

لوصول طاقنل 802.1X لومم نيوكتب مق 9800 مكحتلا ةدحو مادختساب

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[تابلطلتلا](#)

[ةمدختسملاب تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتلا](#)

[ةكبشلالل طيخطلا مسرلا](#)

[802.1x ستملك Lightweight عضولا يف لوصول طاقنل نيوكت](#)

[ةيلحمللا ةكبشلالل يف مكحتلا ةدحو لعلاب ةلصت لوصول طاقنل تانك اذا
\(WLC\) ةيكلساللا](#)

[ةيكلساللا ةيلحمللا ةكبشلالل يف مكحتلا رصنع لوصول طاقنل مضنت مل اذا
\(WLC\) دعوب](#)

[لوحمللا نيوكت](#)

[ISE مداخ نيوكت](#)

[ةحصللا نم ققحتلا](#)

[ةقداصملا عون نم ققحتلا](#)

[انيمجات فملا لعل 802.1x تققد](#)

[اهجالص او عاخذاللا فاشكتسا](#)

[عجارملا](#)

ةمدقملا

م تي ل 802.1x بلط اهنأ لعل Cisco نم (AP) لوصول طاقنل نيوكت ةيفيكي دننتمسمل اذ ه فصي
RADIUS مداخ لباقم switchport ذفنم لعل اهليوخت

ةيساسالاب لطلتلا

تابلطلتلا

ةيللالل عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- عضولا يف لوصول طاقنل و (WLC) ةيكلسالل LAN ةكبشلالل يف مكحتلا ةدحو
Lightweight (LAP).
- ISE و Cisco تالوحم لعل 802.1x
- (EAP) عسوتملا ةقداصملا لوكوتورب
- (RADIUS) ديعلل مدختسمللا لاصلتا بلط ةقداصم ةمدخ

ةمدختسمل اتانوكملا

ةيلالتلة ةيدامل اتانوكملا وجماربل اتارادصلإ لىل دننتسمل اذله ف ةدراول تامولعمل دننتست:

- WS-C3560CX، Cisco IOS® XE، 15.2(3r)E2
- C9800-CL-K9، Cisco IOS® XE، 17.6.5
- ISE 3.0
- |ري-CAP3702
- Air-AP3802

ةصاخ ةيلعمل ةئيب ف ةدووملا ةزهجال نم دننتسمل اذله ف ةدراول تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دننتسمل اذله ف ةمدختسمل ةزهجال عيمج تادب رملأ لمتحمل ريثأتلل كمهف نم دكأتف، ليعشتلل ديقتك تكبش

ةيساسأ تامولعمل

لوحمل ةطساوب اهتقداصم تمت و802.1x مقلمك (AP) لوصول ةطقن لمعت، دادعإل اذله ف EAP-FAST بولسأ مادختساب ISE لباقم.

802.1X ريغ رورم ةكره يأ حمسي ال حاتفملا، 802.1X ةقداصم لنوكي ءانيمل تللكش نإ ام حاجنب قداصي ءانيمل لىل طبري ةادال نأ لىل ءانيمل ربع رمي نأ رورم ةكره.

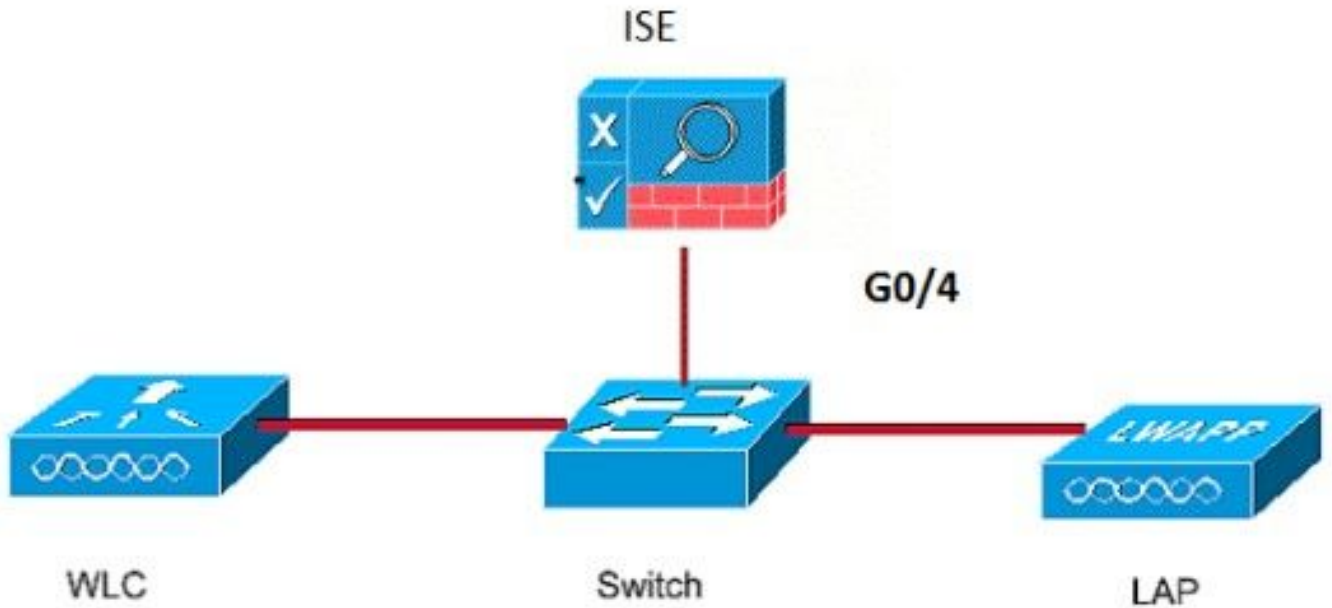
ةيلحمل ةكبشلل ف مكحت ةدحو لىل اهمامضنا لبق ام لوصول ةطقن ةقداصم نكمي ةيكلساللة ةيلحمل ةكبشلل ف مكحت ةدحو لىل اهمامضنا دعب وأ (WLC) ةيكلساللة لىل (LAP) لوصول ةطقن مامضنا دعب لوحمل لىل 802.1X نيوكتب مق، ةلاجل هذه ف (WLC)، (WLC) ةيكلساللة ةيلحمل ةكبشلل ف مكحتل ةدحو.

نيوكتلا

دننتسمل اذله ف ةحصولملا تازيمل نيوكت تامولعمل كل مّدقّت، مسقلا اذله ف.

ةكبشلل يطيختل مسرل

يلالتلة ةكبشلل دادعإ دننتسمل اذله مدختسي:



802.1x سم تلمك Lightweight عضو لوف لوصول طاقن نيوك

ةيكلساللة لةلحملة ةكبشلا فم كحتلة ةدوب لةفلا ةلصتم لوصول ةطقن تناك اذا (WLC):

(LSC): ةلحملة ةمهألا تاذ ةداهشلل AP ةقداصم عونو 802.1x ةقداصم عون نيوك تب مق

فيعرت فلم ةحفص في > AP طبر > اتافي صوتو تامال > نيوك تىل لقتنا 1. ةوطخلا ريرحت وأ ديدج طبر فيعرت فلم ةفاضل ةفاضل لىل رقنا، AP لوصول ةطقن لىل مامضنالا همسا قوف رقتن امدنع لوصول ةطقن طابترا فيعرت فلم

The screenshot shows the configuration page for AP Join profiles on a Cisco Catalyst 9800-CL Wireless Controller. The page title is 'Cisco Catalyst 9800-CL Wireless Controller 17.5.1'. The breadcrumb navigation is 'Configuration > Tags & Profiles > AP Join'. There are '+ Add' and 'X Delete' buttons. A table lists the AP Join Profile Names and their descriptions:

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing '1' items per page and a dropdown menu set to '10' items per page.

لىل لقتنا، ماع > AP نم، لوصول ةطقن لىل مامضنالا فيعرت فلم ةحفص في 2. ةوطخلا EAP-FAST لثم EAP عون رتخأ EAP عون ةلدسنملا ةمئاقلا نم. AP EAP ةقداصم نيوك تمسق ةقداصملا عون وه EAP-FAST. EAP-FAST ةقداصم عون نيوك تل EAP-PEAP وأ EAP-TLS وأ EAP-FAST

بطلطتي .دادعإلل لهسألا وهو طقف رورملا تاملكو مدختسملا مسا مدختسي يذلا ديحول
 م سق عجار) LSC لمع ريس لال خ نم لوصولا طاقن ىلع تاداهش ريفوت كنم EAP-TLS و PEAP
 (عجارملا).

Edit AP Join Profile
✕

General

Client

CAPWAP

AP

Management

Security

ICap

QoS

General

Hyperlocation

Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type Unknown

Injector Switch MAC 00:00:00:00:00:00

Client Statistics Reporting Interval

5 GHz (sec) 90

2.4 GHz (sec) 90

AP EAP Auth Configuration

EAP Type EAP-FAST

AP Authorization Type

EAP-FAST

EAP-FAST

EAP-TLS

EAP-PEAP

Extended Module

Enable

Mesh

Profile Name mesh-profile Clear

Cancel

↩ Update & Apply to Device

CAPWAP اما عونلا رتخأ ، لوصولا ةطقن ضيوفت عون ةلدسنملا ةمئاقلا نم 3. ةوطخل
 زاهجلا ىلع قيبطتو شي دحت قوف رقنا > CAPWAP DTLS و DTLS+.

Edit AP Join Profile

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type Unknown

Injector Switch MAC 00:00:00:00:00:00

AP EAP Auth Configuration

EAP Type EAP-FAST

AP Authorization Type CAPWAP DTLS

- CAPWAP DTLS + DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

Client Statistics Reporting Interval

5 GHz (sec) 90

2.4 GHz (sec) 90

Extended Module

Enable

Mesh

Profile Name mesh-profile [Clear](#)

Cancel Update & Apply to Device

ةم لك و 802.1x username لآ تل لك ش:

رتخأ > رورم لآ ةم لك لآ صاف ت و مدخت س م لآ م س ا Dot1x لآ خ دأ > دام ت ع لآ ا ت ا ن ا ي ب > ة ر ا د ا ن م 1. ة و ط خ لآ ز ا ه ج لآ ل ع ق ي ب ط ت و ش ي د ح ت ق و ف ر ق ن ا > ب س ا ن م لآ 802.1x رورم لآ ةم لك ع و ن

Edit AP Join Profile

General Client CAPWAP AP Management Security ICap QoS

Device User Credentials CDP Interface

Dot1x Credentials

Dot1x Username

Dot1x Password

Dot1x Password Type

Cancel Update & Apply to Device

WLC) ةيكلسلاللا ةيلحمالا ةكبشلا يف مكحتلا رصنع ىلإ لوصولا ةطقن مضمنت مل اذا
دعب:

رطس ةهجاو رماو امدختساو دامتعالا تانايب نييعتل (LAP) لوصولا ةطقن يف مكحت ةدحو
Cisco IOS® APs و Cheetah ليغشتلا ماظنل): ةيلاتلا (CLI) رماوالا

CLI:

<#root>

LAP#

```
debug capwap console cli
```

LAP#

```
capwap ap dot1x username <username> password <password>
```

(رمال مزلا اذا) لوصول ةطقن لىل ع dot1x دامت عا تانايب حسم ل

لوصول ةطقن لىل محت ةداع اى مق ، كلذ دعب ، Cisco IOS® APs لوصول طاقنل

CLI:

```
<#root>
```

```
LAP#
```

```
clear capwap ap dot1x
```

لوصول ةطقن لىل محت ةداع اى مق ، كلذ دعب ، Cisco CoS نم لوصول طاقنل

CLI:

```
<#root>
```

```
LAP#
```

```
capwap ap dot1x disable
```

لوحمل نى وكت

لوحمل لىل ISE م داخ فضا اوماع لكشب لوحمل لىل ع dot1x نى كمتب مق

CLI:

```
<#root>
```

```
Enable
```

```
Configure terminal
```

```
aaa new-model
```

```
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
```

```
dot1x system-auth-control
```

```
Radius-server host <ISE IP address> auth-port <port> acct-port <port>
```

key 7 <server key>

AP لوجم ذفنم نيوكتب مق

CLI:

<#root>

```
configure terminal
```

```
interface GigabitEthernet</>
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```


```
end
```

نوكي نأ يفاضا لليكشت كلذ دع ب، يلجم ليوحت، بولسأ ليوحت Flex يف ap ل نوكي نأ
نوبزلا نأ امب، اعانيم لىل ع {upper}mac address ددعتي حمسي نأ نراق حاتم لىل ع تلجج
: يوتسم ap لىل ع تقلطأ نوكي رورم ةكرح

<#root>

```
authentication host-mode multi-host
```

يتل داوملل عجارم وأ ةديفم تاجارتقا لىل ع تاظحالمل يوتحت. ظحال يئراق ل نأ ينع: ةظحال
ال دنتسم لاهي طغي ال

 حمسي م ث لوأل MAC ناونع ةقداصمب ةددعتمل ةفيضم ل ةزهجال عضو موقوي: ةظحال
لوجم ل ذفانم لىل ع فيضم ل عضو نيكمتب مق. لىل MAC نيوانع نم دودحم ريغ ددعب
حمسي وه. يلجم ل ليوحت ل عضو مادختساب ةلصتم ل لوصول ةطقن نيوكتب م اذا
نيكمتب مق ف، نم رورم ةكرح راسم ديتر تنك اذا. اعانيم حاتم ل رمي رورم ةكرح نوبزلا
ل لىل ع تانايب ةيامحل (WLAN) ةيكل لىل ةيلجم ل ةكبش ل لىل ع dot1x

ISE مداخل نيوكتب

> ةكبش ل دراوم > ةراد لىل لقتنا. ISE مداخل لىل ع ةكبش زاهجك لوجم ل ةفاضاب مق. 1. ةوطخل
ةقداصم تادادع ل نيكمتب، IP ناونع، زاهج ل مسا ل اخلد > ةفاضاب قوف رقنا > ةكبش ل زهجا
ل اسرا > (ةيضارتفا ةمي قك هكرت وأ) COA ذفنم، ةكرتشم ةيرس ةمي ق ددح، RADIUS.

Cisco ISE Administration - Network Resources

Network Devices

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

Network Devices List > New Network Device

Network Devices

* Name MySwitch

Description

IP Address * IP: 10.48.39.100 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

Device Type All Device Types Set To Default

RADIUS Authentication Settings

RADIUS LDP Settings

Protocol RADIUS

* Shared Secret Show

Use Second Shared Secret Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls

> يوهلا ةرادا > ةرادا ىل لقتنا. ISE ىل لوصول ةطقن دامتعا تانايب ةفاضلا 2 ةوطخلا
يتل دامتعالا تانايب لخدأ. مدختسم ةفاضلا ةفاضلا رزلا قوف رقنا ونى مدختسم > تايوه
ةكبشلا يف مكحتلا رصنع ىلع لوصول ةطقن مامضنا فيرعت فلم ىلع اهنيوكتب تمق
، انه ةيضارتفالا ةومجملا يف مدختسملا عضو متي هنا طحال (WLC) ةيكلساللا ةيلحمل
كتابلطتملاقف واذه طبض نكمي نكلو.

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

Network Access User

Name dot1x

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

Login Password

Generate Password

Enable Password

User Information

Account Options

Account Disable Policy

User Groups

ALL_ACCOUNTS (default)

> جهنلا ىل لقتنا .ليوختلا جهنو ةقداصملا ةسايس نيوكتب مق ،ISE في 3 ةوطخلا هذه في .نيميلا ىلع دوجوملا قرزالا مهسلاو نيوكتلل جهنلا ةعومجم ددوج جهنلا تاومجم .تابلطملل اقفو اهصي صخت نكمي نكلو ةيضارتفالا جهنلا ةعومجم مادختسا متي ،ةلاجالا

Cisco ISE Policy - Policy Sets

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	6		

Reset Save

تاسايسلا يه انه ةحضوملا تاسايسلا .ليوختلا جهنو ةقداصملا جهن نيوكتب مق مثاقفو اهصي صختو اهفييكت نكمي نكلو ISE مداخ ىلع اهؤاشن متي ةيضارتفالا .كتابلطمل

مدختسملا ناكو ةيكللس 802.1X مادختسا مت اذا: "ىل نيوكتللا ةمجت نكمي ،لاثملا اذه في ةقداصملا تحجن نيذلا نيمدختسملا ىل لوصولاب حمسن اننإف ،ISE مداخ ىلع افورعم ISE مداخ لوصولو ةطقن ليوخت كلذ دعب متي . "مهل ةبسنلاب

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	⚙️
✓	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy (12)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	Select from list	6	⚙️
✓	Default		DenyAccess x	Select from list	0	⚙️

ريصقت يتي ال اهب حومس مل تالوكوت وربل اي ف EAP-FAST ب حامس ل نم دكأت 4. ةوطخل
 > جئاتن ل > ةقداصل ل > ةسايس ل رصانع > ةسايس ل ل لقتنا . ةكبش ل ل لوصول
 EAP-TLS ب حامس ل نيكم ت > ةكبش ل ل ل يضا رتفال لوصول > اهب حومس مل تالوكوت وربل
 ظفح > TLS

Cisco ISE Policy · Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

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

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

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

ةحصل ل نم ققحت ل

حیحص لكش ب نيوكتل لمع ديكأتل مسقلا اذه مدختسا

ةقداصملا عون نم ققحتلا

AP: فيصوتل ةقداصملا تامولعم show رمألا ضرعي

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

لائم:

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE    : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

ءانيم حاتفملا ىلع 802.1x تقود

لوحمللا ذفنم ىلع 802.1x ةقداصملا ةلاح show رمألا ضرعي

CLI:

```
Switch# show dot1x all
```

جارخإلا ىلع لائم:

```
Sysauthcontrol      Enabled
Dot1x Protocol Version 3

Dot1x Info for GigabitEthernet0/8
-----
PAE                  = AUTHENTICATOR
QuietPeriod          = 60
ServerTimeout        = 0
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30
```

هتقداصم مدع وأ ذفنم لة قداصم نم ققحتل

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

جارجال لىل لاثم:

```
Dot1x Info for GigabitEthernet0/8
```

```
-----  
PAE = AUTHENTICATOR  
QuietPeriod = 60  
ServerTimeout = 0  
SuppTimeout = 30  
ReAuthMax = 2  
MaxReq = 2  
TxPeriod = 30
```

```
Dot1x Authenticator Client List
```

```
-----  
EAP Method = FAST  
Supplicant = f4db.e67e.dd16  
Session ID = 0A30279E00000BB7411A6BC4  
Auth SM State = AUTHENTICATED  
Auth BEND SM State = IDLE  
ED  
Auth BEND SM State = IDLE
```

رم أوأا لرس ةهجاو نم:

```
Switch#show authentication sessions
```

جارجال لىل لاثم:

```
Interface MAC Address Method Domain Status Fg Session ID  
Gi0/8 f4db.e67e.dd16 dot1x DATA Auth 0A30279E00000BB7411A6BC4
```

ليوختل فيصوت عفدو قداصم لاجن نم دكأتو RADIUS فاوح > تاي لمع رتخأ، ISE في
جحصلل.

Cisco ISE Operations - RADIUS

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 1 Client Stopped Responding 0 Repeat Counter 0

Refresh Never Show Latest 20 records Within Last 3 hours

Refresh Reset Repeat Counts Export To Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	✓	🔍		dot1x	A4-53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	Authorization Profiles	IP Address	Network Devi...	FastEther
Nov 28, 2022 08:33:34.4...	✓	🔍		dot1x	A4-53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess		nschyns-SW...	FastEther

اهحال صاوا ءاطخاا فاشكتسا

اهحال صاوا نيوكتلا ءاطخا فاشكتسالا اهمادختسا كنكمي تامولعم مسقلا اذ رفوي

1. لوحملا نم ISE مداخ ىلا لوصولا ءيناكما نم ققحتلا ping رمالا لخدأ.
2. ISE مداخ ىلع AAA لي معك لوحملا نيوكت نم دكأت.
3. لدان ISE لا وحاتفملا ني بسفن لا رسك راشي لا نأ تنمض.
4. ISE مداخ ىلع EAP-FAST ني كمت نم ققحت.
5. Lightweight عضو لا يف لوصولا ءطقنل 802.1x دامتعا تانايب نيوكت مت اذا امم ققحت. ISE مداخ ىلع اهسفن يه تناك اذا امم ققحت (LAP).
6. ءااا ءلاجل ناسسحتم رورملا ءملاك و مدختسملا مسا: ءاطخالم ءيوه ءحص debug dot1x و debug: حاتفملا ىلع رما اذ تلخد، ءيوه ءحص لشفي نا.

و 1.1 رادصاا TLS معدت ال Cisco IOS (802.11ac wave 1) ىلا ءدننتملا لوصولا طاقن نا ااطخال ل طقف حامسلا ل RADIUS و ISE مداخ نيوكت مت اذا ءلكشم ثودح يف لك لبستى دق 1.2 TLS 802.1X ءقاصم لخد.

ءجارملا

[EAP-TLS و PEAP مادختساب لوصولا طاقن ىلع 802.1X نيوكت](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل 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 ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه 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