

AireOS WLC مداخلتساب EAP-TLS نيوكت و مهف و ISE

تايوتحمل

[عمدقمل](#)

[قيساسألابلطمل](#)

[تابلطمل](#)

[عمدختسملتانوكمل](#)

[قيساسأتامولعم](#)

[قفدت EAP-TLS](#)

[EAP-TLS قفدتيف تاوطخ](#)

[نيوكتل](#)

[Cisco نم قيكلسال LAN ةكبشيف مكحتل اءءو](#)

[ISE عم Cisco WLC](#)

[EAP-TLS تاداعل](#)

[ISE يلعل WLC تاداعل](#)

[ISE يلعل مدختسم عاشنا](#)

[ISE يلعل ةقثلا ةءاهش](#)

[EAP-TLS ليمع](#)

[\(Windows بكم حطس\) ليمعلل زاهج يلعل مدختسمل ةءاهش ليزنت](#)

[EAP-TLS ليلكلسال فيصوت](#)

[ءحصلا نم ققحتل](#)

[اهجالص او عاخذأل افاشكتسا](#)

عمدقمل

لوكوتورب مداخلتساب (WLAN) ةيكلسال ةيلحم ةكبش دادع ةيفيك دننتمل اءه حضوي 802.1X و EAP-TLS عسوتمل ةقءاصمل

قيساسألابلطمل

تابلطمل

ءيللال عيضاوملاب ةفرعم كيدل نوكت نأ Cisco يصوت:

- 802.1X رايعمل اقفو ةقءاصم ةيلمع
- تاداهشل

عمدختسملتانوكمل

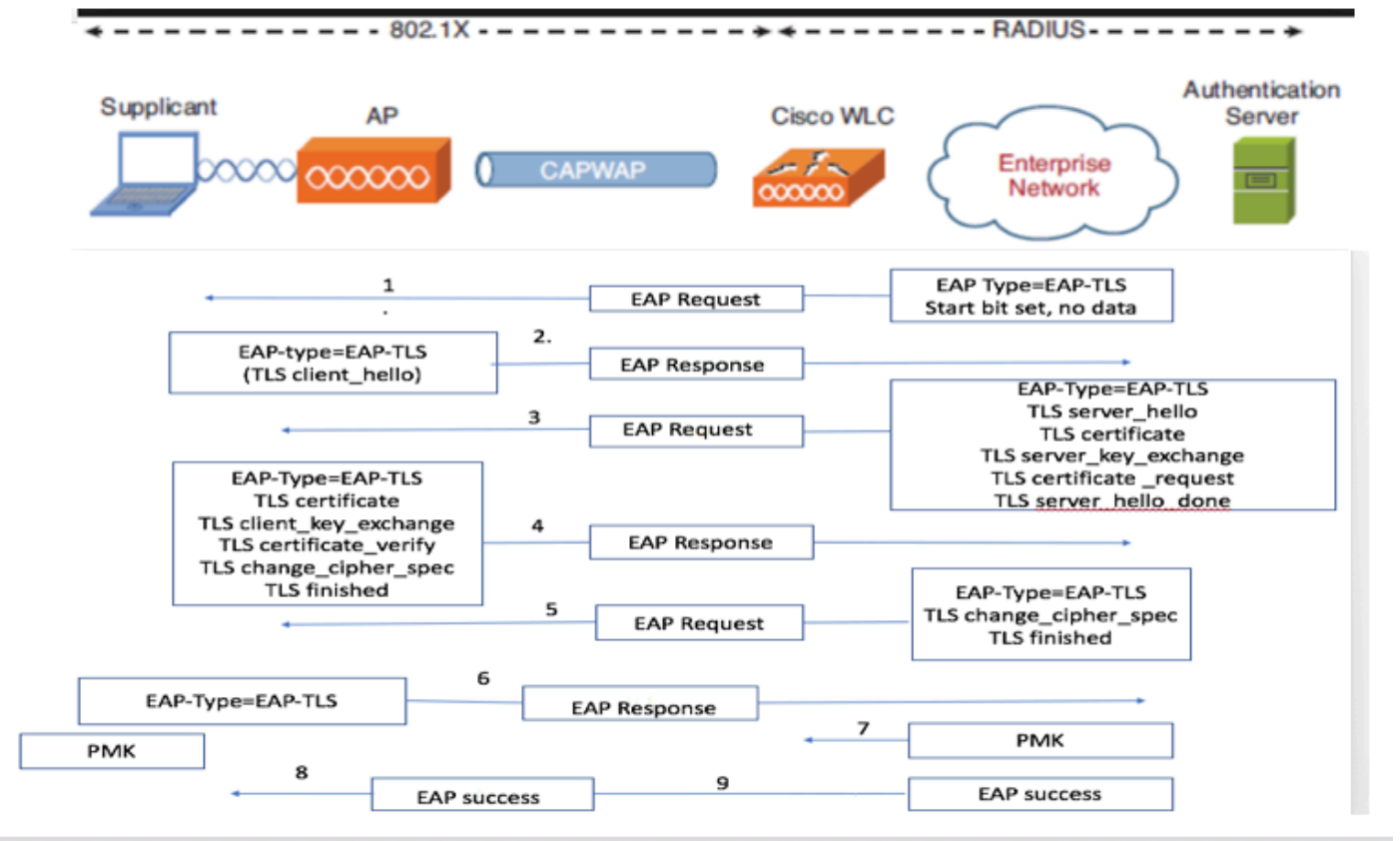
ةيلال الة دامال انوكمل او جماربال ارادصل ال دن تسمل اذ ف ةراول تامول عمل دن تست

- WLC 3504، رادصلال 8.10
- Identity Services Engine (ISE)، رادصلال 2.7

ةصاخ ةيلمع ةئب ف ةدوومل ةزهال نم دن تسمل اذ ف ةراول تامول عمل عاشنم تناك اذا. (يضارتفا) حوسم نيوكتب دن تسمل اذ ف ةمدختسمل ةزهال عيمج تادب رمايال لمحتحمل ريثاتلل كمهف نم دكأتف، ليعشتل ديق كتكبش

ةيساسأ تامول عمل

EAP-TLS قفدت



EAP-TLS قفدت ف تاوطخ

1. ليمعمل لوصول ةطقن حمست ال (AP) لوصول ةطقن بيلس الال ليمعمل طبتري بلامل بيجتسي م. ةقداصم بلط لسرتو ةطقنل هذه دنع تانايب يال لاسراب (WLC) ةيلس الال ةيلحمل ةكبشال ف مكحتل رصنع موقى. EAP-Response ةيوه ب مداخ بيجتسي. ةقداصم ال مداخ ال مدختسمل فرعم تامول عمل ليصوتب كلذ دع هذه دنع EAP-TLS ةتداحم ادبت. EAP-TLS ادب ةمزح مادختساب يرخا ةرم ليمعمل RADIUS ةطقنل.
2. ةلسر ريلع يوتحي يذلا ةقداصم ال مداخ ال يرخا ةرم EAP-Response ريطانل لسري NULL. لهنبيعت مت ريفشت وهو، client_hello لاصتا ديكأت
3. ليلع يوتحت يتل Access-challenge ةمزح مادختساب ةقداصم ال مداخ بيجتسي:

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.

4. على يوتحت يت ال EAP-Response ة لاس رب لي م ع ل ب ي ج ت س ي :

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

5. على يوتحت ي ذ ل او ، ل و ص و ل ا ي د ح ت ل RADIUS م دا خ ب ي ج ت س ي ، ح ا ج ن ب ل ي م ع ل ا ة ق د ا ص م د ع ب .
ة ح ف ا ص م ل ا ة ل م ع ا ه ا ت ن ا و CHANGE_CIPHER_SPEC ة ل ا س ر ل ل ا .

6. RADIUS م دا خ ة ق د ا ص م ل ة ن ج ت ل ل ن م ل ي م ع ل ا ق ق ح ت ي ، ك ل ذ م ل ت س ي ا م د ن ع .

7. TLS ة ح ف ا ص م ا ن ث ا ر س ل ل ن م ا ي ك ي م ا ن ي د د ي د ج ر ي ف ش ت ح ا ت ف م ق ا ق ت ش ا م ت ي .

8. ب ل ط ل ا م د ق م ل ا ل ه ر ي ر م ت م ت ي م ث ق د ص م ل ا ل ا م دا خ ل ل ن م ا ر ي خ ا EAP-SUCCESS ل ا س ر ا م ت ي .

ة ك ب ش ل ل ا ل ل و ص و ل ا EAP-TLS م ع د ي ي ذ ل ا ي ك ل س ل ل ل ا ل ي م ع ل ا ع ي ط ت س ي ة ل ح ر م ل ا ه ذ ه ي ف
ة ل ك ل س ل ل ل ا .

ن ي و ك ت ل ا

Cisco ن م ة ي ك ل س ل ل ل ا LAN ة ك ب ش ي ف م ك ح ت ل ا ة د ح و

RADIUS م دا خ ة ف ا ض ا ل . Cisco WLC على ع RADIUS م دا خ ن ي و ك ت ي ه ل و ا ل ا ة و ط خ ل ا 1. ة و ط خ ل ا
ة ر و ص ل ا ي ف ح ض و م و ه ا م ك د ي د ج ر ق ن ا . ة ق د ا ص م ل ا > RADIUS > ن ا م ا ل ا ل ا ل ق ت ن ا

Security

RADIUS Authentication Servers

Auth Called Station ID Type: AP Name:SSID

Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Colon

Framed MTU: 1300

Network User	Management	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)	Port	IPSec	Admin Status
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1	10.100.120.41	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	10.100.120.41	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3	10.100.120.41	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	10.100.120.41	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5	10.100.120.41	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6	10.100.120.41	1812	Disabled	Enabled

مداوخ RADIUS

in تلمعتسا نوکي نأ <password> كرتشملا رسلاو ناو نعلال لخدني نأ تنأ جاتحي ، انه 2. ةوطخ ةروصلال يف حضوم وه امك ةعباتملا قيبطت قوف رقنا . ise لال لال WLC لال تقود order to

Security

RADIUS Authentication Servers > Edit

Server Index: 7

Server Address(Ipv4/Ipv6): 10.106.35.67

Shared Secret Format: ASCII

Shared Secret: ***

Confirm Shared Secret: ***

Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Apply Cisco ISE Default settings:

Apply Cisco ACA Default settings:

Port Number: 1812

Server Status: Enabled

Support for CoA: Disabled

Server Timeout: 5 seconds

Network User: Enable

Management: Enable

Management Retransmit Timeout: 5 seconds

Tunnel Proxy: Enable

Realm List:

