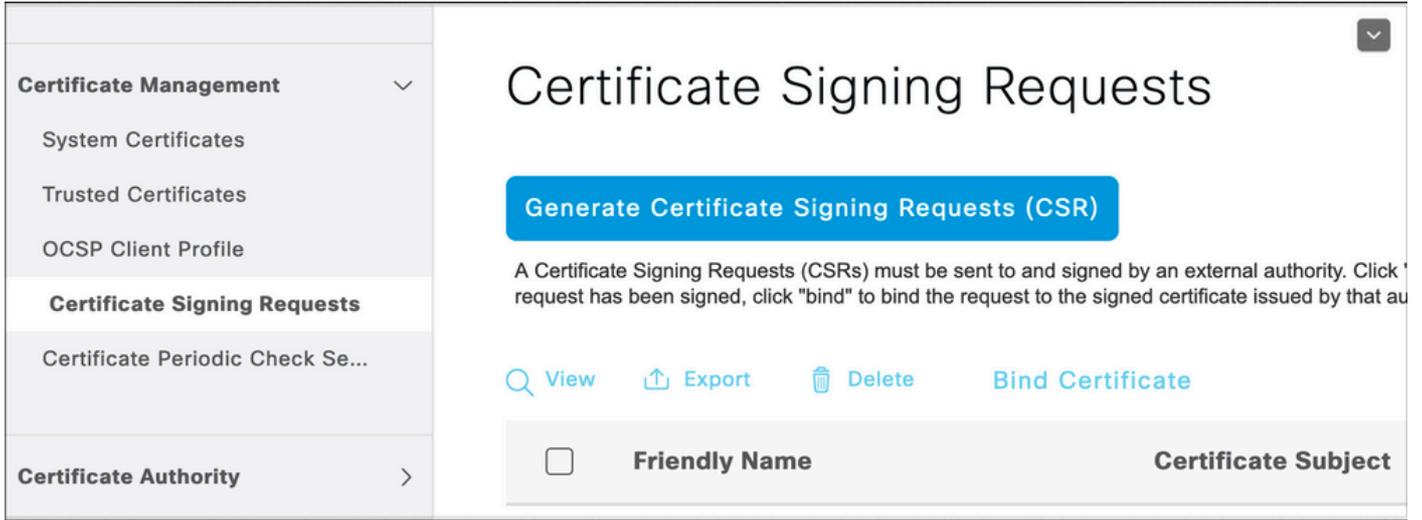


و pxGrid).

نيوكتلا

ءاداهشلا عيقوت تابلط ءاشنإ 1. ةوطخلل

ءاشنإ قوف رقناو ءاداهشلا عيقوت تابلط > ءاداهش > ةرادإلا ىلإ لقتنا، CSR ءاشنإل
(CSR) ءاداهشلا عيقوت تابلط.



The screenshot shows the 'Certificate Management' interface. On the left is a navigation menu with options: 'Certificate Management', 'System Certificates', 'Trusted Certificates', 'OCSP Client Profile', 'Certificate Signing Requests' (highlighted), 'Certificate Periodic Check Se...', and 'Certificate Authority'. The main content area is titled 'Certificate Signing Requests' and features a blue button labeled 'Generate Certificate Signing Requests (CSR)'. Below the button is a note: 'A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click 'request' has been signed, click "bind" to bind the request to the signed certificate issued by that au'. There are four action buttons: 'View', 'Export', 'Delete', and 'Bind Certificate'. At the bottom, a table header is visible with columns 'Friendly Name' and 'Certificate Subject'.

1. مت اذإ. ةلدسنملا ةمئاقلا نم همادختسا متيس يذلا رودلا دح، "مادختسالا" مسق نمض. ءاشنإ درجمب. مادختسالا ددعت مديحت كنكمي، ةددعتملا راودألل ءاداهشلا مادختسا رمألا مزل اذإ راودأل ريغت نكمي، ءاداهشلا.
2. اهل ءاداهشلا ءاشنإ نكمي يتلا ةدقعل دح.
3. (دلبل او ءيالولا، ءنيءملا، ءمظنملا، ءيميظنتلا ءءوللا) ءءاحلا بسح تامولعمل الما.

✎ مساب ايئاقلا ءدقعل ميمعتب (CN) ءئاشلا مسالا لقحب صاخلا ISE موقى: ءظالم
(FQDN) لمكلا لءؤملا لءملا.

لءبلا فرءا:

- لءبلا فرء ءاداهشب ءامسالا عب رنم ققءتف، لءب فرء ءاداهش ءاشنإ وه فءءالا ناك اذإ.
- ءوضوملل CN لقء يف * زمرلا نوئي ال بعجي EAP ءقءاصمل مدءتست ءاداهشلا تناك اذإ. مءاخلا ءاداهش نوضفري Windows يلموم نإ ءءء.
- ءءافاصم لشفء نأ نكمي، بللظملا ىلع مءاخلا ءءوه ءءص نم ققءتلا لءطعت ءنء ىءء CN لقء يف * نوئي امءنء SSL.
- مادءتسا نكمي مء نمو، CN لقء يف مء FQDN مادءتسا نكمي، كذل نم الءبو و DNS مءسا لقء يف (SAN) ءوضوملل لءبلا مسالا *.domain.com.

✎ ةءاهشلل CN فف (*) لءءبلل فرء ةفاضل (CA) ءاءاهشلل عءارم ضعبل نكمف :ةظءالم
صاخ بلط مءءقء مزلف ،وئرانبسلل اءه فف و CSR فف اءوءوم نكمف مل اءل ىءء اءءلءلء
ءاءءال اءه عنمل

فءرفلل مءاءلل ةءاهشلل CSR لءءم

Usage

Certificate(s) will be used for Multi-Use 

 You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates 

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
<input checked="" type="checkbox"/> abtomar30	abtomar30#Multi-Use

Subject

Common Name (CN)
\$FQDN\$ 

Organizational Unit (OU)
Cisco TAC 

Organization (O)
Cisco 

City (L)
Bangalore

State (ST)
Karnataka

Country (C)
IN

Subject Alternative Name (SAN)

 IP Address  10.106.120.87   

* Key type

RSA  

Wildcard CSR:

Usage

Certificate(s) will be used for Multi-Use

 You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates 

Subject

Common Name (CN)

Mycluster.mydomain.com 

Organizational Unit (OU)

Cisco TAC 

Organization (O)

Cisco 

City (L)

Bangalore

State (ST)

Karnataka

Country (C)

IN

Subject Alternative Name (SAN)



IP Address



10.106.120.87



DNS Name



*.mydomain.com



* Key type

RSA



 نېزختل لة قطنم ةكېش ل قح ىل ا رشن (دق) ةدق ل IP ناو ن ل ة فاضا ن كمې : ةظ حال م IP ناو ن ر ب ع م دا خ ل ل ى ل ل و ص و ل ا د ن ع ة د ا ه ش ل ا ر ي ذ ح ت ب ن ج ت ل (SAN)

لا س ر ا ب ج ي ، ه ر ي د ص ت در ج م ب . ا ه ر ي د ص ت ر ا ي خ ع م ة ق ت ب ن م ة ذ ف ا ن ISE ض ر ع ي ، CSR ء ا ش ن ا در ج م ب ع ي ق و ت ل ل ق د ص م ل ا ع ج ر م ل ا ى ل ل ف ل م ل ا ا ذ ه



Successfully generated CSR(s)

Certificate Signing request(s) generated:

abtomar30.abtomar.local#Multi-Use

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

ةديج تاداهش ةلسلس داريتسإ 2. ةوطخل

ام (طيسول/رذجل) ةلمالكلا تاداهشلا ةلسلس عم عقوملا مداخل ةداهش صيخرتلا ةئيه عجرت
ISE: كمداخ إل تاداهشلا دروتست نأ انه تاوطخلاب مق ،تملتسإ نإ

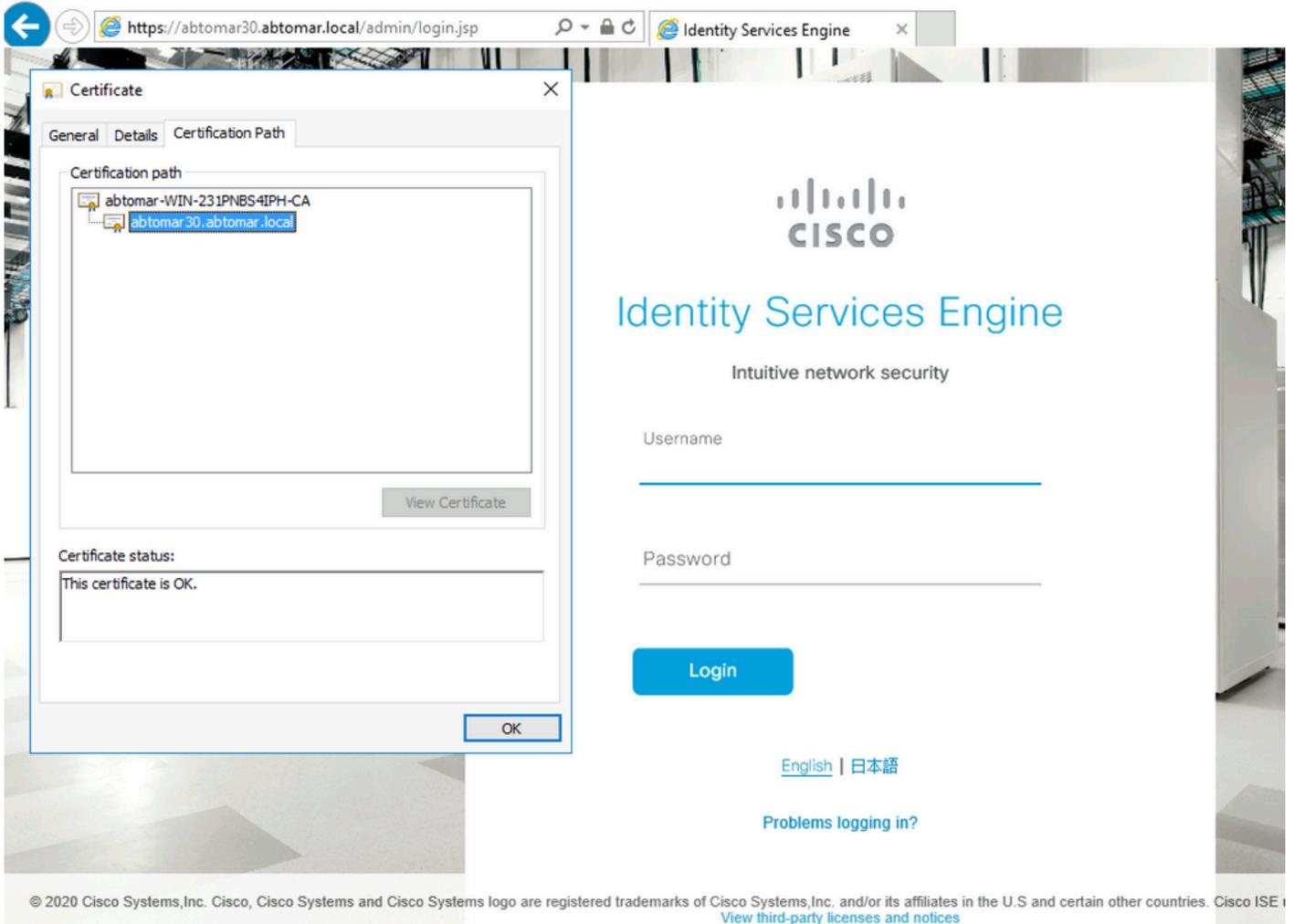
1. إل لقتنا ،قدصملا عجرملا نم ةمدقم ةطيسو تاداهش (وأ) و رذج تاداهش ي داريتسال
اب قووم تاداهش > تاداهش > ةرادإ
2. رايخال تاناخ راتخي و ةطيسولا ةداهشلا وأ/و رذجل راتخي كلذ دعبو داريتسإ ةقطقط
لسري نأ تقبب امك ةلصل تاذ
3. ةداهشلا عيقوت تابلط > تاداهش > ةرادإ إل لقتنا ،مداخل ةداهش داريتسال
4. طببلا ةداهش إلع رقناو اقبسم هؤاشنإ مت يذلا CSR دح
5. هؤاشنإ مت يذلا صخال حااتفملاب ةداهشلا طبرب ISE ماقو ديدجلا ةداهشلا عقوم دح
تانايبل ةدعاق يف هنيختو

ISE مداخل تامدخ ليغشت ةدعإ مت ،ةداهشلا هذل "لوؤسملا رود" ديدحت مت اذا :ةظحالم
ةدحمل

اذو رشنلل ةيساسأل ةرادإل ةدقع صخت اهداريتسإ مت يتلا ةداهشلا تناك اذا :ريذحت
دقعل ةفاك إلع ةدوجوملا تامدخال ليغشت ةدعإ متي ذئدنعف ،ادحم "لوؤسملا" رود ناك
لمعل نع فقوت تقو ثودح نسحتسملا نمو كلذ ثودح عقووملا نم .يرخال ولت ةدحاو
طاشنلا اذه ذيفنتل

ةحصلا نم ققحتلا

ةديجال ةداهشلا نأ نم ققحتلا كنكمي ،ةداهشلا داري ت سا ءانثأ لوؤسملا رود دي دحت مت اذا
ضرعتسملا قثي نأ بجي .ضرعتسملا يف ةرادإلا ءحفص لي دحت قيرط نع ءهنا كم يف
ضرعتسملا ناك اذا وءحي ءص لكشب ءلسلا ءاشنإ مت ءملاط ةديجال لوؤسملا ةداهشب
تاداهشلا ءلسلا يف قثي .



ءوءو نم ققحت صءرءرءلا راسم ءءو ضرعتسملا يف نيءمءءلا زم رءء ،ققءءلا نم دي زم
ءلسلا ريرمء ءلء ارءابم ارءؤم سئل اءه .زاهءاب ءءقء نم ءلمءلا ءلسلا
ةءهشب ءقءلا ءنكمي ضرعتسملا رءؤم ءنكل ءءءلا لبق نم ءءص لكشب ءلمءلا
ءه صءءلا ءءءلا ءءءلا نءءم ءلء اءءءسا ءءءلا

ءءالصا ءاطءالا ءاشءءسا

ءءءء ءءءء

ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء

ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء ءءءء

SSL، ةحفاصم ةي لمع نم عزجك .ةقداصملا ةي لمع نم عزجك يلحلملا ةقثلا نزخم يف هي دل نكمتي نل .هتلسلس يف ةدوجوم ةطس وتم (وأ) و رذج تاداهش يآ ك لذكو هتداهش ISE مدقي ريرمت نم ققحتلل .ةلماك ريغ ةلسلسلا تناك اذا مداخلا ةي وه نم ققحتلا نم بلاطملا ةي لالتا تاوطلخا ذي فننت كنكمي ،لي مالا يلى رخأ ةرم تاداهشلا ةلسلس

1. تاي لمعلا يلى لقتنا ،ةقداصملا ءانثأ (TCPDump) ISE نم طاقثلا طاقثلا لجا نم . TCP غيرفت > ةماع تاودأ > صيخشثلا تاودأ
2. يف ssl.handshake.certificates حشرم قيبطتت مقو طاقثلا لالتا حتف/ليزنتت مق . لوصولا يدحت يلى روثعل او Wireshark
3. > ةميقلا جاوذا صئاصخ > RADIUS لوكوتورب ديدمت يلى لقتنا ،هذي دحت درجمب . ةنمآلا ليصوتلا ذخآم ةقبط > عسوتملا ةقداصملا لوكوتورب > ريخألا عطقملا ةلسلس . تاداهش > ةداهش >

طاقثلا لالتا يف تاداهشلا ةلسلس

No.	Time	Source	Destination	Protocol	Length	Info
334	13:59:41.137274	14.36.157.20	14.36.157.21	TLSv1.2	992	Server Hello, Certificate, Server Hello Done
857	13:59:53.158063	14.36.157.21	14.36.154.5	RADIUS	1178	Access-Challenge(11) (id=198, l=1136)
860	13:59:53.193912	14.36.157.21	14.36.154.5	RADIUS	1174	Access-Challenge(11) (id=199, l=1132)
862	13:59:53.213715	14.36.157.21	14.36.154.5	RADIUS	1174	Access-Challenge(11) (id=200, l=1132)
864	13:59:53.231653	14.36.157.21	14.36.154.5	RADIUS	301	Access-Challenge(11) (id=201, l=259)
1265	14:00:01.253698	14.36.157.20	14.36.157.21	TLSv1.2	992	Server Hello, Certificate, Server Hello Done

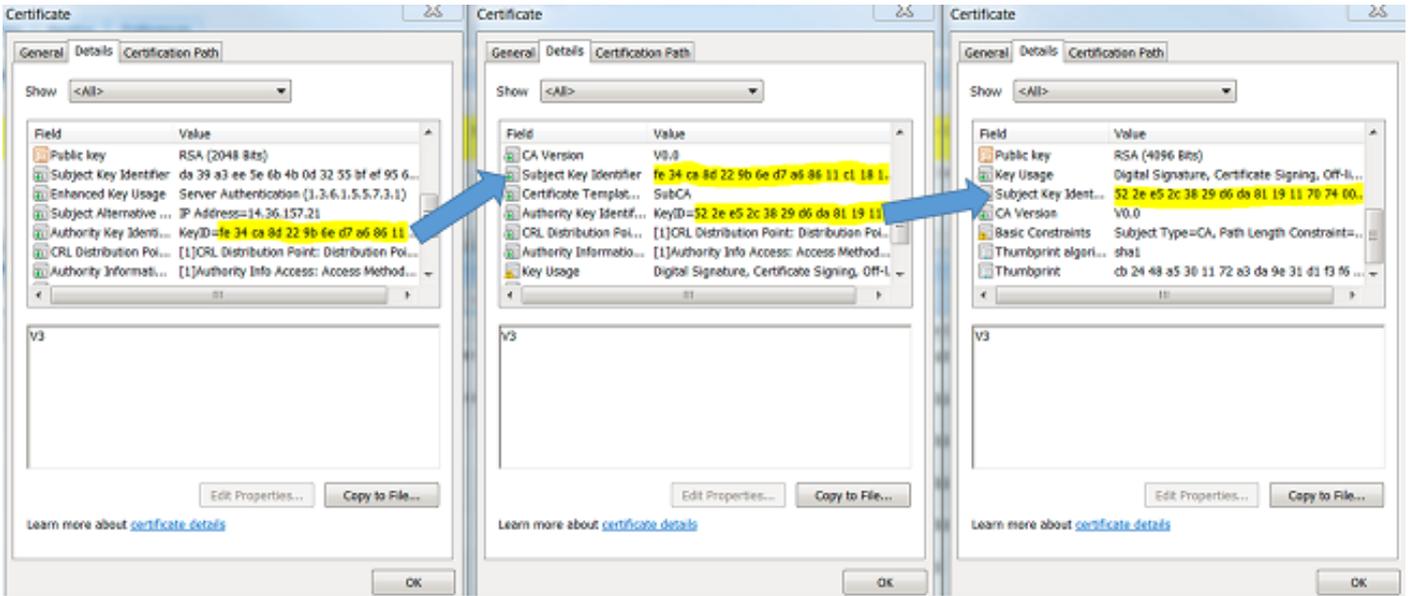
```

AVP: l=255 t=EAP-Message(79) Segment[1]
AVP: l=255 t=EAP-Message(79) Segment[2]
AVP: l=255 t=EAP-Message(79) Segment[3]
AVP: l=255 t=EAP-Message(79) Last Segment[4]
EAP fragment
  Extensible Authentication Protocol
    Code: Request (1)
    Id: 41
    Length: 1012
    Type: Protected EAP (EAP-PEAP) (25)
    EAP-TLS Flags: 0xc0
    EAP-TLS Length: 3141
    [4 EAP-TLS Fragments (3141 bytes): #857(1002), #860(1002), #862(1002), #864(135)]
  Secure Sockets Layer
    TLSv1 Record Layer: Handshake Protocol: Server Hello
    TLSv1 Record Layer: Handshake Protocol: Certificate
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 3048
    Handshake Protocol: Certificate
      Handshake Type: Certificate (11)
      Length: 3044
      Certificates Length: 3041
      Certificates (3041 bytes)
        Certificate Length: 1656
        Certificate (id-at-commonName=TORISE20A.rtpaaa.net,id-at-organizationalUnitName=RTPAAA,id-at-organizationName=CISCO,id-at-localityName=RT
          Certificate Length: 1379
        Certificate (id-at-commonName=rtpaaa-ca,dc=rtpaaa,dc=net)
    TLSv1 Record Layer: Handshake Protocol: Server Hello Done
  
```

نم ققحتو واهب قوثوم تاداهش > تاداهش > ISE ةرادا يلى لقتنا ،ةلماك ريغ ةلسلسلا تناك اذا ققحتلا بجيف ،حاجن تاداهشلا ةلسلس ريرمت مت اذا . رذجلا (وأ) و ةطيسولا تاداهشلا دوجو . انه ةحضوملا ةقيرطلا مادختساب اهسفن ةلسلسلا ةي حالص نم

فرعم ةقباطم لالخنم ةقثلا ةلسلس نم ققحتو (يرذجو طس وتم ،مداخ) ةداهش لك حتفا يف ةي لالتا ةداهشلل (AKI) ةطلسلا حتفم فرعم عم ةداهش لك (SKI) عوضوملا حتفم . ةلسلسلا

تاداهش ةلسلس يلى لالتا

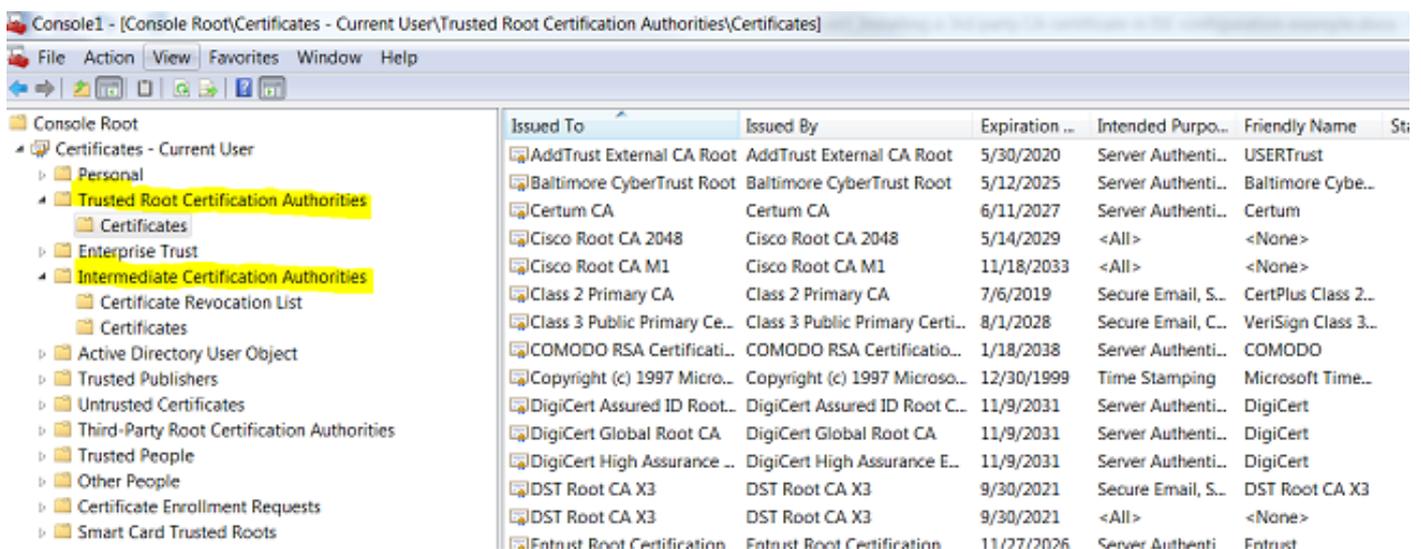


إعدادات ISE مداخل شهادة ضفرت ةيها نلا ةطقن نكلو ةححص ISE ةداهش ةلسلس ةقداصلما

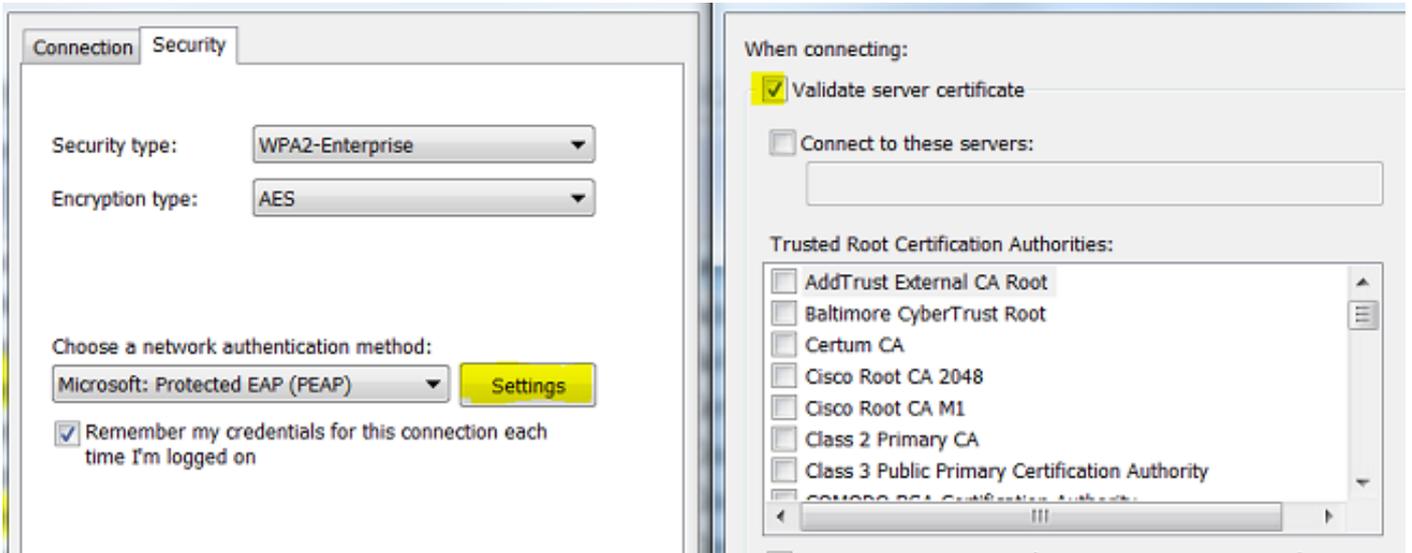
ال بولطم لانا و SSL ةحفاصلما ةانثأ هب ةصاخلا ةلماكل تاداهشلا ةلسلس مدقي ISE ناك اذا (و) و رذل تاداهشلا نأ نم ققحتلا يه ةيالتلا ةوطخل ناف، تاداهشلا ةلسلس ضفري لازي ليمع لابل صاخلا يلحم لال ةقثل نزم يف ةدووم ةطيسولا تاداهشلا

Add-Remove ةيفاضإلا ةادأل mmc.exe فلم لىل لقتنا، Windows زاى نم كلذ نم ققحتلل مدختسملما باسح ام دح. ةفاضل لىل رقناو تاداهشلا دح، رفوتلم ةيفاضإلا تاوادلأ دومع نم م (زاهل و مدختسملما) مدختسملما ةقداصلما عون بسح لىل رتوي بمكل باسح و ايب صاخلا قفاوم لىل رقنا

تاداهشلا عجارمو اب قوئوم لال رذل ةقداصلما عجارم دح، مكحتلا ةدحو ضرع ةقيرط تحت يلحم لال قوئوم لال نزم لىل طسوتلم لال رذل ةداهشلا دوو نم ققحتلل ةطيسولا



يديحت ةاغلاب مق، مداخل ةيوه نم ققحتلا يف ةلكشم هذه نأ نم ققحتلل ةلهس ةقيرط لىل رذل ةداهشلا ةقداصلما باسح ام دح، رفوتلم ةيفاضإلا تاوادلأ دومع نم ققحتلل ةطيسولا



ةلص تاذا تامولعم

- [3.0 رادصالا، Cisco نم ةيوهلا تامدخ كرحم لوؤسم ليلد](#)
- [Cisco نم تاليزنتلاو ينفلا معدلا](#)

