

اهددي دجت و SSL ل ةيمقرلا تاداهشلا تيبتت يلع اهالصل او تاداهشلا هذه عاطخا فاشكتسا و Cisco ISE

تايوتحمل

[ةمدقملا](#)

[ةيساس الابل طتملا](#)

[تابل طتملا](#)

[قم دختس مملاتان وكملا](#)

[ةيساس تامولعم](#)

[نوي وكتلا](#)

[ماتن ةداهش داريتسا](#)

[ةيخالصل ةيمت نم ةداهش لادبتسا](#)

[ةعئاشلا تالكش ممل](#)

[ISE ةدقع يلع اهتخيخالص يهتنت لخدم ةداهش لادبتسا يلع رداق ريغ: 1 وييرانيسلا](#)

[أطخلا](#)

[لجلا](#)

[ددعت ممدختسا عم ISE ةدقع س فنل CSR يخالصم عاشنانكم يال: 2 وييرانيسلا](#)

[مادختسا ل](#)

[أطخلا](#)

[لجلا](#)

[مدع والخدملا مادختسا ل قدصملا عجملا نم ةعقوملا ةداهش لابل رذعت: 3 وييرانيسلا](#)

[أطخ يلع لوصحل او ةداهش لابل لخدملا ةمالع نوي عت يلع ةردقلا](#)

[أطخلا](#)

[لجلا](#)

[نم ةيخالصل ةيمت نمل او ايتاذ ةعقوملا ةيضارتفالا ةداهش لابل فذح رذعت: 4 وييرانيسلا](#)

[اهب قووملا تاداهش لابل نذخم](#)

[أطخلا](#)

[لجلا](#)

[ISE ةدقع يلع CSR عم pxGrid ب ةعقوملا CA ةداهش لابل رذعت: 5 وييرانيسلا](#)

[أطخلا](#)

[لجلا](#)

[نم ةيخالصل ةيمت نمل او ايتاذ ةعقوملا ةيضارتفالا ةداهش لابل فذح رذعت: 6 وييرانيسلا](#)

[دووملا SCEP RA و LDAP فيرعت فلم نوي وكت ب بسبب قووملا تاداهش لابل نذخم](#)

[أطخلا](#)

[لجلا](#)

[ةيفاضا دراوم](#)

ةمدقملا

يتلا ةعئاشلا لكاشملا مظعمل اهلولحو اهددي دجت و SSL ةداهش تيبتت دنتسملا اذه فصوي

ةوهل تامدخ كرحم ىلع اهتظحالم تمت

ةيساسأل تابلطتمل

تابلطتمل

ةيلاتل عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت

- ةوهل ةمدخ كرحمل (GUI) ةيموسرللا مدختسمللا ةهجاو

ةمدختسمللا تانوكمل

ةيلاتل جامانربللا رادصلإ ىلإ دننتسمللا اذله ةف ةدراوللا تامولعمللا دننتست

- 2.7 رادصلإ، Cisco Identity Service Engine

ةصاخ ةيلمعم ةئيب ي ةدوجومللا ةزهجالا نم دننتسمللا اذله ي ةدراوللا تامولعمللا عاشنإ مت تناك اذإ. (يضايرتفا) حوسمم نيوكتب دننتسمللا اذله ي ةمدختسمللا ةزهجالا عيمج تأدب رما يال لم تحمللا ريثأتلل كمهف نم دكأف، ليغشتللا دي قكتكبش

ةيساسأ تامولعم

بجي يتللا ةعئاشللا لكاشم لل ةي عجرمللا ةمئاقلاو اهب ىصومللا تاوطخللا دننتسمللا اذله مدقي Cisco معدادتساو احوالصلإو Cisco اطاخأ فاشكتسا ي ءدبلا لبق اهتجالعمو اهنم ققحتللا ينقتللا

نايكللا كلذ طبرتو رخآ انايك وأ ةكرش وأ امداخ وأ اصخش فرعت ةينورتكللا ةقيثو يه ةداهشلا ماعحاتفمب

ايتاذا ةعقوم تاداهشللا نوكت نأ نكمي. اهئشنم لبق نم ايتاذا ةعقومللا ةداهشللا عي قوت متي (CA) يجراخ قدصم عجرم لبق نم اي مقرة عقوم وأ

انامأ رثكأو ايعانص اراي عم (CA) قدصم ل عجرملا ىلع ةعقومللا ةيمقرللا ةداهشللا ربتعت

نمأ لوصولل ري فو تل ةكبش ي ةتاداهشللا مدختست

مداخ لثم ةيجراخللا مداوخللا عم لي صوتللو، دقعللا نيبل لاصلتاللا تاداهش Cisco ISE مدختسلي لي فكللاو فيضللا تاباوب) يئاهنللا مدختسمللا تاباوب عي مجو بيولا زجوم مداخو Syslog (ةي صخشلا ةزهجالاو

كلت ةي اهنللا ةطقن نيبل لاصلتاللا نمؤتو ةي اهنللا ةطقن ىلإ Cisco ISE ةدقع تاداهشللا فرعت Cisco ISE ةدقعو

عسوتمللا ةقداصملا لوكوتورب تالاصلتاللا HTTPS تالاصلتاللا عي مجل تاداهشللا مادختسا متي (EAP).

بجي يتللا ةعئاشللا لكاشم لل ةي عجرمللا ةمئاقلاو اهب ىصومللا تاوطخللا دننتسمللا اذله مدقي

تحت لخدملا رود ةفاضإو، EAP ةقداصم مادختساب اهريحتو ةداهشلا ديدحت 1. ةوطخلال
ظفحلل او مادختسالال

ةيحلل اصلال ةيهتنملا لخدملا ةداهش فذح 2. ةوطخلال

لاسراو (مادختسالال ديق) رود ياديدحت نود ةديجلال لخدملا ةداهش ليدحت 3. ةوطخلال

ظفحلل او مادختسالال تحت لخدملا رود نييعتو اهريحتو ةديجلال لخدملا ةداهش ديدحت 4. ةوطخلال

مادختسالال عم ISE ةدقع سفنل CSR يحيصلصم عاشنل نكمي ال: 2 ويرانيسالال
مادختسالال ددعت

أطخلال

أطخلال عم مادختسالال ددعت مادختسالال عم ةدقعلال سفنل ديدج CSR عاشنل لشفي
ةديرف ةفولأملا عامسالال نوكت نأ بجي. فولأملا مسالال سفنل يرخأ ةداهش لعفلال دجوت

لحلل

2 عاشنل ابحمست ال تحت ISE ةدقع لكل اثبات ازيمرت CSR ل ةفولأملا عامسالال زيمرت متي
كانهو، ةنيعم ةدقعي ف مادختسالال ةلاح دجوت. ددعتمال مادختسالال عم ةدقعلال سفنل CSRs
نم ةعقوم يرخأ ةداهشو EAP و Admin ةقداصم مادختسالال اهمادختسالال متي CA نم ةعقوم ةداهش
ءاهتنالال ديق تاداهشلال الكو لخدملاو SAML مادختسالال اهمادختسالال متي CA

ويرانيسالال اذه ي:

مادختسالال ددعت مادختساب لوال CSR عاشنل 1. ةوطخلال

EAP و Admin ةقداصم رود نييعتو لوال CSR عم CA لبق نم ةعقوملا ةداهشلا طبر 2. ةوطخلال

مادختسالال ددعت مادختساب نال CSR عاشنل 3. ةوطخلال

لخدملا رودو SAML نييعتو يئانلال CSR ب CA نم ةعقوملا ةداهشلا طبر 4. ةوطخلال

لخدملا مادختسالال قداصملا عجرملا نم ةعقوملا ةداهشلا طبر رذعت: 3 ويرانيسالال
أطخلال لوصحلل او ةداهشلل لخدملا ةمالع نييعت يلع ةردقلا مدع وأ

أطخلال

أطخلال ثودح يلى لخدملا مادختسالال CA لبق نم ةعقوملا ةداهشلا طبر ي دؤي:

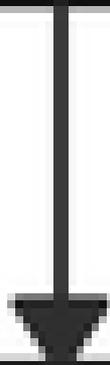
وأ لخدملا ماظن تاداهش ةلسلس نم اعزج لكشت رثكأ وأ ةدحاو اب قوئوم (تاداهش) ةداهش دجوت
مقر هل نكلو عوضوملا مسالال سفنل ةداهش يلى دنننل لوؤسملال ةقداصم رود عم ةدح
حجانلال شيحتلال/داريئالال. شيحتلال/داريئالال ةي لمع ضاهج مت. فلل تخم يلسلسلست
قوئوم ةداهش نم قوستلال ةلس يلى دنننل لوؤسملال ةقداصم رود ليدعت يلى امجاتحت
اب قوئوملا ةداهشلا يلع يوتحت يئالال ماظنلال ةداهش نم لخدملا رود ريغت وأ ةرركم اب
اهتللسلس ي ةرركملا

لحل

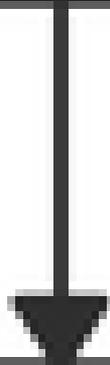
ننضم يفو (لخدملا مادختسال) CA نم ةعقوملا ةداهشلا تاداهش ةلسلس نم ققحت 1. ةوطخلا تاداهشلا ةلسلس نم ةرركم تاداهش يا دوجو نم ققحت ،اهب قوٲوملا تاداهشلا ةقداصل Trust رايٲخالال ةناخ ديدحت ااعلاب مق و ا ةرركملا ةداهشلا ةلازاب مق 2. ةوطخلا ةرركملا ةداهشلا نم ةداهش ىل دنٲسمل لوؤسمل

تاداهشلا ةلسلس ىل ع CA لبق نم ةعقوملا لخدملا ةداهش يوتحت ،لاٲملا لىبس ىل ع ةيلاتلا:

Root CA



Intermediate CA



Issuing CA

تاداهشلا ةلازاب مقو (ةيحالصلا ةيهت نم ةداهش نوكت نأ نكمي) تاداهشلا ةلسلس ي ف 3 ل
اهب قووثوملا تاداهشلا نزخم نم ةرركملا

ةيهت نم لاو ايتاذ ةعقوملا ةيضارتفالا ةداهشلا فذح رذعت :4 ويراني سلا
اهب قووثوملا تاداهشلا نزخم نم ةيحالصلا

أطخل

تاداهشلا نزخم نم ةيحالصلا ةيهت نم لاو ايتاذ ةعقوملا ةيضارتفالا ةداهشلا فذح يدوي
أطخل ثودح ل اهب قووثوملا
تاداهش ي ف اهاه ل اءراش ل اءم ت ه نأ ل اءرن ةقثلا و اء فذح و اءداهشلا ل ل طعت ب حوم سم ريغ
دعب نع ل ل ج س ت ل ف اءه ن م ص ن م آ ل syslog فده و اء م اءن ل ل

لحل

1. ي أب ةيحالصلا ةيهت نم لاو ايتاذ ةعقوملا ةيضارتفالا ةداهشلا نارتقا مدع نم ققحت .
ل ل ج س ت > م اءن ل ل > ةرادل ل تحت اءر ل اءه نم ققحت ل نكمي . دوجوم دع ب نع ل ل ج س ت فده
اهريحت و (ت) SecureSyslogCollector ديحت > دع ب نع ل ل ج س ت ل ف اءه > ل وءدل
ةنرتقم ريغ ايتاذ ةعقوملا ةيحالصلا ةيهت نم لاو ايتاذ ةيضارتفالا ةداهشلا نأ نم ققحت .
> تاداهش ل ل > م اءن ل ل > ةرادل ل تحت ل ل ذ نم ققحت ل نكمي . (م اءخ ت س ل) ن ي ع م ر و د ي أب
م اءن ل ل تاداهش .

TAC. ب ل ص ت ا ، ةل ك ش م ل ت ر م ت س ل اءا

ISE ةدقع ل ل ع CSR عم pxGrid ب ةعقوملا CA ةداهش طبر رذعت :5 ويراني سلا

أطخل

أطخل عم ةداهشلا طبر ةي لمع ل ش ف ت ، CSR ب ةديءل pxGrid ةداهش طبر اءن اء
ءات ف م ل اءخ ت س ل ق ح ل م ي ف مءا ء ل ل و ل ي م ع ل ل ةقءاصم ل ل ع PxGrid ةداهش ي و ت ح ت نأ ب ج ي
م ل ل (EKU) ع س و م ل ل

لحل

TLS ب ي و مءا ء ةقءاصم نم ل ل ك ل ل ع CA نم ةعقوملا pxGrid ةداهش ي و ت ح ت نأ ب ج ي ه نأ نم ءك اء
م ت ي ه نأ ل ع س و م ءات ف م اءخ ت س ل ب (1.3.6.1.5.5.7.3.2) TLS ب ي و ل ي م ع ةقءاصم و (1.3.6.1.5.7.3.1)
(مءا ء ل ل و PxGrid ل ي م ع ن ي ب ل ل ص ت ل ل ن ي م اء ل ل) مءا ء ل ل و ل ي م ع ل ل ةقءاصم نم ل ل ك ل ه م اءخ ت س ل

ي ع ج ر م ل ط ب ا ر ل ل : https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

ةيهت نم لاو ايتاذ ةعقوملا ةيضارتفالا ةداهشلا فذح رذعت :6 ويراني سلا
و اء LDAP ف ي ر ع ت ف ل م ن ي و ك ت ب ب س ب ه ب قووثوملا تاداهشلا نزخم نم ةيحالصلا

دوجوم ال Scep Ra

أطخل

تاداهش ال نزم نم ةيحلصل ةيهت نمل او ايتاذ ةعقوم ال ةيضارت فال ةداهش ال فذح يدؤي
أطخل ثودح ال اهب قووم ال

Scep فيرعت فلم نم ام بر، رخ آنكم في اه ي ال ةراش ال امتت هنأل "ةقث ال ةداهش" فذح رذعت
LDAP ةيوه ردصم و RA

* ةيضارت فال ايتاذ ال عيقوت ال مداخ ةداهش *

مادختس ال مدعل LDAP فيرعت ردصم ررح و RA Scep فيصوت فذح، (تاداهش ال) ةداهش ال فذح
ةداهش ال هذه.

لحل

1. لاصت ال > مداخ ال مس ا > LDAP > ةيجراخ ال ةيوه ال رداصم > ةيوه ال ةرادا > ةرادا ال لقتنا
2. "ايتاذ ةعقوم ال ةيضارت فال مداخ ال ةداهش" مدختسي ال LDAP Server Root CA أن نم دكأت
3. > ةرادا ال لقتنا، نم آل ليصوت ل ةبولطم ال ةداهش ال مدختسي LDAP مداخ نكي مل اذا
Scep Ra تافيصوت > ةيجراخ ال CA تادادع > تاداهش عجرم > تاداهش > ماظن
4. ةيضارت فال عيقوت ال ةيتاذ ةداهش مدختست ال Scep Ra تافيصوت نم ي أن نم دكأت

ةيفاضا دراوم

لدب فرح ةداهش تيبتت ةيفي

<https://www.cisco.com/c/en/us/td/docs/security/ise/2->

[6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html)

ISE تاداهش ةرادا

<https://www.cisco.com/c/en/us/td/docs/security/ise/2->

[6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html](https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html)

ISE ال ةيجراخ ةهج نم قدصم عجرم ةداهش تيبتت

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295->

[Install-a-3rd-party-CA-certificate-in-IS.html](https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html)

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 م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
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 م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م 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 م ل ا ح ل ا و ه
ل ا ا م ا د ا د ع و چ 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 چ ن ا ل ا دن ت س م ل ا