PAC Provisioning: Enable

IPSec: Enable

Cisco ACA: Enable

RADIUS ةقداصلم WLAN ةكبش عاشنإب مق 3. ةوطخلال

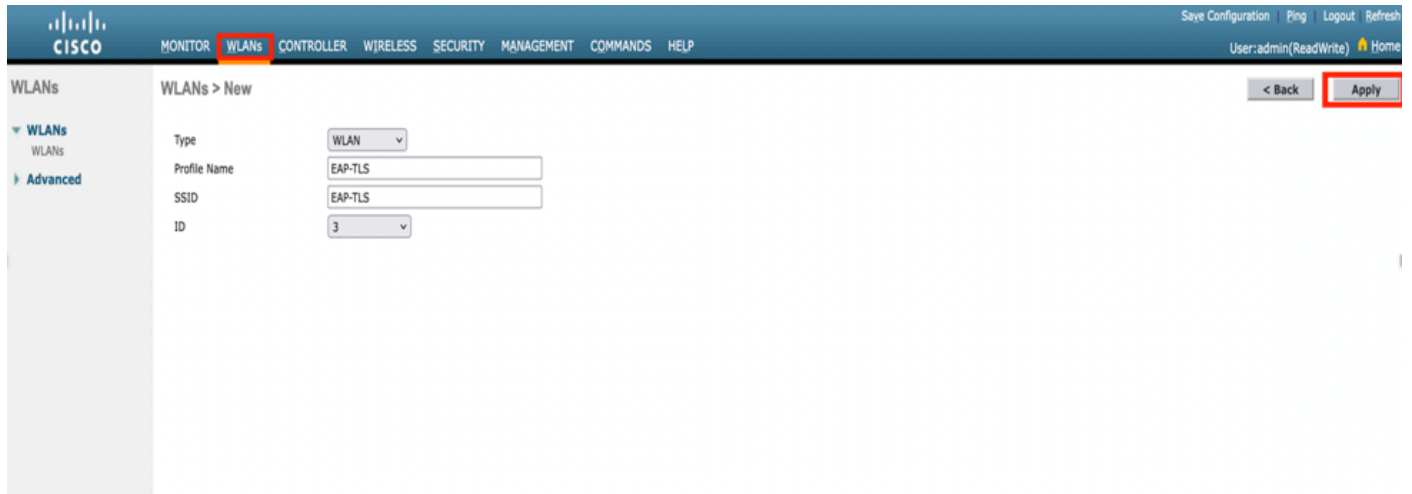
يسسؤم-WPA عضو مادختسال اهنوكتو ةديج WLAN ةكبش عاشنإ كنكمي ، نآلا ةقداصلم RADIUS مادختسال اهنكمي .

وه امك للاقنا رقناو ديجم عاشنإ رتخأ ، ةيسئيرلا ةمئاقلا نم WLAN تالكبش دح 4. ةوطخلال

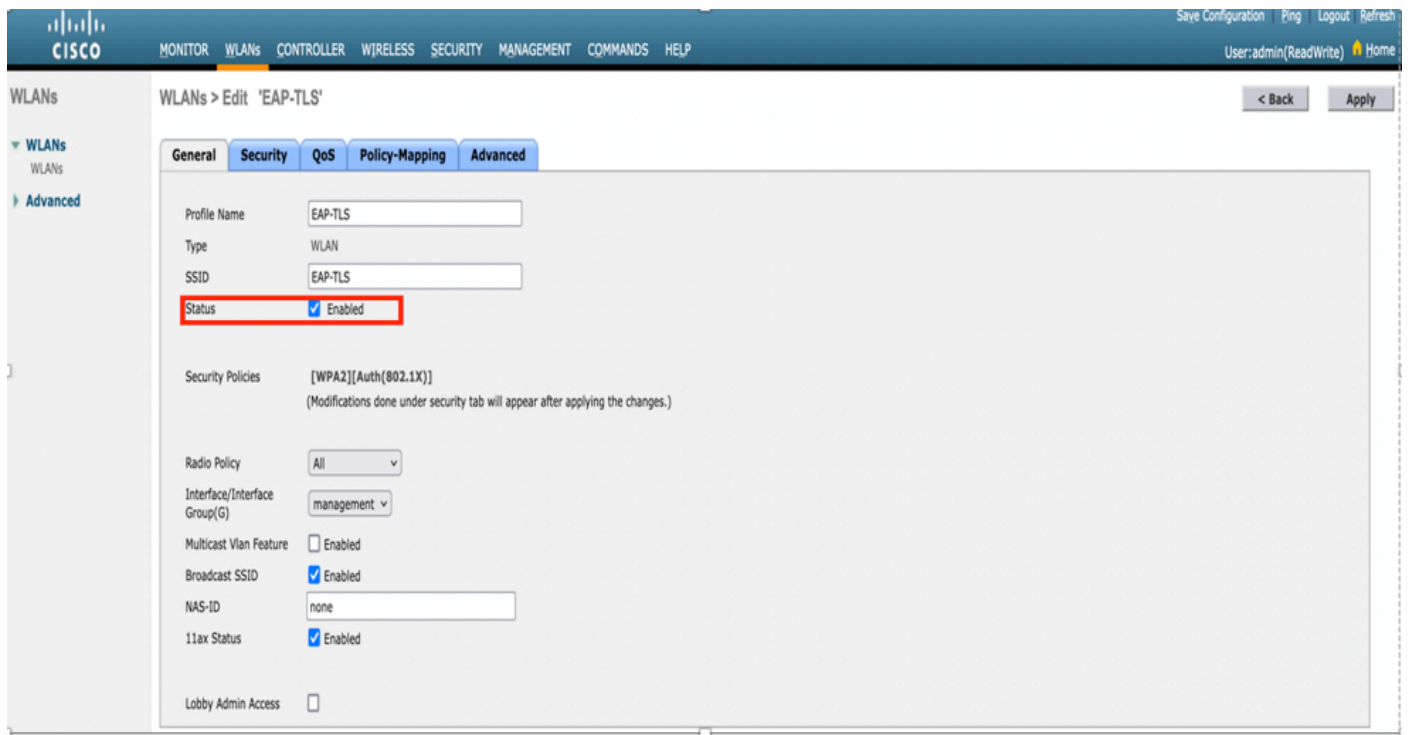
ةروصلال ي ف حضموم.



امك ةعباتملل قيبطت قوف رونا WLAN ةكبشل ديدجل EAP-TLS ةيمستب مق 5 ةوطخلال ةروصلال ي ف حضموم وه.



يه ةيضا رتفالال ني مأتال تاسايس .ةلحالل ني كمت نم دكأتو ماع قوف رونا 6 ةوطخلال ةروصلال ي ف حضموم وه امك WPA2 و 802.1X ةقداصم.



تمق يذل RADIUS م داخ دح، AAA م داوخ نامأل بيوبتال ةمالع ل لقتنا ، نآال 7 ةوطخلال ةروصلال ي ف حضموم وه امك هنيوكتب.

ةروصلال يف حضوم وه امك ةميقلا. 2 ةوطخ لخددي

Network Devices List > New Network Device

Network Devices

* Name:

Description:

IP Address: /

* Device Profile:

Model Name:

Software Version:

* Network Device Group

Location:

IPSEC:

Device Type:

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: **RADIUS**

* Shared Secret:

Use Second Shared Secret:

CoA Port:

RADIUS DTLS Settings

ISE لىل عديج مدختسم عاشنإ

حضوم وه امك ةفاضإ > نيمدختسملا > تايوهلا > ةيوهلا ةرادإ > ةرادإلا لىل لقتنا. 1 ةوطخال
ةروصلال يف

Network Access Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Action
--------	------	-------------	------------	-----------	---------------	----------------------	--------

ةروصلال يف حضوم وه امك ةمولعمل. 2 ةوطخ لخددي

Identity Services Engine 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 > Identity Source Sequences > Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name:

Status: Enabled

Email:

Passwords

Password Type:

Password: Re-Enter Password:

* Login Password: ⓘ

Enable Password: ⓘ

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login:

Account Disable Policy

Disable account if date exceeds: (yyyy-mm-dd)

User Groups

Select an item

ISE ىلع ةقثلا ةداهش

اهب قوٲوملا تاداهشلا > تاداهشلا ةرادا > تاداهشلا > ماظنلا > ةرادا ىلإ لقتنا 1. ةوطخلا

ةكبشلا يف مكحت رصنع ةفاضل درجم ب. ISE ىلإ ةداهش داريتسال داريتسإ ىلع رقنا ةيمهأ رثكال اعزلاب مايقلا كمزلي، ISE ىلع مدختسم عاشنإو (WLC) ةيكلساللا ةيلحمل CSR عاشنإ ىلإ جاتحت، كلذل. ISE ىلع ةداهشلا يف ةقثلا وهو EAP-TLS نم

تاداهش عيقتو تابلط عاشنإ > تاداهش عيقتو تابلط > تاداهش > ةرادا ىلإ لقتنا 2. ةوطخلا ةروصللا يف حضوم وه امك (CSR)

Identity Services Engine Administration Work Centers

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

View Export Delete Bind Certificate

Show All

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
No data available					

Certificate Authority

ام ادخست متي (تاداهشال) ةداهشال نمو مادختسالال ال لقتنا CSR، عاشنال 3. ةوطخلال ةروصلال يف حضوم وه امك EAP ةقداصم ددح، ةلدسنملا تارايلخلل

Identity Services Engine Administration Work Centers

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Setti...

Certificate Authority

Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA

Usage

Certificate(s) will be used for: EAP Authentication

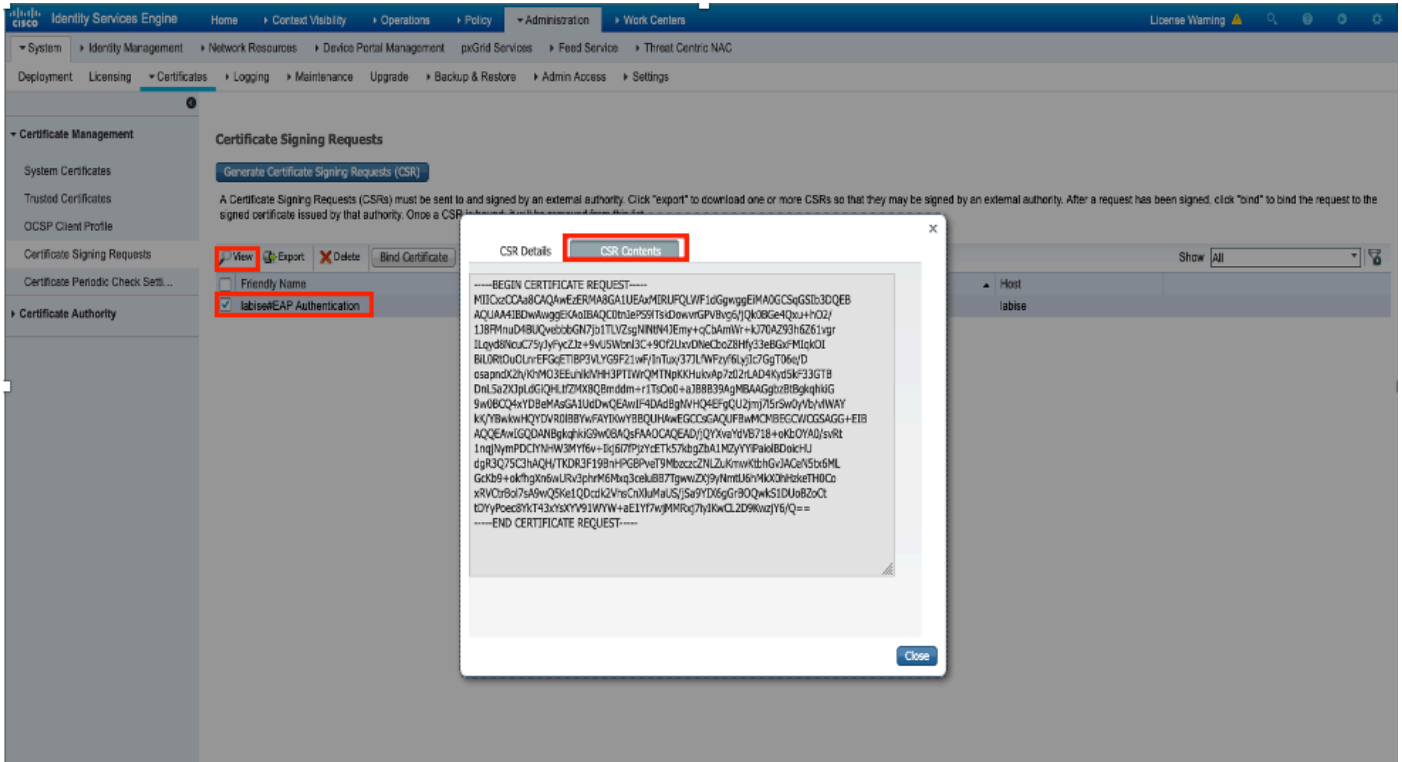
Allow Wildcard Certificates

Node(s)

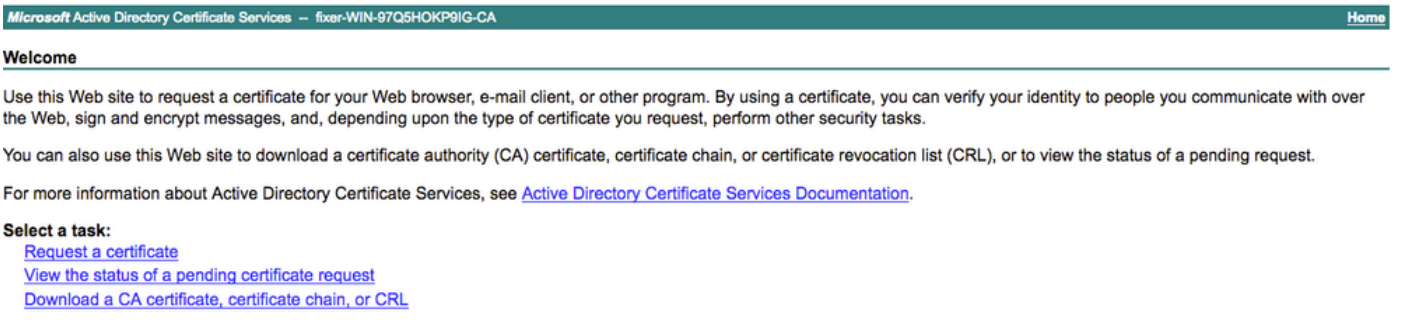
Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> labise	labise#EAP Authentication

يف حضوم وه امك ضرع قوف رونا ISE. ال لع هؤاشنال مت يذل CSR ضرع نكمي 4. ةوطخلال ةروصلال



ي ف حضورم وه امك ةداهش بلط قوف رقن او CA مداخل ل ح ف ص ت ، CSR ءاشن ل درجم ب .5 ةوطخلال
 ةروصلال:



م د ق ت م ةداهش بلطو م د خ ت س م ل ا ةداهش ل ت ا ر ا ي خ ل ع ل ص ح ت ، ةداهش بلط درجم ب .6 ةوطخلال
 ةروصلال ي ف حضورم وه امك م د ق ت م ةداهش بلط قوف رقن 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](#)

ر ا ي خ ل ل ن م . Base-64 ل ةز م ر م ل ا ةداهش ل ا بلط ي ف وه ءاشن ل م ت ي ذل ا CSR ق ص ل ا .7 ةوطخلال
 ةروصلال ي ف حضورم وه امك ل ا س ر ا قوف رقن او ب ي و ل ا م د خ ل ر ت خ ، ةداهش ل ا بلط ل د س ن م ل ا

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

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:

Additional Attributes:

Attributes:


BASE-64 ددح .ةداهشلا عون ديدحتل رايخلا لىل لصحت ،لاسرا قوف رقنلا درجم ب .8 ةوطخلا ةروصلال يف حضورم وه امك تاداهشلا ةلسلس ليزنت رقناو زمرملا

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

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)

[Download certificate chain](#)

ىل ةداهشلا يوتحت .ةداهشلا جارختسا كنكمي .ISE مداخل ةداهشلا ليزنت لمتكا .9 ةوطخلا > تاداهش > ةرادا تحت رذجال ةداهشلا جاردا نكمي .ةطس وتم ىرخأ ةداهش و رذج ةداهش و ني تاداهش روصلال يف حضورم وه امك داريتسا > اهب قوئوم تاداهش > تاداهش

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 Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Click here to do wireless setup and visibility setup Do not show this again.

Certificate Management

System Certificates

Trusted Certificates

Show All

<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
--------------------------	---------------	--------	-------------	---------------	-----------	-----------	------------	-----------------

Identity Services Engine Administration Work Centers

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Import a new Certificate into the Certificate Store

* Certificate File Choose file No file chosen

Friendly Name EAP-TLS

Trusted For:

Trust for authentication within ISE

Trust for client authentication and Syslog

Trust for authentication of Cisco Services

Validate Certificate Extensions

Description

Submit Cancel

اهب قوتوملا تاداهشللا ةمئاق ىلى ةداهشلا ةفاضل مت ، لاسرا قوف رقنلا درجمب 10 ةوطخلال ةروصلال يف حضوم وه امك CSR عم طبرلل ةطيسولا ةداهشلا مزلي ، اضيأ

Identity Services Engine Administration Work Centers

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

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.

View Export Delete Bind Certificate

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
<input checked="" type="checkbox"/>	ise#EAP Authentication	CN=ise.c.com	2048	Mon, 9 Jul 2018	ise

Created by Paint X

ىلى ع ظوفحمل ةداهشلا فلم راي تخال رايخ دجوي ، طبرلا ةداهش قوف رقنلا درجمب 11 ةوطخلال ةروصلال يف حضوم وه امك لاسرا رقنلا ةطيسولا ةداهشلا ىلى حفصت . بتكملال حطس

Identity Services Engine Administration Work Centers

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

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Bind CA Signed Certificate

* Certificate File Choose file No file chosen

Friendly Name

Validate Certificate Extensions

Usage

EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

Submit Cancel

يفي حضوره وه امك ماطنلا تاداهش > تاداهش > قراد اىل ا لقتنا ،ةداهشلا ضرعل 12. ةوطخللا ةروصللا

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
Default self-signed saml server certificate - CN=SAML_ise.c.com	SAML		SAML_ise.c.com	SAML_ise.c.com	Wed, 11 Jul 2018	Thu, 11 Jul 2019
Intermediate	EAP Authentication, Admin, Portal	Default Portal Certificate Group	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020

EAP-TLS لىمعم

(Windows بتكم حطس) لىمعمل زاهج لىل مدختسملا ةداهش لىزنن

مق . لىمعم ةداهش ءاشن ا كىل لىمعم ، EAP-TLS لال خ نم كىل لسال مدختسم ةقداصل م . 1 ةوطخللا حتفا . مداخل لىل لوصولا نم نكمتت لىتحت ةكبشلاب Windows رتووىبمك لىصوتبم <https://<server-ip addr>/certsrv> : ناوعلل اذه لخدأوبىو ضرعتسم

ISE ل اهل لىزنن مت لىتلا ةداهشلا هسفن وه نوكل نأ بچى قداصلل اعجرمل نا طحال 2. ةوطخللا

لىل . مداخل ةداهشلا لىزننل هتمدختسأ لىل CA مداخل سفن ضارعتسال جاتحت ببسال اذه لىل جاتحت ةرملل هذه ،كلذعمو ، اقبسم مت امك ةداهش بلط قوق رقتنا ، قداصلل اعجرمل سفن ةروصلل لىمعم وه امك ةداهش بلل قك مدختسم دىدحت

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  
dD7LeujkxFlj3SwvLTKLDJq+00VtAhrxlp1PyDZ3  
ieC/XQshm/OryD1XuMF4xhq5ZWoloDOJHG1g+dKX  
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

Attributes:

Submit >

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

لومحم رتوي بمك ىل ةداهشال داريتسال تاوطخل هذه مدختسأ، تاداهشال ىل ةلوصحل درجمب
Windows لىغشتال ماظنب لمعي

نم (MMC) ةرادال مكحت ةدحو نم اهيل لوصول ىل جاتحت، ةداهشال داريتسال 4 ةوطخل
Microsoft.

1. MMC > لىغشت > ادبا ىل MMC ةكرح حتفل.
2. باذجانا ةلازا / ةفاضل > فلم ىل لقتنا.
3. تاداهش ىل ةجودزم ارقن رقنا.
4. SelectComputer باسح.
5. ءاهن > لىلحمال رتوي بمكال دح.
6. ةذفان ةيفاضال ةادلل تجرخ ok in order to ةقطقط.
7. تاداهشال > لىصخش > تاداهشال راوجب [+] قوف رقنا.
8. داريتسال > ماهمال عيجم دحو تاداهشال قوف نميال سوامال رزب رقنا.
9. (لىلاتال) Next قوف رقنا.

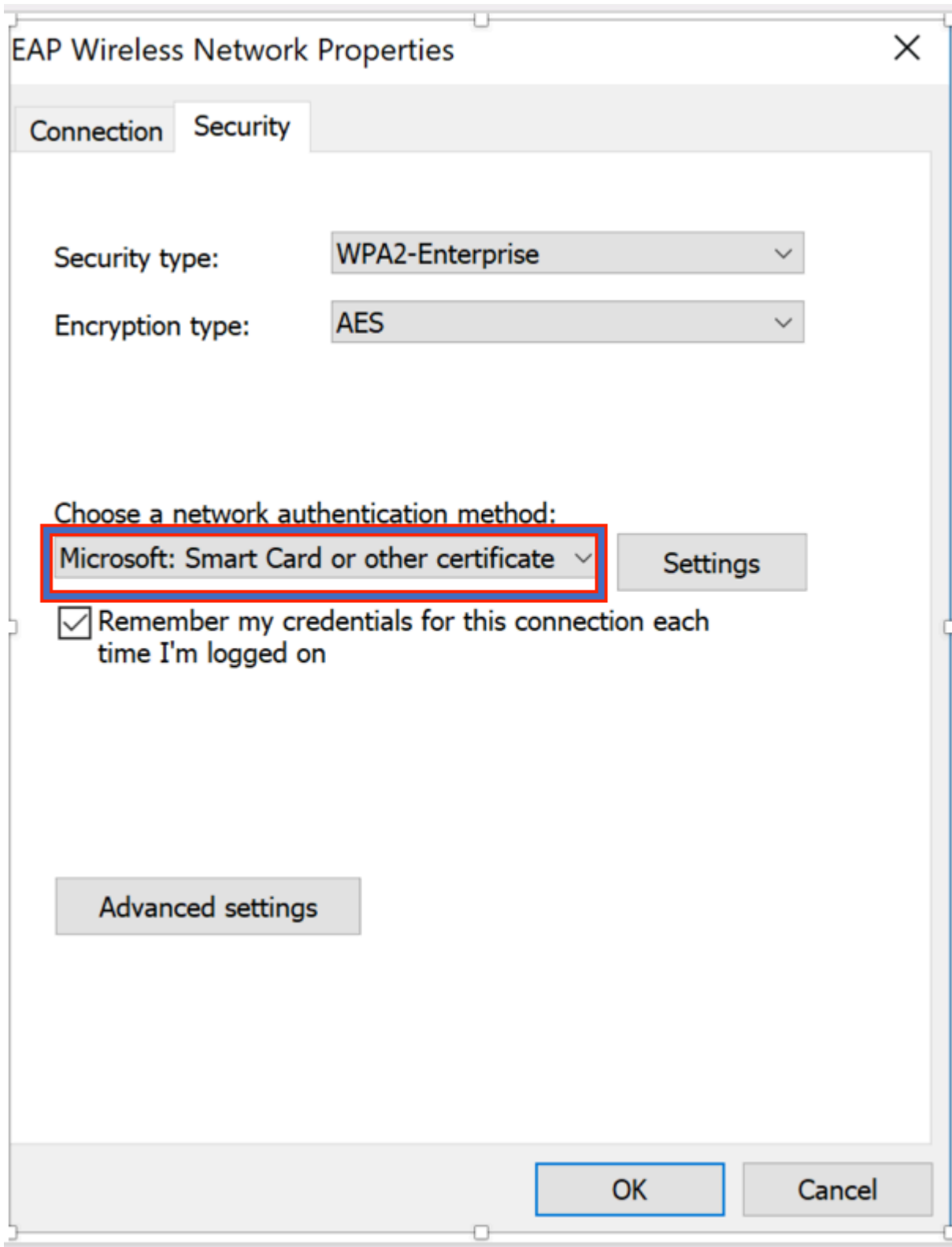
10. ضارعتسا ىلع رقنا .
11. هداريتسا ىديرت يذلا pfx . وأ .crt ، .cer . ددح .
12. حتف قوف رقنا .
13. (يلااتلا) Next قوف رقنا .
14. ةداهشلا عون ىلع ءانب اىئاقلت تاداهشلا نزخم ىديحت ددح .
15. ok و زاجن ةقطقط .

يف Windows ، بتكم حطس) ىكلساللا كلىممع نىوكت كمزلي ، ةداهشلا داريتسا ىمتي نإ ام
EAP-TLS ل (لاثلما اذه

EAP-TLS ل ىكلسال فيصوت

ةقداصملا لوكوتوربل اقباس هؤاشنإ مت يذلا ىكلساللا فيصوتلا ريغ . 1 ةوطخلا
EAP فيصوت ىلع رقنا . كلذ نم ال دب EAP-TLS مادختسال (PEAP) ىمحمل عسوتملا
ىكلساللا .

ةروصلال في ضرعم قفاوم رقناو ىرخأ ةداهش يأ وأ ةيكدلا ةقابطلا : Microsoft ددح . 2 ةوطخلا



في حضوره وه امك CA مداخل نم ةرداصل الرذل ةداهشلا ددحو تادادعإل قوف رقنا 3. ةوطخل ةروصل.

Smart Card or other Certificate Properties

When connecting:

Use my smart card

Use a certificate on this computer

Use simple certificate selection (Recommended)

Advanced

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

عمله نم رتوي بمك الة قداصم وأ مدخت سمل ددحو ةمدقتم تادادع| قوف رونا 4. ةوطخلال ةروصلال ي ف حضوم وه امك 802.1x تادادع| بيوبتلال

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

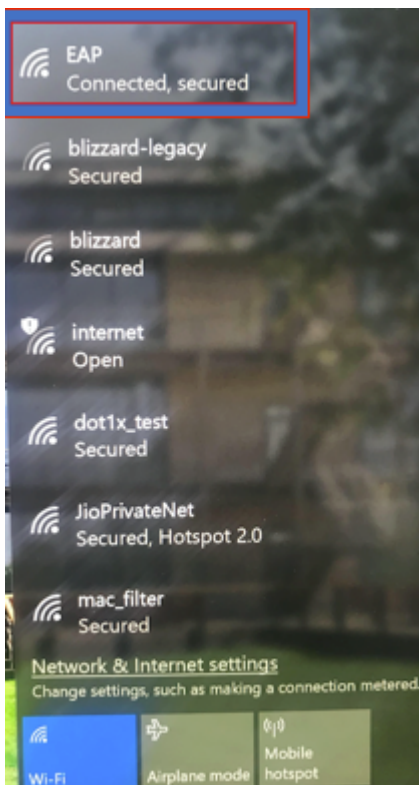
Maximum delay (seconds):

10

Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

حی حاصل فی صورت لادح مة كلساللة كة بشلاب ى رخأ ةرم لى صورت لالوا نآلا 5 ةوطخلال ةروصلال فى حضورم وه امك ةكلساللة كة بشلاب لصورم تنأ لصورم (لالامل اذه فى EAP).



ةحصل ال نم ققحت ال

ححص لكشب نيوكت ال لمع ديكأتل مسقلا اذه مدختسا

لمكأ دق ليمع ال نأ ينعي اذه. RUN ك ليمع ال جهن ري دم ةلا ح رهظت نأ بجي 1. ةوطخال
ةروصلال في ةحضوم ال رورم ال ةكرح ريرمتل زهاج وهو، IP ناو نع لعل لصحو، ةقداصلال

Monitor

Summary

Access Points

Cisco CleanAir

Statistics

CDP

Rogues

Redundancy

Clients

Sleeping Clients

Multicast

Applications

Lync

Local Profiling

Clients > Detail

Max Number of Records 10 Clear AVC Stats

General AVC Statistics

Client Properties

MAC Address 34:02:86:96:2f:b7

IPv4 Address 10.106.32.239

IPv6 Address fe80::2818:15a4:65f9:842,

Client Type Simple IP

User Name Administrator

Port Number 1

Interface management

VLAN ID 32

Quarantine VLAN ID 0

CCX Version CCXv1

E2E Version Not Supported

Mobility Role Local

Mobility Peer IP Address N/A

Mobility Move Count 0

Policy Manager State RUN

Management Frame Protection No

UpTime (Sec) 146

AP Properties

AP Address 00:d7:8f:52:db:a0

AP Name Alpha2802_3rdfloor

AP Type 802.11bn

AP radio slot Id 0

WLAN Profile EAP

WLAN SSID EAP

Data Switching Central

Authentication Central

Status Associated

Association ID 1

802.11 Authentication Open System

Reason Code 1

Status Code 0

CF Pollable Not Implemented

CF Poll Request Not Implemented

Short Preamble Not Implemented

PBCC Not Implemented

Channel Agility Not Implemented

Re-authentication timeout 1682

Remaining Re-authentication timeout 0

WEP State WEP Enable

Lync Properties

Lync State Disabled

Audio Qos Policy Silver

في حملات التشفير، يمكن أن تكون هناك حاجة إلى حل مثل EAP بولس أو نيم اضي أو قحت 2. أو إدخال
 أو وصل في حضوره، وهو يمكن أن يعمل على تصفية (WLC) أو كالتالي.

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Auth Key Mgmt	802.1x
Encryption Cipher	CCMP (AES)
EAP Type	EAP-TLS
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied	Unavailable

صق مت) مكحتللا ةدحوب ةصاخلا رماوألارطس ةهجاو نم ليلعمللا ليلصافات ليل اميف 3. ةوطخلال (جاخلال):

```
(Cisco Controller-Standby) >show client detail 34:02:86:96:2f:b7
Client MAC Address..... 34:02:86:96:2f:b7
Client Username ..... Administrator
AP MAC Address..... 00:d7:8f:52:db:a0
AP Name..... Alpha2802_3rdfloor
AP radio slot Id..... 0
Client State..... Associated
Wireless LAN Id..... 5
Wireless LAN Network Name (SSID)..... EAP
Wireless LAN Profile Name..... EAP
Hotspot (802.11u)..... Not Supported
BSSID..... 00:d7:8f:52:db:a4
Connected For ..... 48 secs
Channel..... 1
IP Address..... 10.106.32.239
Gateway Address..... 10.106.32.1
```

```

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..... EAP-TLS

```

في حضوره وه امك تامس لل > ةياهن لل طاقن > قاي س لل ةيؤر لل ل لقتنا، ISE لى لى 4. ةوطخل ل روص لل

The screenshot displays the Cisco ISE interface for an endpoint with MAC address 34:02:86:96:2F:B7. The endpoint profile is 'Intel-Device' and the current IP address is not shown. The 'Attributes' tab is selected, showing 'General Attributes' and 'Other Attributes'.

General Attributes

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

Custom Attributes

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	5
AllowedProtocolMatchedRule	Dot1X
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	x509_PKI

BYODRegistration	Unknown
Called-Station-ID	00-d7-8f-52-db-a0:EAP
Calling-Station-ID	34-02-86-96-2f-b7
Days to Expiry	363
DestinationIPAddress	10.106.32.31
DestinationPort	1812
DetailedInfo	Invalid username or password specified
Device IP Address	10.106.32.223
Device Port	32775
Device Type	Device Type#All Device Types
DeviceRegistrationStatus	NotRegistered
ElapsedDays	7
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, 1.3.6.1.4.1.311.1
FailureReason	-
IdentityGroup	Profiled
InactiveDays	5
IsThirdPartyDeviceFlow	false
Issuer	CN=fixer-WIN-97Q5HOKP9IG-CA,DC=fixer,DC=c
Issuer - Common Name	fixer-WIN-97Q5HOKP9IG-CA
Issuer - Domain Component	fixer, com

Location	Location#All Locations
MACAddress	34:02:86:96:2F:B7
MatchedPolicy	Intel-Device
MessageCode	5200
NAS-IP-Address	10.106.32.223
NAS-Identifier	HA_Pri
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
Network Device Profile	Cisco
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	HA_Pri
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"
OpenSSLErrorStack	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	AccessRequest
SSID	00-d7-8f-52-db-a0:EAP
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	EAPTLS
SelectedAuthorizationProfiles	PermitAccess
Serial Number	10 29 41 78 00 00 00 00 11...

اه حال صاوا عا طخال فاشك سا

ليكشت اذه ل ىرحتي نا رفوتي ةددم ةمولعم نم ام ايلاح كانه

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل