

ISE و WLC مداخلتساب هنيوكتو EAP-TLS مهف

تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطتم](#)

[تابلطتم](#)

[عمدختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[EAP-TLS قفدت](#)

[EAP-TLS قفدت يف تاوطخ](#)

[ننيوكتل](#)

[Cisco نم ةيكللسال LAN ةكبش يف مكحتل ةدحو](#)

[Cisco WLC عم ISE](#)

[EAP-TLS تادادع](#)

[ISE ىلع WLC تادادع](#)

[ISE ىلع ديدج مدختسم عاشن](#)

[ISE ىلع ةقثل ةداهش](#)

[EAP-TLS ليمع](#)

[\(Windows بتكم حطس\) ليمعلا زاغ ىلع مدختسملا ةداهش ليزنت](#)

[EAP-TLS ل يكللسال فيصوت](#)

[ةحصلل نم ققحتل](#)

[اهجالص او ءاطخأل افاشكتسا](#)

عمدقمل

لوكتورب مداخلتساب (WLAN) ةيكللسال ةيلحم ةكبش دادع ةيفي دننتملا اذه حضوي 802.1X و EAP-TLS عسوتمل ةقداصل

ةيساسأل تابلطتم

تابلطتم

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت

- 802.1X راي عمل اقفو ةقداصل ةيلمع
- تاداهشل

عمدختسمل تانوكمل

ةيلاتل ةيدامل تانوكمل او جماربل تارادصل ىل دننتملا اذه يف ةدراول تامولعمل دننست

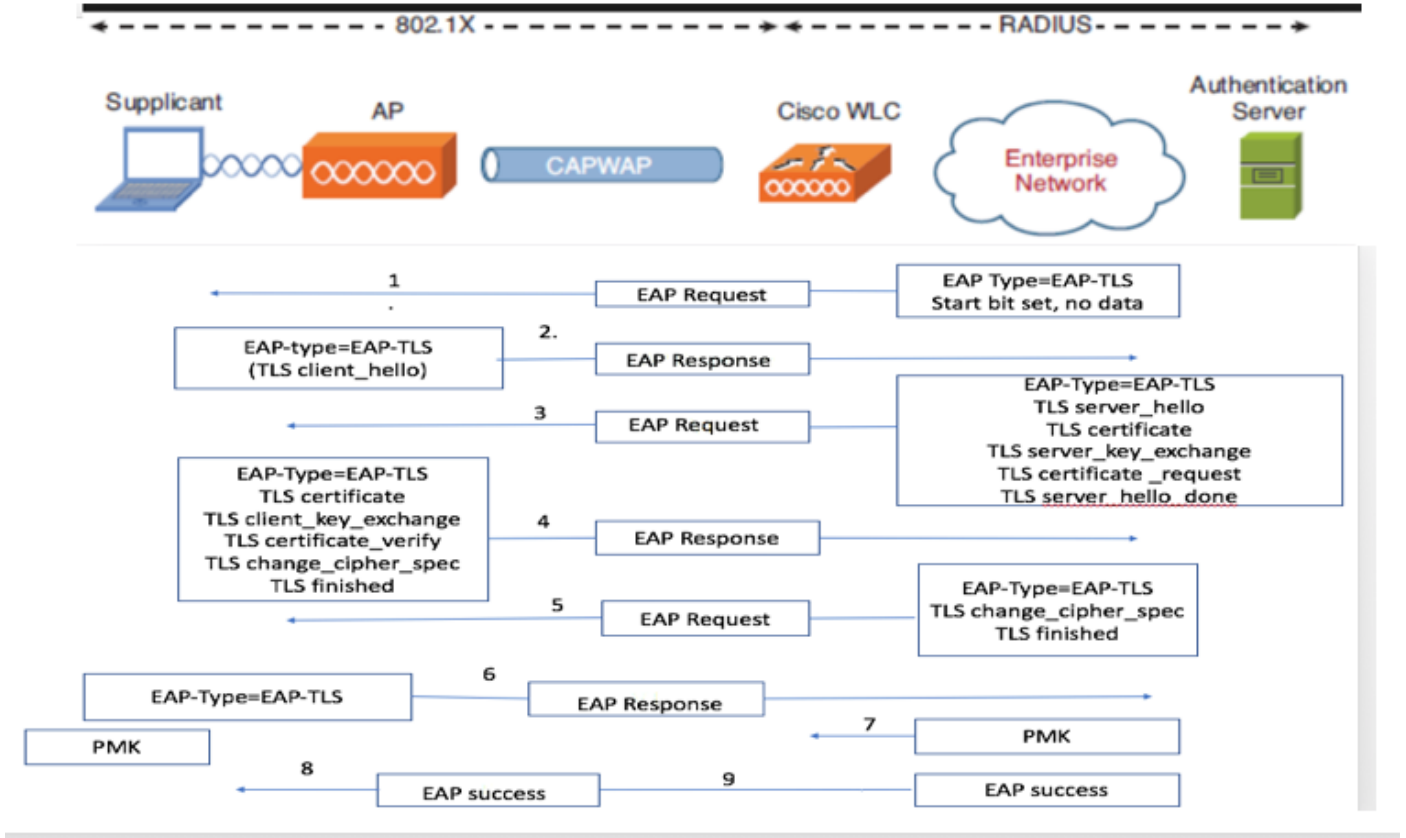
- 8.10 رادصل، WLC 3504

• Identity Services Engine (ISE)، رادصالا 2.7

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسمل اذه يف ةدراولامول عملا عاشن امت تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجالا عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش

ةيساسا تامولعم

قفتد EAP-TLS



قفتد يف تاوطخ EAP-TLS

1. ليمعمل لوصول ةطقن حمست ال (AP) لوصول ةطقن بكي كلساللا ليمعمل طبتري بلطل مدقم بيجتسي مث .ةقداصم بلط لسرتو ةطقنلا هذه دنع تانايب يال لاسراب ةيكلساللا ةيلحمل ةكبشلا يف مكحتل رصنع موقبي .EAP-Response ةيوه ب مداخ بيجتسي .ةقداصملا مداخىل مدختسمل فرعم تامولعم لىصوتب كلذ دعب هذه دنع EAP-TLS ةثدام أدبت .EAP-TLS ةمدب ةمزم مادختساب ىرخأ ةرم لىمعمل RADIUS ةطقنلا .
2. ةلاسرىل عيوتحي يذلا ةقداصملا مداخىل ىرخأ ةرم EAP-Response ريظنلا لسري NULL لىل هنييعت مت ريفشت يهو ،"client_hello" ةحفاصم لىل عيوتحت يتلا Access-challenge ةمزم مادختساب ةقداصملا مداخ بيجتسي .

TLS server_hello
handshake message
certificate
server_key_exchange
certificate request
server_hello_done.

4. ىلع يوتحت يتل EAP-Response 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

ىلع يوتحتي يذلا لوصولو يوتحتل RADIUS مداخل بيجتسي، حاجنب ليمعلا ةقداصم دعب. ةحفاصملا ءاهتناو "change_cipher_spec" ةلاسربلا.

6. RADIUS مداخل ةقداصملا ةئزجتلا نم ليمعلا ققحتي، اذم ملتسي ام دنع.

7. TLS ةحفاصم ءانثا رسلا نم ايكي مانيدي ديدج ريفشت حتفم قاقشتا متي.

8/9. بلابلاب هقاحلا متي مث قداصملا ىلا مداخللا نم اريخا Success لاسربا متي-EAP.

ةكبشلا ىلا لوصولو EAP-TLS معدي يذلا يكلساللا ليمعلا عيظتسي ةلحرمل هذه يفة. ةيكلساللا.

نيوكتلا

Cisco نم ةيكلساللا LAN ةكبش يفة مكلحتلا ةدحو

RADIUS مداخل ةفاضلا Cisco WLC ىلع RADIUS مداخل نيوكت يه ىلوالا ةوطخل. 1. ةوطخل ةروصل يفة حضورم وه امك ديدج رقنا. ةقداصملا > RADIUS > نامالا ىلا لقتنا

The screenshot shows the Cisco WLC Security configuration page for RADIUS Authentication Servers. The left sidebar has a navigation menu with 'Authentication' highlighted. The main content area shows configuration options for 'Auth Called Station ID Type' (set to AP Name:SSID), 'Use AES Key Wrap' (unchecked), 'MAC Delimiter' (set to Colon), and 'Framed MTU' (set to 1300). Below these options is a table of RADIUS servers:

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	138.77.0.84	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2	138.77.0.83	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	3	138.77.97.20	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	4	138.77.97.21	1812	Disabled	Disabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5	172.27.1.71	1812	Disabled	Enabled
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	6	10.100.120.41	1812	Disabled	Enabled

in تلمعتسا نوكتي نأ <password> كرتشملا رسلاو ناو نعللا لخد ي نأ تنأ جاتحي، انه. 2. ةوطخل order to ةروصل يفة حضورم وه امك ةعباتملا قيبطت قوف رقنا. ISE لىلع WLC لىلقتن.

The screenshot shows the 'RADIUS Authentication Servers > Edit' configuration page in the Cisco ISE GUI. The 'Shared Secret' and 'Confirm Shared Secret' fields are highlighted with a red box. The 'Apply' button is also highlighted. The configuration includes fields for Server Index (7), Server Address (10.106.35.67), Shared Secret Format (ASCII), and various other settings like Key Wrap, Network User, and Management.

3. ةوطخلل RADIUS ةقداصم ل WLAN ةكبش ءاشنإ .

ىت ح ،يسسؤم-WPA عضو مادختسال اهنىوكتو ةديج WLAN ةكبش ءاشنإ كنكمي ،نآل ةقداصم ل RADIUS مادختسال اهنكمي .

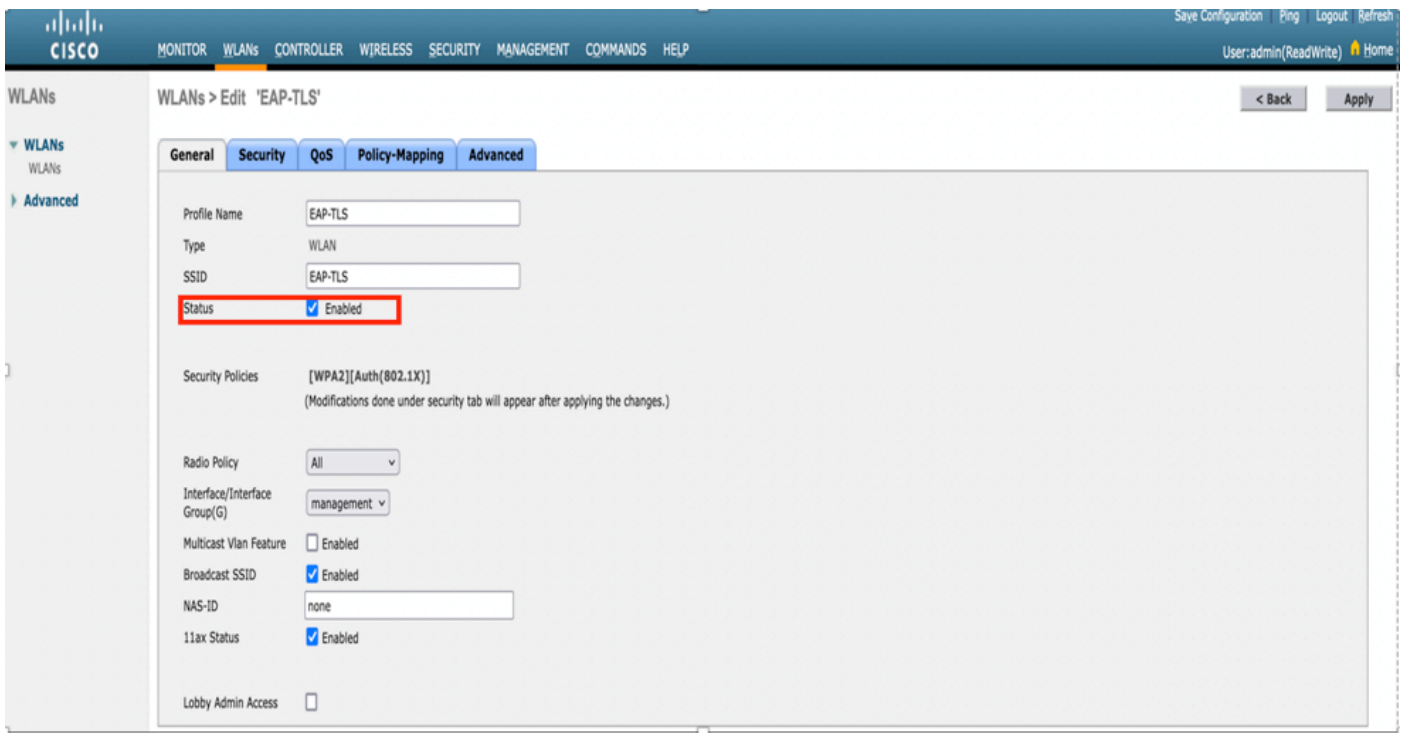
وه امك لاقتنا رقناو ديچ ءاشنإ رتخأ ،ةيسىئرلا ةمئاقلا نم WLAN تاكبش دح . 4 ةوطخلل ةروصلال ي ف حضورم .

The screenshot shows the 'WLANs' configuration page in the Cisco ISE GUI. The 'Create New' button is highlighted with a red box. The page displays a table with columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The 'Current Filter' is set to 'None'.

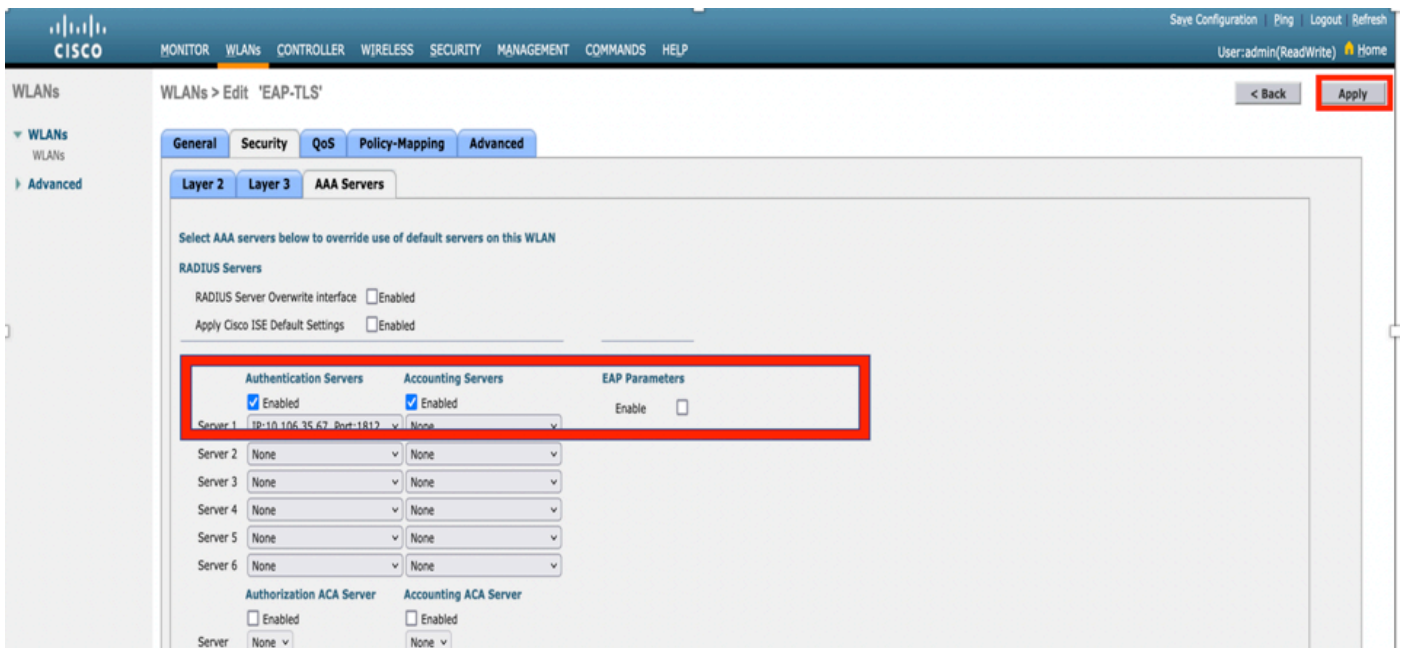
امك ةعباتم ل قىبطت قوف رقنا . WLAN ةكبش ل ديجل ال EAP-TLS ةيمستب مق . 5 ةوطخلل ةروصلال ي ف حضورم وه .

The screenshot shows the 'WLANs > New' configuration page in the Cisco ISE GUI. The 'Apply' button is highlighted with a red box. The configuration includes fields for Type (WLAN), Profile Name (EAP-TLS), SSID (EAP-TLS), and ID (3).

يه ةيضارتفالال نيأتال تاسايس . ةنكمم ةلاجل نأ نم دكأتو ماع ىلع رقنا . 6 ةوطخلل ةروصلال ي ف حضورم وه امك WPA2 و 802.1X ةقداصم .



تمت في ذلك RADIUS مداخل دمج AAA مداخل بيوت التل عمال > نيت التل إلى لقتنا ، نآل 7. ةوطخل ةروصل ال في حضورم وه امك هنيوكت ب.



مكحت ال رصنع نم RADIUS مداخل إلى لوصول ةينام نم ققحت ال لصفأل نم : ةظالم UDP ذف نم RADIUS مداخل لبق (WLC) ةيكل سال ال ةيلحمل ال ةكبش ال في في نام في هذه رورم ال ةكر رطح مدم نم دك التل إلى جاتحت كذل ، (ةقداصل لل) 1812 ةكبش ال.

ISE عم Cisco WLC

إعداد عAP-TLS

انتسايس ي ف اهم ادختساب حومسمل تالوكوتوربل ا عمئاق عاشن ا ل ا جاتحت ، جهنل ا عاشن ا ل
نيوكت ا عي ف ي ك ا ل ع ا ن ب ه ب حومسمل EAP عون ددح ، اهتباتك تم ت dot1x ا سايس ن ا م ب
ا سايس ل .

ر ي غ ا ق د ا ص م ل ل EAP عاون ا م ط ع م ب ح م س ت ك ن ا ف ، ي ض ا ر ت ف ا ل ا د ا د ع ا ل ا م د خ ت س ت ت ن ك ا ذ ا
ن ي ع م EAP عون ا ل ل ا ل و ص و ل ا ن ي م ا ت ا ل ا ع ج ا ب ت ن ك ا ذ ا ا ق ل ص ف م ل ا

حومسمل تالوكوتوربل ا > ا ق د ا ص م ل ا > جئائنا ل ا > جهنل ا رصان ع > Policy ا ل ل ا ل ق ت ن ا . 1 ا و ط خ ل ا
ا ر و ص ل ا ي ف ح ص و م و ه ا م ك ا ق ا ص ا ا ل ع ر ق ن ا ا ه ب

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionary Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allowed Protocols Services

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

Edit Add Duplicate Delete

Service Name	Description
<input type="checkbox"/> Default Network Access	Default Allowed Protocol Service

ا ل ا ح ل ا ه ذ ه ي ف . ا م ا ق ل ا م س ا ل ا خ ا ذ ا ك ن ك م ي ، ا ه ب حومسمل تالوكوتوربل ا عمئاق ي ف . 2 ا و ط خ ل ا
ي ف ح ص و م و ه ا م ك ا ر خ ا ت ا ع ب ر م ا د ي د ح ت ا غ ل ا م ت ي و EAP-TLS ع ب ر م ل ح ا م س ل ا د ي د ح ت م ت ي
ا ر و ص ل ل ا .

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 Hours

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 ىلع WLC تاداعإ

ةفاضإ > ةكبشلا ةزهجأ > ةكبشلا دراوم > ةرادإلا ىلإ لقتناو ISE مكحت ةدحوتف ا. 1 ةوطخلا ةروصلال يف حضوم وه امك

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pCloud Services Feed Service Threat Center 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

Device Security Settings

Name	Profile Name	Location	Type	Description

ةروصلال يف حضوم وه امك ميقلال لاخداپ مق. 2 ةوطخلا

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service 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

Device Security Settings

Network Devices List > New Network Device

Network Devices

* Name

Description

IP Address * IP: /

* 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 یل ع ديدج مدختسم عاشن

يف حضورم وه امك ةفاضل > نيمدختسم > تايوه > ةيول ةراد > ةرادى ل لقتنا 1. ةوطخل ةروصل.

Identity Services Engine Administration Work Centers

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

Users

Network Access Users

Latest Manual Network Scan Results

SEAS	Name	Description	First Name	Last Name	Email Address	User Identity Group	Admin

ةروصل ي ف حضورم وه امك تامولعمل لاخداب مق 2. ةوطخل.

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: bharti

Status: Enabled

Email: [Redacted]

Passwords

Password Type: Internal Users

Password: [Redacted] Re-Enter Password: [Redacted] Generate Password

* Login Password: [Redacted] Re-Enter Password: [Redacted] Generate Password

Enable Password: [Redacted] Generate Password

User Information

First Name: [Redacted]

Last Name: [Redacted]

Account Options

Description: [Redacted]

Change password on next login:

Account Disable Policy

Disable account if date exceeds: 2018-02-17 (yyyy-mm-dd)

User Groups

Select an item [Redacted] - +

Submit Cancel

ISE ىلع ةقثلا ةداهش

اهب قوئوم تاداهش > تاداهشلا ةرادا > تاداهش > ماظن > ةرادا ىلإ لقتنا 1. ةوطخلا

ةكبشلا يف مكحت رصنع ةفاضل درجم ب ISE ىلإ ةداهش داريتسال داريتسإ ىلع رقنا ةيمهأ رثكالل اعزلاب مايقلل كمزلي، ISE ىلع مدختسم عاشنإو (WLC) ةيكلسالل ةيلحملل CSR ديلاوت ىلإ ةجاحب نحن كلذل ISE ىلع ةداهشلا يف ةقثلا وهو EAP-TLS نم

عيقوت تابلط عاشنإ > ةداهشلا عيقوت تابلط > تاداهشلا > ةرادا ىلإ لقتنا 2. ةوطخلا ةروصلال يف حضوم وه امك (CSR) ةداهشلا

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

اهم ادخات سإ متي (تاداهش ل) ةداهش ل نمو ادخات سإ ل لقتنا CSR ءاشن ل 3. ةوطخ ل ةروصل ل ي حضورم وه امك EAP ةقداصم دح ةلدسنم ل تارايخلل

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

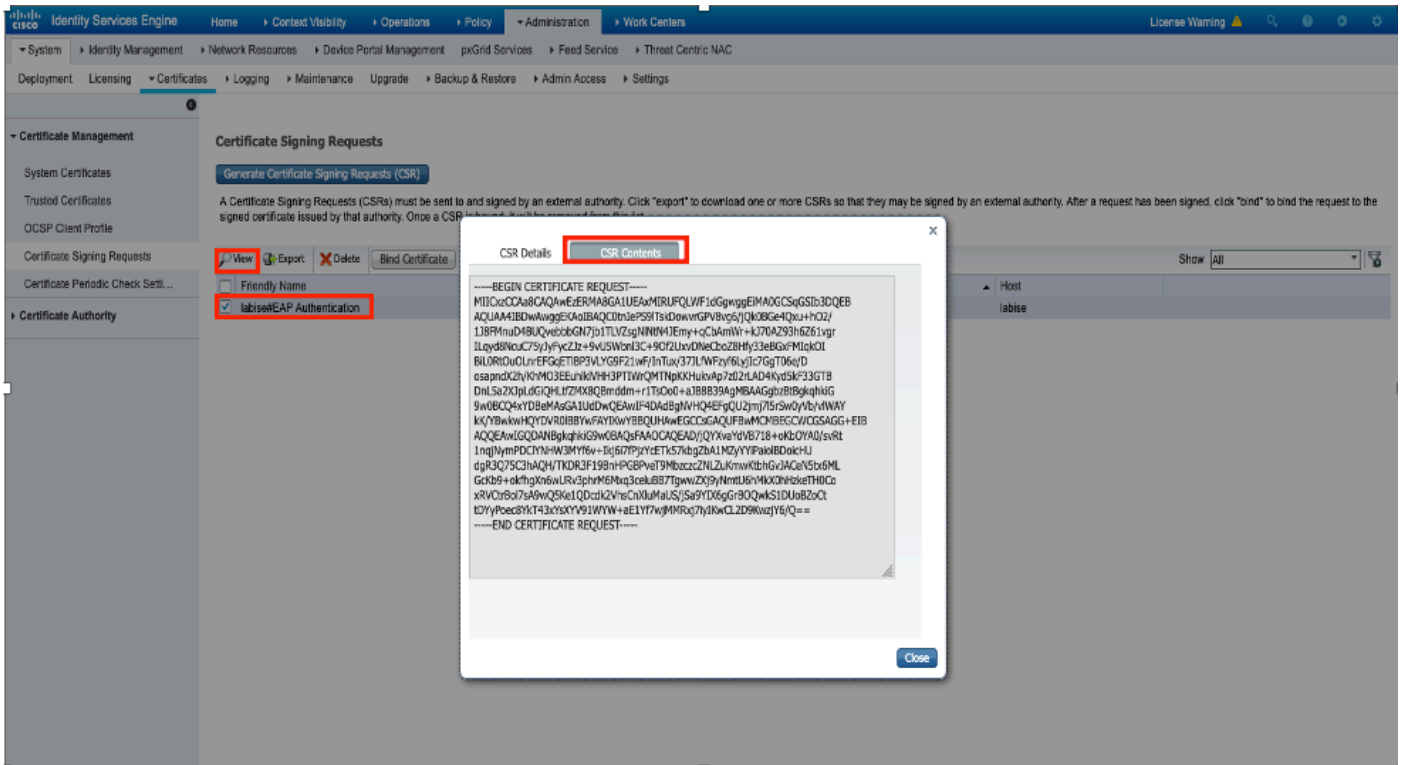
Allow Wildcard Certificates:

Node(s)

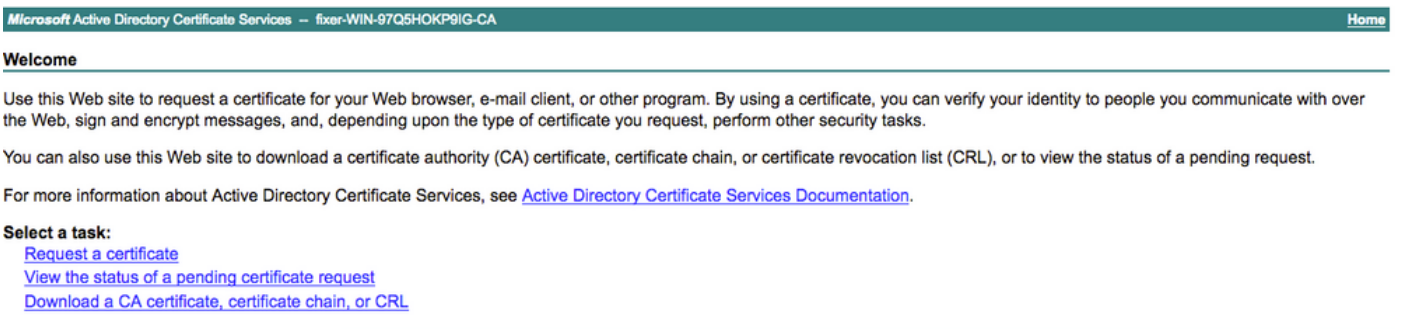
Generate CSR's for these Nodes:

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

ي حضورم وه امك ضرع قوف رقنا ISE. ل ع هؤاشن إ مت يذل CSR ضرع نكمي 4. ةوطخ ل ةروصل ل.



يف حضورم وه امك ةداهش بلط قوف رقناو CA مداخل لى حفصت، CSR ءاشن ا درجم ب. 5 ةوطخلال ةروصلال:



مدقتم ةداهش بلطو مدختسمل ةداهشل تاراخي لى لصرحت، ةداهش بلط نأ درجم ب. 6 ةوطخلال ةروصلال يف حضورم وه امك مدقتم ةداهش بلط لى رقنا.

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

Request a Certificate

Select the certificate type:

[User Certificate](#)

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

بلاق نم. Base-64 ل ةزمرملا ةداهشل بلط يف هؤاشن ا مت يذلا CSR قصلال. 7 ةوطخلال يف حضورم وه امك لاسر قوف رقناو بيول مداخل رتخأ، ةلدسنملا ةمئال ل راخي: ةداهشل ةروصلال.

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 قوٹوملا تاداهشلا عمئاق ىلإ ةداهشلا ةفاضل متت ، لاسرا قوف رقنلا درجمب 10 ةوطخل ابروصلا يف حضورم وه امك CSR عم طبرلل ةطيسولا ةداهشلا مزلي ، اضيا

Identity Services Engine 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

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

طوفحمل صيخرتل فلم رايتخال رايخ كانه ، طبرلل صيخرت ىلع رقنلا درجمب 11 ةوطخل ابروصلا يف حضورم وه امك ميلست رقناو ةطيسولا ةداهشلا ىلإ حفصت . كبتكم حطس ىلع

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

يف حضورم وه امك ماظنلا تاداهش > تاداهش > ةرادل ىلإ لقتنا ، ةداهشلا ضرعل 12 ةوطخل ابروصلا

System Certificates	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 (1)	ise.c.com	fixer-WIN-97Q5HOKP9IG-CA	Fri, 13 Jul 2018	Sun, 12 Jul 2020

عملي EAP-TLS

Windows (بتم حطس) ليمعلا زاهج لى عمختمسلا ةداهش ليزنت

مق. ليمع ةداهش عاشن إكي لى بجي، EAP-TLS لالخ نم يكلسال مخرتمس ةقداصل م. 1 ةوطخل احتفا. مداخل لى لوصولو نم نكمتت ىتح ةكبشلاب Windows رتوي بمك لى صوتب ناونعلا اذه لخدأو بيوضرعتسم: <https://severipaddr/certsrv>

ل ةداهشلا ليزنت هب مت يذلا هسفن وه قدصملا عجرملا نوكي نأ بجي هنا طحال 2. ةوطخل ISE.

في مداخل ةداهشلا ليزنتل هتمخرتسأ يذلا CA مداخل سفن ضارعتسال جاتحت ببسلا اذه لى جاتحت ةرملا هذه ك لدمو، اقبس ممت امك ةداهش بلط قوف رقنا، هسفن قدصملا عجرملا ةروصل ي فضوم وه امك ةداهش بلقك مخرتمس ديدحت.

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

لومح رتويبمك نم ةداهشال داريتسال ةيلاتال تاوطخل عبتا ،تاداهشال يلع لوصحل درجمب
Windows ليغشتال ماظنب لمعي:

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

1. MMC > ليغشت > ادبا ال MMC ةكرححت فل .
2. باذجنا ةلازا / ةفاضل > فلم ال لقتنا .
3. تاداهش ال ع اجودزم ارقن رقنا .
4. SelectComputer باسح .
5. اهان |> ليح م رتويبمك دي دحت .
6. ةذفان ةيفاضال ةادال تحرخ ok in order to ةق طقط .
7. تاداهشال > ي صخش > تاداهشال راوجب [+] قوف رقنا .
8. داريتسال > ماهم لك دحو تاداهشال ال ع نميال سوامل رزب رقنا .
9. (يلاتال) Next قوف رقنا .
10. ضارعتسال ال ع رقنا .
11. هداريتسال ديرت يذال .cer و .crt و .pfx . دح .

12. حتف قوف رقنا .

13. (يلاال) Next قوف رقنا .

14. ةداهشلا عون ىلع ءانب ايئاقلت تاداهشلا نزخم ديدحت ددح .

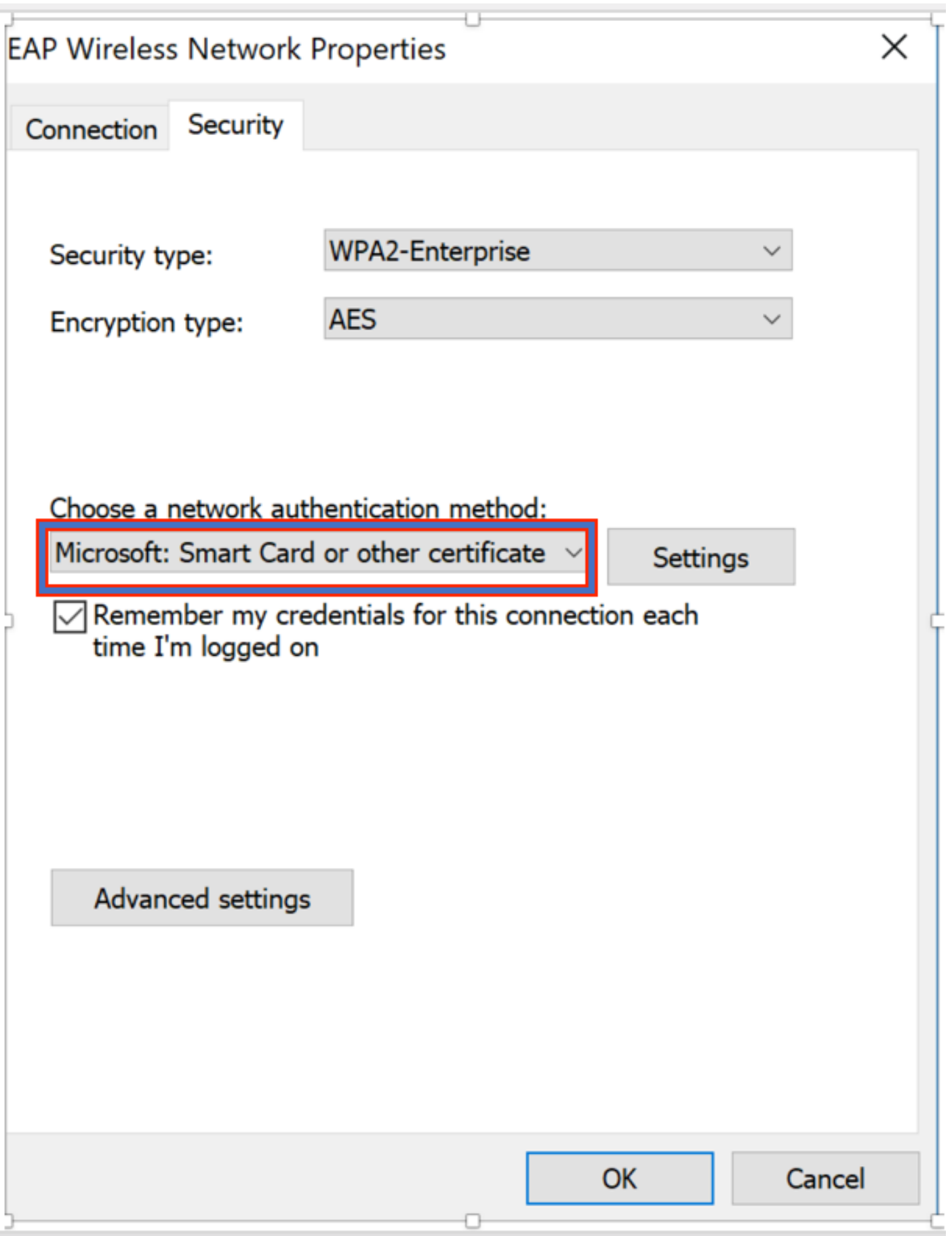
15. ok وزاجن ةقطقط .

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

EAP-TLS ل يكلسال في صوت

ةقداصملا لوكوتوربل اقباس هؤاشنإ مت يذلا يكلساللا في صوتلا ريغبتب مق 1. ةوطخللا
EAP في صوت ىلع رقنا . كلذ نم ال دب EAP-TLS مادختسال (PEAP) يمحمللا عسوتملا
يكلساللا .

يف ضرعم قفاوم ىلع رقنا وىرخأ ةداهش يأ وأ ةيكذلا ةقابطلا : Microsoft ددح 2. ةوطخللا
ةروصللا .



وه امك قدصم الم عجرم الم مداخ نم ةرداصل الم رذجل ةداهش الم ددحو تادادع الم الى ع رقنا 3. ةوطخل الم ةروصل الم يف حضورم.

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

ةمالة نم رتوي بمكلا وأ مدخت سمل اة قداصم ددحو ةمدقتم تاداع| قوف رقنا 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

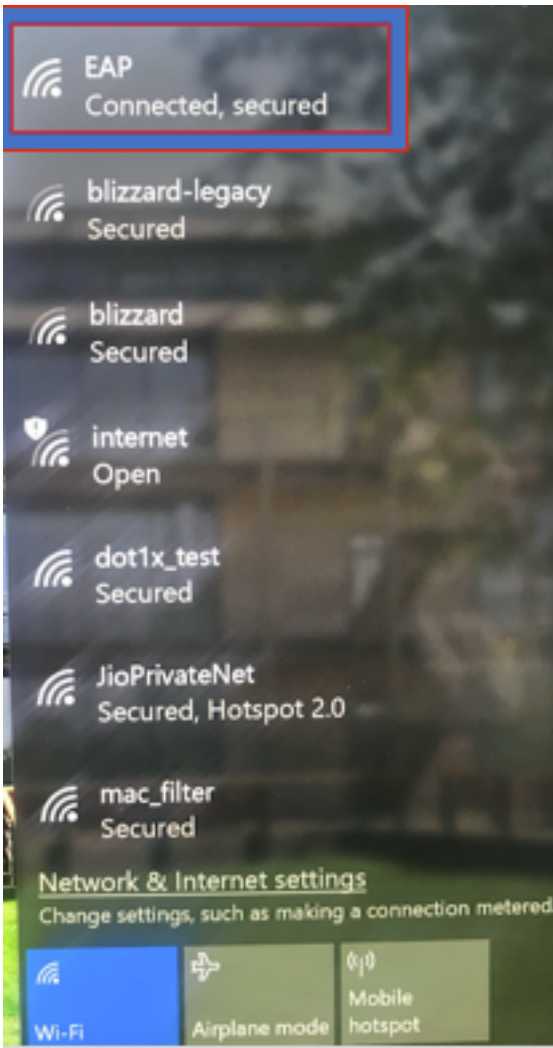
Maximum delay (seconds):

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 ر خ أ ة ر م ل ي صوت ل ل و ا ح ن آ ل 5 ة و ط خ ل ا
ي 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 أ . ل ي ص و ت م ث (ل ا ث م ل ا ذ ه ي ف EAP)
ة ر و ص ل ل ا .



ةحصلال ن م ققحتال

ححص لكشب نيوكتال لمع ديكأتل مسقلا اذه مدختسا

لمكأ دق ليمعلا نأ ينعي اذه. **RUN** اهانأ ىلع ليمعلا جهن ريديم ةلاح رهظت نأ بجي. 1 ةوطخلا ةروصلال يف ةحصولال رورمال ةكرح ريرمتل زهاج وهو IP ناوع ىلع لصحو ةقداصلال

Monitor

Clients > Detail

Max Number of Records Clear AVC Stats

General **AVC Statistics**

Client Properties		AP Properties	
MAC Address	34:02:86:96:2f:b7	AP Address	00:d7:8f:52:db:a0
IPv4 Address	10.106.32.239	AP Name	Alpha2802_3rdfloor
IPv6 Address	fe80::2818:15a4:65f9:842,	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
Client Type	Simple IP	Reason Code	1
User Name	Administrator	Status Code	0
Port Number	1	CF Pollable	Not Implemented
Interface	management	CF Poll Request	Not Implemented
VLAN ID	32	Short Preamble	Not Implemented
Quarantine VLAN ID	0	PBCC	Not Implemented
CCX Version	CCXv1	Channel Agility	Not Implemented
E2E Version	Not Supported	Re-authentication timeout	1682
Mobility Role	Local	Remaining Re-authentication timeout	0
Mobility Peer IP Address	N/A	WEP State	WEP Enable
Mobility Move Count	0		
Policy Manager State	RUN		
Management Frame Protection	No		
UpTime (Sec)	146		

Lync Properties

Lync State	Disabled
Audio Qos Policy	Silver

وهو امك ليمعلا ليرصافات ءحفص في WLC لى ع EAP بولسأ ءحص نم اضيأ ققحت 2. ءوطخلا ءروصلال في ءضوم.

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 م (م كحت ل ا ءءول (CLI) رم او ا ل رطس ءه ءو نم ل لم عل ا ل ص ا ف ت ي ل ي ام ي ف 3. ءو طء ل ا (ء ا رء ا ل):

```
(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

حضوره امك تامسلا > ةياهنلا طاقن > قاي سلا ةيؤر ةيناكمإ لىل لقتنا، ISE لىل 4. ةوطخلل روصلا يف

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Endpoints Network Devices

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	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...

اهحالص او ءاطخ ال فاشكتسا

ليكشت اذه ل ىرحتي نأ 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 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