

# Mobility م ادختساب هنيوكتو EAP-TLS مهف Express و ISE

## تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطتم](#)

[تابلطتم](#)

[عمدختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[EAP-TLS قفدت](#)

[EAP-TLS قفدت يف تاوطخ](#)

[نيوكتل](#)

[Cisco Mobility Express](#)

[ISE عم Cisco Mobility Express](#)

[EAP-TLS تاداع](#)

[ISE لىل Cisco Mobility Express تاداع](#)

[ISE لىل ةقثلا ةداهش](#)

[EAP-TLS لىمع](#)

[\(Windows بتكم حطس\) لىمعل زاهج لىل عمدختسمل ةداهش لىل زنت](#)

[EAP-TLS لىل لىل سأل فى صوت](#)

[ةحصلل نم ققحتل](#)

[اهجالص او ءاطخأل افاشكتسا](#)

## عمدقمل

ةدحو يف 802.1x نيمأت عم (WLAN) ةيكلسال ةيلحم ةكبش دادع ةيفيكن دننتمسمل اذه حضوي  
عسوتمل ةقداصل لوكوتورب م ادختسا اضا دننتمسمل اذه حرشي. Mobility Express م كحت  
ددحم لكش ب (TLS) لقلنل ةقبط نامأ- (EAP).

## ةيساسأل تابلطتم

### تابلطتم

ةيلال عيضاوملاب ةفرعم كيذل نوكت نأ Cisco ي صوت

- لىلأل Mobility Express دادع
- 802.1x راي عمل اقفو ةقداصل ةيلعم
- تاداهشل

### عمدختسمل تانوكمل

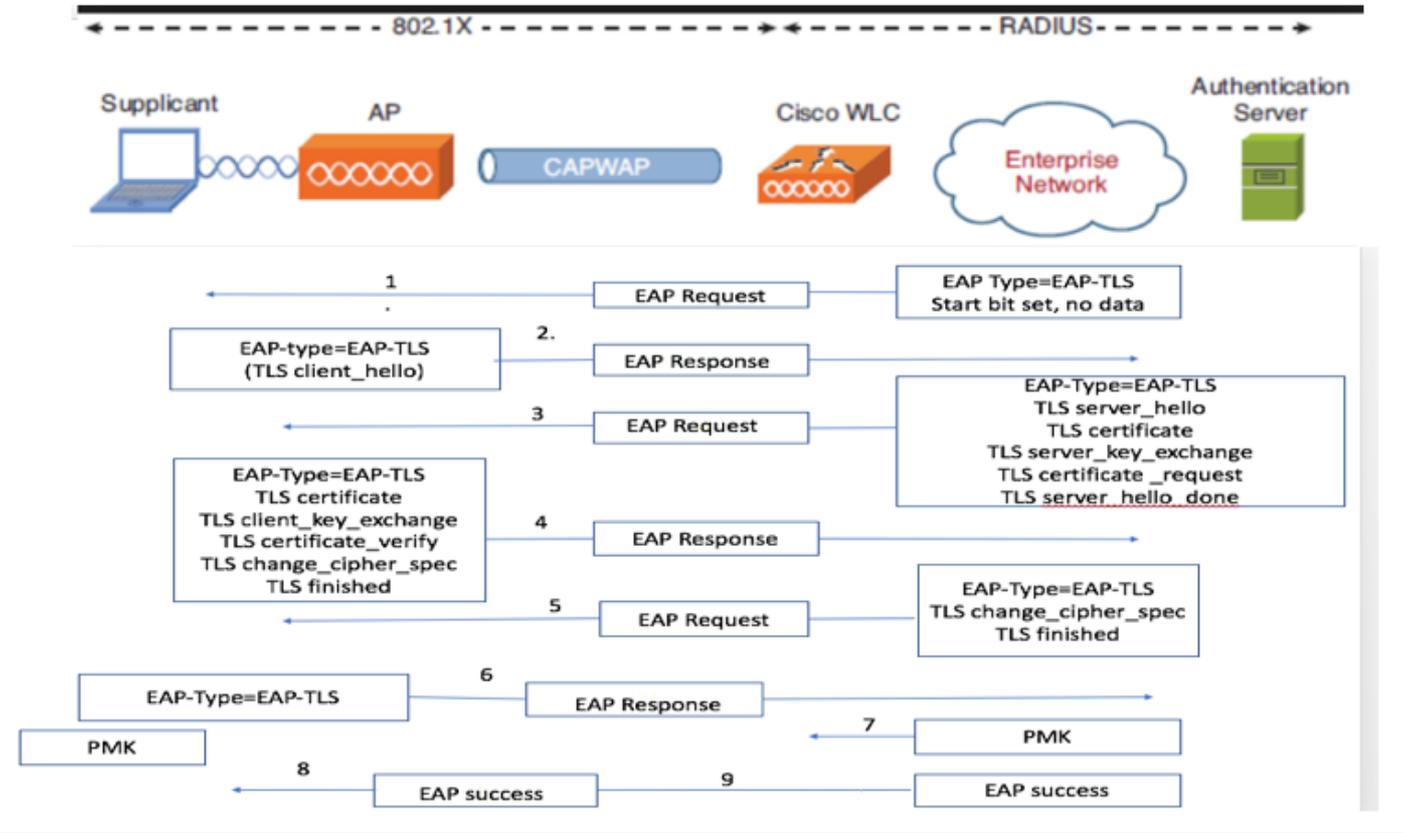
ةيلال ةيدامل تانوكمل او جماربلل تارادصل لىل دننتمسمل اذه يف ةدراول تامولعمل دننتمس

- WLC 5508، رادصإلإ، 8.5
- Identity Services Engine (ISE)، رادصإلإ، 2.1

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسمل اذ ه ي ف ةدراولإ تامولعمل اءاشنإ م ت تناك اذإ .(يضا رتفا) حوسمم نيوكتب دنتسمل اذ ه ي ف ةمدختسمل ةزهجالا عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكاتف ،ليغشتلا دي قكتك بش

## ةيساسأ تامولعمل

### قفتدت EAP-TLS



### قفتدت ي ف تاوطخ EAP-TLS

1. لوصولا ةطقنب يكلساللا ليمعلا طبتري (AP).
2. بلط لسرتو ةطقنلا هذه دنع تانايب ي لاسراب ليمعلا لوصولا ةطقن حمست ال ةقداصم.
3. ةكبشلا ي ف مكحتلا رصنع موق ي .EAP-Response ةي وه ب بلاطملا بيحتسي م ت مداخلإ مدختسمل فرعم تامولعمل ليصوتب كلذ دع ب (WLC) ةيكلساللا ةي لحمل ةقداصملا.
4. ةثداحم أدبت .EAP-TLS ءدب ةمزح مادختساب ىرخأ ةرم ليمعلا ل RADIUS مداخل بيحتسي ي .ةطقنلا هذه دنع EAP-TLS.
5. ةلاسر ىلع يوتحي يذلا ةقداصملا مداخلإ ىرخأ ةرم EAP-Response ريظنلا لسري . NULL ل هنييعت مت ريغشت ي هو ،"client\_hello" ةحفاصم.
6. ىلع يوتحت ي تال Access-challenge ةمزح مادختساب ةقداصملا مداخل بيحتسي ي .

TLS server\_hello  
handshake message  
certificate  
server\_key\_exchange  
certificate request  
server\_hello\_done.

7. ىل ع يوتحت EAP ةباجتسا ةلاسرب ليمعلا بيجتسي .

Certificate → Server can validate to verify that it is trusted.

client\_key\_exchange

certificate\_verify → Verifies the server is trusted

change\_cipher\_spec

TLS finished

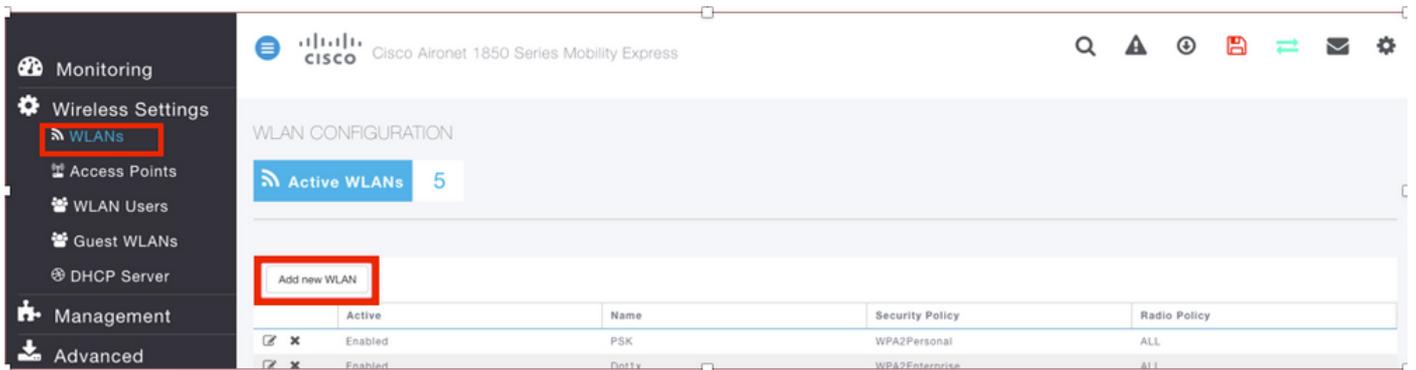
8. ىل ع يوتحتي يذلا لوصولي دحتب RADIUS مداخل بيجتسي ، حاجنب ليمعلا ةقداصم دع ب . ققحتي ، عارجلا اذم التسا دنعو . ةحفاصملا ءاهتنا و "change\_cipher\_spec" ةلاسربلا ديديج ريفشت حاتفم قاقشتشا متي . RADIUS مداخل ةقداصملا ةئزجتلا نم ليمعلا TLS ةحفاصم ءانثا رسلال نم ايكيمايني .

9. ةلا لوصولي EAP-TLS م عدي يذلا يكل سلال ليمعلا عي طتسي ةلحرمل ا هذ ه ي ف . ةيكل سلالا ةكبشلا .

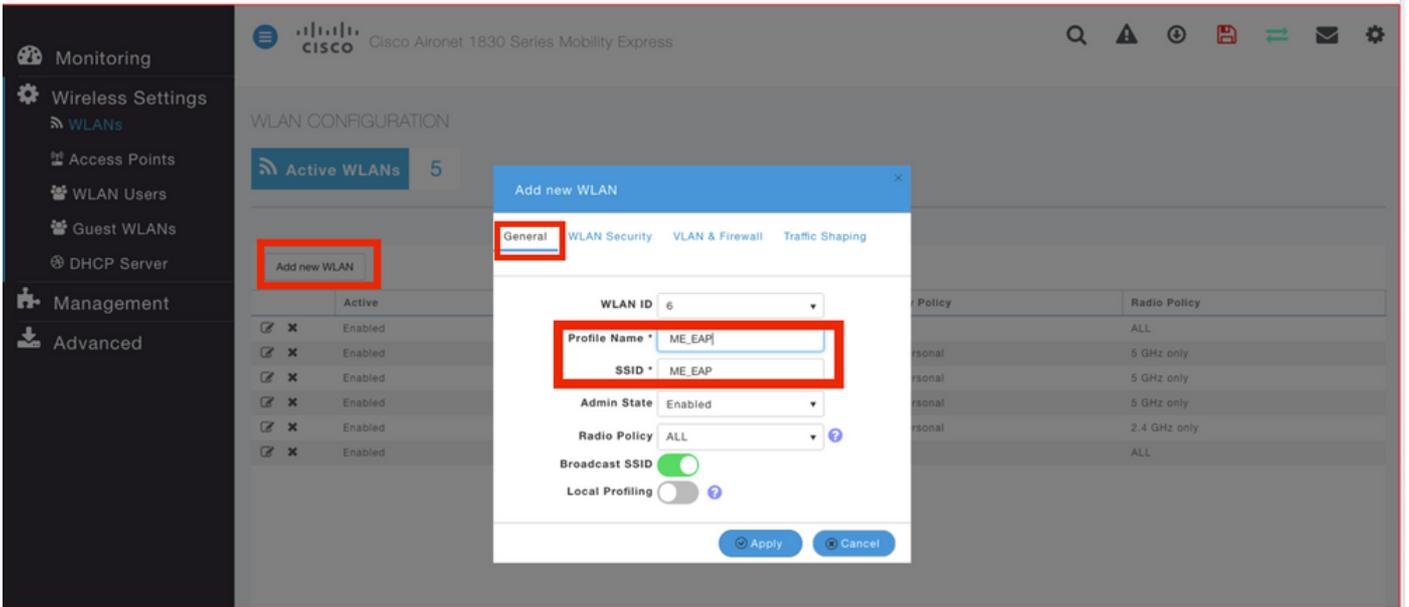
## نيوكتلا

### Cisco Mobility Express

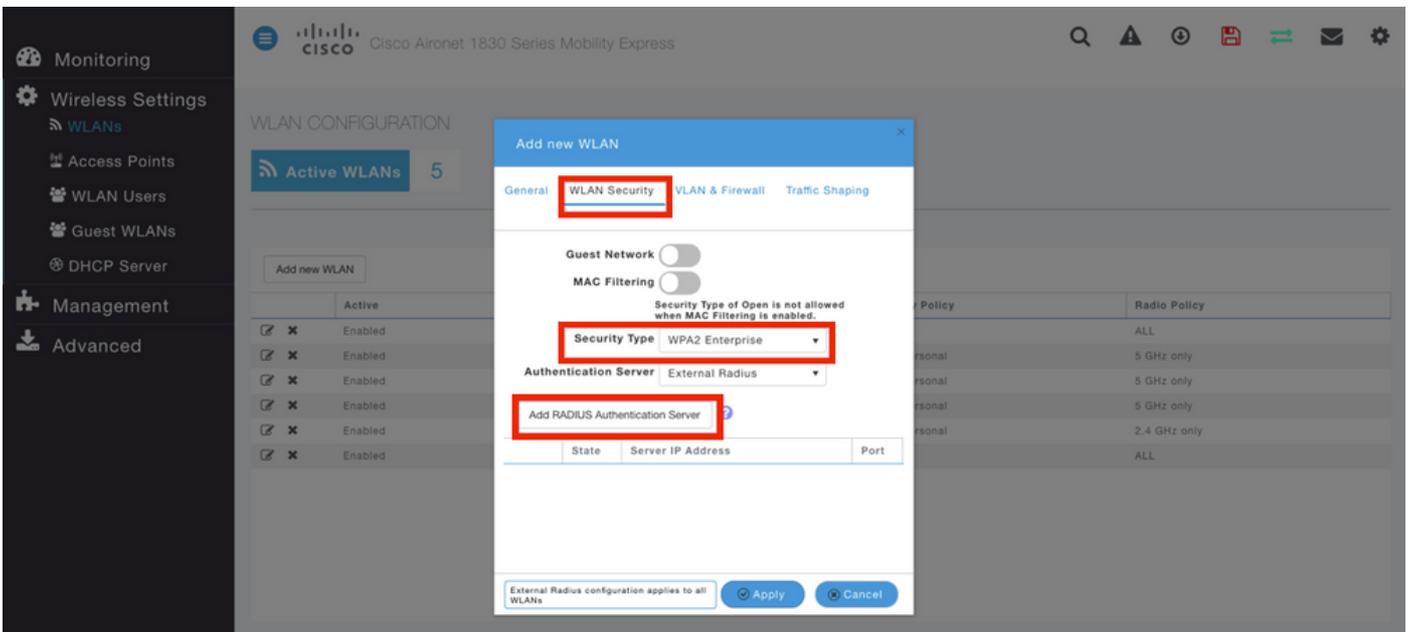
WLAN ةكبش ءاشنإل . Mobility Express ىل ع WLAN ةكبش ءاشنإل يه ىل وائل ةوطخلال 1 . ةوطخلال ، ةروصلال ي ف حضوم وه امك ةديج WLAN ةكبش ءاشنإل > WLAN ىل لقتنا .



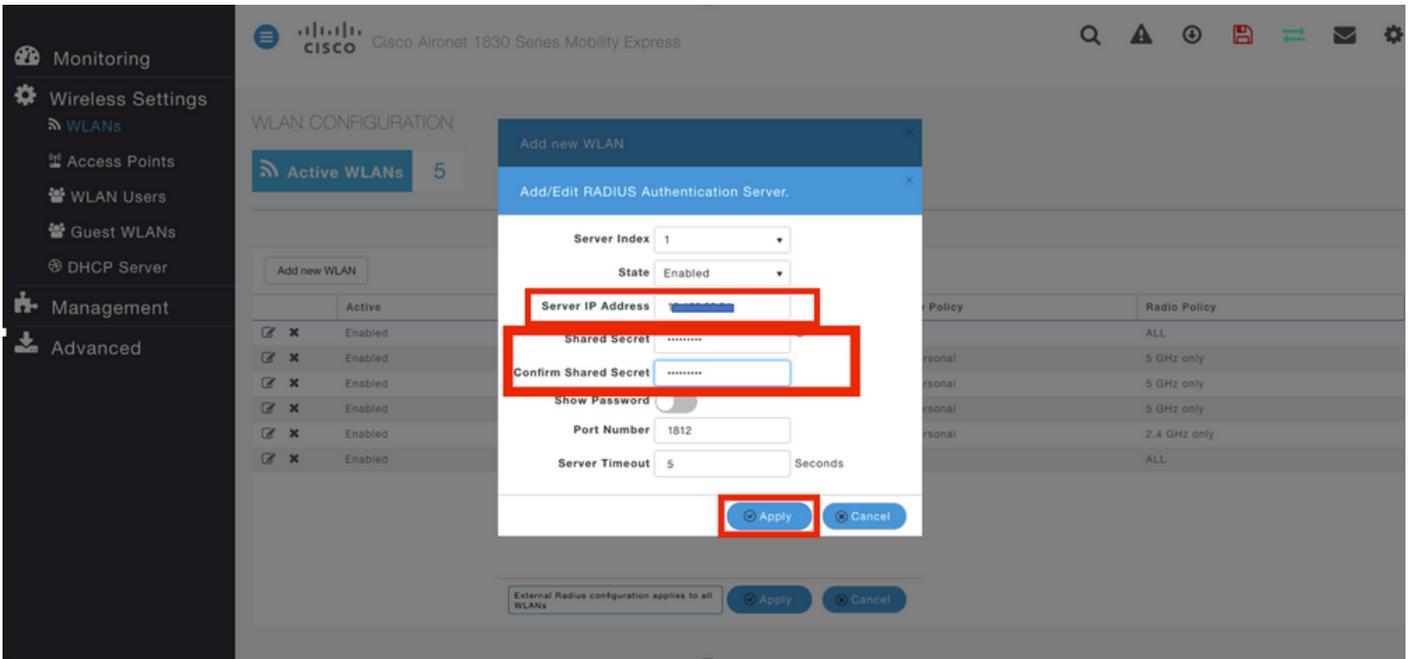
ةديج WLAN ةكبش ءاشنإل قوف رقنلا درجمب ةديج ةقثب نم ةذفان رهظتس 2 . ةوطخلال > ةديج (WLAN) ةيكل سلال ةكبش ءاشنإل ىل لقتنا ، صيصخت فلم مسا ءاشنإل . ةروصلال ي ف حضوم وه امك ءامع .



3. ةوطخلال RADIUS Server ت لكش و 802.1x ل WPA Enterprise لثم ةقداصلما عون نيوك ت ب مق 3. ةوطخلال ةروصلال ي ف حضورم وه امك WLAN ني مات > ديج WLAN ةفاضل تحت



رسلاو RADIUS مداخ ب صاخال IP ناوع رفوو RADIUS ةقداصلم مداخ ةفاضل قوف رقنا 4. ةوطخلال وه امك قي بطت يلع رقنا م ث ISE يلع هنيوك ت م ت ام امامت قباطي نا ب جي يذلا كرتش مالا ةروصلال ي ف حضورم.



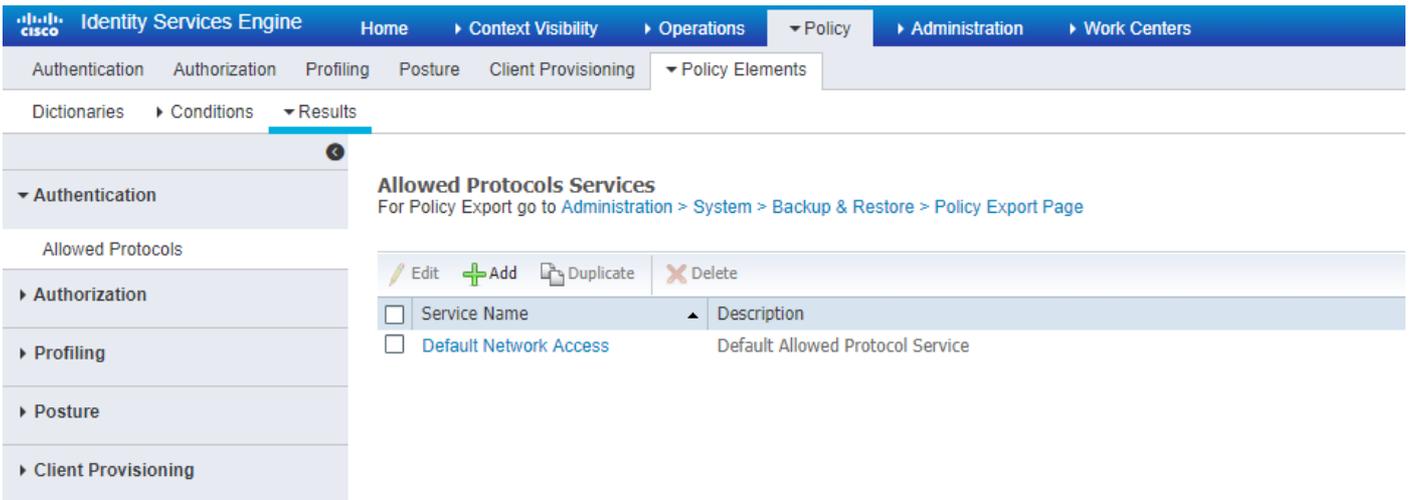
## ISE مع Cisco Mobility Express

### EAP-TLS تاداع

جهنلا يف اهم ادختساب حوم سمل تالوكوت وربلا عمئاق عاشنإ ىلإ جاتحت، جهنلا عاشنإل ةيفيك ىلإ عانب هب حوم سمل EAP عون دح، اهتباتك تمت dot1x ةسايس نأ امب. كب صاخلا ةسايسلا نيوكت.

نوكي ال دق ام وهو ةقداصم لل EAP عاونأ مطعمل حمست كإناف يضارتفال مدختست تنك اذإ ن. عي EAP عون ىلإ لوصول نيمنات ىلإ ةجاحب تنك اذإ الضفم.

تالوكوت وربلا > ةقداصم > جئاتنلا > ةسايسلا رصانع > ةسايسلا ىلإ لقتنا 1. ةوطخلا ةروصولا يف حضورم وه امك ةفاضل رقنا وه حوم سمل.



ةلاجل هذه يف. عمئاقلا مسال لادإ كنكمي، اهب حوم سمل تالوكوت وربلا عمئاق يف 2. ةوطخلا يف حضورم وه امك ىرخأ تاعبرم ديدحت باعلا متي و EAP-TLS عبرم لحمسلا ديدحت متي ةروصولا.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionaries Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services List > New Allowed Protocols Service

**Allowed Protocols**

Name

Description

Allowed Protocols

**Authentication Bypass**

Process Host Lookup

**Authentication Protocols**

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live

Proactive session ticket update will occur after  % of Time To Live has expired

Allow LEAP

Allow PEAP

**PEAP Inner Methods**

Allow EAP-MS-CHAPv2

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries  (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Require cryptobinding TLV

## ISE Mobility Express تاداع

ةفاضل > ةكبشلل ةزهج > ةكبشلل دراوم > ةرادلال لىل لقتناو ISE مكحت ةدحوتفا 1. ةوطخلل ةروصلل يف حضوم وه امك

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

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

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Network Devices

Selected 0 | Total 1

Name	IP/Mask	Profile Name	Location	Type	Description

ةروصلال ي ف حصوصم وه امك تامولعملال لاخداب مق 2. ةوطخلال

Network Devices List > New Network Device

Network Devices

\* Name

Description

\* IP Address:  / 32

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

Location

RADIUS Authentication Settings

Enable Authentication Settings

Protocol RADIUS

\* Shared Secret

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

## ISE لىل ةقثلال ةداهش

اهب قووثوم تاداهش > تاداهشلال ةرادا > تاداهش > ماظن > ةرادا لىل لقتنا 1. ةوطخلال

ةكبشلال ي ف مكحت رصنع ةفاضل درجمب . ISE لىل ةداهش داريتسال داريتسال لىل رقنا ةيمه ا رثكالال اعزلاب مايقلال كمزلي ، ISE لىل مدختسم عاشن او (WLC) ةيكلسالال ةيلحملال CSR ديوت لىل اجاتحت ،كلذل . ISE لىل ةداهشلال ي ف ةقثلال وهو EAP-TLS نم

عيقوت تابلط عاشن | ةداهشلال عيقوت تابلط > تاداهشلال > ةرادال لىل لقتنا 2. ةوطخلال ةروصلال ي ف حصوصم وه امك (CSR) ةداهشلال

Certificate Management

Overview

System Certificates

Endpoint Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Setti...

Certificate Authority

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

Show

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input type="checkbox"/> is#EAP Authentication	CN=ise.c.com	2048	ise	Wed, 11 Jul 2018	ise

اهمادختسال متيس (تاداهشلال) ةداهشلال نمو مادختسالال لىل لقتنا ، CSR عاشنال 3. ةوطخلال ةروصلال ي ف حصوصم وه امك EAP ةقداصم دح ةلدسنملا تارايللل



## Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

### Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

مدقتم ةداهش ب ل ط و م د خ ت س م ل ا ة د ا ه ش ل ت ا ر ا ي خ ي ل ع ل ص ح ت ، ة د ا ه ش ب ل ط ت ن ا درج م ب 6. ة و ط خ ل ا ة ر و ص ل ا ي ف ح ض و م و ه ا م ك م د ق ت م ة د ا ه ش ب ل ط ي ل ع ر ق ن ا .

## Microsoft Active Directory Certificate Services -- fixer-WIN-97Q5HOKP9IG-CA

### Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#)

ب ل ا ق ن م Base-64 ل ة ز م ر م ل ا ة د ا ه ش ل ا ب ل ط ي ف ه و ا ش ن ا م ت ي ذ ل ا C S R ق ص ل ا 7. ة و ط خ ل ا ي ف ح ض و م و ه ا م ك ل ا س ر ا ق و ف ر ق ن ا و ب ي و ل ا م د ا خ ر ت خ ا ، ة ل د س ن م ل ا ة م ئ ا ق ل ا ر ا ي خ : ة د ا ه ش ل ا ة ر و ص ل ا .

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

#### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

#### Certificate Template:

Web Server

#### Additional Attributes:

Attributes:

Submit >

Base-64 د د ح ، ة د ا ه ش ل ا ع و ن د ي د ح ت ل ر ا ي خ ل ا ي ل ع ل ص ح ت ، ل ا س ر ا ق و ف ر ق ن ل ا درج م ب 8. ة و ط خ ل ا ة ر و ص ل ا ي ف ح ض و م و ه ا م ك ة د ا ه ش ل ا ل ي ز ن ت ة ل س ل س ق و ف ر ق ن ا و ر ف ش م ل ا .

## Certificate Issued

The certificate you requested was issued to you.

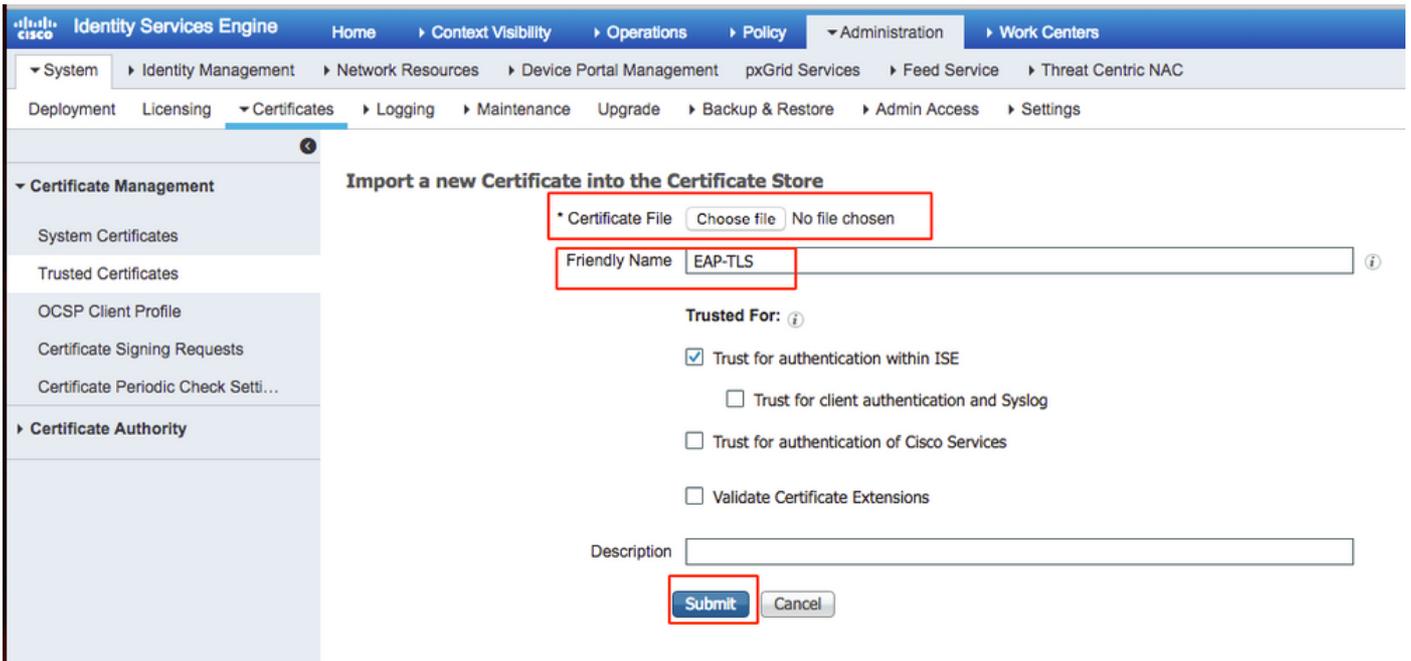
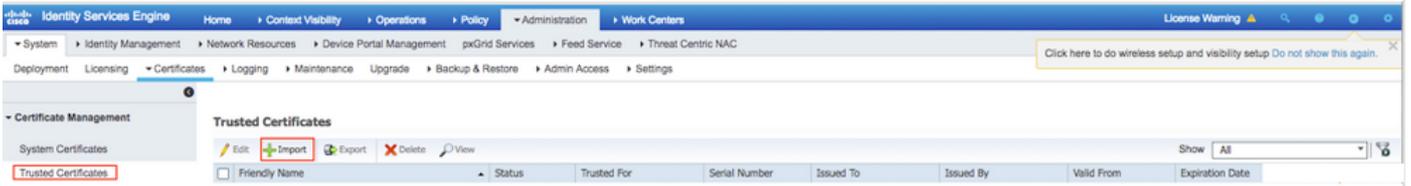
DER encoded or  Base 64 encoded



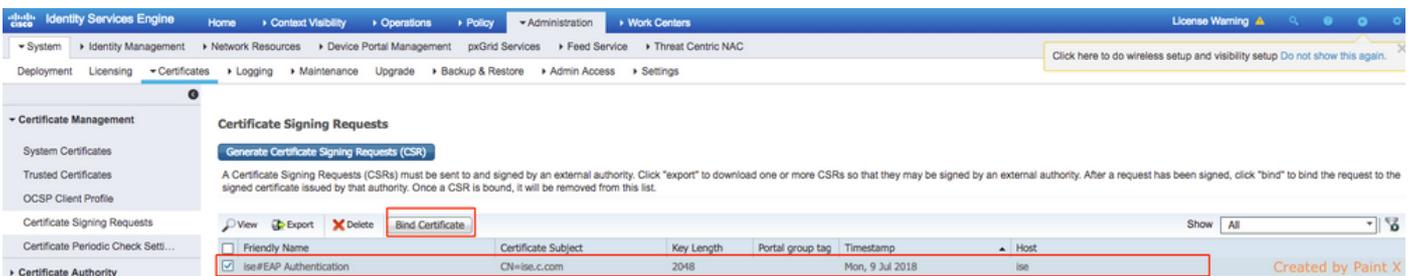
[Download certificate](#)

[Download certificate chain](#)

إداهش لآ يوتحتسو ،إداهش لآ آارختس لآ كنكمي .ISE مداخل إداهش لآ ليزنت لمتك لآ 9 ةوطخل آراد تحت رذجل إداهش لآ داري تس لآ نكمي .يرآ ةطيسو ةداهش و رذج ةداهش ،ني تدهاش يلع روصول آي حضورم وه امك داري تس لآ > اهب قوئوم تاداهش > تاداهش > تاداهش



اهب قوئوم لآ تاداهش لآ ةمئاق يلآ إداهش لآ ةفاض لآ مت ،لآس لآ قوف رقل لآ درجم 10 ةوطخل آروصول آي حضورم وه امك CSR عم طبرلل ةطيسولآ ةداهش لآ مزلي ،اضيأ





## Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC server) in the Saved Request box.

### Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
ZzAJVkd0PEONkCsBJ/3qJJeeM1ZqxnL7BVIspJry  
aF412aLpmDFp1PfvZ3VaP6Oa/mej3IXh0RFxBUII  
weOh06+V+eh7ljeTgiwzEZGr/ceYJIakco5zLjgR  
dD7LeujkxF1j3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

### Certificate Template:

User

### Additional Attributes:

Attributes:

Submit >

مداخل اقباس مت امك تاداهشال ةلسلس ليزنت قوف رقنا ،كلذ دعب .3 ةوطخل

لومحم رتويبمك نم ةداهشال داريتسال تاوطخل هذه عبتا ،تاداهشال يلع لوصحل درجمب  
Windows ليغشتال ماظنب لمعي

ل (MMC) ةرادال مكحت ةدحو نم اهيل لوصولا يلجاتحت ،ةداهشال داريتسال .4 ةوطخل  
Microsoft.

1. MMC > ليغشت > ادبا يل MMC ةكرحتفل .
2. باذجنا ةلازا / ةفاضل > فلم يل لقتنا .
3. تاداهش يلع اجودزم ارقن رقنا .
4. رتويبمكال باسح دح .
5. اهان > يلحمال رتويبمكال دح .
6. ةذفان ةيفاضال ةادال تخرخ ok in order to ةقطقط .
7. تاداهشال > ي صخش > تاداهشال راوجب [+ ] قوف رقنا .
8. داريتس > ماهملا لك دحو صيخارثال يلع نميال سواملا رزب رقنا .
9. (يلال) Next قوف رقنا .
10. ضارعتس يلع رقنا .
11. هداريتس ديرت يذال .pfx او .crt او .cer . دح .

12. حتف قوف رقنا .

13. Next قوف رقنا (يالاتل).

14. ةداهشلا عون ىلع ءانب ايئاقلت تاداهشلا نزخم ديحت دح .

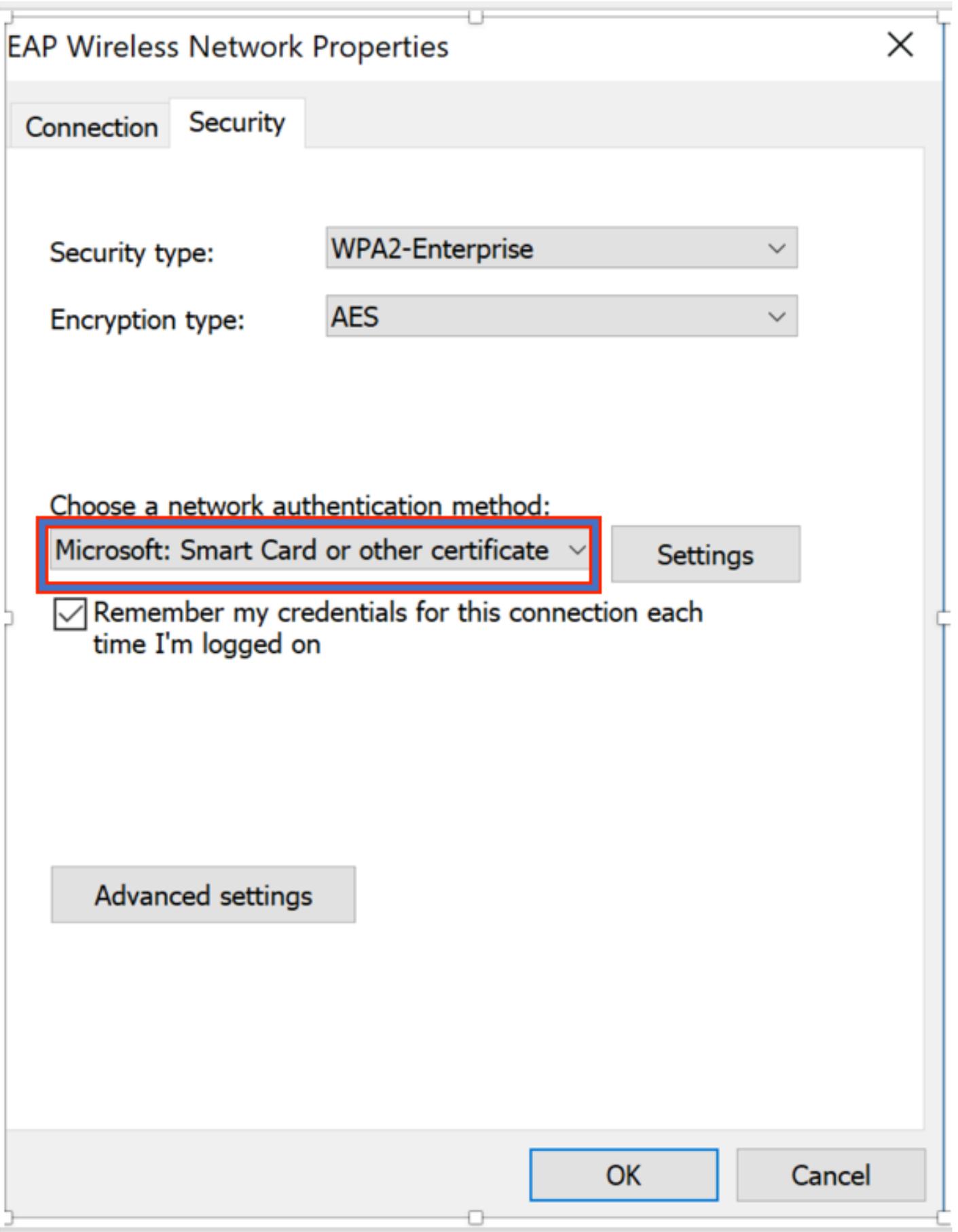
15. ok وزاجن ةقطق .

اذه يف Windows بتكم حطس) يكلساللا كليمع نيوكت كمزلي ، ةداهشلا داريتسا متي نإ ام EAP-TLS لجا نم (لاثلل

## EAP-TLS ل يكلسال في صوت

ةقداصلل لوكونوربل اقباس هؤاشنإ مت يذلا يكلساللا في صوتلا ريغتت ب مق 1. ةوطخلا EAP في صوت ىلع رقنا . كلذ نم ال دب EAP-TLS مادختسال (PEAP) يمحملل عسوتملل يكلساللا .

يف حضورم وه امك قفاوم ىلع رقنا وىرخأ ةداهش يأ وأ ةكذلا ةقابطلا : Microsoft دح 2. ةوطخلا ةروصلل .



وه امك قدصم الم عجرم الم م داخ نم ةرداصل الم رذجل ةداهش الم ددحو تادادع الم ال ع رقنا 3. ةوطخل الم ةروصل الم ف حضورم.

## Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Advanced

Use simple certificate selection (Recommended)

Verify the server's identity by validating the certificate

Connect to these servers (examples: srv1; srv2; \*.srv3.com):

Trusted Root Certification Authorities:

Entrust.net Certification Authority (2048)

Equifax Secure Certificate Authority

fixer-WIN-97Q5HOKP9IG-CA

GeoTrust Global CA

GeoTrust Primary Certification Authority

GeoTrust Primary Certification Authority - G3

GlobalSign

GlobalSign

GlobalSign Root CA

View Certificate

ةمالة نم رتوي بمكلا وأ مدخت سمل اة قدا صم ددحو ةمدقتم تاداع | قوف رونا 4. ةوطخلا  
ةروصل ايف حضوم وه امك 802.1x تاداع | بيوتلا

## Advanced settings

802.1X settings

802.11 settings

Specify authentication mode:

User or computer authentication

Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

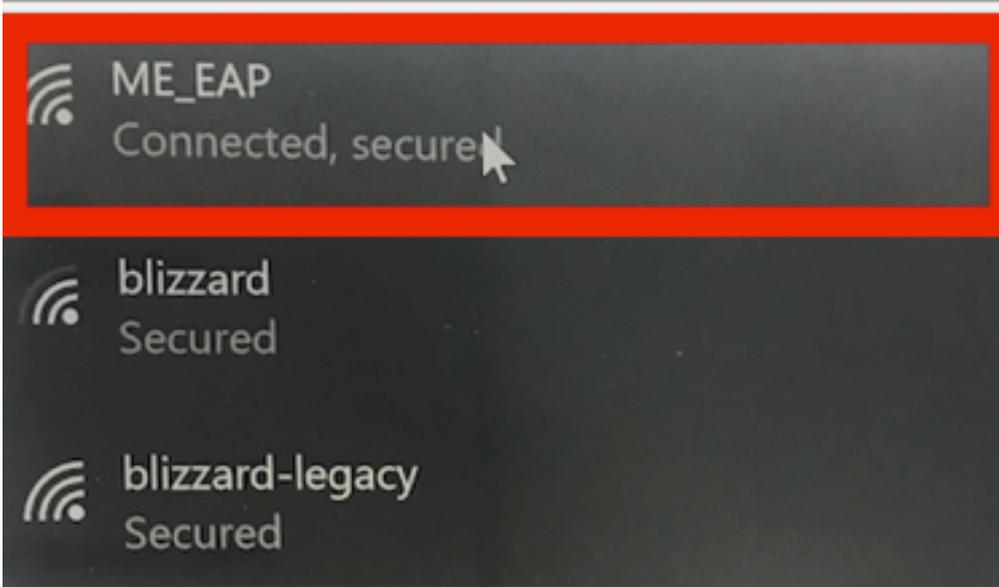
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

حيصل في صوت لادح مة كس الة كة بش ل ا ب رة ر م ل ل صوت ل ل و ا ح ن آ ل 5. ة و ط خ ل ا  
ف ف ح ص و م و ه ا م ك ة ك س ال ل ا كة بش ل ا ب ل ص و م ت ن ا . ل ل ص و ت م ت ( ل ا ث م ل ا ذ ه ف ي ف EAP )  
ة ر و ص ل ل ا .



## ةحصلال نم ققحتلال

ححص لكشب نيوكتلال لمع ديكأتل مسقلا اذه مدختسا.

ةقداصملا لمكأ دق ليمعلل نأ ينعي اذهو. EAP-TLS ليمعلل EAP عون نوكي نأ بجي 1. ةوطخلل يف حضورم وه امك رورملا ةكرح ريرمتل زهاج وهو IP ناووع ىلع لصحو EAP-TLS مادختساب روصول.

The screenshot displays a 'CLIENT VIEW' page in a network management system. The left sidebar contains navigation options: Monitoring (Network Summary, Access Points, Clients), Applications, Rogues (Access Points, Clients), Interferers, Wireless Dashboard (AP Performance, Client Performance), Best Practices, Wireless Settings, Management, and Advanced.

The main content area is titled 'CLIENT VIEW' and shows details for a client with SSID 'ME\_EAP'. The 'GENERAL' section includes:

- User Name: Administrator
- Host Name: Unknown
- MAC Address: 34:02:86:96:2f:b7
- Uptime: Associated since 37 Seconds
- SSID: ME\_EAP (highlighted with a red box)
- AP Name: AP442b.03a9.7f72 (Ch 56)
- Nearest APs: (None listed)
- Device Type: (None listed)
- Performance: Signal Strength: 0 dBm, Signal Quality: 0 dB, Connection Speed: 0, Channel Width: 40 MHz
- Capabilities: 802.11n (5GHz) Spatial Stream: 0
- Cisco Compatible: Supported (CCX v 4)
- Connection Score: 0%

The 'CONNECTIVITY' section shows a flow diagram with steps: Start, Association, Authentication, DHCP, and Online, all marked as successful.

The 'TOP APPLICATIONS' section shows a table with columns 'Name', 'Usage', and '% Usage', with the note 'No Data Available!'.

The 'MOBILITY STATE' section shows a diagram of the network path: WLC (LOCAL) -> Wired (CAP-WAP) -> AP (FlexConnect) -> Wireless (802.11n (5GHz)) -> Client (VLAN1).

The screenshot displays the Cisco WLC monitoring interface for a specific client. The top section, 'MOBILITY STATE', shows a flow from WLC (LOCAL) to Wired (CAPWAP), then to AP (FlexConnect), then to Wireless (802.11n (5GHz)), and finally to the Client (VLAN1). Below this, the 'NETWORK & QOS' section provides details on the client's network configuration, including IP Address (10.127.209.55), IPv6 Address (fe80::2818:15a4:65f9:842), VLAN (1), and QoS Level (Silver). The 'SECURITY & POLICY' section shows the client's security settings, with 'Key Management' set to 802.1x and 'EAP Type' set to EAP-TLS, both highlighted with red boxes. The bottom section, 'CLIENT TEST', offers options for PING TEST, CONNECTION, EVENT LOG, and PACKET CAPTURE.

صق م (م كحتل ا ءءول (CLI) رم اوالا رطس ءه اونم ل لمعلا ل لصافات ل ل امف 2. ءوطلالا (ءاخالالا):

```
(Cisco Controller) > show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... c8:f9:f9:83:47:b0
AP Name..... AP442b.03a9.7f72
AP radio slot Id..... 1
Client State..... Associated
Client User Group..... Administrator
Client NAC OOB State..... Access
Wireless LAN Id..... 6
Wireless LAN Network Name (SSID)..... ME_EAP
Wireless LAN Profile Name..... ME_EAP
Hotspot (802.11u)..... Not Supported
BSSID..... c8:f9:f9:83:47:ba
Connected For ..... 18 secs
Channel..... 56
IP Address..... 10.127.209.55
Gateway Address..... 10.127.209.49
Netmask..... 255.255.255.240
IPv6 Address..... fe80::2818:15a4:65f9:842
--More-- or (q)uit
Security Policy Completed..... Yes
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..... EAP-TLS
```

ءصوم وه امك تامسالا > ءياهنللا طاقن > قاي سالا ءيؤر ءي ناكم | ل ل ل قننا ، ISE ل ل 3. ءوطلالا روصلالا ف.

Endpoints > 34:02:86:96:2F:B7

34:02:86:96:2F:B7   



MAC Address: 34:02:86:96:2F:B7  
Username: Administrator@fixer.com  
Endpoint Profile: Intel-Device  
Current IP Address:  
Location:

Attributes Authentication Threats Vulnerabilities

General Attributes

Description

Static Assignment	false
Endpoint Policy	Intel-Device
Static Group Assignment	false
Identity Group Assignment	Profiled

Custom Attributes

Filter 

Attribute Name	Attribute Value
<input type="text" value="Attribute Name"/>	<input type="text" value="Attribute Value"/>

No data found. Add custom attributes here.

Other Attributes

AAA-Server	ise
AKI	88:20:a7:c9:96:03:5a:26:58:fd:67:58:83:71:e8:bc:c6:6d:97:bd
Airespace-Wlan-Id	6
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access

BYODRegistration	Unknown
Called-Station-ID	c8-f9-f9-83-47-b0:ME_EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	344
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.127.209.56
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	21
EnableFlag	Enabled
EndPointMACAddress	34-02-86-96-2F-B7
EndPointPolicy	Intel-Device
EndPointProfilerServer	ise.c.com
EndPointSource	RADIUS Probe
Extended Key Usage - Name	130, 132, 138
Extended Key Usage - OID	1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.4, 1.3.6.1.4.1.311.1f
FailureReason	12935 Supplicant stopped responding to ISE during
IdentityGroup	Profiled
InactiveDays	0
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9\G-CA,DC=fixer,DC=cc
Issuer - Common Name	fixer-WIN-97Q5HOKP9\G-CA
Issuer - Domain Component	fixer, com
Key Usage	0, 2
Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7

MatchedPolicy	Intel-Device
MessageCode	5411
NAS-IP-Address	10.127.209.56
NAS-Identifier	ryo_ap
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	ryo_ap
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
NetworkDeviceProfileName	Cisco
OUI	Intel Corporate
OpenSSLErrorMessage	SSL alert: code=0x230=560 \; source=local \; type=fatal \; message="Unknown CA - error unable to get issuer certificate locally"
OpenSSLStack	140160653813504:error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned:s3_srvr.c:3370:
PolicyVersion	0
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	Wireless802_1x
RadiusPacketType	Drop
SSID	c8-f9-f9-83-47-b0:ME_EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
StepData	4=Dot1X

## اه حال ص او عا ط خ ال فاش ك ت سا

ن ي و ك ت ل ا ذ ه ل ا ه ح ال ص او عا ط خ ال فاش ك ت سا ل ة د د ح م ت ا م و ل ع م ا ي ل ا ح ر ف و ت ت ال

