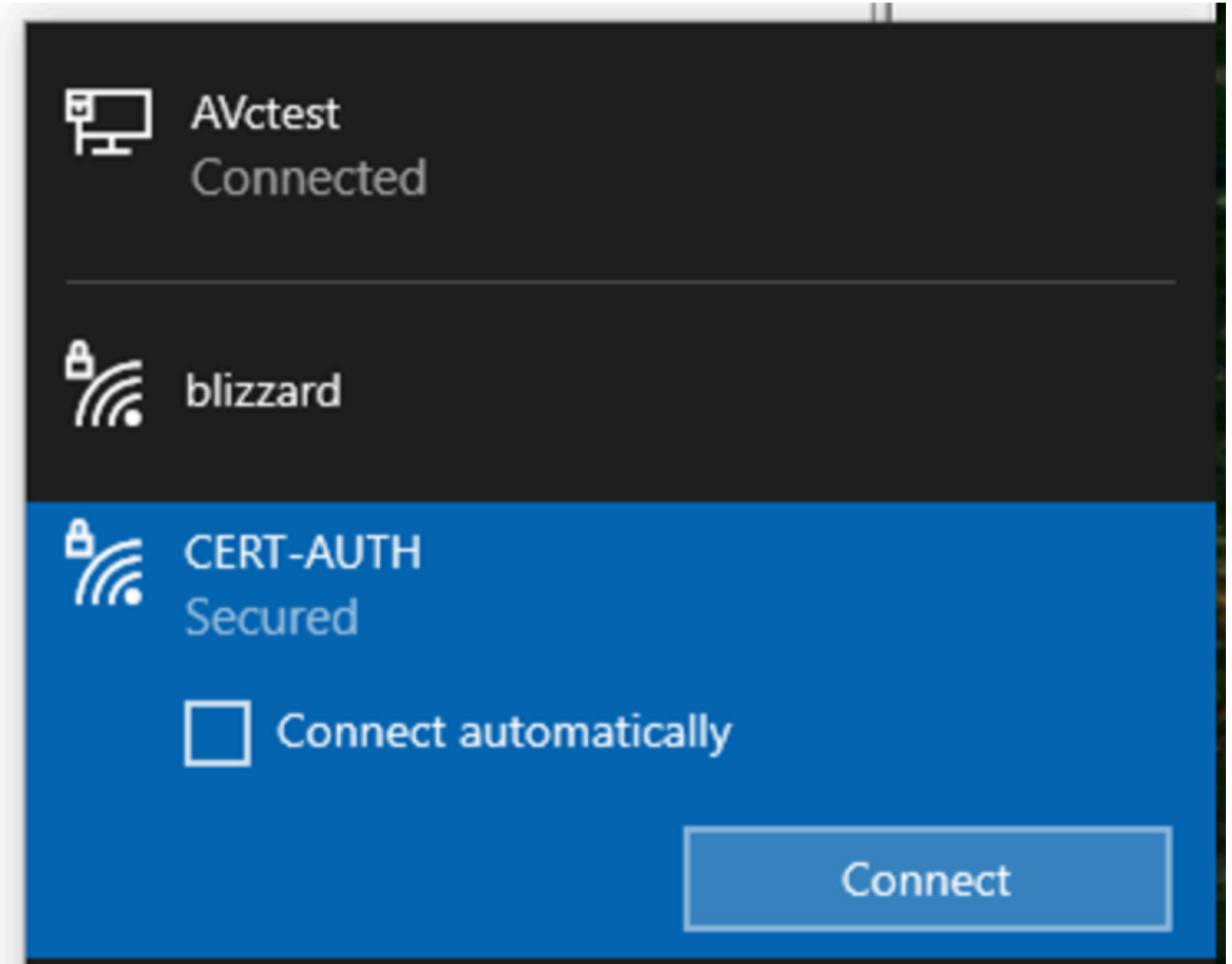
Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Statu
Certificate Services Endpoint Sub CA - ise3genvc	Certificate Services Node CA - ise3genvc	1/3/2035	<All>	EndpointSubCA	
Certificate Services Node CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate_nodeCA	
Certificate Services Root CA - ise3genvc	Certificate Services Root CA - ise3genvc	1/3/2035	<All>	certificate	
emp	Certificate Services Endpoint Sub CA - ise3genvc	1/6/2027	Client Authentication	emp_C4-E9-0A-00-...	
ise3genvc.lab.local	ise3genvc.lab.local	1/3/2027	Server Authentication, Client Authentication	Self-Signed	

مهجاتم يف صيخارتلا لقن

Windows زاخ لى صوت

ةكبشلاب لاصتال لةيلاتلا تاوطخل مدختسأ ،ةححصلا نزاخمللا إ تاداهشلل لقن درجمب
ةيكللساللا ةيحلجملا (WLAN):

1. ةحاتم لاة كلساللا تاكلشللا ضرعل ماظنلا جرد يف ةكبشلا زمرىل ع رقنا .
2. لاصتاللا يف بقرت يتلا (WLAN) ةكلساللا ةلحمللا ةكبشلا مساىل ع رقناو ثحبا .
اها .
3. مادختساب لىصوتلا ةللمع لامكلا ةففاضلا تابلاطم ةأعباتو لىصوتىل ع رقنا .
ةقداصم لل كتداهش .



ةكلساللا ةكبشلاب لىصوتلا

راىخ ددح ، (WLAN) ةكلساللا ةلحمللا ةكبشلاب لىصوتلا ةللمع ءانثأ كنم بلطى ام دنع .
صىخرت مادختساب لىصوتلا



CERT-AUTH
Secured

Enter your user name and password

Connect using a certificate

OK

Cancel

دامتعا تانايا بك ةداهشلا مادختسا

حاجن ب صيخرتلا مادختسا ب ةيكلساللا ةكبشلاب ليصوتلا اذه كل حيتي

```
C:\>netsh wlan show interface
```

```
There is 1 interface on the system:
```

```
Name : Wi-Fi 3
Description : TP-Link Wireless USB Adapter
GUID : ee5d1c47-43cc-4873-9ae6-99e2e43c39ea
Physical address : 24:2f:d0:da:a5:63
State : connected
SSID : CERT-AUTH
BSSID : a4:88:73:9e:8d:af
Network type : Infrastructure
Radio type : 802.11ac
Authentication : WPA2-Enterprise
Cipher : CCMP
Connection mode : Profile
Channel : 36
Receive rate (Mbps) : 360
Transmit rate (Mbps) : 360
Signal : 100%
Profile : CERT-AUTH
```

```
Hosted network status : Not available
```

```
C:\>netsh wlan show profiles CERT-AUTH | find "Smart"
```

```
EAP type : Microsoft: Smart Card or other certificate
```

يكلس الال في صوت الال نم ققحت الال

ةحصل الال نم ققحت الال

WLC: الال ةطساوب ثبلال دي قق نوكل الال WLAN الال نأ تققود

```
<#root>
```

```
POD6_9800#show wlan summ
```

```
Number of WLANs: 2
```

```
ID Profile Name SSID Status Security
```

```
-----
```

```
17
```

```
CERT-AUTH
```

```
CERT-AUTH
```

```
UP [WPA2][802.1x][AES]
```

WLC: الال قوف نوكل الال ap الال نأ تققود

```
POD6_9800#show ap summ
Number of APs: 1
CC = Country Code
RD = Regulatory Domain
AP Name Slots AP Model Ethernet MAC Radio MAC CC RD IP Address State Location
-----
AP1 3 C9130AXI-D cc7f.75ae.1fc0 a488.739e.8da0 IN -D 10.78.8.78 Registered default location
```

WLAN: ةكباش ثبت لوصولا ةطقون نا نم دكأت

<#root>

```
POD6_9800#show ap name AP1 wlan dot11 24ghz
Slot id : 0
WLAN ID BSSID
-----
17 a488.739e.8da0
```

```
POD6_9800#show ap name AP1 wlan dot11 5ghz
Slot id : 1
WLAN ID BSSID
-----
17
a488.739e.8daf
```

EAP-TLS: مادتس اب ليمعلا لاصتا

<#root>

```
POD6_9800#show wire cli summ
Number of Clients: 1
MAC Address AP Name Type ID State Protocol Method Role
-----
242f.d0da.a563 AP1 WLAN
```

```
17
IP Learn 11ac
```

Dot1x

Local

```
POD6_9800#sho wireless client mac-address 242f.d0da.a563 detail | in username|SSID|EAP|AAA|VLAN
Wireless LAN Network Name (SSID): CERT-AUTH
```

BSSID : a488.739e.8daf

EAP Type : EAP-TLS

VLAN : 2124

Multicast VLAN : 0

Authentication Details

Source Timestamp 2025-01-08 11:58:21.055

Received Timestamp 2025-01-08 11:58:21.055

Policy Server ise3genvc

Event 5200 Authentication succeeded

Username emp

Endpoint Id 24:2F:D0:DA:A5:63

Calling Station Id 24-2f-d0-da-a5-63

Endpoint Profile TP-LINK-Device

Identity Group User Identity Groups:Employee,Profiled

Audit Session Id 4D084E0A0000007E46F0C6F7

Authentication Method dot1x

Authentication Protocol EAP-TLS

Service Type Framed

Network Device lab-9800

Device Type All Device Types

Location All Locations

NAS IPv4 Address 10.78.8.77

NAS Port Type Wireless - IEEE 802.11

Authorization Profile PermitAccess

Security Group Employees

ةيلصفتال ISE تالجس

EAP-TLS: مزح رهظي يذلا WLC EPC طاقنلا

No.	Time	Source	Destination	Protocol	Length	Info
65	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
68	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	95	Request, Identity
69	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
70	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, Identity
73	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
74	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	304	Client Hello
78	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	182	Request, TLS EAP (EAP-TLS)
79	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
83	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	178	Request, TLS EAP (EAP-TLS)
84	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
87	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	248	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
95	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
100	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
102	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
107	17:36:58	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
109	17:36:58	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	640	Response, TLS EAP (EAP-TLS)
114	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	96	Request, TLS EAP (EAP-TLS)
115	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	TLSv1.2	347	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
118	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
119	17:36:59	TpLinkPte_da:a5:63	Cisco_9e:8d:af	EAP	110	Response, TLS EAP (EAP-TLS)
126	17:36:59	Cisco_9e:8d:af	TpLinkPte_da:a5:63	EAP	94	Success

EAP رهظي يذلا WLC طاقالت

- ةقوثولا ةيادب يف فصي قفدت EAP-TLS ل ا يف 8 ةوطخلال 87 مقر طبر لثامي
- ةقوثولا ةيادب يف فصي قفدت EAP-TLS ل ا يف 9 ةوطخلال 115 مقر طبر لثامي
- ةقوثولا ةيادب يف فصي قفدت EAP-TLS ل ا يف 10 ةوطخلال 118 مقر طبر لثامي

دع ضرعل اذه RA عبتت ةيفصت تمت :لئيمعلا لاصتا رهظي يذلا Radio Active (RA) عبتت ةقداصملا ةكرحل ةلصللا تا ذ دونبال نم لئلق

متي (debug) [15655] [ewlc-capwapmsg-sess] [20.816875191] {wncd_x_r0-2}{1} 2025/01/08 11 58
 499 لوطال، IP 10.78.8.78[5256]. ةرفشملا DTLS ةلاسرا لاسرا

متي (تامولعم) [15655] [radius] {wncd_x_r0-2}{1} 2025/01/08 11 58
 10.106.33.23 1812 id 0/25. len 390 رادصلا ل لوصولا

متي (تامولعم) [15655] [radius] {wncd_x_r0-2}{1} 2025/01/08 11 58
 10.106.33.23 1812/25 id 1812/25. Access-Challenge. len 123 ن م هيقلت

متي (تامولعم) [15655] [dot1x] {wncd_x_r0-2}{1} 2025/01/08 11 58
 [242f.d0da.a563 capwap_9080005] EAP- ةلومحل لوط، EAP، عونلا EAPOL - ةمزح لاسرا مت [capwap_9080005] EAP-Type = EAP-TLS

متي (تامولعم) [15655] [dot1x] {wncd_x_r0-2}{1} 2025/01/08 11 58
 [242f.d0da.a563 capwap_9080005] EAP، عونلا EAPOL - ةمزح مالتسا مت [capwap_9080005] EAP-Type = EAP-TLS

متي (تامولعم) [15655] [radius] {wncd_x_r0-2}{1} 2025/01/08 11 58
 10.106.33.23 1812 id 0/26. len 663 رادصلا ل لوصولا

متي (تامولعم) [15655] [radius] {wncd_x_r0-2}{1} 2025/01/08 11 58
 10.106.33.23 1812/26 id 1812/26. Access-Challenge. len 1135 ن م هيقلت

متي (تامولعم) [15655] [dot1x] {wncd_x_r0-2}{1} 2025/01/08 11 58
 [242f.d0da.a563 capwap_9080005] EAP، عونلا EAPOL - ةمزح لاسرا مت [capwap_9080005] EAP-Type = EAP-TAP Is

متي (تامولعم) [15655] [dot1x] {wncd_x_r0-2}{1} 2025/01/08 11 58
 [242f.d0da.a563 capwap_9080005] EAP، عونلا EAPOL - ةمزح مالتسا مت [capwap_9080005] EAP = EAP-TLS

متي (تامولعم) [15655] [radius] {wncd_x_r0-2}{1} 2025/01/08 11 58
 10.106.33.23 1812 id 0/27. len 465 رادصلا ل لوصولا

متي (تامولعم) [15655] [radius] {wncd_x_r0-2}{1} 2025/01/08 11 58
 10.106.33.23 1812/27 id 1812/27. Access-Challenge. len 1131 ن م هيقلت

متي (تامولعم) [15655] [dot1x] {wncd_x_r0-2}{1} 2025/01/08 11 58
 [242f.d0da.a563 capwap_9080005] EAP، عونلا EAPOL - ةمزح لاسرا مت [capwap_9080005] EAP-Type = EAP-TAP Is

2025/01/08 11 58 21.013571608 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS مت
ت هيقلت id 1812/32 10.106.33.23، Access-Challenge، len 174
2025/01/08 11 58 21.013987785 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563
capwap_9080005] مت لاسرا م EAPOL - رادصلإ 3، EAPOL عون ل لوط ، EAP-
EAP-57، ةلومحل لوط = EAP-TLS
2025/01/08 11 58 21.02429150 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563
capwap_9080005] مت لاسرا م EAPOL - رادصلإ 1، EAPOL عون ل لوط ، EAP-
EAP = EAP-TLS
2025/01/08 11 58 21.024737996 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS لاسرا
ل لوصولا بلط id 0/33، len 465
2025/01/08 11 58 21.057794929 {wncd_x_r0-2}{1} [radius] [15655] (تامولعم) RADIUS
يقلت مت (تامولعم) [242f.d0da.a563
capwap_9080005] مت لاسرا م EAPOL - رادصلإ 1، EAPOL عون ل لوط ، EAP-
EAP = EAP-TLS
2025/01/08 11 58 21.058149893 {wncd_x_r0-2}{1} [dot1x] [15655] (تامولعم) [242f.d0da.a563
capwap_9080005] مت لاسرا م EAPOL - رادصلإ 3، EAPOL عون ل لوط ، EAP-
EAP-57، ةلومحل لوط = EAP-TLS

اهحالصلإ و عااطخأل فاشكتسا

اهحالصلإ و عااطخأل فاشكتسا تاءارجإ زواجتي اميف ةلكشملا هذه لحل ةددم تاوطخ دجوت ال
ةيذومنلا ةيكلساللا 802.1x ةكبشب ةصاخلا:

1. ةقداصلما ةيلمع نم ققحتلل ليمعلا RA عبتت عااطخأ حيحصت ذخاب مق .
2. RADIUS مداخو WLC و ليمعلا نيب مزحلا صحفل WLC EPC طاقتلا ذيفنت .
3. حيحصلا جهنلل بلطال ةقباطم نم ققحتلل ةرشابملا ISE تالجس نم ققحت .
4. ةلسلس دوجو نم و Windows ةياهن ةطقن يلع حيحص لكشب ةداهشلا تيبثت نم ققحت .
لمالكلا ةقثلا

عجارملا

- [3.2 رادصلإ، لخدملل ةداهشلا ريفوت لوح ةلواتملا ةلئسألا](#)
- [ISE ليلخادلا قداصلما عجارملا تامدخ مهف](#)
- [ISE و WLC مادختساب هنيوكتو EAP-TLS مهف](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ل ا ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا