

ISE في TLS/SSL تاداهش نيوكت

تايوتحمل

[قمدقمل](#)

[قيساسأل تابلطتمل](#)

[تابلطتمل](#)

[قمدختسمل تانوكمل](#)

[مداخل تاداهش](#)

[ISE تاداهش](#)

[ماظنل تاداهش](#)

[اهب قووثومل تاداهشل نزم](#)

[قيساسأل مامل](#)

[ايتاذ قوقوم قداهش عاشنا](#)

[ايتاذ قوقوم قداهش ديذجت](#)

[اهب قووثوم قداهش تيبتت](#)

[CA نم قوقوم قداهش تيبتت](#)

[قصاخل حيتافل او يطايتحال خسنل تاداهش](#)

[احالصل او عاخال فاشكتسا](#)

[قداهشل قحص نم ققحتل](#)

[قداهش فذح](#)

[802.1x ققداصم في ISE مداخ قداهش بلاط قثي ال](#)

[ققداصملا اناثأ ISE مداخ قداهش ضفرت قياهنل عطقن نكلو قححص ISE قداهش قلسلس](#)

[قركتمل قلائسأل](#)

[قلفلاب قدوجوم قداهشل ناب هيبتت هيچوتب ISE موقوي امذنع هلغف بجي يذلا ام](#)

[قطساوب قمدقم ISE نم لخدمل قحفص نأ ل ريشي ريذحت هيچوتب ضرعتسمل موقوي اذامل
قهب قووثوم ريغ مداخ](#)

[قحلصل ريغ تاداهشل ببسب قيقرتل لشف ذنع هلغف بجي يذلا ام](#)

[قلص تاذ تامولعم](#)

قمدقمل

قيفيكو، ISE تاداهش راودأو عاونأو، Cisco ISE في TLS/SSL تاداهش دننتمل اذه فصفي
قوادتمل قلائسأل لعل تابلجال او، احوالصل او عاخال فاشكتساو قعئاشل مامل ذي فنن

قيساسأل تابلطتمل

تابلطتمل

قيلال عيضاوملاب قفرعم كيدل نوكت ناب Cisco قيصوت:

1. Cisco (ISE) نم قيوهل تامدخ كرحم
2. AAA و ISE رشن تايلمع نم قفلتخم عاونأ فصول قمدختسمل تاحلطصمل
3. AAA تايساسأو أو RADIUS لوكتورب
4. x509 و SSL/TLS تاداهش

(PKI) ماعلاجات فملا لسياسا ألي نبال تايساسا 5.

ةمدختس م تانوكملا

نم 2.4 - 2.7 تارادصا او، Cisco ISE تارادصا لى دن تس م اذ ه ي ف ة دراو لا تامول عمل دن تست نوكي نا ب جي، كلذ عمو، 2.7 لى 2.4 رادصا لى نم ISE يطغي وهو. ةمدختس م تانوكملا او جماربلا كلذ فالخ لى صني مل ام ISE 2.x نم ىرخا لى جماربلا تارادصا لى اقباطم و الاثام

ةصاخ ةيلم عم ةئيب ي ف ةدوجوملا ةزهجال نم دن تس م اذ ه ي ف ة دراو لا تامول عمل عاشن ا م تناك اذ ا. (يضا رتفا) حوسم م نيوك ت ب دن تس م اذ ه ي ف ةمدختس م ةزهجال ا عي مج ت اذ ب رم ا لى ل م ت ح م ل ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل د ي ق ك ت ك ت ب ش

مداخلا تاداهش

اهتلاصا لى لى لوصحلل ماعلا م داخلا ةي وه م ي د ق ت ل مداخلا تاداهش مداخلا م دختس ت ةداهش لى مداخلا ردي شي) ايتاذ ةعقوم هذ ه نوك ت نا نكمي. لاصتال ةنما ةانق ري فوتلو (فورعم دروم نم و ا ةسس و م ل ل ي ل خ ا د ا م ا) ق د ص م ع ج ر م ن م ة ر د ا ص و ا (هس فنل

لهوملا لاجملا مسا) FQDN و ا فيض م ا م س ا لى لى ج ذوم ن ل ك ش ب مداخلا تاداهش رادصا م تي و ا (فيض م ل) فيض م ل (.domain.com*) ل د ب فرح ةداهش اضيا نوك ت نا نكمي و ا ، مداخلا ل (لمك ل اب (مسالا) مسالا) يلقح ي ف صاخ ل ك ش ب روك ذم ه ل ل ا رادصا م تي ي ذل ا ي عرف ل ل ا ج م ل و ا ل ا ج م ل (SAN) لى د ب ل ا ع و و م ل م س ا و ا (CN) عئاش ل

مسا نم ال د ب ةي م جن ةمالع) ل د ب فرح نيودت م دختس ت SSL تاداهش ي ه ل د ب ل فرح ا تاداهش ةسس و م ي ف ني د د ع ت م ني فيض م ر ب ع ةداهش ل س فن ة ك ر ا ش م ب ح م س ت ي ل ا ت ل اب و (فيض م ل) ع و و م ل م س ا ل د ب ل فرح ا تاداهش ل SAN و ا CN ةمي ق و د ب ت نا نكمي ، ل ا ث م ل ل ي ب س لى لى server1.com، ل ث م ل ا ج م ل ا ذ ه ل ني فيض م ي ا ني م ا ت ل ه م ا د خ ت س ا ن ك م ي و *.company.com ل ل ث ا م م ا ذ ك ه و ، server2.com.

ل. ل ا ث م ت م ل ر ي غ ر ي ف ش ت ل و ا م ا ع ل ا ح ا ت ف م ل ر ي ف ش ت ة د ا ع ت ا د ا ه ش ل م د خ ت س ت

- هت ك ر ا ش م م ت ي و ، ل و ق ح ل ا د ح ا ي ف ة د ا ه ش ل ا ي ف ا د و ج و م م ا ع ل ا ح ا ت ف م ل ن و ك ي : م ا ع ل ا ح ا ت ف م ل . ه ب ل ا ص ت ا ل ا م ز ا ه ج ل و ا ح ي ا م د ن ع م ا ط ن ة ط س ا و ب م ا ع ل ك ش ب
- ن ك م ي . م ا ع ل ا ح ا ت ف م ل ا ب ن ر ت ق ي و ي ة ا ه ن ل ا م ا ط ن ل ا ب ص ا خ ص ا خ ل ا ح ا ت ف م ل : ص ا خ ل ا ح ا ت ف م ل . ص ا خ ل ا ح ا ت ف م ل ا ط س ا و ب ط ق ف م ا ع ح ا ت ف م ا ط س ا و ب ة ر ف ش م ل ا ن ا ي ب ل ر ي ف ش ت ك ف س ك ع ل ا ب س ك ع ل ا و د د ح م ل ا ج و د ز م ل ا

ISE تاداهش

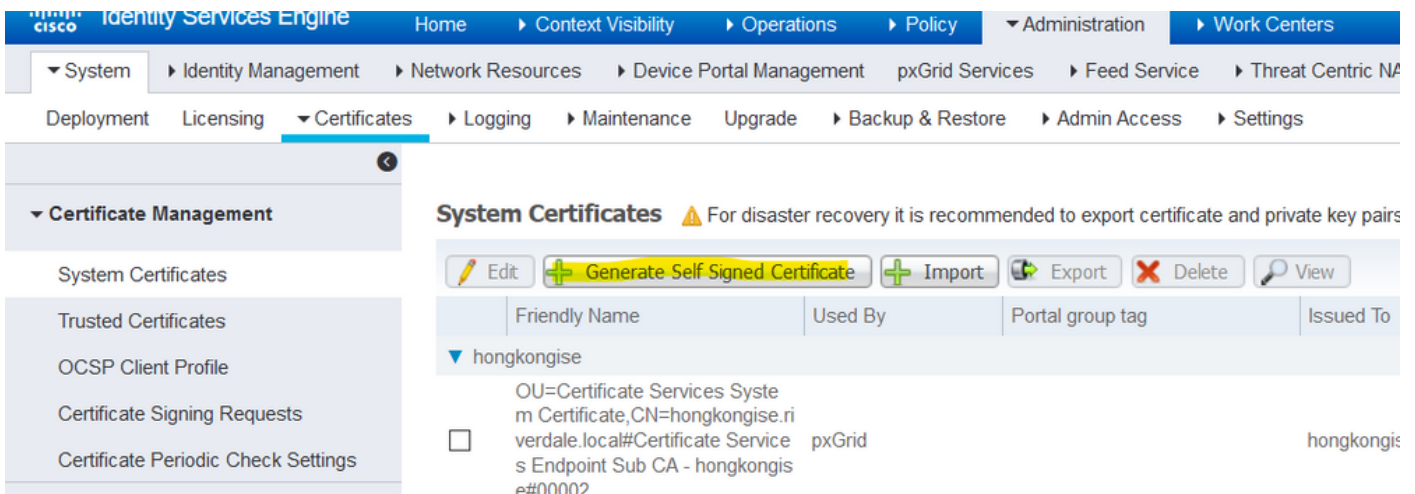
طاقن عم نم ا لاصت ا ري فوتل (PKI) ماعلاجات فملا لسياسا ألي نبال لى لى Cisco ISE دم تعي ددعت م رشن ي ف Cisco ISE دق نيب كلذكو، كلذ لى امو ني راد ا ل ا و ني م دختس م ل ا و ةي ا ه ن ل ا ري ف ش ت ل ة م ا ع ل ا ح ا ت ا ف م ل ل ق ن ل X.509 ل ةمي ق ر ل ا تاداهش لى لى PKI دم تعت . تايس ن ج ل ا ني م دختس م ل نم ةمدقملا ىرخا لى تاداهش ل ا لاصا نم ق ق ح ت ل ل و ، ا ه ر ي ف ش ت ك ف و ل ل ا س ر ل ا ة د ا ع ة م د خ ت س م ل ا ت ا د ا ه ش ل ا ن م ن ي ت ئ ي ف لى لى Cisco ISE ي و ت ح ي . ةزهجال او

إذا. ام. عطقن دنع اهلا دبت ساب ةبل لاطملا واهلا طب انكم يو ةي حالص اهتنا خيرات ةداهش لل ةداهش اهلا دبت سا م تي مل ام ةري طخ تال كشم رهظت دق ف، ISE مداخ ةداهش ةي حالص تهتنا ةحالص ةديج.

(EAP)، عسوت ملة قداصملا لوكوت و ربل ةمدختسملا ةداهشلا ةي حالص تهتنا اذا: **ةظحال**، ةلاح يف. نألا دعب ISE ةداهش ب قثي ال لي معةل نأل االمعلا ةقداصم لشفت دق ضفر تاضرعتسملا و االمعلا نكمي، لخادم لل مدختست ةداهش ةي حالص اهتنا رطاخملا نوكت، لوؤسملا مادختسا ةداهش ةي حالص اهتنا ةلاح يف. لخدملاب لاصتال رشنل فقوتي نأ نكمي و نألا دعب ISE لي لوخدلا لي جست نم لوؤسملا عنمي ام ربكأ ب. جي امك لمعلا نع عزوملا

ايتاذ ةعقوم ةداهش عاشن

Administration > System > Certificates > System
 قوف رقنا Generate Self Signed Certificate.



ايتاذ ةعقوم ةداهش عاشن ةحفص يف ةدوجوملا لوقحلا ةمئاقلا هذه فرصت.

ايتاذ ةعقوملا ةداهشلا تاداعل ل قح مسا مادختسا تاداشرا

- ماظنلا ةداهش عاشن ال اهلي جاتحت ي تال ةدقعل (ةبولطم): ةدقعل دح.
- CN ف، يضارثفا لكش ب ((SAN) نيزختلا ةقطنم ةكبش ديدحت متي مل اذا بولطم): CN اهلا ي تاذل عي قوتل ةداهش عاشن متي ي تال ISE ةدقعل FQDN ه.
- ةسدنهل، لاثملا ل ب س يلع، ةيم يظنتلا ةدحول مسا: ةيم يظنتلا ةدحول.
- لاثملا ل ب س يلع، ةس س ؤملا مسا (O): ةس س ؤملا.
- ه س و ن اس، لاثملا ل ب س يلع، ةني دمل مسا (ر ص ت خ ت ال): (J) ةني دمل.
- اي ن ر و في ل ل اك، لاثملا ل ب س يلع، ةي ال اول مسا (ر ص ت خ ت ال): (ST) ةي ال اول.
- لاثملا ل ب س يلع. ني فرحلا يذ ISO دلبل زمر لاخدا مزلي. دلبل مسا (ج): دلبل، ةدحتل تايال اول.
- (URI) دحول دراوملا فرعم و DNS مسا و IP ناوع (SAN) نيزختلا ةقطنم ةكبش ةداهشلاب نرتقملا.
- و RSA: امال جاتفملا عاشن ال اهم ادختسا متي س ي تال ةيم زراوخل دح: جاتفملا عون ECDSA.
- و RSA: 512 1024 2048 ل تارايخل هذه رفوتت. امال جاتفملا تبال م ج دح: جاتفملا لوط و ECDSA: 256 384 ل ةرفوتم تارايخل هذه و 4096.

- هذه ةئزجتلا تايمزراوخ دحاً رتخاً: مادختساب عي قوتلل صخلم
- اهم قفاوتت نأ بجي يتلا OID تافرع م ةمئاق وأ ةداهشلا جهن فرعم لخدأ: ةداهشلا جهن ةيصلال ةزهجال تافرع لمصفل تافاسملا وأ لصاوفال مدختسا. ةداهشلا
- ةداهشلا ةيصالص اه دع ب يه تنت يتلا مايألا ددع دح: ةيصالص اهت نا ةدم
- موقت Cisco ISE نإف ،مسا دي دحت متي مل اذا. ةداهشلل افولأم امسا لخدأ: فولأم مسا تاناخ سمخ نم ديرف مقرر وه نيأ قي سننتلاب مسا عاشنإب ايئاق لت
- اي تاذ ةعقوم لدب فرح ةداهش عاشنإل هذه راي تخالال ةناخ دح: لدبلا فرح تاداهشب حامسلا ةكبش يف DNS مسا وأ/و عوضوملا يف CN يأي ف (*) ةي مجن ةمالع يلع يوتحت ةداهش) هني عت مت يذل DNS مسا نوكي نأ نكمي ،لاثملا ل يبس يلع (SAN) ني زختلا ةقطنم ل SAN *.domain.com.
- يه ةحاتملا تارايلال. اهل هذه ماظنلا ةداهش مادختسا بجي يتلا ةمدخلال رتخاً: مادختسالا ةبوابل ماس EAPRADIUS DTLSpGrid ةقداصل م لوؤس مالا

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

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 Settings

► Certificate Authority

Generate Self Signed Certificate

* Select Node

Subject

Common Name (CN)

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN)

* Key type

* Key Length

* Digest to Sign With

Certificate Policies

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

OCSF Client Profile

Certificate Signing Requests

Certificate Periodic Check Settings

Certificate Authority

Subject Alternative Name (SAN) IP Address 10.127.196.248

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

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

فعلتخم حيتافم لاوطأ ECDSA و RSA ل عماعلا حيتافم لل نوكي نأ نكمي: **ةظحالم**
 نم ةعقوم عماع ةداهش لعل لوصحلل يه ةينل تناك اذا 2048 رتخأ. نامألا يوتسم سفنل
 فIPS عم قفاوتم ةسايس ةرادإ ماظنك Cisco ISE رشن وأ CA.

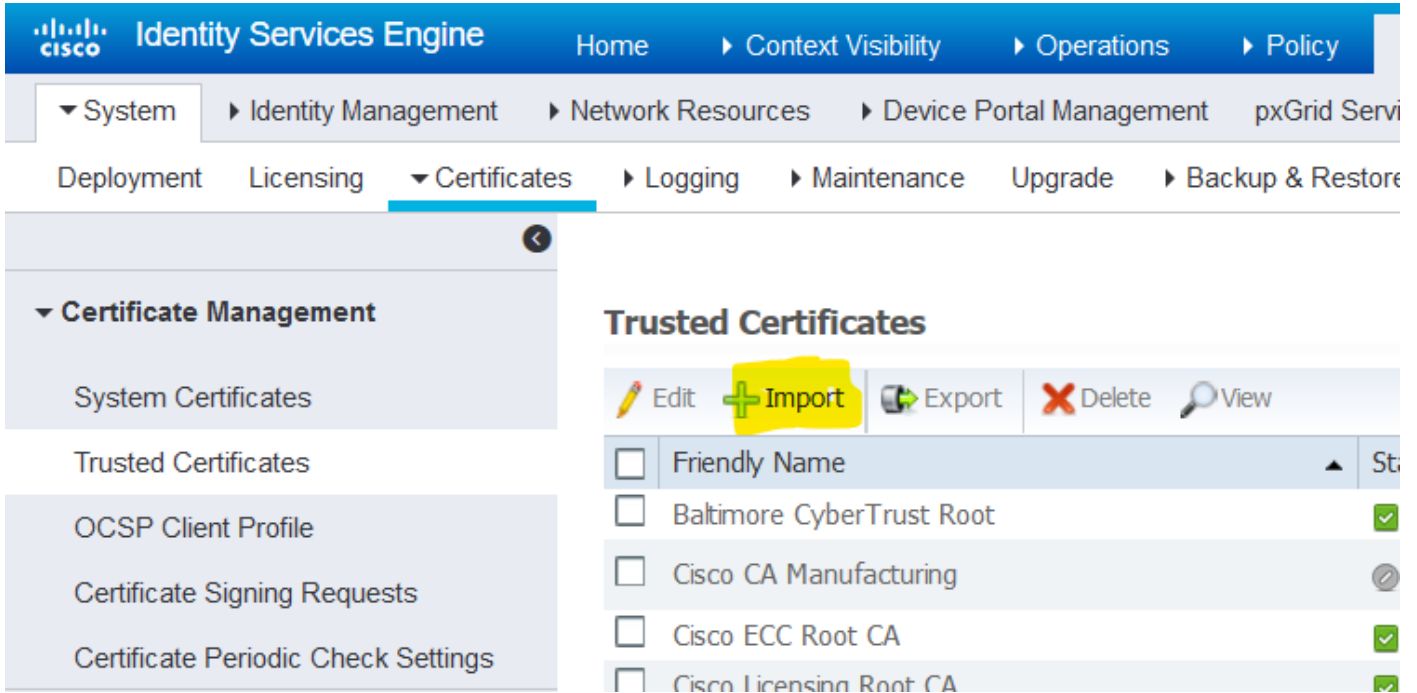
ايتاذ ةعقوم ةداهش ديذجت

Administration > System > Certificates > System Certificates
 ISE Server يف اهركد مت اذا 'Issued To' و 'Issued By' عم ةداهش ي. ISE مكحت ةدحو يف Certificates
 Edit. قوف رقناو، ةداهشلا هذه رتخأ. ايتاذ ةعقوم ةداهش نوكت اهنإف، هسفن FQDN
 اءاتنال (TTL) عاقبالا ةدم نييعتب مق مث Renewal Period نم ققحت، Renew Self Signed Certificate تحت
 Save. رقنا، اريخأ. ةجالحل بسح ةيحلصل.

اهب قووم ةداهش تيبتت

(CA) قوصملا عجرملا نم 64 ساسألل اهزيمرت مت يتلا (تاداهشلا) ةداهشلا لعل لوصحلل
 ةقتلل ةبولطملا ةفيضملا ةزهجالا وأو طيسولا (CA) قوصملا عجرملا وأو رذجالا.

1. Administration > System > Certificate > Certificate Management > Trusted Certificates
إلى لقتناو ISE ةدقع ىلى لوخدلا لجس 1. ةروصلا هذه يف حضوم وه امك Import، قوف رقتناو Trusted Certificates

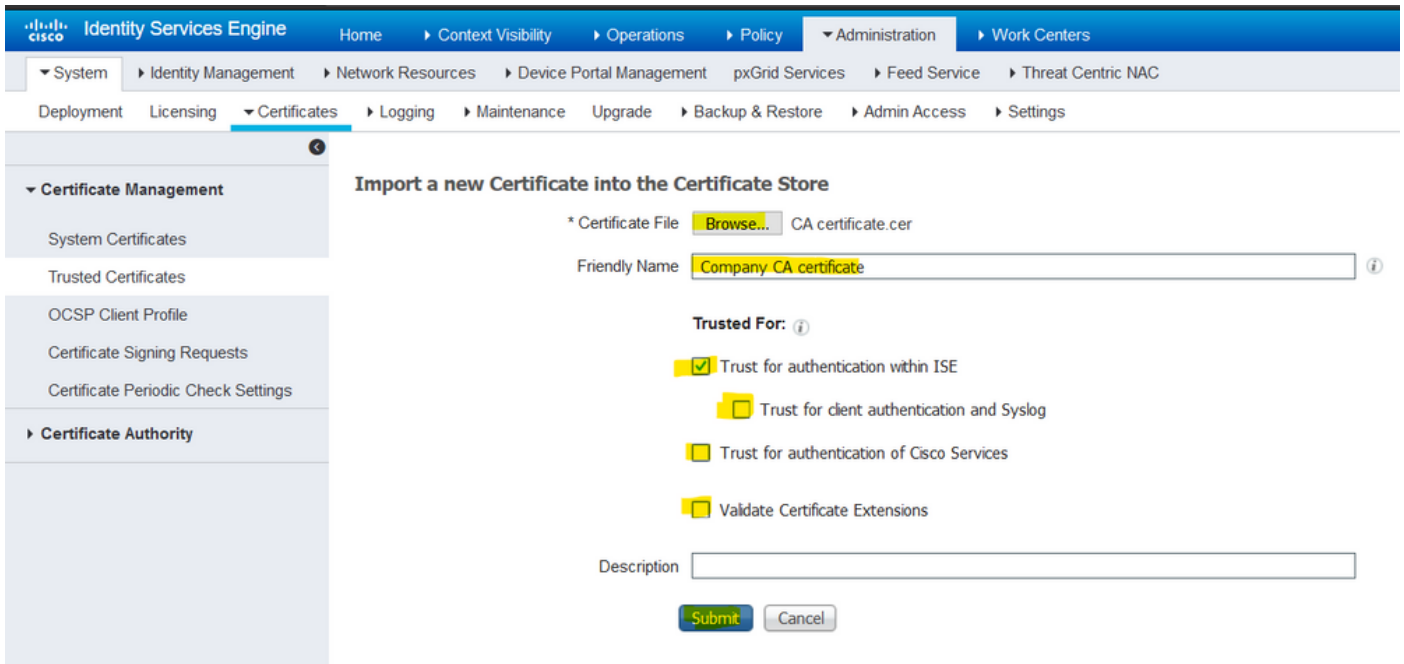


2. لوصلحلا مت يتلا قدصملا عجرملا (تاداهش) ةداهش ليمحتب مق، ةيلاتلا ةحفصللا يف ضرغل حضوي فصول اول فولأم مسا نييعتب مق. (اقتباس حضوملا بيترتللس فنب) اهيلع راسملا ةعباتم لجأ نم ةداهشلا نم

ل: ةرواجملا تاعبرملا ددح، مادختسال تاجايتح بسح

- نوكت ام دنع ةديج ISE دقع ةفاضلا يف ةزيملا هذه لثمتت - ISE لخد ةقداصملا ب ةقثلا اهب صاخلا اهب قوثلوملا تاداهشلا نزخم ىلع ةلمحم ةقوثلوملا CA ةداهش سفن اول
- ةقداصملا ةداهشلا مادختسال كلذ نيكتب مق - syslog وأو ليمملا ةقداصملا ب ةقثلا ةنم آلل syslog مداوخ يف ةقثلا وأو EAP مادختسال ISE ب لصتت يتلا ةياهنلا طاقن
- ةمدخ لثم ةيجراخلا Cisco تامدخ يف ةقثلل طقف اذه مزلي - Cisco تامدخ ةقداصملا ب ةقثلا ببول زجوم

3. عم اهتنامزمو "هب قوثلوملا نزخملا" يف ةيئرم ةداهشلا نوكت نأ نألل بجي Submit. رقتنا، اريخأ (رشنلا ةلاح يف) ةيوناتل ISE دقع عيجم



CA نم ةقووم ةداهش تيبت

هـب قووثوملا تاداهشلا نزم ىل طسوتملاو روجل (CA) قدصملا عجرملا تاداهش ةفاضل درجمب، CSR ىل ةدنتسملا ةقووملا ةداهشلا طبر نكمي و (CSR) ةداهشلا عيقوت بلط رادصل نكمي ISE ةدق ب.

1. رقنا م Administration > System > Certificates > Certificate Signing Requests م اش ن CSR ءاش ن ال Generate Certificate Signing Requests (CSR) قوف.

2. نم همادختس ا متيس يذلا رودلا رتخ ا، "مادختس ال" مسق نمض، رهظت يتلا ةحفصل ي ف. ةلدسنملا ةمئاقلا.

نكمي، ةداهشلا ءاش ن ا درجمب. ددعت م مادختس ا رتخ ا، ةددعت م راودأل ةمدختسم ةداهشلا تناك اذ ا همادختس ا متيل ةداهشلا نييعت نكمي، تالاحل مطعم ي ف. رم ال مزل اذ ا راودأل رييغت ةداهشلا نوكت ناب حمسي اذ هو؛ ةمدختسم ال ةلدسنملا ةمئاقلا ي ف ددعت م ال مادختس ال ال ISE بي و تاباوب عي مچل مادختس ال ال ةلباق.

3. اهل ةداهشلا ءاش ن ا متي يتلا (دق ال) ةدق ال رايتخال ISE (تادحو) ةدق ال رواجم ال ع برم ال دح.

4. ع برم Allow Wildcard Certificates نم ققحتف، لدب فرح ةداهش ءاش ن ا/ تيبت وه ضرغل اناك اذ ا.

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

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 Settings

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 Messaging Service - This is not a signing request, but an ability to generate a brand new Messaging 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  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 type="checkbox"/> hongkongise	hongkongise#Multi-Use

Usage

Certificate(s) will be used for  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 type="checkbox"/> hongkongise	hongkongise#Multi-Use

5. (دحول) ةمظنملا وأ فيضم لاب ةق لعتملا ليصافتلا إلى اذانتسا عوضوملا تامولعم ألما (دلبلاو، ةلودلا، ةنديملا، ةمظنملا، ةيميظنتلا).

6. يتأي يذلا قثب نملا إلى ل Export رقنا مث Generate قوف رقنا، اذءءاهنإل.

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

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 Settings

Certificate Authority

hongkongise hongkongise#Multi-Use

Subject

Common Name (CN) \$FQDN\$

Organizational Unit (OU) Security

Organization (O) IT

City (L) Kolkata

State (ST) West Bengal

Country (C) IN

Subject Alternative Name (SAN) IP Address 10.127.196.248

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

Certificate Policies

Generate Cancel

Country (C) IN

Subject Alternative Name (SAN) |

- DNS Name
- IP Address
- Uniform Resource Identifier
- Directory Name

* Key type RSA

* Key Length 2048

* Digest to Sign With SHA-256

اذه PEM فلم لاسرا بچي - وتلل هؤاشنل مت Base-64 لىل زمزم ةداهش بلط لىل زنتب اذه موقى
 اذى (زمزم Base 64) جتانلل عقومال CER ةداهش فلم لىل لوصحلاو ،عقوتلل لىل

دقعلل FQDN ءلمب اىلئاقلل CN لقحب صاخلا ISE موقى :ةظالم

مادختسال لقألا لىل CSR لىل لصلصم رادصل ابولطم ناك ، 1.4 و 1.3 ISE لىل :ةظالم
 لىل اذه لك ،هدعب امو 2.0 ذنم .تامدخال ةقبقل ،رخألاو ،PXgrid ل صصخم امهدحأ .pxGrid
 دحاو CSR

CN لقح يف "*" زمرلا نوكي ال ا ب جي ، EAP ةقداصل م ةداهشل ا مادختسا ةلاح يف : ةظحال م Verify ليطعت دنع ىتح .مداخل ةداهش نوضفري Windows يلومم ن ا ثيح عوضوملل ةحفاصلم لشفت ن ا نكمي ، بولطلم ال ع (مداخل ةيوه ةحص نم ققحتل) Server Identity ، CN لقح يف ماع FQDN مادختسا نكمي ، كلذ نم ال دبو . CN لقح يف "*" نوكي ام دنع SSL ، تاداهشل ا عجارم ضعبل نكمي . SAN DNS مسا لقح يف هم ادختسا نكمي *.domain.com م ث CSR يف ادوجوم نكي مل اذا ىتح ايئاقلت ةداهشلل CN يف (*) لدبل فرح ةفاضل (CA) .ءارجل ا اذ ءنم مل صاخ بلط مي دقت مزلي ، وييرانيسل ا اذ ء يف .

7. ويديفل ا يف حضورم وه امك CSR نم اهؤاشن ا مت يتل (CA لقب نم ةداهشل ا عيقوت درجم ب .ه) ، ءيموسرلا مدختسمل ا ءهءو ال لقتنا ، (Microsoft CA مادختسا مت اذا [انه](#) ل رواجمل ا ع برمل ا دح ؛ ةداهشل ا عيقوت بلط > ةداهشل ا ءراد ا > تاداهشل ا > ماظنل ا > ءرادال ا Bind Certificate رزل ا قوف رقنا و ، اق بسم هؤاشن ا مت يذل ا

The screenshot shows the Cisco ISE Administration console. The main content area is titled 'Certificate Signing Requests'. It features a 'Generate Certificate Signing Requests (CSR)' button and a text box explaining that CSRs must be signed by an external authority. Below this, there is a table of existing CSRs with columns for Friendly Name, Certificate Subject, Key Length, Portal group tag, Timestamp, and Host. A 'Bind Certificate' button is visible above the table.

Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
hongkongse#Mub-Use	CN=hongkongse.riverdale.local,O=...	2048		Tue, 14 Apr 2020	hongkongse

8. ISE ل افولأم امسا اهطعأو ، وتلل اهيقلت مت يتل ا ءعقومل ا ءداهشل ا ليحتب مق ، كلذ دعب . Admin ءقداصلم لثم) ةداهشل ا ءءاحل ا بسح تام ادختسال ل ءرواجمل ا تاع برمل ا راي تخ ا عبات م ث ءروصل ا هذ ء يف حضورم وه امك ، Submit رقنا و (كلذ ال ا مو ، لءدمل ا و ، EAP ،

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

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

Certificate Management

- System Certificates
- Trusted Certificates
- OCSF Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings

Certificate Authority

Bind CA Signed Certificate

* Certificate File certnew(1).cer

Friendly Name ⓘ

Validate Certificate Extensions ⓘ

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
- Portal: Use for portal

* Portal group tag ⓘ

Portal(s) using this tag

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

اهتمامدخ لي غشت ةداع اإ ISE ةدقع موقت نأ بجي ف ، ةداهشلا هذهل "لوؤس مل ا رود" راي تخ ا مت اذ ا . ةقوي قد 15 ا ا 10 نم كل ذ قيرغت س ي دق ، VM ل ةص صخ م ل ا دراوم ل ا و رادص ا ل ا ا ا ا ن س ا . show application status رم ا ل ا ر دص ا و ISE رم ا و ا رط س ح ت ف ا ، ق ي ب ط ت ل ا ة ل ا ح نم ق ق ح ت ل ل lse erase cat4000_flash:.

next visibility Operations Policy Administration Work Centers

es Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Maintenance

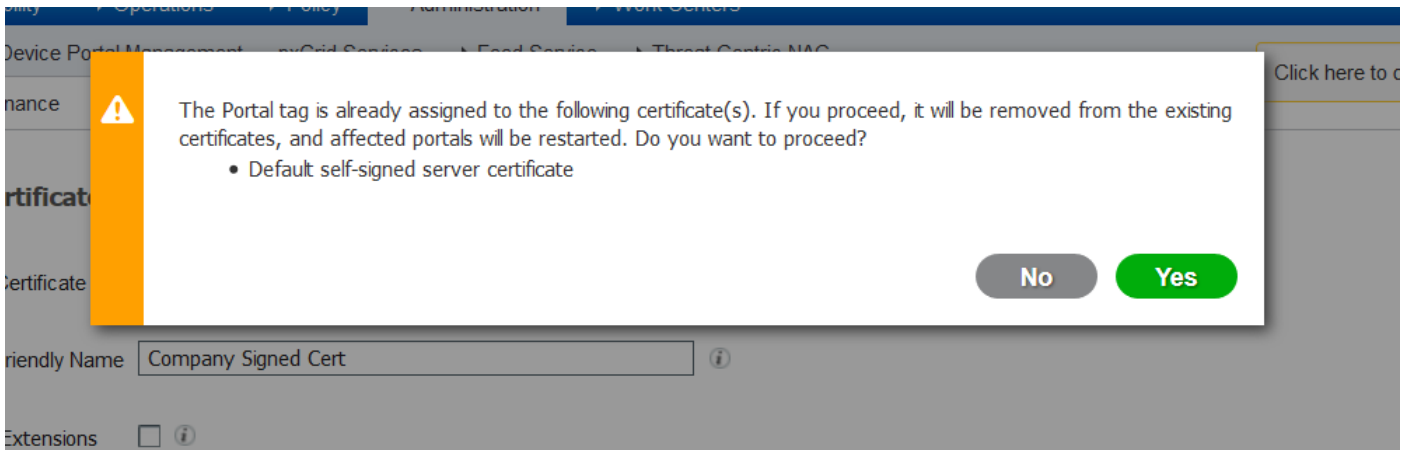
Bind CA Signed Certificate

* Certificate

Friendly Name ⓘ

Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates



ةداهشلا نأ نم ققحتلا نكمي ،ةداهشلا داريتسا دنع لخدملا وأ لوؤسمل رود رايخا مت اذا زمر رتخا .ضرعتسملا يف لخدملا تاحفص وأ لوؤسمل الىا لوصولا دنع ةدوجوم ةديدل ةدوجوملا ةلمكلا ةلسلسلا نم راسملا ققحتي ،صخيخرتلا تحت وحقصت مل يف نيماألا لخدملا وأ لوؤسمل ةداهش يف ضرعتسملا قثي نأ بجي .زاهجلا لبق نم اهب قوئوملاو ةلسلس يف قثي ضرعتسملا ناك اذا وحقص لكشب ةلسلسلا عاشنا مت املاط ةديدل ةداهشلا .

طبرو ،ديج CSR عاشنا ب مق ،CA لبق نم ةعقوم ماظن ةداهش ديديت لجأ نم :**ةظالم** لىل ةديج ةداهش تيبتت نكمملا نم هنا امب .تاراخلا سفنبا هب ةعقوملا ةداهشلا ةيخالص ءاهتنا لبق ةديدل ةداهشلا تيبتتل ططخ ،ةطشن نوكت نأ لبق ISE ةميديل ةداهشلا ةيخالص ءاهتنا خيرات نيي هذه لخادتل ةرتف .ةميديل ةداهشلا تقوعم اهلا دابتل طيطختلاو تاداهشلا ديديت اتقوحنمت ةديدل ةداهشلا ءدب خيراتو خيراتب ةديج ةداهش لىل لصح .لمعل نع فقوت تقو دجوي ال وأ ليلق لمعل نع فقوت نيي هذه نيي نمزلا ةرتفلا .ةميديل ةداهشلا ةيخالص ءاهتنا خيرات قبسي ءدب خيحصلا خيراتلا قاطن ةديدل ةداهشلا لخدت نأ درجم .رييغتلا ءذفان يه نيي خيراتلا مت اذا هنا ركذت .(admin/EAP/Portal) ةبولطملا تالوكوتوربلا نيي كمتب مق ،اهب صاخلا ةمدخل ليغشت ءداعا متتس ف ،Admin مادختسا نيي كمت

EAP و Admin تاداهشلا ءكرشل ليلا خادلا قوصملا عجرملا مادختساب ي صوي :**خيملت** اذا هنا وه ببسلا .كلذ الىا امو/Guest/Sponsor/Hotspot تابلما ل لكشب ةعقوم ةداهشو عاقللا نم ةعقوم ةداهش ISE ةباب تم دختساو ءكبشلا الىا فيض وأ مدختسم لخد نأ لم تحي وأ ةداهشلا يف عاطخا لىل مدختسملا لصحيس ف ،"فويضلا لخدم" ل صاخلا ةداهش مدختسا ،كلذ لك بنجت .ةبابلا ءحفص نم عاطخالا رطحب ضرعتسملا موي ءفاضا لابلو .لصفأ مادختسا ءبجت نامضل ةبابلا مادختسال ءمعل لبق نم ةعقوم نييختلا ءكبش لىل رشن (دقع) ءدقع IP ناو نع ناو نع لك ءفاضا بجي ،كلذ الىا IP ناو نع ربع مداخل الىا لوصولا دنع ةداهش ريديت بنجتلا (SAN)

ةصاخلا خي تافملاو يطايتخالا خسنلا تاداهش

ريديتلاب ي صوي :

1. (مزلي) ءصاخلا اءحي تافم الىا ءفاضا لابل (رشنلا يف دقعلا عيجم نم) ماظنلا تاداهش عيجم .مت يتل ءمدخل) ةداهشلا نيوكتل ءظالمب طاقتحالا .نم ءقوم الىا (ءهتيبتت ءداعا (اهل ءداهشلا مادختسا)

2. طاقتحالا .ءيساسالا ءرادالا ءدقعل اهب قوئوملا تاداهشلا نزم نم تاداهشلا ءفاك .(اهل ءداهشلا مادختسا مت يتل ءمدخل) ءداهشلا نيوكتل ءظالمب

3. تاداهش لة ئيه تاداهش عيمج .

كذذب مايقوللو

1. رتخأ Administration > System > Certificates > Certificate Management > System Certificates. لىل لقتنا .
ةم لك لخدا . ةصاخلا حيتافملا اقاقتنا رزو Export Certificates راتخن . Export. رقناو صيخرتل
Export. رقنا . رورملا ةم لك دي كأتب مقو صاخلا حاتفملا رورم
2. رتخأ Administration > System > Certificates > Certificate Management > Trusted Certificates. لىل لقتنا .
ةداهشلا ري دصت ل Save File رقنا . Export. رقناو صيخرتل
3. رتخأ Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates. لىل لقتنا .
ةم لك لخدا . ةصاخلا حيتافملا اقاقتنا رزو Export Certificates راتخن . Export. رقناو صيخرتل
Save File رقنا . Export. رقنا . رورملا ةم لك دي كأتب مقو صاخلا حاتفملا رورم
ةداهشلا .

اهحالص او اطاخال فاشكتسا

ةداهشلا ءحص نم ققحتلا

وأ ماظنلا تاداهش نزم يف ةداهش ية ءي حالص اءاتنا ءلا ح يف ءي قرتلا ءي لمع لشفت
ءاتنا خيرت ل قح يف ءي حالصلا نم ققحتلا نم دكأت . Cisco نم اءب قوٲوملا ISE تاداهش
(Administration > System > Certificates > Certificate Management) ماظنلا تاداهشو اءب قوٲوملا تاداهشلا تاراطال ءي حالصلا
ءي قرتلا لبق ، رمال مزلا اذا ، اءدي دجتو ،

تاداهش ءذفان يف ءدووملا تاداهشلا ءي حالصلا ءاتنا خيرت ل قح يف ءي حالصلا اضيا عجار
(Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates) ،
ءي قرتلا لبق ، رمال مزلا اذا ، اءدي دجتو .

ةداهش فذح

ري دصت نم دكأت . اءتلازا مزلي ، اءم ادختسا مدع و ISE يف ءداهش ءي حالص اءاتنا ءلا ح يف
فذل ل لبق (نكم نإ ، ءصاخلا اءحيتافمب) تاداهشلا

Administration > System > Certificates > Certificate Management. لىل لقتنا ، ءي حالصلا ءي هت نم ءداهش فذل
رقناو اءتي حالص تهتنا يتلا (تاداهشلا) ءداهشلا رتخأ . System Certificates Store. قوف رقنا
Delete. قوف
ةلوخملا عجارملاو ءلوخملا تاداهشلا نزاخم لئيشلا سفن عجار

802. 1x ءقداصم يف ISE مءاخ ءداهش بلاط قٲي ال

SSL. ءحفاصم ءي لمعل ءلمالكلا تاداهشلا ءلسلس لسري ISE ناك اذا ام ققحت

يف مءاخلا ءي وه نم ققحتلاو (PEAP ية) مءاخ ءداهش بلاطت يتلا EAP بيلاسا دي دجت عم
تاداهشلاب تاداهشلا ءلسلس نم بلاطلا مءقم ققحتي ، ليمعلا لئيشت ماظن تاداع
ءحفاصم ءي لمع نم ءزك . ءقداصملا ءي لمع نم ءزك لئيلحمل ءقٲل نزم يف هيءل ءدووملا
ال . ءصاخلا ءلسلسلا يف ءدووم طيسو و/و رءج تاداهش ية لكذكو هتداهش ISE مءقي ، SSL
تناك اذا و ءلماك ريغ ءلسلسلا تناك اذا مءاخلا ءي وه نم ققحتلا نم بلاطملا نكم تي
ءب صاخلا ءقٲل نزم يف ءلسلسلا هءه لىل رقتت

ISE (Operations > نم ءمزح طاقتلا نءاب مق ، ليمعلا لىل تاداهشلا ءلسلس ءداع) نم ققحتلا

تقوي فة ياهنللا ةطقن ىلع Wireshark طاقنللا وأ (Diagnostic Tools > General Tools > TCP Dump) ةقداصللا Wireshark ةكرش يف ssl.handshake.certificates حشرملا قيبطت ب مقو طاقنللا حتفا . ةقداصللا لوصوللا يدحت ىلع روثللاو

Expand Radius Protocol > Attribute Value Pairs > EAP-Message Last segment > Extensible Authentication Protocol > Secure Sockets Layer > Certificate > Certificates. رايخالا درجم ب ىللا لقتنا ،

ISE Administration > Certificates > Trusted Certificates ىللا لقتنا ، ةلماك ريغ ةلسلسلا تناك اذا بجي ، حاجن ب تاداهشلا ةلسلسلا ريرمت ةلاح يف . ةطيسولا تاداهشلا وأ/و رذللا تاداهش دوجو نم انه ةحضوملا ةقيرطللا اقفو اهسفن ةلسلسلا ةحص نم ققحتلا

حاتفم فرعم ةقباطملا ةقثلا ةلسلسلا نم ققحتو (رذجو ، طسوت م ، مداخ) ةداهش لك حتفا يف ةيالاتلا ةداهشللا (AKI) ةطلسللا حاتفم فرعم ىللا ةداهش لكل (SKI) عوضوملا ةلسلسلا .

ءانثأ ISE مداخ ةداهش ضفرت ةياهنللا ةطقن نكلو ةحيجص ISE ةداهش ةلسلسلا ةقداصللا

ةلسلسلا ضفري ستمتللما لظو SSL ةحفاصلم ةلماك تاصيخرت ةلسلسلا ISE مدق اذا يف ةدوجوم ةطيسولا وأ/و رذللا تاداهشلا نأ نم ققحتلا يه ةيالاتلا ةوطخللا نإف ، تاداهشلا يلمحلالا ينامتتساللا ءالمعللا نزم .

mmc.exe (Microsoft Management Console) ليغش تب مق ، Windows زاھج نم كلذ نم ققحتلل رقناو Certificates رتخأ ، رفوتملا ةيفاضللا تاوداللا دومع نم . File > Add-Remove Snap-in ىللا لقتنا مدختسمللا ةقداصلملا عون ىللا ادانتسا Computer account وأ My user account ام رتخأ . Add قوف OK . قوف رقنا م (زاھج وأ مدختسم)

قيدصتلا تاطلسو اهب قوثلوملا رذللا ةقداصلم عجارم رتخأ ، مكحتلا ةدحو ضرع تحت يلمحلا ةقثلا نزم يف طسوتملاو رذللا تاداهشلا دوجو نم ققحتلل ةطسوتملا

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

ةرركتملا ةلئساللا

ةدوجوم ةداهشلا نأب ريذحت هيچوتب ISE موقيا ام دنع هل عف بجي يذلا ام ل عف لاب ؟

تمت دقو ، طبضلاب OU ةملمعم سفن اهل ماظن ةداهش نع تفشك ISE نأ ةلاسرا هذه ينعن ةطاسبب حصني ، ةمومدم ريغ ةرركملا ماظنلا ةداهش نأ ام ب . ةرركم ةداهش تيبتت ةلواجم ةداهشلا نأ نامضل اليلق ةفلتخم ةميق ىللا مسقلا/ةلاجل/ةلنيدملا ميق نم ي ريغتتب ةفلتخم ةديجلا .

ISE نم لخدملا ةحفص نأ ىللا ريشي ريذحت هيچوتب ضرعتسمللا موقيا اذامل هب قوثلوم ريغ مداخ ةطساوب ةمدقم ؟

مداخلا ةيوه ةداهش ب ضرعتسمللا قثي ال ام دنع كلذ تحدي

اهنيوكت متواعقوتم ناك ام يه ضرعتسملاليلع ةيئرملال ةباوبال ةداهش نأ نم دكات ،الوأ ةباوبال ل ISE يلع
نم دكات ،مادختسالال دي ق IP ناووع ةلاح يف - FQDN ربع ةباوبال ليل لوصولال نم دكات ،ايناث
ةداهشلال نم CN وأ/و SAN يلقح يف IP ناووعو FQDN نم لك دوجو
CA تاداهش ،طيسوالا (CA) CA (ISE لخدم) ةباوبال تاداهش ةلسلس داريتسإ نم دكات ،اريخأو
ليمعالاب صاخلال ضرعتسملال/الليغشتلال ماظن جمانرب ةطساوب اهب قوتوم/يلع (رذجال

ال Chrome/Firefox و Android OS و iOS تاحفصتم نم ثدخال تارادصالإ ضع ب: **ةظحال**
لاصلالاضفراهنكم يف ،طاقنلال هذه ةيبلت مت اذا يتح .ةداهشلال ةمراص نامأ تاعقوت
SHA-256 نم لقا ةطيسوالا CAs و Portal ةميق تناك اذا

ةحلاصلال ريغ تاداهشلال ببسب ةيقرتلال لشف دنع هل عف بجي يذالام

وأ ماظنلال تاداهش نزم يف ةداهش يأ ةيخالص اءاتنا ةلاح يف ةيقرتلال ةيلمع لشفت
ءاتنا خيرات لققح يف ةيخالصلال نم ققحتلال نم دكات . Cisco نم اهب قوتومال ISE تاداهش
Administration > System > Certificates > Certificate Management) ماظنلال تاداهشو اهب قوتومال تاراطلال ةيخالصلال
ةيقرتلال لبق ،رمال مزل اذا ،اهديجتو ،

تاداهش ةذفان يف ةدوجومال تاداهشلال ةيخالصلال ءاتنا خيرات لققح يف ةيخالصلال اضيأ عجار
Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates) ،
ةيقرتلال لبق ،رمال مزل اذا ،اهديجتو

ةيلخاللال CA تاداهش ةلسلس ةحص نم دكات ، ISE ةيقرت لبق

رتخأ ،رشنلال يف ةدقع لكل . Administration > System > Certificates > Certificate Authority Certificates. يلق لقتنا
فولأمال مسالال دومع يف تاداهشلال تامدخ ةيها ن ةطقنل يعرفلال قدصمال عجرملا تاذ ةداهشلال
ةيئرمو ةديج ةلسر ةداهشلال ةلاح تناك اذا ام ققحتو View رقنا

لجأ نم . ةيلمع نيسحت ISE ل Cisco نأ لبق رادصالإ تبثي نأ تنمض ،ترسك ةداهش يأن
Administration > System > Certificates > Certificate Management > Certificate Signing
Requests، ISE Root CA رايل دخال دحاو ءاشنإو ،

ةلص تاذ تامولعم

- [تاداهشلال نزم تاداعواو تاداهشلال ةرادا ISE 2.7](#)
- [ISE يف ةيقرتلال تاداهشلال ذيفنت](#)
- [Cisco Systems - تادنتسملالو يبقنقتلال معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت 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 د ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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