# ISE يف TLS/SSL تاداەش نيوكت

### تايوتحملا

<u>ةمدق مل ا</u> <u>ةيساسألا تابلطتملا</u> <u>تابلطتملا</u> ةمدختسملا تانوكملا مداخلا تاداهش ISE تاداەش <u>ماظنلا تاداەش</u> اهب قوثوملا تاداهشلا نزخم <u>قىساسالا ماەملا</u> ا<u>ىتاذ ةعقوم ةداەش ءاشنا</u> <u>ایتاذ ةعقوم ةداهش دیدجت</u> <u>اەب قوثوم ةداەش تېپثت</u> <u>CA نم ةعقوم ةداەش تىپەت</u> <u>ةصاخلا جيتافملاو يطايتحالا خسنلا تاداهش</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>ةداەشلا ةحص نم ققحتلا</u> <u>ةداەش فذح</u> <u>امداخ ةداەش بالط ق ال ISE مداخ ةداەش بالاط ق يال</u> <u>ققداصملا ءانثاً ISE مداخ ةداهش ضفرت ةياهنلا ةطقن نكلو ةحيحص ISE ةداهش ةلسلس</u> <u>ةرركتملا ةلئسألا</u> <u> ؟لءفلاب ةدوجوم ةداهشلا نأب هيٻنت هيجوتب ISE موقي امدنع هلءف ٻجي يذلا ام</u> <u>قطساوب ةمدقم ISE نم لخدماا ةحفص نأ يلا ريشي ريذحت هيجوتب ضرعتسماا موقى اذامل</u> <u> جەب قوثوم رىغ مداخ</u> <u> ؟ةحلاصلا ريغ تاداهشلا ببسب ةيقرتلا لشف دنع ملعف بجي يذلا ام</u> <u>ةلص تاذ تامولعم</u>

### ەمدقملا

ةيفيكو ،ISE تاداەش راودأو عاونأو ،Cisco ISE يف TLS/SSL تاداەش دنتسملا اذه فصي ةلوادتملا ةلئسألا ىلع تاباجإلاو ،اەحالصإو ءاطخألا فاشكتساو ةعئاشلا ماەملا ذيفنت.

## ةيساسألا تابلطتملا

### تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- Cisco (ISE) نم ةيوەلا تامدخ كرحم .1
- .AAA و ISE رشن تايلمع نم ةفلتخم عاونأ فصول ةمدختسملا تاحلطصملا .2
- AAA تايساسأو RADIUS لوكوتورب .3
- x509 و SSL/TLS تاداەش .4

(PKI) ماعلا حاتفملل ةيساسألا ةينبلا تايساساً .5

#### ةمدختسملا تانوكملا

نم 2.7 - 2.4 تارادصإلاو ،Cisco ISE تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست نوكي نأ بجي ،كلذ عمو ،2.7 ىلإ 2.4 رادصإلا نم ISE يطغي وهو .ةيداملا تانوكملاو جماربلا .كلذ فالخ ىلع صني مل ام ISE 2.x نم ىرخألا جماربلا تارادصإل اقباطم وأ الثامم

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

### مداخلا تاداهش

اەتلاصأ ىلع لوصحلل ءالمعلل مداخلا ةيوە مېدقتل مداخلا تاداەش مداوخلا مدختست ةداەشلا مداخلا ردصي ثيح) ايتاذ ةعقوم ەذە نوكت نأ نكمي .لاصتالل ةنمآ ةانق ريفوتلو (فورعم دروم نم وأ ةسسؤملل يلخاد امإ) قدصم عجرم نم ةرداص وأ (ەسفنل.

لەؤملا لاجملا مسا) FQDN وأ فيضملا ءامسأ ىلإ يجذومن لكشب مداخلا تاداەش رادصإ متي وأ (فيضملا) فيضملا..(domain.com؛ لدب فرح ةداەش اضيأ نوكت نأ نكمي وأ ،مداخلل (لماكلاب (مسالا) مسالا) يلقح يف صاخ لكشب روكذم هيلإ هرادصإ متي يذلا يعرفلا لاجملا وأ لاجملا (SAN).

مسا نم الدب ةيمجن ةمالع) لدب فرح نيودت مدختست SSL تاداەش يە لدبلا فرحأ تاداەش ةسسؤم يف نيددعتم نيفيضم ربع ةداەشلا سفن ةكراشمب حمست يلاتلابو (فيضملا. عوضوملا مسا لدبلا فرحأ تاداەشل SAN وأ CN ةميق ودبت نأ نكمي ،لاثملا ليبس ىلع server1.com، لثم لاجملا اذەل نيفيضم يأ نيمأتل ەمادختسإ نكميو server2.com. ل لثامم server2.com،

ل الثامتمل اريغ ريفشتلا وأ ماعل حاتفمل اريفشت ةداع تاداهشلا مدختست.

- هتكراشم متيو ،لوقحلا دحأ يف ةداهشلا يف ادوجوم ماعلا حاتفملا نوكي :ماعلا حاتفملا هب لاصتالا ام زامج لواحي امدنع ماظن ةطساوب ماع لكشب.
- نكمي .ماعلاا حاتفملاب نرتقيو يئاەنلا ماظنلاب صاخ صاخلا حاتفملا :صاخلا حاتفملا صاخلا حاتفملا ةطساوب طقف ماع حاتفم ةطساوب ةرفشملا تانايبلا ريفشت كف سكعلاب سكعلاو ددحملا جودزملا.

### ISE تاداەش

طاقن عم نمآ لاصتا ريفوتل (PKI) ماعلا حاتفملل ةيساسألا ةينبلا ىلع Cisco ISE دمتعي ددعتم رشن يف Cisco ISE دقع نيب كلذكو ،كلذ ىلإ امو نييرادإلاو نيمدختسملاو ةياهنلا ريفشتل ةماعلا حيتافملا لقنل X.509 ل ةيمقرلا تاداهشلا ىلع PKI دمتعت .تايسنجلا نيمدختسملا نم ةمدقملا ىرخألا تاداهشلا قلاصأ نم ققحتللو ،اهريفشت كفو لئاسرلا :قداع ةمدختسملا تاداهشلا نم نيتئف يلع Sisco ISE يوتحي .قزهجألاو

- كال نوكي .ءالمعلل Cisco ISE ةدقع فرعت مداخ تاداهش هذه :ماظنلا تاداهش صاخلا حاتفملا عم ةدقعلا ىلع اهنم لك نيزخت متيو ،ةصاخلا ةيلحملا اهصيخرت ISE ينعملا
- ققحتلل مدختست (CA) قيدصت عجرم تاداهش يه :تاداهشلا اهب قوثوملا تاداهشلاً نزخت يف ةدوجوملا تاداهشلا هذه ةرادا متتو .ةفلتخم ضارغال ISE ىلا قمدقملا تاداهشلا نم عيمج ىلا الثامتم اخسن اهخسن متيو "قيساسألا قرادالا" قدقع ىلع "تاداهشلا نزخم" متي تاداهش ىلع اضيأ تاداهشلا نزخم يوتحي .عزوملا Cisco ISE رشن يف ىرخالا دقعلا BYOD.

### ماظنلا تاداهش

ەحرش يرجيو افلتخم ادصق مدخي رود لكو .رثكأ وأ دحاو رودل ماظنلا تاداەش مادختسإ نكمي انە:

- Admin: ةفاضإلاب ،(Admin GUI) 443 ربع تالاصتالا عيمج نيمأتل رمألا اذه مادختسإ متي (Admin GUI)، ةفاضإلاب ، انه جردم ريغ مادختسإ/ذفنم يألو ،لثامتملا خسنلا يلإ.
- ةقداصم ةباوب لثم لخادملا ربع HTTP لاصتا نيمأتل رايخلا اذه مادختسإ متي :ةباوبلا عالمعلا دادمإ تاباوبو ،ليمعلا دادمإو BYOD، و ،فيضلاو ،(CWA) ةيزكرملا بيولا وه يضارتفالا) لخدم ةعومجم ةمالع ىلع لخدم لك نييعت بجي .كلذ ىلإ امو ،نييلصألا متيس يتلا ةددحملا قداهشلا ىلع لخدملا دشرت يتلاو (ةيضارتفا لخدم ةعومجم ةمالع ريرحت تارايخ يف لخدملا ةعومجم مسا مسال قلدسنملا قمئاقلا كل حيتت .اهمادختسإ دوميرا الالالي عاميا
- عم تاداهشلا مدختست .802.1x ققداصمل ءالمعلا ىلا قمدقملا قداهشلا ددجي رود اذه :EAP مادختساب .اذكهو EAP-FAST و PEAP و EAP-TLS لثم ابيرقت نكمم EAP بولسأ لك نيمأتل (TLS) لقنلا ققبط نامأ مدختسي ،FAST و PEAP لثم يقفنلا EAP بيلاسأ اذه ءاشنإ دعب الإ مداخلا ىلإ ليمعلا دامتعا تانايب لاسرا متي ال .دامتعالا تانايب لدابت .نمآ لدابت قيقرحت نامضل قفنلا
- RADIUS DTLS لاصتال مدختست يتلا ةداهشلا رودلا اذه ددحي :DTLS لاصتال DTLS وربع TLS (ربع TLS لاصتا) و UDP نا بجيو نأ بجيو .ISE و (NAD) ةكبشلا ىل لوصولا زاهج نيب RADIUS رورم ةكرح ريفشتل (UDP رأ بجيو .SE و DTLS ريفشت نوكي
- نكمي ال .(IdP ةيوه رفومب لاصتالا نيمأتل مداخلا ةداهش مدختست :SAML مداخلا الله عنه مدختست :SAML مادختسا امو EAP ةقداصمو Admin لثم ىرخأ ةمدخ يأل SAML مادختسال ةصصخم ةداهش مادختسإ كلذ ىلإ.
- syslog لوكوتورب نم الدب ISE ةلسارم ةمدخ ISE مدختسي ،2.6 ماع ذنم :ISE ةلسارم ةمدخ لامت الدوريفشتل اذه مدختسي .تانايبلا ليجستل ميدقلا.
- PxGrid تامدخل ةداهشلا هذه مدختست :ISE دلع SE

ا عاشناب موقي ەنإف ،ISE تېبثت دنع Default Self-Signed Server Certificate ، الموقي ەنإف ،ISE تېبثت دنع قدصم عجرم ىلإ راودألا ەذە لقنب ىصوي .ايضارتفا RADIUS DTLS و ،لخدملاو ،لوؤسملاو فورعم قدصم عجرم نم ةعقوم ةداەش وأ يلخاد.

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	License Warning 🔺 🔍 🔞	• •
▼ System → Identity Management →	Network Resources		
Deployment Licensing	s + Logging + Maintenance Upgrade + Backup & Restore + Admin Access + Settings		
0			
	System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.		
System Certificates	📝 Edt 🛛 🖶 Generate Self Signed Certificate 🛛 🛉 Import 🚱 Export 🔀 Delete 🔎 View		
Trusted Certificates	Friendly Name Used By Portal group tag Issued To Issued By Va	alid From Expiration Date	
OCSP Client Profile	▼ hongkongise		
Certificate Signing Requests Certificate Periodic Check Settings	OU:Certificate Services Syste m Certificate, CN-hongkongise; riverdale local s Endpoint Sub CA - hongkongise em0002 Certificate Service Endpoint Su Mc	lon, 13 Apr 2020 Sun, 14 Apr 203/	
Certificate Authority	OU-ISE Messaging Service,CN  Thicate Services Endpoint Suc Services  CA - hongkongise riverdale local  Certificate Services Endpoint Suc Service  A - hongkongise riverdale local  Certificate Services Endpoint Su Mc  A - hongkongise	lon, 13 Apr 2020 Sun, 14 Apr 2030	
	Default self-signed saml server certificate - CN-SAML_hongkongise riverdale loc SAML_hongkongise riverdale loc al gise riverdale local al	ue, 14 Apr 2020 Wed, 14 Apr 202	81 🔽
	Default seif-signed server cettil     cate     cate	ue, 14 Apr 2020 Wed, 14 Apr 202	•

المداخب ةصاخلاا IP نيوانعو FQDN نم لك ةفاضإ نامض ةديجلا تاسرامملا نم :**حيملت** ISE مداخب ةصاخلا DSN يوانعو SAN لقح يل Cisco يف ةداهشلا ةقداصم نأ نامضل ،ماع لكشب ISE. ماظن ةداهش يف SAN لقح يلإ الماذ الما يا الماذي الما الماذي ال الماذي ا الماذي الم الماذي الماذي الماذي الماذي الماذي الماذي الماذي

وأ (PEM) "ةيصوصخلل نسحملا ديربلا" وه ISE ةداهش قيسنت نوكي نأ بجي :**قظحالم** "قزيمملا زيمرتلا دعاوق" (DER).

### اەب قوثوملا تاداەشلا نزخم

نأ بجيو Administration > System > Certificates > Certificate Store كلع قدصملا عجرملا تاداهش نيزخت بجي تاداهشلا هذه مدختسي ISE نأ نامضل مادختسإ قلاح Trust for client authentication مهيدل نوكي يرخالا ISE دقع وأ ةزهجألا وأ ةياهنلا طاقن نم ةمدقملا تاداهشلا نم ققحتلل.

Home  → Context Visibility  → Operations  → Polic	y • Administra	tion			Licens	e Warning 🔺 🛛 🔍	
Network Resources	Services Fee	d Service > Threat Cent	ric NAC				
Logging      Maintenance Upgrade      Backup & F	lestore + Admin	Access					
Trusted Certificates							
🖊 Edit 📲 Import 🚱 Export 🗙 Delete 🔎 View					SI	Now Al	* 5
Friendly Name	<ul> <li>Status</li> </ul>	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date
<ul> <li>Baltimore CyberTrust Root</li> </ul>	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Mon, 12 May 20
Cisco CA Manufacturing	Ø Disabled	Endpoints	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 20
Cisco ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 2053
Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 20
Cisco Manufacturing CA SHA2	Enabled	Endpoints	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20
Cisco Root CA 2048	Ø Disabled	Endpoints	5F F8 7B 28 2B 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2
Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Sun, 9 Aug 209
Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 203
Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 20
Cisco RXC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034
Default setf-signed server certificate	Enabled	Endpoints	SE 95 93 55 00 00	hongkongise.riverdale.local	hongkongise.riverdale.local	Tue, 14 Apr 2020	Wed, 14 Apr 20
DigiCert Global Root CA	Enabled	Cisco Services	08 3B E0 56 90 42	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov 2
DigiCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 08	DigiCert High Assurance	DigiCert High Assurance	Fri, 10 Nov 2006	Mon, 10 Nov 20
DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints	04 E1 E7 A4 DC 5C	DigiCert SHA2 High Assu	DigiCert High Assurance	Tue, 22 Oct 2013	Sun, 22 Oct 20
DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A3	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 20
HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 20
QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2
Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wed, 16 Jul 20
VerSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D	VeriSign Class 3 Public Pr	VeriSign Class 3 Public Pr	Wed, 8 Nov 2006	Wed, 16 Jul 20
VerSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03	VerSign Class 3 Secure	VeriSign Class 3 Public Pr	Mon, 8 Feb 2010	Fri, 7 Feb 2020
	Home       ♦ Context Visibility       ♦ Operations       ♦ Polic         Network Resources       > Device Portal Management       pxGrid         ▶ Logging       ♦ Maintenance       Upgrade       ♦ Backup & F         Trusted Certificates	Home <ul> <li>Context Visibility</li> <li>Operations</li> <li>Policy</li> <li>Administra</li> <li>Network Resources</li> <li>Device Portal Management</li> <li>pxGird Services</li> <li>Fede</li> <li>Logging</li> <li>Maintenance</li> <li>Upgrade</li> <li>Backup &amp; Restore</li> <li>Administra</li> <li>Trusted Certificates</li> <li>Fede</li> <li>Fede</li> <li>Import</li> <li>Export</li> <li>Device Portal Management</li> <li>pxGird Services</li> <li>Fede</li> <li>Administra</li> <li>Casco Certificates</li> <li>Finendly Name</li> <li>Status</li> <li>Baltmore CyberTrust Root</li> <li>Enabled</li> <li>Casco CA Manufacturing</li> <li>Desabled</li> <li>Casco LCensing Root CA</li> <li>Enabled</li> <li>Casco Root CA 2048</li> <li>Desabled</li> <li>Casco Root CA 2048</li> <li>Desabled</li> <li>Casco Root CA 2099</li> <li>Enabled</li> <li>Casco Root CA 2099</li> <li>Enabled</li> <li>Casco Root CA 2099</li> <li>Enabled</li> <li>Casco Root CA M2</li> <li>Enabled</li> <li>Casco Root CA M2</li> <li>Enabled</li> <li>Casco Root CA M2</li> <li>Enabled</li> <li>DigCert Global Root CA</li> <li>Enabled</li> <li>DigCert SHA2 High Assurance Server CA</li> <li>Enabled</li> <li>DigCert S</li></ul>	Home <ul> <li>Context Visability</li> <li>Operations</li> <li>Policy</li> <li>Administration</li> <li>Work Centers</li> <li>Network Resources</li> <li>Device Portal Management</li> <li>pxGrid Services</li> <li>Feed Service</li> <li>Trusted Certificates</li> <li>Feld</li> <li>Feld</li> <li>Enging</li> <li>Maintenance</li> <li>Upgrade</li> <li>Backup &amp; Restore</li> <li>Administration</li> <li>Administructure</li> <li>Status</li> <li>Trusted For</li> <li>Batmore CyberTrust Root</li> <li>Enabled</li> <li>Cisco ECR Root CA</li> <li>Enabled</li> <li>Cisco Force Root CA</li> <li>Enabled</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Infrastructure</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Services</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Root CA 2048</li> <li>Cisco Services</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Root CA 2048</li> <li>Cisco Services</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Services</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Root CA 2048</li> <li>Disabled</li> <li>Cisco Services</li> <li>Cisco Root CA 2048</li> <li>Discritic Trusture</li> <li>Cisco Root CA 2048</li> <li>Discret root CA</li> <l< td=""><td>Home       ♦ Context Visibility       ♦ Operations       ♦ Policy       ← Administration       ♦ Work Centers         Network Resources       &gt; Device Portal Management       pxGird Services       &gt; Feed Service       &gt; Threat Centric NAC         &gt; Logging       &gt; Maintenance       Upgrade       &gt; Backup &amp; Restore       &gt; Admin Access       &gt; Settings         Trusted Certificates         // Edit       ● Inport       ● Deshe       ● Vew             Friendy Name        Status       Trusted For       Serial Number           Scico CA Manufacturing        &gt; Desheled       Enabled       Cico Services       02 00 00 B9           Cisco ECR Root CA        &gt; Enabled       Cisco Services       01            Cisco Root CA        &gt; Enabled       Enabled       Enabled       Enabled       Enabled       Enabled       Disco Services       01            Cisco Root CA 2048        &gt; Disabled       Infrastructure       01        Disco Services       01 9A 33 58 78 CE           Cisco Root CA 2048        &gt; Disabled       Infrastructure       01        Disco Services       01 9A 33 58 78 CE           Cisco Root CA Mau        = Enabled       Eisco Services       01       &lt;</td><td>Home       ♦ Context Visibility       ♦ Ciperations       ♦ Policy       ● Administration       ♦ Work Centers         Network Resources       &gt; Device Portal Management       pxGind Services       &gt; Feed Service       &gt; Threat Centric NAC         &gt; Logging       &gt; Maintenance       Upgrade       &gt; Backup &amp; Restore       &gt; Admin Access       &gt; Settings         Trusted Certificates         // Edit       ● Dirport       ▲ Destore       &gt; Status       Trusted For       Serial Number       Issued To         Batmore CyberTrust Root       © Enabled       Cisco Services       02 00 00 B9       Batmore CyberTrust Roo.         Cisco CR Root CA       © Enabled       Enabled       Cisco Services       01       Cisco ECC Root CA         Cisco ECR Root CA       © Enabled       Enabled       Cisco Services       01       Cisco Calcensing Root CA         Cisco Root CA 2048       © Disabled       Infrastructure       First Piperits       Cisco Root CA 2048       Cisco Services       01 94 33 58 78 CE       Cisco Root CA 2049         Cisco Root CA       Enabled       Cisco Services       01 94 33 58 78 CE       Cisco Root CA 2049         Cisco Root CA       Enabled       Enabled       Cisco Services       01 Cisco Root CA 2049         Cisco Root CA       Enabled&lt;</td><td>Home       • Cortext Visibility       • Operations       • Parloy       • Administration       • Work Certers       Uscons         Network Resources       • Device Pottal Management       pxGird Services       • Threat Centric NAC         • Logging       • Maintenance       Upgrade       • Backup &amp; Restore       • Admini Access       • Settings           <b>Trusted Certificates</b> <bb></bb>       Finding Name       <bb></bb>       Bachmore Cyber Trust Rot               Bachmore Cyber Trust Rot               Enabled               Caso CA Manufacturing               O Isabled               Infrastructure               Caso Roct CA               Caso Roct CA 2048               Caso Roct CA 2048               Caso Roct CA 2049               Caso Roc</br></br></td><td>Home       • Contrast Vacibility       • Operations       • Padary       • Administration       • Werk Centers       • License Warring A       Q         Network Resources       • Device Portal Management       priorid Services       • Feed Service       • Threat Centric NAC         • Logging       • Maintenance       Upgrade       • Backup &amp; Restore       • Administration       • Padary       • Status       • Trusted Centrificates                 freed Synthem       • Status       Trusted Fer       Servine       Issued To       Issued To       Issued To       Nainf       Nainf       Name       Issued To       Issued To       Issued To       Nainf       Name       Issued To       Nainf       Name       Issued To       Name       Name       Issued To       Name       Name</td></l<></ul>	Home       ♦ Context Visibility       ♦ Operations       ♦ Policy       ← Administration       ♦ Work Centers         Network Resources       > Device Portal Management       pxGird Services       > Feed Service       > Threat Centric NAC         > Logging       > Maintenance       Upgrade       > Backup & Restore       > Admin Access       > Settings         Trusted Certificates         // Edit       ● Inport       ● Deshe       ● Vew             Friendy Name        Status       Trusted For       Serial Number           Scico CA Manufacturing        > Desheled       Enabled       Cico Services       02 00 00 B9           Cisco ECR Root CA        > Enabled       Cisco Services       01            Cisco Root CA        > Enabled       Enabled       Enabled       Enabled       Enabled       Enabled       Disco Services       01            Cisco Root CA 2048        > Disabled       Infrastructure       01        Disco Services       01 9A 33 58 78 CE           Cisco Root CA 2048        > Disabled       Infrastructure       01        Disco Services       01 9A 33 58 78 CE           Cisco Root CA Mau        = Enabled       Eisco Services       01       <	Home       ♦ Context Visibility       ♦ Ciperations       ♦ Policy       ● Administration       ♦ Work Centers         Network Resources       > Device Portal Management       pxGind Services       > Feed Service       > Threat Centric NAC         > Logging       > Maintenance       Upgrade       > Backup & Restore       > Admin Access       > Settings         Trusted Certificates         // Edit       ● Dirport       ▲ Destore       > Status       Trusted For       Serial Number       Issued To         Batmore CyberTrust Root       © Enabled       Cisco Services       02 00 00 B9       Batmore CyberTrust Roo.         Cisco CR Root CA       © Enabled       Enabled       Cisco Services       01       Cisco ECC Root CA         Cisco ECR Root CA       © Enabled       Enabled       Cisco Services       01       Cisco Calcensing Root CA         Cisco Root CA 2048       © Disabled       Infrastructure       First Piperits       Cisco Root CA 2048       Cisco Services       01 94 33 58 78 CE       Cisco Root CA 2049         Cisco Root CA       Enabled       Cisco Services       01 94 33 58 78 CE       Cisco Root CA 2049         Cisco Root CA       Enabled       Enabled       Cisco Services       01 Cisco Root CA 2049         Cisco Root CA       Enabled<	Home       • Cortext Visibility       • Operations       • Parloy       • Administration       • Work Certers       Uscons         Network Resources       • Device Pottal Management       pxGird Services       • Threat Centric NAC         • Logging       • Maintenance       Upgrade       • Backup & Restore       • Admini Access       • Settings <b>Trusted Certificates</b> <bb></bb> Finding Name <bb></bb> Bachmore Cyber Trust Rot Bachmore Cyber Trust Rot Enabled Caso CA Manufacturing O Isabled Infrastructure Caso Roct CA 	Home       • Contrast Vacibility       • Operations       • Padary       • Administration       • Werk Centers       • License Warring A       Q         Network Resources       • Device Portal Management       priorid Services       • Feed Service       • Threat Centric NAC         • Logging       • Maintenance       Upgrade       • Backup & Restore       • Administration       • Padary       • Status       • Trusted Centrificates                 freed Synthem       • Status       Trusted Fer       Servine       Issued To       Issued To       Issued To       Nainf       Nainf       Name       Issued To       Issued To       Issued To       Nainf       Name       Issued To       Nainf       Name       Issued To       Name       Name       Issued To       Name       Name

### ةيساسألا ماەملا

اذإ .ام ةطقن دنع اهلادبتساب ةبلاطملا وأ اهلاطبإ نكميو ةيحالص ءاهتنا خيرات ةداهشلل ةداهشب اهلادبتسإ متي مل ام ةريطخ تالكشم رهظت دقف ،ISE مداخ ةداهش ةيحالص تهتنا ةحلاص ةديدج.

ر(EAP) عسوتملاا ةقداصملاا لوكوتوربل ةمدختسملا ةداەشلاا ةيحالص تەتنا اذإ :**قظحالم** قلاح يف .نآلا دعب ISE قداەشب قثي ال ليمعلاا نأل ءالمعلا ةقداصم لشفت دقف ضفر تاضرعتسملاو ءالمعلل نكمي ،لخادملل مدختست قداەش قيحالص ءاەتنا رطاخملا نوكت ،لوؤسملا مادختسإ قداەش قيحالص ءاەتنا قلاح يف .لخدملاب لاصتالا رشنلا فقوتي نأ نكميو نآلا دعب ISE ىلإ لوخدلا ليجست نم لوؤسملا عنمي امم ربكا

#### ايتاذ ةعقوم ةداهش ءاشنإ

القتنا، عيقوتاا ةيتاذ قديدج تاداەش ءاشنإل Administration > System > Certificates > System Certificates. قوف رقنا Generate Self Signed Certificate.

cisco Identity Services Engine	Home	<ul> <li>Operations</li> <li>Policy</li> </ul>	<ul> <li>Administration</li> </ul>	<ul> <li>Work Centers</li> </ul>
	Network Resources	ortal Management pxGrid Se	rvices Feed Servic	e Fhreat Centric NA
Deployment Licensing	► Logging ► Maintenance	Upgrade Backup & Resto	Admin Access	<ul> <li>Settings</li> </ul>
G				
- Certificate Management	System Certificates 🛕	For disaster recovery it is recom	mended to export certifie	cate and private key pairs
System Certificates	📝 Edit 🛛 🕂 Generate Self S	Signed Certificate	💽 Export 🗙 D	elete 🔎 View
Trusted Certificates	Friendly Name	Used By	Portal group tag	Issued To
OCSP Client Profile	▼ hongkongise			
Certificate Signing Requests Certificate Periodic Check Settings	OU=Certificate Service m Certificate,CN=hong verdale.local#Certificate s Endpoint Sub CA - ho e#00002	es Syste kongise.ri e Service pxGrid ongkongis		hongkongis

ايتاذ ةعقوم ةداهش ءاشنإ ةحفص يف ةدوجوملا لوقحلا ةمئاقلا هذه فصت.

ايتاذ ةعقوملا ةداهشلا تادادعإ لقح مسا مادختسإ تاداشرإ:

- . ماظنلا ةداهش ءاشنإل اهيلإ جاتحت يتلا ةدقعلا (ةبولطم) :ةدقعلا ددح •
- CN: نإف ،يضارتفا لكشب ((SAN) نيزختال ةقطنم ةكبش ديدحت متي مل اذإ بولطم) CN نإف ،يضارتفا لكشب (FQDN يه اهل يتاذلا عيقوتال ةداهش ءاشنإ متي يتال ISE ةدقعل FQDN يه.
- ا.ةسدنەلا، الاثمال اليبس ىلع ،ةيميظنتال ةدخولا مسا :ةيميظنتال ةدخولا.
- الثملال اليبس ىلع ،ةسسۇملا مسا:(O) الامارا اليامارا اليامارا اليابى الايارى الى الى الى الى الى الى الى الى ا
- الميسوخ ناس ،لاثملا ليبس ىلع ،ةنيدملا مسا (رصتخت ال) :(ل) ةنيدملا.
- اينروفيلاك ،لاثملا ليبس ىلع ،ةيالولا مسا (رصتخت ال) :(ST) ةيالولا
- الثمل اليبس ىلع .نيفرجلا يذ ISO دلبلا زمر لاخدا مزلي .دلبلا مسا. ةدجتملا تايالولا.
- الالك) دحوملا دراوملا فرعم وأ DNS مسا وأ IP ناونع (SAN) نيزختلا ةقطنم ةكبش (URI) دحوملا دراوملا فرعم وأ ةداهشلاب نرتقملا.
- وأ RSA :ماعلا حاتفملا ءاشنإل اهمادختسإ متيس يتلا ةيمزراوخلا ددح :حاتفملا عون ECDSA.
- ل تارايخلا هذه رفوتت .ماعلا حاتفملل تبلا مجح ددح :حاتفملا لوط RSA: 512 1024 2048 ل تارايخلا هذه رفوتت .ماعل حال حاتفمل ل قرفوتم تارايخلا هذهو 4096 ECDSA: 256 384.

- SHA-256. وأ SHA-1 :هذه ةئزجتلا تايمزراوخ دحأ رتخأ :مادختساب عيقوتلل صخلم
- اهعم قفاوتت نأ بجي يتلا OID تافرعمب ةمئاق وأ ةداهشلا جهن فرعم لخدأ :ةداهشلا جهن ةيلصألا ةزهجألا تافرعم لصفل تافاسملا وأ لصاوفلا مدختسأ .قداهشلا.
- . ةداەشلا ةيحالص اەدعب يەتنت يتلا مايألا ددع ددح :قيحالصلا ءاەتنا ةدم •
- موقت Cisco ISE نإف ،مسا ديدحت متي مل اذإ .ةداهشلل افولأم امسا لخدأ :فولأم مسا تاناخ سمخ نم ديرف مقر وه نيأ قيسنتلاب مسا ءاشنإب ايئاقلت.
- ايتاذ ةعقوم لدب فرح ةداهش ءاشنإل هذه رايتخالا ةناخ ددح :لدبلا فرحأ تاداهشب حامسلا ةكبش يف DNS مسا وأ/و عوضوملا يف CN يأ يف (\*) ةيمجن ةمالع ىلع يوتحت ةداهش) هنييعت مت يذلا DNS مسا نوكي نأ نكمي ،لاثملا ليبس ىلع .(SAN) نيزختلا ةقطنم ل SAN \*.domain.com.
- يە ةحاتملا تارايخلا. اەل ەذە ماظنلا قداەش مادختسإ بجي يتلا قمدخلا رتخأ:مادختسالا. قوداصملوؤسملا EAPRADIUS DTLSpxGrid

cisco Identi	ity Services I	Engine	Home 🕨 Co	ntext Visibility	<ul> <li>Operations</li> </ul>	▶ Policy	▼ Administrati	ion 🔹 🕨 Work C	enters
▼ System	Identity Man	agement I	Network Resource	es Device P	ortal Manageme	ent pxGrid Serv	vices Feed	d Service	eat Centric NAC
Deployment	Licensing		Logging	<ul> <li>Maintenance</li> </ul>	Upgrade •	Backup & Restor	re 🕨 Admin A	Access > Settin	gs
		0							
	Management		Generate S	elf Signed Cer	rtificate				
System Cer	rtificates			* Select N	Node hongkon	gise	•		
Trusted Cer	rtificates					-			
OCSP Clier	nt Profile		Subject						
Certificate S	Signing Reques	sts		Common Name	(CN) SFODNS				
Certificate F	Periodic Check	Settings							
Certificate /	Authority		0	rganizational Unit (	(OU) Security				
				Organization	n (O) IT				۲
				Cit	ty (L) Kolkata				
				State	(ST) West Be	engal			
				Country	y (C) IN				
			Subject A	Iternative Name (S	SAN)	idress	▼ <u>10.12</u>	27.196.248	
				* Key	type RSA	• •			
				* Key Le	ength 2048	•			
				* Digest to Sign	With SHA-256	Ţ			
				Certificate Pol	licies				]

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
▼ System → Identity Management	Network Resources
Deployment Licensing - Certificate	s ► Logging ► Maintenance Upgrade ► Backup & Restore ► Admin Access ► Settings
0	
✓ Certificate Management	Subject Alternative Name (SAN)
System Certificates	
Trusted Certificates	* Key type RSA 💽 🕧
OCSP Client Profile	* Key Length 2048 🔹 👔
Certificate Signing Requests	
Certificate Periodic Check Settings	* Digest to Sign With SHA-256
Certificate Authority	Certificate Policies
	* Expiration TTL 10 years
	Friendly Name
	Allow Wildcard Certificates
	Usage
	Admin: Use certificate to authenticate the ISE Admin Portal
	EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
	RADIUS DTLS: Use certificate for the RADSec server
	pxGrid: Use certificate for the pxGrid Controller
	SAML: Use certificate for SAML Signing
	Portal: Use for portal
	Submit Cancel

ةفلتخم حيتافم لاوطأ ECDSA و RSA ل ةماعلا حيتافملل نوكي نأ نكمي :**قظحالم** نم ةعقوم ةماع ةداهش ىلع لوصحلا يه ةينلا تناك اذإ 2048 رتخأ .نامألا ىوتسم سفنل CA عم قفاوتم ةسايس ةرادإ ماظنك ISE رشن وأ Cisco ISE رشن وأ

#### ايتاذ ةعقوم ةداەش ديدجت

كل لقتنا ،ةدوجوملا ايتاذ ةعقوملا تاداەشلا ضرعل Administration > System > Certificates > System Certificates يف امركذ مت اذإ 'Issued By'و 'Issued To' عم ةدامش يأ ISE. مكحت ةدجو يف ISE Server FQDN قوف رقناو ،ةدامشلا مذه رتخأ .ايتاذ ةعقوم ةدامش نوكت امنإف ،مسفن FQDN عامتنال (TTL) عاقبلا ةدم نييعتب مق مث Renewal Period نم ققحت ،تجاحلا بسح ةيحالصلا Save.

```
اەب قوثوم ةداەش تيبثت
```

(CA) قدصملا عجرملا نم 64 ساسألل اهزيمرت مت يتلا (تاداهشلا) ةداهشلا ىلع لوصحلا ةقثلل ةبولطملا ةفيضملا ةزهجالا وأ/و طيسولا (CA) قدصملا عجرملا وأ/و رذجلا. 1. يل لقتناو ISE قدقع يل لوخدلا لجس Administration > System > Certificate > Certificate Management > Trusted Certificates قوف رقناو Import، قروصلا هذه يف حضوم وه امك

dentity Ser	vices Engine	Home	Context \	Visibility	<ul> <li>Operations</li> </ul>	s ► Policy	
▼ System ► Ident	tity Management	Network R	esources	Device Po	rtal Managen	nent pxGrid Ser	rvi
Deployment Licer	nsing - Certificate	es 🕨 Logg	ing 🔹 Mai	intenance	Upgrade	Backup & Resto	ore
	•						
	ement	Truste	ed Certific	ates			
System Certificates	S	🦯 Edit	- Import	Export	XDelete	Niew 🔎	
Trusted Certificates	S	E Fri	endly Name			▲ S	Sta
OCSP Client Profile	e	🗆 Ba	ltimore Cybe	erTrust Root			~
Certificate Signing	Requests	Cis	sco CA Manu	facturing		(	0
Certificate Periodic Check Settings		Cis	sco ECC Root	t CA		1	~
	oncon counigo	Cie	sco Licensina	Root CA		1	1

2. لوصحلا مت يتلا قدصملا عجرملا (تاداهش) ةداهش ليمحتب مق ،ةيلاتلا ةحفصلا يف ضرغلا حضوي فصوو اهل فولأم مسا نييعتب مق .(اقباس حضوملا بيترتلا سفنب) اهيلع راسملا ةعباتم لجأ نم ةداهشلا نم.

ل ةرواجملا تاعبرملا ددح ،مادختسالا تاجايتحإ بسح

- نوكت امدنع ةديدج ISE دقع ةفاضإ يف ةزيملا هذه لثمتت ISE لخاد ةقداصملاب ةقثلا اهب صاخلا اهب قوثوملا تاداهشلا نزخم ىلع قلمحم ةقوثوملا CA قداهش سفن اهل.
- ةقداصمل ةداهشلا مادختُسال كلذ نيكمَتُب مقَ syslog وأ/و ليمعلا ةقداصمب ةقثلاً .ةنمآلا syslog مداوخ يف ةقثلاً وأ/و EAP مادختساب ISE ب لصتت يتلاً ةياهنلاً طاقن
- ةمدخ لثم ةيجراخلا Cisco تامدخ يف ةقثلل طقف اذه مزلي Cisco تامدخ ةقداصمل ةقثلا بيولا زجوم.

3. عم اهتنمازمو "هب قوثوملا نزخملا" يف ةيئرم ةداهشلا نوكت نأ نآلا بجي .submit رقنا ،اريخأ دقع عيمج (رشنلا ةلاح يف) ةيوناثلا

dentity Services Engine	Home  ► Context Visibility  ► Operations  ► Policy  ► Administration  ► Work Centers
▼ System  → Identity Management	Network Resources
Deployment Licensing	s   Logging   Maintenance Upgrade   Backup & Restore   Admin Access   Settings
✓ Certificate Management	Import a new Certificate into the Certificate Store
System Certificates	* Certificate File Browse CA certificate.cer
Trusted Certificates	Friendly Name Company CA certificate
OCSP Client Profile	Trusted For: 👔
Certificate Signing Requests	Trust for authentication within ISE
Certificate Periodic Check Settings	Trust for client authentication and System
Certificate Authority	Trust for authentication of Cisco Services
	Validate Certificate Extensions
	Description
	Submt Cancel

#### CA نم ةعقوم ةداەش تيبثت

،ەب قوثوملا تاداەشلا نزخم ىلإ طسوتملاو رذجلا (CA) قدصملا عجرملا تاداەش ةفاضإ درجمب، CSR ىلإ ةدنتسملا ةعقوملا ةداەشلا طبر نكميو (CSR) ةداەشلا عيقوت بلط رادصإ نكمي CSR قدقعب iSE. ةدقعب

1. رقنا مث Administration > System > Certificates > Certificate Signing Requests دقنا مث Generate Certificate Signing Requests (CSR) عاشنإل CSR.

2. نم ەمادختسإ متيس يذلا رودلا رتخأ ،"مادختسالا" مسق نمض ،رەظت يتلا ةحفصلا يف قادسنملا ةمئاقلا.

نكمي ،ةداەشلا ءاشنا درجمب .ددعتم مادختسإ رتخأ ،ةددعتم راودأل ةمدختسم ةداەشلا تناك اذا اەمادختسا متېل ةداەشلا نېيعت نكمي ،تالاحلا مظعم يف .رمألا مزل اذإ راودألا رېيغت ةداەشلا نوكت نأب حمسي اذەو ؛ةمدختسملا ةلدسنملا ةمئاقلا يف ددعتملا مادختسالل ISE.

.اەل ةداەشلا ءاشنإ متي يتلا (دقعلا) ةدقعلا رايتخال ISE (تادحو) ةدقعل رواجملا عبرملا ددح .3

.عبرم Allow Wildcard Certificates نم قرقحتف ،لدب فرح ةداهش ءاشن|/تيبثت وه ضرغلا ناك اذا .4

disco Ide	ntity Services Engine	Home	tions   Policy	Administration	Work Centers	
- System	Identity Management	Network Resources Device Portal Mana	gement pxGrid Services	Feed Service	Threat Centric NAC	
Deployme	nt Licensing - Certificates	→ Logging → Maintenance Upgrade	<ul> <li>Backup &amp; Restore</li> </ul>	Admin Access	<ul> <li>Settings</li> </ul>	
Deployme Certificat System ( Trusted ( OCSP C Certificat Certificat	nt Licensing Certificates	<ul> <li>Logging Maintenance Upgrade</li> <li>Certificate Signing Request</li> <li>Certificate types will require different</li> <li>ISE Identity Certificates:</li> <li>Multi-Use (Admin, EAP, Portal</li> <li>Admin - Server Authentication</li> <li>EAP Authentication - Server A</li> <li>DTLS Authentication - Server A</li> <li>DTLS Authentication - Server Authentication</li> <li>portal - Server Authentication</li> <li>portal - Server Authentication</li> <li>SAML - SAML Signing Certificat</li> <li>ISE Messaging Service - This</li> <li>ISE Root CA - This is not a si</li> <li>SE Intermediate CA - This is</li> <li>Renew ISE OCSP Responde</li> <li>ISE Root CA/ISE Intermediate</li> <li>Usage</li> <li>Certificate(s) wil be used for Mutation</li> </ul>	Backup & Restore      Action Act	Admin Access Admin Access ist below outlines with r Authentication ut an ability to generat to generate a brand g Request. signing request, bu	<ul> <li>Settings</li> <li>hich extended key usages are required f</li> <li>ate a brand new Messaging certificate.</li> <li>I new Root CA certificate for the ISE CA</li> <li>It an ability to renew the OCSP responder</li> <li>You can use a single certificate for n doing so is not a recommended prac should obtain individual certificates as service (for example, one certificates</li> </ul>	for each certificate type: functionality. er certificate that is signed by the nultiple services, but trice. Rather, you pecifically for each each for Guest
		Allow Wildcard Certificates	D		Portals, EAP, and pxGrid).	
		Node	C	SR Friendly Name		
		hongkongise	h	ongkongise#Multi-Us	se	
Usage				_		
Cert	tificate(s) will be used fo	or Multi-Use Multi-Use Admin EAP Authentication	-	You car doing so should o service Portals,	n use a single certificate for o is not a recommended pra obtain individual certificates s (for example, one certificat EAP, and pxGrid).	multiple services, but actice. Rather, you specifically for each e each for Guest
Allov	v Wildcard Certificates	RADIUS DTLS Portal		,		
Node(s	)	ISE Messaging Service				
Gene	rate CSR's for these N	ode SAML				
		ISE Root CA				
Nod	le	ISE Intermediate CA		2		

hongkongise

hongkongise#Multi-Use

ةدحولا) ةمظنملا وأ فيضملاب ةقلعتملا ليصافتلا ىلا ادانتسا عوضوملا تامولعم ألما .5 (دلبلاو ،ةلودلا ،ةنيدملا ،ةمظنملا ،ةيميظنتلا

6. يتأي يذلا قثبنملا ىلع Export رقنا مث Generate، قوف رقنا ،اذه ءاهنإل.

Renew ISE OCSP Responder Certificates

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
▼System → Identity Management →	Network Resources	
Deployment Licensing - Certificates	► Logging ► Maintenance Upgrade ► Backup & Restore ► Admin Access ► Settings	
Certificate Management     System Certificates     Trusted Certificates	✓ hongkongise hongkongise#Multi-Use Subject	
OCSP Client Profile	Common Name (CN) <b>\$FQDN\$</b>	
Certificate Signing Requests		
Certificate Periodic Check Settings		
Certificate Authority	Organization (O) IT	
	City (L) Kolkata	
	State (ST) West Bengal	
	Country (C)	
	Subject Alternative Name (SAN)	<b>i</b> )
	* Key type RSA 🝸 🕡	
	* Key Length 2048.	
	* Digest to Sign With SHA-256	
	Certificate Policies	
	Generate	
Country (C	C) IN	
Subject Alternative Name (SAM	N) DNS Name	
* Key typ	De RE IP Address Uniform Resource Identifier	
* Key Leng	th 2048	
* Disset to Diss Mit		

اذه PEM فلم لاسرا بجي - وتلل هؤاشنا مت Base-64 ىلإ زمرم ةداهش بلط ليزنتب اذه موقي قداهش فلم ىلع لوصحلاو ،عيقوتلل CA ىلإ Base 64).

.دقعلل FQDN ءلمب ايئاقلت CN لقحب صاخلا ISE موقي :**ةظحالم** 

مادختسال لقألاا ىلع CSR يحلطصم رادصإ ابولطم ناك ،1.4 و ISE 1.3 يف :**قظحالم** pxGrid. ىلع اذه لك ،هدعب امو 2.0 ذنم .تامدخلا ةيقبل ،رخآلاو ،PXgrid ل صصخم امهدحأ CSR .دحاو CN لقح يف '\*' زمرلا نوكي الأ بجي ،EAP ةقداصمل ةداەشلا مادختسإ ةلباح يف :**قظحالم** Verify ليطعت دنع ىتح .مداخلا ةداەش نوضفري Windows يلومم نإ ثيح عوضوملل قحفاصم لشفت نأ نكمي ،بولطملا ىلع (مداخلا ةيوه ةحص نم ققحتلا) Server Identity مادختسإ نكمي ،كلذ نم الدبو .CN لقح يف '\*' نوكي امدنع SSL SSL لقح يف ماع FQDN مادختسإ نكمي ،كلذ نم الدبو .CN لقح يف '\*' نوكي امدنع CN، تاداەشلا عجارم ضعبل نكمي SAN DNS مسا لقح يف همادختسإ نكمي (CA) مثل SSL يف الا عجارم ضعبل نكمي .SAN DNS مسا لقح يف همادختسا نكمي .ac

7. بويديفلا يف حضوم وه امك CSR نم اهؤاشنا مت يتلاا) CA لبق نم ةداهشلا عيقوت درجمب. ىلإ لقتناو ،(ISE) ةيموسرلا مدختسملا ةهجاو ىلإ لقتنا ،(Microsoft CA مادختسا مت اذإ <u>انه</u> ىلإ لقتناو ،(ISE) درواجملا عبرملا ددح ؛**قداهشلا عيقوت بلط < قداهشلا قرادا < تاداهشلا < ماظنلا < قرادالا** CSR ل رواجمل عبرمل ددح ؛**قداهشلا عيقوت بلط < قداهشلا قرادا < تاداهشلا < ماظنل**ا < قرادالا



8. ال افولأم امسا اهطعأو ،وتـلل اهيقلت مت يتلا ةعقوملا ةداهشلا ليمحتب مق ،كلذ دعب. و Admin ةقداصم لثم) ةداهشلل ةجاحلا بسح تامادختسالل ةرواجملا تاعبرملا رايتخإ عبات مث EAP، قروصلا هذه يف حضوم وه امك Submit، رقناو (كلذ ىلإ امو ،لخدملاو عالي الع



اەتامدخ ليغشت ةداعإب ISE ةدقع موقت نأ بجيف ،ةداەشلا ەذەل "لوؤسملا رود" رايتخإ مت اذا ققيقد 15 ىلإ 10 نم كلذ قرغتسې دق ،VN ل ةصصخملا دراوملاو رادصإلا ىلإ ادانتسا. مألا ردصاو ISE رماوأ رطس حتفا ،قيبطتلا قلاح نم ققحتلل ise erasecat4000\_flash:.



Device Portel	Annarament - puCrid Caprison - L. Faced Caprison - L. Threat Captris NAC	Click here to c
nance 🕂	The Portal tag is already assigned to the following certificate(s). If you proceed, it will be removed from the existing certificates, and affected portals will be restarted. Do you want to proceed? • Default self-signed server certificate	
rtificat		
Certificate	No Yes	
riendly Name	Company Signed Cert	
Extensions		

ةداەشلاا نأ نم ققرحتلا نكمي ،ةداەشلا داريتسإ دنع لخدملا وأ لوؤسملا رود رايتخإ مت اذا زمر رتخأ .ضرعتسملا يف لخدملا تاحفص وأ لوؤسملا ىلإ لوصولا دنع ةدوجوم ةديدجلا ةدوجوملا ةلماكلا ةلسلسلا نم راسملا ققرحتي ،صيخرتلا تحتو حفصتملا يف نيمأتلا لخدملا وأ لوؤسملا ةداەش يف ضرعتسملا قثي نأ بجي .زاهجلا لبق نم اەب قوثوملاو ةلسلس يف قثي ضرعتسملا ناك اذاو حيحص لكشب ةلسلسلا ءاشنإ مت املاط ةديدجلا

#### ةصاخلا حيتافملاو يطايتحالا خسنلا تاداهش

#### ريدصتلاب یصوي:

ا مزلي) ةصاخلا اهحيتافم ىل قفاض لاب (رشنلا يف دقعلا عيمج نم) ماظنلا تاداهش عيمج . مت يتلا ةمدخلا) ةداهشلا نيوكتل ةظحالمب ظافتحالا .نمآ عقوم ىل (اهتيبثت ةداع (اهل ةداهشلا مادختس).

ظافتحالا. .ةيساسألا ةرادإلا ةدقعل اهب قوثوملا تاداهشلا نزخم نم تاداهشلا ةفاك .2 (اهل ةداهشلا مادختسإ مت يتلا ةمدخلا) ةداهشلا نيوكتل ةظحالمب. .تاداەشلا ةئيە تاداەش عيمج .3

،كلذب مايقللو

- 1. رتخأ Administration > System > Certificates > Certificate Management > System Certificates. رتخأ قملك لخدأ .قصاخلا حيتافملا ءاقتنا رزو Export Certificates راتخن Export. رقناو صيخرتلا وينا .رورملا قملك ديكأتب مقو صاخلا حاتفملا رورم
- 2. رتخأ Administration > System > Certificates > Certificate Management > Trusted Certificates. رتخأ قداەشلا ريدصتل Save File رقناو صيخرتلا.
- 3. رتخأ Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. كلإ لقتنا ةمرك لخدأ .ةصاخلا حيتافمرا ءاقتنا رزو Export Certificates راتخن Export. رقناو صيخرترا ريدصتل Save File رقنا. رورملا قمرك ديكأتب مقو صاخلا حاتفمرا رورم قداهشرا

### اهحالصإو ءاطخألا فاشكتسا

#### ةداەشلا ةحص نم ققحتلا

وأ ماظنلاا تاداهش نزخم يف ةداهش يأ ةيحالص ءاهتنا ةلاح يف ةيقرتلا ةيلمع لشفت ءاهتنا خيرات لقح يف ةيحالصلا نم ققحتلا نم دكأت .Cisco نم اهب قوثوملا ISE تاداهش < Administration > System > Certificates) ماظنلا تاداهشو اهب قوثوملا تاداهشلا تاراطإل ةيحالصلا Certificate Management)، مايزلا ا مزل اذإ ،اهديدجتو ،

تاداهش ةذفان يف ةدوجوملا تاداهشلل ةيحالصلا ءاهتنا خيرات لقح يف ةيحالصلا اضياً عجار قدصملا عجرملا (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)، قيقرتلا لبق ،رمألا مزل اذإ ،اهديدجتو.

#### ةداەش ڧذح

ريدصت نم دكأت .اەتلازا مزلي ،اەمادختسا مدع وأ ISE يف ةداەش ةيحالص ءاەتنا ةلاح يف فذحلا لبق (نكمأ نإ ،ةصاخلا اەحيتافمب) تاداەشلا.

كل لقتنا ،ةيحالصلا ةيەتنم ةداەش فذحل Administration > System > Certificates > Certificate Management. رقناو اەتيحالص تەتنا يتلا (تاداەشلا) ةداەشلا رتخأ System Certificates Store. قوف رقنا Delete. قوف عجارملاو قلوخملا تاداەشلا نزاخمل ئيشلا سفن عجار.

#### ISE ةقداصم يف ISE مداخ ةداهش بلاط قثي ال

.SSL ةحفاصم ةيلمعل ةلماكلا تاداهشلا ةلسلس لسري ISE ناك اذإ امم ققحت

يف مداخلاا ةيوه نم ققحتلاو (PEAP يأ) مداخ ةداهش بلطتت يتلا EAP بيلاسأ ديدحت عم تاداهشلاب تاداهشلا قلسلس نم بلطلا مدقم ققحتي ،ليمعلا ليغشت ماظن تادادعإ قحفاصم ةيلمع نم ءزجك .ةقداصملا ةيلمع نم ءزجك يلحملا ةقثلا نزخم يف هيدل ةدوجوملا ال .هب قصاخلا قلسلسلا يف قدوجوم طيسو وأ/و رذج تاداهش يأ كلذكو هتداهش ISE مدقي ، SSL مدقي ، SSL ال .هب قصاخلا قلسلسلا يف قدوجوم طيسو وأ/و رذج تاداهش ي كا فلاكو هتداهش ال .هب تناك اذا وأ قلماك ريغ قلسلسلا تناك اذا مداخلا قيوه نم ققحتان ان م بل اطملا نكمتي

< ISE (Operations نم ةمزح طاقتلا ذخأب مق ،ليمعلا ىلإ تاداهشلا ةلسلس ةداعإ نم ققحتلل

Diagnostic Tools > General Tools > TCP Dump) طاقتلا وأ Wireshark تقو يف ةياهنلا ةطقن ىلع Wireshark طاقتلا وأ Wireshark ةكرش يف SsI.handshake.certificates حشرملا قيبطتب مقو طاقتلالا حتفا .ةقداصملا لوصولا يدحت ىلع روثعلاو.

رايتخال درجمب، القتنا، رايتخال درجمب Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates.

ققحتلاو ISE Administration > Certificates > Trusted Certificates القتنا ،ةلماك ريغ ةلسلسلا تناك اذإ بجي ،حاجنب تاداهشلا ةلسلس ريرمت ةلاح يف .ةطيسولا تاداهشلا وأ/و رذجلا تاداهش دوجو نم انه ةحضوملا ةقيرطلل اقفو اهسفن ةلسلسل اقحص نم ققحتلا.

حاتفم فرعم ةقباطمل ةقثلا ةلسلس نم ققحتو (رذجو ،طسوتم ،مداخ) ةداهش لك حتفا يف ةيلاتلا ةداهشلل (AKI) ةطلسلا حاتفم فرعم ىلا ةداهش لكل (SKI) عوضوملا قلسلسلا.

#### ءانثأ ISE مداخ ةداەش ضڧرت ةياەنلا ةطقن نكلو ةحيحص ISE ةداەش ةلسلس ةقداصملا

ةلسلس ضفري سمتلملا لظو SSL ةحفاصمل ةلماك تاصيخرت ةلسلس ISE مدق اذإ يف ةدوجوم ةطيسولا وأ/و رذجلا تاداهشلا نأ نم ققحتلا يه ةيلاتلا ةوطخلا نإف ،تاداهشلا يلحملا ينامئتسالا ءالمعلا نزخم.

نام ققحتال Windows، ليغشتب مق mmc.exe(Microsoft Management Console)، رقى تارك سترية المارك المعنية المارك المع رقناو Certificates رتخأ ،رفوتملا قيفاضإلا تاودألا دومع نم Certificates رتخأ ،رفوتملا قيفاضإلا تاودألا دومع نم مدختسمل اققداصمل عون ىلإ ادانتسا Computer account وأ My user account امإ رتخأ مدختسم) والما مثر (زامج وأ مدختسم)

قيدصتلا تاطلسو اهب قوثوملا رذجلا ةقداصم عجارم رتخأ ،مكحتلا ةدحو ضرع تحت .يلحملا ةقثلا نزخم يف طسوتملاو رذجلا تاداهشلا دوجو نم ققحتلل ةطسوتملا

نم ققحتلا ءاغلإب مق ،مداخلا ةيوه نم ققحتلا يف ةلكشم هذه نأ نم ققحتلل ةلهس ةقيرط ىرخأ ةرم اهربتخا مث بولطملا فيرعتلا فلم نيوكت تحت مداخلا ةداهش ةحص.

### ةرركتملا ةلئسألا

#### ةدوجوم ةداەشلا نأب ريذحت ەيجوتب ISE موقي امدنع ەلعف بجي يذلا ام كلعفلاب

تمت دقو ،طبضلاب OU ةملعم سفن اهل ماظن ةداهش نع تفشك ISE نأ ةلاسرلا هذه ينعت ةطاسبب حصني ،ةموعدم ريغ ةرركملا ماظنلا ةداهش نأ امب .ةرركم ةداهش تيبثت ةلواحم ةداهشلا نأ نامضل اليلق ةفلتخم ةميق ىلإ مسقلا/ةلاحلا/ةنيدملا ميق نم يأ رييغتب .ةفلتخم قديدجلا

#### ا نم لخدملا ةحفص نأ ىلٍ ريشي ريذحت ەيجوتب ضرعتسملا موقي اذامل ISE ؟ەب قوثوم ريغ مداخ ةطساوب ةمدقم

مداخلا ةيوه ةداهشب ضرعتسملا قثي ال امدنع كلذ ثدحي.

اەنيوكت متو اعقوتم ناك ام يە ضرعتسملا ىلع ةيئرملا ةباوبلا ةداەش نأ نم دكأت ،الوأ قباوبلل ISE ىلع.

َنم دكأت ،مادختسالا ديق IP ناونع ةلاح يف - FQDN ربع ةباوبلا ىلا لوصولا نم دكأت ،ايناتُ نم لك دوجو IP ناونعو SAN وأ/و SAN يلقح يف IP ناونعو FQDN نم لك دوجو

CA تاداەش ،طيسولا (أي أي أي الخدم) ةباوبلا تاداەش ةَلْسلس داريَتسا نم دكأت ،اريخَأو ليمعلاب صاخلا ضرعتسملا/ليغشتلا ماظن جمانرب ةطساوب اەب قوثوم/ىلع (رذجلا.

اهل Chrome/Firefox و Android OS تاحفصتم نم ثدحألا تارادصإلا ضعب :**قظحالم** لاصتالا ضفر اهنكميف ،طاقنلا هذه ةيبلت مت اذإ ىتح .قداهشلل قمراص نامأ تاعقوت SHA-256. نم لقأ قطيسولا CAs و Portal قميق تناك اذإ

#### ؟ةحلاصلا ريغ تاداهشلا ببسب ةيقرتلا لشف دنع هلعف بجي يذلا ام

وأ ماظنلاا تاداهش نزخم يف ةداهش يأ ةيحالص ءاهتنا ةلاح يف ةيقرتلا ةيلمع لشفت ءاهتنا خيرات لقح يف ةيحالصلا نم ققحتلا نم دكأت .Cisco نم اهب قوثوملا ISE تاداهش حملا تاداهش (Administration > System > Certificates ما ما ما فال ما ما فال ما ما في المالات Certificate Management)، ماظنلا لبق ،رمألا مزل اذإ ،اهديدجتو ،(Certificate Management)،

تاداهش ةذفان يف ةدوجوملا تاداهشلل ةيحالصلا ءاهتنا خيرات لقح يف ةيحالصلا اضياً عجار قدصملا عجرملا (Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates)، قيقرتلا لبق ،رمألا مزل اذإ ،اهديدجتو.

.ةيلخادلا CA تاداەش ةلسلس ةحص نم دكأت ،ISE ةيقرت لبق

ىلإ لقتنا Administration > System > Certificates > Certificate Authority Certificates. كل لقتنا فولأملا مسالا دومع يف تاداهشلا تامدخ ةياهن ةطقنل يعرفلا قدصملا عجرملا تاذ ةداهشلا. قيئرمو ةديج قلاسر قداهشلا قلاح تناك اذإ امم ققحتو View رقنا

ل أ نم .ةيلمع نيسحت cisco ISE لا نأ لبق رادصإلا تبثي نأ تنمض ،ترسك ةداهش يأ نإ مل عن المن المراح ال

### ةلص تاذ تامولعم

- <u>تاداەشلا نزخم تادادعاو تاداەشلا قرادا ISE 2.7</u> •
- <u>ISE يف ةيمقرلا تاداەشلا ذيفنت</u> •
- <u>Cisco Systems تادنتسملاو ينقتلا معدلا</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما