

IOS نم ايتاذ ةعقوملا ةداهشلا ةيحلص اهاتنا 2020 رياني 1 يف

تايوتحمللا

ةمدقملا

ةيساس الابلطتلا

تابلطتلا

ةمدختس مملاتانوكملا

ةيفلخلا

قماع تانيم

نواعتلا تانيم

ةيكلس الابل تانيملا

ةلكشملا

ةرثاتملا تاجت نملا يلغ فرعوتلا ةيفيك

(لولحلا) لولحلا

1. (CA) ةيچراخ ةهج نم ةحلص ةداهش يلغ لولحلا.

2. ةديج ةداهش ءاشنال Cisco IOS CA مداخ مدختسأ.

3. ةديج ايتاذ ةعقوم ةداهش ءاشنال OpenSSL مداخ مدختسأ.

Cisco IOS XE و Cisco IOS هجوم يلغ للاثم

4. ةديجلا ةداهشلا تيبثت نم دكأت.

ةبوج أو ةلئسأ

ةلكشملا يه ام نلاؤس

اهجت نم ايتاذ ةعقوم ةداهش ةيحلص تهت نا اذا لي مملاتان ةكبش يلغ ريثاتلا وه ام نس

ةيفيض قولا هذهب ارثاتم تنك اذا ام فرعأ نأ يل فيك نس

ةرثاتم تنك اذا ام يرأل هلي غشت عيظتسأ صت كانه له

ةلكشملا هذهل ةيچمرب لولح Cisco تمدقم له.

ةداهش مدختس ي Cisco نم جت نم يأ يلغ ةلكشملا هذو رثوت له.

طوقف ي تاذلا عي قوتلا تاداهش Cisco تاجت نم مدختس له نس

ةلئسأ مملاتان هذو تشرح اذا مل نس

تي قوتلاب 2020 00:00:00 ي ناثلا نوناك 1 يف ةيحلصلا ءاهت نا خيرات راي تخلا مت اذا مل نس
ي مملاتان

ةلكشملا هذو رثاتت يتلا تاجت نملا يه ام نس

هلغف ني مدختس مملاتان بچي يذلا ام نلاؤس

ةيفي نم أ فعض ةطقن لكشت ةلئسأ مملاتان هذو له نس

SSH لوكوتورت رثاتت له نس

يف ةفل فال 2 ةعرب ةيدي لولحلا Catalyst ةمظنأب ةرفوت مملاتان ةتباتلا تارادص الابل يه ام نس
يف ةفل فال 6 و ةقي قودلا يف ةفل فال 4 و ةقي قودلا يف ةفل فال 3 و ةقي قودلا
ةقي قودلا

ي مملاتان لمعلاتان ةي عمج رثاتت له نس

ةلص تاذ تامولعم

ةمدقملا

cisco ىلع (SSC) يتاذلا عيقوتلا تاداهش ةيخالص ءاهتنا نع جتنني أطخ ةقويثو اذه فصوي ةلديب لولج مدقي و ماظن ةيجمررب.

ةيساسال تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco يوصوت:

- (SSC) يتاذلا عيقوتلا تاداهش
- Cisco نم ثدخال تارادصلال او 12.x رادصلال IOS®

ةمدختسملا تانوكملا

SSC ةيخالص ءاهتنا ب ةرثاتملا جماربلا ةمظنأ يه تانوكملا.

يوتحت ال يتلاو، ايتاذ ةعقوم ةداهش مدختست يتلا Cisco IOS XE و Cisco IOS ةمظنأ عيجم فرعم خالصا ىلع يوتحت مل يتلا وأ، تبثي [CSCvi48253](#) Cisco نم ءاطخال حيصت فرعم ىلع يلى ام كلذل لمشي و. SSC ءاشن دن ع [CSCvi48253](#) Cisco نم ءاطخال حيصت

- All Cisco IOS، رادصلال 12.x
- Cisco IOS 15.x لبق 15.6(3)M7، 15.7(3)M5، 15.8(3)M3، 15.9(3)M
- Cisco IOS XE لبق 16.9.1

ةصاخ ةيلعم ةئيبي يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراولا تامولعمل ءاشنإ مت تناك اذإ. (يضايرتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجال عيجم تادب رمأ يال لمحتملا ريثاتلل كمهف نم دكأتف، ليغشتلا ديقتك تبش

ةيفلخال

قاييس ىلإ ةفاضلاب ، [FN40789 زارطلا](#) تايوتحم ىلع دنتسملا اذه يوتحي: ةظحالم ةبوجأو ةلئسأو تاتيحت و ةلثمأو يفاضل.

ةيخالص ءاهتنا نييعت مت، يملعلا تيقتوتلاب 2020 يناثلا نوناك 1 نم 00:00 ةعاسلا يف Cisco IOS و Cisco IOS XE، يماظن ىلع اهؤاشنإ مت يتلا (SSC) ايتاذ ةعقوملا تاداهشلا عيجم ءاشن دن ع Cisco IOS و Cisco IOS XE نم تبث رادصلال ليغشتب ماق دق ماظنلا نكي مل ام ةديج SSC تالكبش ءاشنإ ةتباتلل ريغ Cisco IOS ةمظنأ ىلع رذعتي، تقولا كلذل دعب SSC. دعب هئاهنإ وأ نم لاصتا ءاشنإل ايتاذ ةعقوملا تاداهشلا هذه ىلع دمعت ةمدخي لمعت ال ةداهشلا ةيخالص ءاهتنا.

و Cisco IOS زاهج ةطساوب اهؤاشنإ مت يتلا ايتاذ ةعقوملا تاداهشلا ىلع طقف رادصلال اذه رثوي ةطساوب اهؤاشنإ مت يتلا تاداهشلا رثاتت ال. زاهجال ىلع ةمدخي ىلع اهقبيبطتو Cisco IOS XE Cisco IOS ةزيم ةطساوب اهؤاشنإ مت يتلا تاداهشلا كلت نمضتت يتلاو، (CA) قدصم عجرم

ةل كشملا هذهب ،CA

ايم قرة ع قوملا X.509 تاداهش ىلع Cisco IOS و Cisco IOS XE جم انرب يف تازيملا ضعب دمتعت زاهج ىلع وأ ،يجراخ يجراخ CA ةطساوب تاداهشلا هذه عاشن ان مرتي .ةرفشملا ةي وهلا نم ققحتلل و Cisco IOS جم انرب تارادص اددحت .ايتاذ ع قوم ةداهشك هسفن Cisco IOS XE او Cisco IOS 2020-01-01 00:00:00 ىل ايتاذ ع قوملا ةداهشلا ةي حالص اهاتنا خيرات ةرثأتتملا Cisco IOS XE ةحلل اص ريغ نوكتو ةداهشلا ةي حالص يهتنت ،خيراتلا اذه دعب .يملال تي قوتلاب

لمشت ايتاذ ع قوم ةداهش ىلع دمتعت نا نكمي يتلا تامدخل:

ةماع تازيم

- اهاتنا ىل اريشي ضرعتسملا يف أطخ HTTPS جتني - (HTTPS) TLS ربع HTTP مداخل ةداهشلا ةي حالص
- ةقداصم لل X.509 تاداهش نومدختسي نيذلل نومدختسملا لشفي نا نكمي - SSH مداخل ةقداصم رثأتت ال .X.509 تاداهش مداخل سدانل (نم) .ةقداصملا يف SSH ةسلج ىلع (صاخلا/ماعلا حاتفملا ةقداصم و رورملا ةم لك/مدختسملا مسا)
- RESTCONF تالاصتلا لشفت نا نكمي - RESTCONF.

نواعتلا تازيم

- TLS ربع (SIP) لمع ةسلج ادب لوكوتورب
- ةرفشملا تاراشلا ني كمت عم Cisco نم (CME) قئافلا ةدحوملا تالاصتالا ري دم
- ةرفشملا تاراشلا ني كمت عم Cisco Unified Survivable Remote Site Telephony (SRST)
- ني كمت عم (زيمرتلا ةداعا و طئاسولا اهان اطقن و ارم ةوملا) دراوملا Cisco dspfarm نم IOS ةرفشملا تاراشلا
- مكحتلل Skinny لوكوتوربل (STCAPP) يف فاهلا لاصتالا يف مكحتلا قيبطت ذفانم ةرفشملا تاراشلا مداخلتساب اهني وكت مت يتلا (SCCP) ءالمعلا يف
- نام ا ربع H.323 تاملكملا ةراشلا لاسراو (MGCP) طئاسولا ةرابع يف مكحتلا لوكوتورب اقبس م كرتشم حاتفم نودب (IPSec) IP
- عضولا يف Cisco نم ةدحوملا تالاصتالا ةرابع تامدخل (API) تاقبب طتلا ةجمر رب ةهجاو (HTTPS مدختسي نيذلل) نم آلا

ةيكللساللا تازيملا

- يف ةعنصملا) Cisco IOS نم ةمي دقلا لوصولا طاقن ني ب LWAPP/CAPWAP تالاصتلا ا راعش ا عجار .ةيكللساللا (LAN) ةي ل حمللا ةكبشلا يف مكحتلا ةدحوو (هلبق ام و 2005 ماع لي صافاتلا نم ديزم ىلع لوصحلل [FN63942](#) يناديملا Cisco

ةل كشملا

Cisco IOS او Cisco جم انرب نم رثأتتم رادصا ىلع ايتاذ ع قوم ةداهش عاشن ا ةل و احم نع جتني اطاخلا اذه 2020-01-01 00:00:00 UTC دعب Cisco IOS XE

../cert-c/source/certobj.c(535) : E_VALIDITY : validity period start later than end

لثام لليبس يلع . "يتاذللا عيقوتللا ةداهش" يلع دمعت تامدخ يلمعت ال

- TLS تاملكم ربع SIP لمتكي ال
- لمعت ةرفشملا تاراشللا نيكمتم عم Cisco Unified CME يفلجسمللا ةزهجال دعتمل
- ليجستلاب ةزهجال ةرفشملا تاراشللا نيكمتم عم Cisco Unified SRST حمست ال
- عم (زيمرتللا ةداعل وأ طئاسوللا ةهنا ةطقن وأ رمتؤملا) Cisco IOS DSPFARM دراوم دعتمل ليجستللا ديقل ةرفشملا تاراشللا لاسرلا نيكمتم
- ليجست ةرفشملا تاراشللا مادختساب اهنيوكت مت يتلل STCAPP ذفانم دعتمل
- كرتشم حاتفم نودب IPsec ربع تاراشللا اعادتساب موقت ةبواب لالخ نم لاصتالا H.323 وأ MGCP ةطساوب اقبسبم
- Cisco Unified تاقيبطت ةجرم ربه ةهجاو مدختست يتلل API تاملكم لشفت نأ نكمي Cisco Unified Communications Gateway Services API يفلعضوللا (ذللا) نماللا عضوللا يفل (HTTPS مدختستي يذللا)
- لشف ي نأ نكمي فنوكساير
- اهتتنا يلى ريشي يذللا ، ضرعتسمللا ريذحت زاهجال ةرادل HTTPS لمعت تاسلج ضرعت ةداهشللا ةيخالص
- غالبالا وأ ةحيحص ريغ ةداهش ءاشن يفل AnyConnect SSL VPN لمعت تاسلج تلشف اهنع
- ءاشنالا يفل IPsec تالاصتلا لشفت نأ نكمي

ةرثاملا تاجتتملا يلع فرعتللا ةيفيك

ةعقوم ةداهش هيدل نوكتي نأ بجي ، نياديمللا راعشللا اذهب زاهجال رثاتي يكل : ةظالم هاندأ نيبلل وحنلا يلع رثكأ وأ ةزيم يلع يتاذللا عيقوتللا ةداهش قيبطت بجيو اي تاذ ةداهشللا ةيخالص اهتتنا دنع زاهجال ليغشت يلع طقف اي تاذ ةعقوم ةداهش دوجو رثوي ال نم لك يفل رييعامللا يفتوسي نأ بجي ، زاهجال رثاتي يكل . ايروف ءارجل بلطتت الو هاندأ 4 ةوطخلالو 3 ةوطخلال

اي تاذ ةعقوم ةداهش مدختست تنك اذام ديذحتل

1. كزاهج يلع دوجوملا رمال show running-config | begin crypto لخدأ .
2. ريفشتلل PKI ةقث ةطقن نيوكت نع ثحبا .
3. بجي . ةقثللا ةطقن ليجست نيوكت نع ثحبا ، ريفشتلل PKI ةقث ةطقن نيوكت يفل ةفاضالاب . اي تاذ اهنيوكت مت يتلل رصانعللا رثاتت يتح ةقثللا ةطقن ليجست نيوكت ةطقن مسا نأ ظحال . نيوكتللا يفل اي تاذ ةعقوملا ةداهشللا اضيأ رهظت نأ بجي ، كلذل يلى يلاتللا لثملا اذبه يفل حضورم وه امك "اي تاذ ةعقوم" تاملك يلع يوتحي ال ةقثللا

<#root>

```
crypto pki trust-point TP-self-signed-XXXXXXXXX
  enrollment
```

selfsigned

```
  subject-name cn=IOS-Self-Signed-Certificate-662415686  revocation-check none
  rsakeypair TP-self-signed-662415686 ! ! crypto pki certificate chain TP-self-signed-XXXXXXXXX certi
```

self-signed

01

3082032E 31840216 A0030201 02024101 300D0609 2A864886 F70D0101 05050030 30312E30 2C060355 040313
2D536967 6E65642D 43657274 ... ECA15D69 11970A66 252D34DC 760294A6 D1EA2329 F76EB905 6A5153C9
D19BFB22 9F89EE23 02D22D9D 2186B1A1 5AD4

راعش اب زاهجلا رثأتې نلف ؛ "ايتاذ عقوم" ل ةقثلا ةطقن ليجست نيوكت متي مل اذا
ءارج يا بولطم سيل . اذه لقحلا

ايتاذ ةعقوملا ةداهشلا ترهظ اذوا "ايتاذ عقوم" ل ةقثلا ةطقن ليجست نيوكت مت اذا
4. ةوطخلال لىل عبات . اذه لقحلا راعش لالخال نم زاهجلا رثأتې نأ نكمي ، نيوكتلا يف

نأو "ايتاذ عيقوت" ل هنيوكت مت ةقثلا ةطقن ليجست نأ 3 ةوطخلال يف ديدحتب تمق اذا . 4.
ءداهش تناك اذا ام ةفرعمل ققحت مت ، نيوكتلا يف رهظت ايتاذلا عيقوتلا ةداهش
زاهجلا لىل ع ةزيم لىل ع ةقبطم ايتاذلا عيقوتلا

ةنيعلال نيوكتلا تايلمع يف SSC ب اهطبر نكمي يتلا ةفلتخمل تازيمل ضرع متي
هذه:

- ادوجوم صنلا اذه نوكتي نأ بجي ، HTTPS مداخل ةبسنلاب :

```
ip http secure-server
```

اذا . يلاتلا زمرلا لاثم يف حضورم وه امك ةقث ةطقن فيرعت اضيا نكمي ، كلذ لىل ةفاضلاب
ايتاذ ةعقوملا ةداهشلا مادختسا وه يضارثفالا كولسلا نإف ، ادوجوم رمألا اذه نكي مل

```
ip http secure-trust-point TP-self-signed-XXXXXXXX
```

نلف ، ايتاذ ةعقوملا ةداهشلا ريغ ىرخأ ةداهش لىل ريشت تناك و ةقث ةطقن فيرعت مت اذا
رثأتت .

تاداهشلا نأل افيفط اهتيجالصل تهتنا يتلا ةداهشلا ريثأت نوكتي ، HTTPS مداخل ةبسنلاب
ننح ىتح ريدحت ءاشنإو بيولا تاضرعتسم لبق نم لعفلاب اهب قوئوم ريغ ايتاذ ةعقوملا
ريدحتلا ريغت لىل ةيجالصلل ةيهتنم ةداهش دوجو دؤي نأ نكمي . اهتيجالصل ءاهتنا مدع
ضرعتسملال يف هاقلتت يذلا

- نيوكتلا فلم يف ادوجوم صنلا اذه نوكتي ، TLS ربع SIP لىل ةبسنلاب :

```

voice service voip
  sip
    session transport tcp tls
  !
  sip-ua
  crypto signaling default trust-point <self-signed-trust-point-name>
  ! or
  crypto signaling remote-addr a.b.c.d /nn trust-point <self-signed-trust-point-name>
  !

```

- ادوجوم صننلا اذه نوكي، ةرفشملا تاراشإلا نيكمت عم Cisco Unified CME لى ةبس نلاب نيوكتللا فلم ي ف:

```

telephony-service
  secure-signaling trust-point <self-signed-trust-point-name>
  tftp-server-credentials trust-point <self-signed-trust-point-name>

```

- صننلا اذه نوكي، ةرفشملا تاراشإلا نيكمت عم Cisco Unified SRST لى ةبس نلاب نيوكتللا فلم ي ف ادوجوم:

```

credentials
  trust-point <self-signed-trust-point-name>

```

- ةداعإ وأ طئاسولا ةهاون ةطقن وأ رمتؤم) صننلا اذه دروم dspfarm Cisco نم IOS لجا نم نيوكتللا فلم ي ف ادوجوم، ةرفشملا تاراشإلا نيكمت عم (زيمرتلا:

```

dspfarm profile 1 conference security
  trust-point <self-signed-trust-point-name>
  !
dspfarm profile 2 mtp security
  trust-point <self-signed-trust-point-name>
  !
dspfarm profile 3 transcode security
  trust-point <self-signed-trust-point-name>
  !
sccp ccm 127.0.0.1 identifier 1 priority 1 version 7.0 trust-point <self-signed-trust-point-name>
  !

```

- اذه نوكي، ةرفشملا تاراشإلا مادختساب اهن نيوكت مت يتلا STCAPP ذفانم ل ةبس نلاب نيوكتللا فلم ي ف ادوجوم صننلا:

```

stcapp security trust-point <self-signed-trust-point-name>

```



```
ip ssh server certificate profile
! Certificate used by server
server
trust-point sign TP-self-signed-xxxxxx
```

- درېم لېكشنتلې ف رضاح صن اذه، RESTCONF ل

```
restconf
! And one of the following
ip http secure-trust-point TP-self-signed-XXXXXXXXXX
! OR
ip http client secure-trust-point TP-self-signed-XXXXXXXXXX
```

(لولحل) لولحل

حالصلال نمضتې رادصلال ل Cisco IOS XE او Cisco IOS جم انرب ةقرت وه لولحل

- ثدلأل تارادصلال او 16.9.1 رادصلال Cisco IOS XE جم انرب
- او؛ ثدلأل تارادصلال او 15.7(3)M5؛ ثدلأل تارادصلال او 15.6(3)M7 رادصلال Cisco IOS جم انرب
- ثدلأل تارادصلال او 15.8(3)M3


دق ةزهجأ يأل ل اهرېدصتو "ايتاذ ةعقوملا ةداهشلا" عاشنل ةداعل بجي، جم انربلا ةقرت دعب اهب صاخلل قيثوتللا نزم ي ف ةداهشلا بلطتت

جم انربلل ةقروفلل ةقرتللا ةقروملا مدع ةلاح ي ف ةلېدب لولحل ةثالث رفوتت

1. (CA) ثلثلل عزجلال نم قدصم عجرم نم ةحللص ةداهش لولل لوصحلل.
2. ةدېدج ةداهش عاشنل Cisco IOS CA مداخ مدختسأ.
3. ةدېدج ايتاذ ةعقوم ةداهش عاشنل OpenSSL مدختسأ.

1. (CA) ةقراخ ةهج نم ةحللص ةداهش لولل لوصحلل

و رېفشنتللا Comodo، Let's، لي ام ةعئاشلل CA عاونأ نمو. قدصم عجرم نم ةداهش تېبثت لېدبلا لولحل اذه مادختسأب. كلذل لولل امو Symantec و GeoTrust و Sectigo و Thawte و RapidSSL، لولل هم دقو، بلطال لوؤسملل خسني م ث. Cisco IOS ةطساوب هضرعو ةداهش بلط عاشنل م تې ةحيتنلل عجرتسيو، ثلثل فرط نم قدصم عجرم

 م تې. ةقروم ةسرامم لصفأ تاداهشلل عيقوتل قدصملا عجرملا مادختسأ ربتعي: ةظحالم ي ف رارمستسالل لصفملا نم، كلذ عمو، اذه لولل راعشل ي ف لېدب لولل لولل اذه رېفوت نم ال دب لېدبلا لولحل اذه قېببطت دعب رېغلل CA لولل نم ةعقوملا ةداهشلا مادختسأ ايتاذ ةعقوم ةداهش مادختسأ.

ي جراخ قدصم عجرم نم ةداهش تېبثت:

1. ةداهش عيقوت بلط ءاشنإ: (CSR):

```
<#root>
```

```
Router#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#
```

```
crypto pki trustpoint TEST
```

```
Router(ca-trustpoint)#
```

```
enrollment term pem
```

```
Router(ca-trustpoint)#
```

```
subject-name CN=TEST
```

```
Router(ca-trustpoint)#
```

```
revocation-check none
```

```
Router(ca-trustpoint)#
```

```
rsakeypair TEST
```

```
Router(ca-trustpoint)#
```

```
exit
```

```
Router(config)#
```

```
crypto pki enroll TEST
```

```
% Start certificate enrollment ..
```

```
% The subject name in the certificate will include: CN=TEST
```

```
% The subject name in the certificate will include: Router.cisco.com
```

```
% The serial number in the certificate will be: FTX1234ABCD
```

```
% Include an IP address in the subject name? [no]: n
```

```
Display Certificate Request to terminal? [yes/no]:
```

```
yes
```

```
Certificate Request follows:
```

```
-----BEGIN CERTIFICATE REQUEST-----
```

```
A Base64 Certificate is displayed here. Copy it, along with the ---BEGIN and ---END lines.
```

```
-----END CERTIFICATE REQUEST-----
```


```
---End - This line not part of the certificate request---
```


REMOVED
-----END CERTIFICATE-----

% Router Certificate successfully imported

2. ةديج ةداهش ءاشنإل Cisco IOS CA مءاخ مءخءسأ

ةديج ةداهش عيقوءو ءاشنإل يلءمإل IOS ءاداهش عءرم مءاخ مءخءسأ

 ءاءءنمإل عيمء ىلء يلءمإل CA مءاخ ةزيم رفوءء ال :ةظءالم

<#root>

Router#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

ip http server

Router(config)#

crypto pki server IOS-CA

Router(cs-server)#

grant auto

Router(cs-server)#

database level complete

Router(cs-server)#

no shut

%Some server settings cannot be changed after CA certificate generation.

% Please enter a passphrase to protect the private key

% or type Return to exit

Password:

Re-enter password:

% Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

% Certificate Server enabled.

<#root>

Router#

show crypto pki server IOS-CA Certificates

```
Serial Issued date Expire date Subject Name
1 21:31:40 EST Jan 1 2020 21:31:40 EST Dec 31 2022 cn=IOS-CA
```

<#root>

Router#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

crypto pki trustpoint TEST

Router(ca-trustpoint)#

enrollment url http://

:80

<<<< Replace

with the IP address of an interface on the router

```
Router(ca-trustpoint)#
```

```
subject-name CN=TEST
```

```
Router(ca-trustpoint)#
```

```
revocation-check none
```

```
Router(ca-trustpoint)#
```

```
rsakeypair TEST
```

```
Router(ca-trustpoint)#
```

```
exit
```

Router#

configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

crypto pki auth TEST

Certificate has the following attributes:

Fingerprint MD5: C281D9A0 337659CB D1B03AA6 11BD6E40

Fingerprint SHA1: 1779C425 3DCEE86D 2B11C880 D92361D6 8E2B71FF

% Do you accept this certificate? [yes/no]:

yes

Trustpoint CA certificate accepted.

Router(config)#

crypto pki enroll TEST

%

% Start certificate enrollment ..

% Create a challenge password. You will need to verbally provide this

password to the CA Administrator in order to revoke your certificate.

For security reasons your password will not be saved in the configuration.

Please take note of it.

Password:

Re-enter password:

% The subject name in the certificate will include: CN=TEST

% The subject name in the certificate will include: Router.cisco.com

% Include the router serial number in the subject name? [yes/no]: yes

% The serial number in the certificate will be: FTX1234ABCD

vrhus6LFRvVxBNPeQz2ADgLikGxatwV5EDgooM+IEucKDURGLEotaRrVU5Wk3EGM
mjC6Ko90aM30vhAGEEXrk26cq+0WsEuF3qudggRYv2gIBcrJ2iUQNFsBIrvlGHRo
FphOTqhVaAPxZS7h0B30cK1tMKHOIa8EwygyBvQPfjjBT79QFgeexIJFmUtqYX/P

tT6r4SuibYKu6HV45ffjSz0imcJI+D9LKhLWR6pK/k5ge8v7aK9/rsVbjavbdy7b
CSqGSib3DQEJFTEWBBS96DY/gRfN1dSx46P1EqjPvSYiETAxMCEwCQYFKw4DAhOF
AAQU+EX0kNvuNz6XmFxxER8w1qKTGvgECA+D+Z81uwafAgIIAA==

Cisco IOS و Cisco IOS XE جوم ىلع لاثم

```
<#root>
```

```
Router#
```

```
configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#
```

```
crypto pki trustpoint TEST
```

```
Router(ca-trustpoint)#
```

```
enrollment terminal
```

```
Router(ca-trustpoint)#
```

```
revocation-check none
```

```
Router(ca-trustpoint)#
```

```
exit
```

```
R1(config)#
```

```
crypto pki import TEST pkcs12 terminal password Cisco123
```

Enter the base 64 encoded pkcs12.

End with a blank line or the word "quit" on a line by itself:

```
MIIII8QIBAZCCCLcGCSqGSIb3DQEHAAcCCCKgEggiKMIIIoDCCA1cGCSqGSIb3DQEH  
BqCCA0gwgGNEAgEAMIIDPQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQYwDgQItyCo  
Vh05+0QCaggAgIIDENUWY+UeuY5sIRZuoBi2nEhdIPd1th/auBYtX79aXGiz/iEW
```

```
IY11273y9bC3qPVJ0UGoQW8SGfarqEjaqxdAet66E5V6u9Yvd4oMsIYGsa70m+FN  
CsUVj+115hzGjK78L0ycXWpH4gDOGYBVf+D7mgWqaqZvxYUoEkOrTMmW5zE1MCMG  
CSqGSib3DQEJFTEWBBSgiBJIYpJLzo/GYN0sesZh3wGmPTAxMCEwCQYFKw4DAhOF  
AAQUdeUrLIC2uo/mbyE86he5+qEjmPYECKu76GWaeKb7AgIIAA==
```

```
quit
```

```
CRYPTO_PKI: Imported PKCS12 file successfully.
```

```
R1(config)#
```

4. ديدجلا ءءاهشلا لآبببب نم ءكاآ

<#root>

R1#

```
show crypto pki certificates TEST
```

```
Load for five secs: 5%/1%; one minute: 2%; five minutes: 3%
```

```
Time source is SNTP, 15:04:37.593 UTC Mon Dec 16 2019
```

```
CA Certificate
```

```
Status: Available
```

```
Certificate Serial Number (hex): 00A16966E46A435A99
```

```
Certificate Usage: General Purpose
```

```
Issuer:
```

```
cn=SelfSignedCert
```

```
Subject:
```

```
cn=SelfSignedCert
```

```
Validity Date:
```

```
start date: 14:54:46 UTC Dec 16 2019
```

```
end date: 14:54:46 UTC Nov 28 2030
```



2020 ينائل نوناك 1 00:00 في اباتاءة عقوملا تاءاهشلا ءءءال صءهتنت :ءظءالم
تقوللا كلء ءعب اهءاشنل كنكمي الوي ملءال لآبببب.

ءبوءاء ءلئساء

ءة لكشملل لل ام :لاؤس

يآللا آاءآنمل لل علل اهؤاشنل مآ يآلل X.509 ءءقوآلل ءءءال PKI آاءاهش ءءءال صءهتنت
ال .ملءال لآبببب 01/01/2020:00:00 في Cisco IOS و Cisco IOS XE آاراء صءاب لمآءآ
01/01/2020 00:00:00 ءعب ءرآأآملل ءزهأل لل علل ءءقوآلل ءءءال صءهتنت ءءءال صءهتنت
ءعب لمآءآ نأ اباتاءة عقوملا تاءاهشلا هءه لل ءمآءآ ءمءءل الل نكمي ال .ملءال لآبببب
ءءاهشلا ءءءال صءهتنت.

ابآاءة عقوم ءءاهش ءءءال صءهتنت اءل لمءلل ءءبش لل رءآأآلل وه ام :س
اهآءنمل

ءءءال صءهتنت اءعب لمآءآ اباتاءة عقوم تاءاهش لل ءمآءآ ءرآأآءل ءنم لآ ءففظو ءوآء نل
ءففاضل لمءل صءافآء لل علل لوصللل لءءال راعشل ءءءارم اعءلل .ءءاهشلا

ءءففرضقلا هءهب ارآأآءل تنك اءل ام فرءأ نأ لل فءك :س

ناك اءل امو اباتاءة عقوم ءءاهش مءءءسآءل تنك اءل ام ءءءلل آاءاشرل لءءال راعشل رفوي
لل فرءآل ءففك" مءسق ءءءارم لءءرل .ءل لكشملل هءهب رآأآءل ءب صلءال نل ءوآءلل
لآبببب راعشل الل في "ءرآأآءل لآبببب آاءآنمل

ةرثأت م تنك اذا ام ىرأل هليغشت عي طتسأ صن كانه له

ليغشت ليغشتب مق ، Cisco نم رماوأل رطس ةهجاو ل لحم) Cisco CLI Analyzer مدختسأ .معن
هضرع نكمي هي بنت مادختسأ متو ةدوجوم ةداهشلا تنك اذا .ماظنلا صيخشت ليغشت
<https://cway.cisco.com/cli/>

ةلكشملا هذهل ةيجمرب لولح Cisco تم دق له .q

ةلاحي في ةليدب لولح لىل ةفاضل اب ةلكشملا هذهل ةيجمرب لولح رادصاب Cisco تماق .معن
ليصافتلا لىل لوصحلل لولح لراعش ةعجارم عاجرلا .روفلا لىل عجماربلا ةيقرت ةينكما مدع
ةلماللا .

ةداهش مدختسي Cisco نم جتنم ي لىل ةلكشملا هذهل رثوت له .q

مت ي تلاو ايتا ةعقوم تاداهش مدختست ي تلا تاجتنم لىل طقف ةلكشملا هذهل رثوت .ال
مدخل لىل ةقبطملا ةداهشلا عم Cisco IOS و Cisco IOS XE نم ةدجم تارادصا ةطساوب اهؤاشن
عجرملا لبق نم اهؤاشن مت ي تلا تاداهشلا مدختست ي تلا تاجتنم لىل رثوت ال .جتنم لىل
ةلكشملا هذهل (CA) قدصملا .

طقف ي تاذلا عيقوتلا تاداهش Cisco تاجتنم مدختست له :س

Cisco زاهج لىل و اةيجراخ ةهجل عبات ي جراخ تاداهش عجرم ةطساوب ام تاداهشلا عاشن نكمي .ال
ةدجملا مدختستم تابلطم بلطت دق .ايتا ةعقوم ةداهشك هسفن Cisco IOS و Cisco IOS XE
ال (CA) قدصملا عجرملا لبق نم اهؤاشن مت ي تلا تاداهشلا .ايتا ةعقوم تاداهش مادختسأ
ةلكشملا هذهل رثوت .

ةلأسملا هذهل تثدح اذامل .س

نإف ، ايجولونكتلا وعئاب اهذب ي تلا ةثيثلحلا دوهجل نم مغرلا لىل هنأ فسؤملا نم نكلو
تاينقت نم ةينقت ي ا ي أطخ فاشتك متي ام دنع .ةدوجوم لازت ال تايجمربلا ي فبويعل
ةياملح نومدختسمل اجاتحي ي تلا تامولعمل ريفوتبو ةيفافشلاب نومزتل م انإف ، Cisco
مهتكبش .

ةرثأت م تارادصا ل نكمي شيح فورعم يجمرب أطخ نع ةجتان ةلكشملا نوكت ، ةلاجل هذهل
لىل ايتا ةعقوملا ةداهشلا ةيصالص اهت نا خيرات نييعت امئاد Cisco IOS و Cisco IOS XE نم
دق امم ، ةلص ريغ نوكتو ةداهشلا ةيصالص يهتنت ، خيراتلا اذله دعب . 01/01/2020:00:00 UTC
جتنم لىل ةفيظو لىل رثوت .

2020 00:00:00 ي ناثلا نوناك 1 ي ةيصالصلا اهت نا خيرات رايخا مت اذامل :س
ي ملاءل تي قوتلاب

1 خيرات مادختسأ مت ، اذله جم انربلا أطخ ةلاحي في .ةيصالص اهت نا خيرات ةداع تاداهشلل نوكتي
أطخ وهو تاونس 10 نم رثكأ ذنم Cisco IOS و Cisco IOS XE جم انرب ريوطت اناثا 2020 ريان ي
يرشب .

ةلكشملا هذهل رثوت ي تلا تاجتنم لىل ام :س

و 15.6(03)M07 تارادصل لبق Cisco IOS تارادصل لغشت Cisco تاجت نم نم جت نم ي
Cisco IOS XE تارادصل لغشي Cisco نم جت نم ي أو 15.9(03)M و 15.8(03)M03 و 15.7(03)M05،
لق 16.9.1

هل عرف نيمدختس ملال على بجي يذلا ام: لاؤس

رمألا ناك اذو، ةلكشملا هذو ارثأتم تنك اذا ام مبيقتل ينادي ملال راعش الة عجارم على جاتحت
ةلكشملا هذو نم دحلل ليدبلال لحل/لحل تاداشرا مادختس على لعلف، كذلك

ةينمأ فعض ةطقن لكشت ةلأس ملال هذو له: س

جت نم ملال ةمالس على رطخي أكانه سي لو، ينمأ فعض ةطقن تسيل هذو. ال

SSH لوكوتورب رثاتي له: س

يكل. ردان نيوكت يف ال تاداهشل مادختس ي ال هنكلو RSA حيتافم جاوزا SSH مدختس ي. ال
ادوجوم يلاتل نيوكتل نوكي نأ بجي، تاداهشل Cisco IOS مدختس ي.

```
ip ssh server certificate profile
server
trust-point sign TP-self-signed-xxxxxx
```

ة عرسب ةيدي لقتل Catalyst ةمظنال ةرفوت ملال ةتبال تارادصل ال يه ام: س
ة قيقدل ي ة فل فال 4 و ة قيقدل ي ة فل فال 3 و ة قيقدل ي ة فل فال 2
ة قيقدل ي ة فل فال 6 و

رفوتي، (Polaris (3650/3850/Catalyst 9K Series) على ةدنتس ملال ةيساس ال ةمظنال ةبس نلاب
هدعب ام و 16.9.1 نم حالصل ال
هدعب ام و 15.2(7)E1a حالصل ال رفوتي، CDB يساس ال ماظن لل ةبس نلاب

ىرخال ةيدي لقتل ال ةيساس ال لي وحتل تا صن مل ةبس نلاب

CCO رادصل يوتحي نأ نكمي. وأ يس حارس قالط رشنن مل اننكل مدقتل ديقتامازتل كانه
حالصل ال على يلاتل

تنرتن ال ي ةرفوت ملال ىرخال لولحل دأ مادختس ي جري

ي م ال س ال لمع ال ةي عمج رثات له: س

لاصتا عطق مت، كلذ عمو، رورم ال ةكرح نيسحت وحي حص لكشب لمع ال ي WAAS رمتس ي
اذو. ةي حالصل ال ةيهت نم اي تاذ ةعقوم ةداهش هي دل يذل زاوجل اب Central Manager و AppNav-XE
WAAS ل صاوي، زاجي اب و WAAS ل جهن ي أري غت و AppNav-Cluster ةبقارم كنكمي ال هنأ ينعي
ةداهشل ةلكشم لحت نأ على اتقوم افقوت ةبقارم لاو ةرادال نكلو، ميلس وحن على لمع ال
ةرادال" على ال اداري تس م Cisco IOS على ةديج ةداهش عاشن مزلي دق، ةلكشم لال حل
"ةيزك رمل"

ةلص تاذا تامولعم

- يف عيقوتلا ةيتاذ PKI ةداهش ةيخالص ءاهتنا - FN - 70489 :يناديم راعشا | [FN70489](#) عجار
Cisco IOS و Cisco IOS XE جم انرب
- عجار [CSCvi48253](#) Cisco نم ءاطخال احيصت فرعم عجار

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل