

تالوحم ىلع بىولا ةرادا تاداهش تىبثت Catalyst 9000 Switches

تايوتحملا

[ةمدقملا](#)

[ةيساسالابلاطتلا](#)

[تابلطتلا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتلا](#)

[حاتفم ديدحت 1: ةوطخلا](#)

[\(CSR\) ةداهش عي قوت بلط عاشنا 2: ةوطخلا](#)

[\(CA\) قديملا عجرملا لىلا CSR مديقت 3: ةوطخلا](#)

[64 ةيساسالارنجلال قديملا عجرملا ةداهش ةقداصم 4: ةوطخلا](#)

[Device Base64 ةداهش ةقداصم 5: ةوطخلا](#)

[Catalyst 9000 switch لوجملا ىلع زاولا نم ةعقوم ةداهش داريتسا 6: ةوطخلا](#)

[ةديدل ةداهشلا مادختسا 7: ةوطخلا](#)

[بىولا تاضرعتسم لبق نم اهب قوتوم ةداهشلا نأ نم دكأتلا ةيفيك 8: ةوطخلا](#)

[ةحصلا نم ققحتلا](#)

[اهخالصاو ءاطخال فاشكتسا](#)

[ةلصتا اذ تامولعم](#)

ةمدقملا

حاتفم 9000 sery ةزافح ةدام ىلع ةداهش تىبثتو ،بلجي ،قلخي نأ ةيلمعلا ةقيثو اذه فصى

ةيساسالابلاطتلا

تابلطتلا

ةيلالتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- Catalyst 9000 Series Switches تالوحم نيوكت ةيفيك
- Microsoft Windows Server مادختساب تاداهشلا عي قوت ةيفيك
- ةيمقرلا تاداهشلاو (PKI) ماعلا حاتفملا ةيساسالابلا ةينبلا

ةمدختسملا تانوكملا

ةيلالتلا ةيداملا تانوكملا وجماربلا تارادصا لىلا دنتسملا اذه يف ةدراولا تامولعملا دنتست

- Cisco Catalyst 9300 Switch، Cisco IOS® XE، رادصا 17.12.4 لوجملا

- Microsoft Windows Server 2022 لي غشتال ماظن

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنتسملا اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذإ .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجال عيمج تادب رما يال لمحتحمل ريثاتلل كمهف نم دكأتف ،لي غشتال دي ق ك تكبش

ةيساسأ تامولعمل

نم هعيقوتو ،(CSR) ةداهشل عيقوت بلط عاشنإل ةوطخب ةوطخ ليلد دنتسملا اذه مدقي Catalyst 9000 لوحم يلع (CA ةداهش عم) ةجتانلا ةداهشل تي ب ثتو ،(CA) قدصم عجرم لبق switch.

نمضي امم ،اهب قوثوم ةداهش مادختساب لوحملل (HTTPS) ةنمآل بيولا ةرادا ني كمت وه فدهل ةيميظنتلا نامآل تاسايس عم قفاوتلاو ةثيدحل بيولا تاضرعتسم عم قفاوتلا

نيوكتلا

يلع اهتي ب ثتو اهعيقوتو بيو ةرادا ةداهش عاشنإل يلي صفت لمع ريس مسقلا اذه رفوي لاثملا تاجرخمو ،تاري سفتو ،ةلص تاذا CLI رماو ةوطخ لك نمضتت .Catalyst 9000 switch لوحم

حاتفم ديدحت :1 ةوطخل

نوكي نا بجي .ةداهشل ني مأتل همادختساو ةماعل ضارغلل RSA حي تافم جوز عاشنإ ب مق (تب 4096 ىلإ 1024 نم) نامآل تاجايتحال اقفو همجح ديدحت نكمي و ري دصتلل الباق حاتفملا

```
<#root>
```

```
device(config)#
```

```
crypto key generate rsa general-keys label csr-key exportable
```

ل:ماعم مجح بلطي ام دنع جرخملا لاثم

```
<#root>
```

```
The name for the keys will be:
```

```
csr-key
```

```
Choose the size of the key modulus in the range of 512 to 4096 for your General Purpose Keys. Choosing How many bits in the modulus [1024]:
```

```
4096
```

```
% Generating 4096 bit RSA keys, keys will be exportable...
```

```
[OK] (elapsed time was 4 seconds)
```

CSR (Certificate Signing Request) إعدادات بلطاشنإ 2: ةوطخل

ةدحول ربق ليجستل ددحيو، بيولا لوؤسم ةداهشل لوحمل ىلع TrustPoint نيوكتب مق
عوضومل مسا فيرعتل تامولعم ريفوتو، لاطبالا نم ققحتل ليطعتو، ةيفرطل
(ةلبدل عوضومل امساو، حاتفملا).

```
<#root>
```

```
device(config)#  
crypto pki trustpoint webadmin-TP  
device(ca-trustpoint)#  
enrollment terminal pem  
device(ca-trustpoint)#  
revocation-check none  
device(ca-trustpoint)#  
subject-name C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain  
device(ca-trustpoint)#  
rsakeypair csr-key  
device(ca-trustpoint)#  
subject-alt-name mywebadmin.com  
device(ca-trustpoint)#exit
```

ميدقت؛ ةددعتم تاراخي ميدقت كنم بلطي نا بجي. CSR عاشنإل ةقثل ةطقن ليجستب مق
ةيفرطل ةدحول ىلع ةداهشل بلط ضرع بجي. ةجالح بسح "ال" وأ "معن"

```
device(config)#crypto pki enroll webadmin-TP
```

جاخلال لاثم:

```
<#root>
```

```
% Start certificate enrollment ..  
% The subject name in the certificate will include:  
  
C=SJ, ST=CA, L=CA, O=TAC, OU=LANSW, CN=myc9300.local-domain  
  
% The subject name in the certificate will include: C9300.cisco.com  
% Include the router serial number in the subject name? [yes/no]: yes  
% Include an IP address in the subject name? [no]: yes  
Display Certificate Request to terminal? [yes/no]: yes  
Certificate Request follows:  
-----BEGIN CERTIFICATE REQUEST-----
```

```
-----END CERTIFICATE REQUEST-----  
---End - This line not part of the certificate request---  
Redisplay enrollment request? [yes/no]:  
  
no
```

عوضومال مسا نيوكتل ةرفوتمال تاملعمل:

- (ةدحتمال تاياالوال) طقف نييري بك ني فرح، دلبل: C:
- ةعطاقمال وأ ةيالوال مسا: تناس
- (ةني دمال) عقومال مسا: ل:
- (ةكرشال) ةسسؤمال مسا: س:
- (مسقلال/مسقلال) ةي ميظنتال ةدحوال مسا: ش:
- (هلال لوصول م تيس يذل IP ناو نع وأ FQDN) عئاشال مسالال: ن ي س

(CA) ق دصمال عجرمال الى CSR مي دقت: 3 ةوطخلال

عجرمال الى اهل اسراو (ةياهنل او ةي ادبل يطخ كلذ ي ف امب) ةلماكلال CSR ةلسلس خسنا عي قوتمل ق دصمال.

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

ةعقومال ةداهشال لي زنتب مق Microsoft Windows Server، ل ق دصم عجرم مدختست تنك اذا رذل ق دصمال عجرمال ةداهش ام برو عقومال زاهال ةداهش ىقلتت ام ةدعو. Base64 قيسننتب

64 ةيساسأل رذل ق دصمال عجرمال ةداهش ةق داصم: 4 ةوطخلال

كلزاه ةداهش ردصأ يذل CA ي ف ةقث عاشنال لوحمال الى (Base64 قيسننتب) CA ةداهش تبث

```
<#root>  
  
device(config)#  
  
crypto pki authenticate webadmin-TP
```

لاثم. اهبلط دنع (ةياهنل او ةي ادبل رطسأ كلذ ي ف امب) ق دصمال عجرمال ةداهش قصلال

```
<#root>  
  
Enter the base 64 encoded CA certificate.  
End with a blank line or the word "quit" on a line by itself  
-----BEGIN CERTIFICATE-----
```

```
-----END CERTIFICATE-----
Certificate has attributes:
    Fingerprint MD5: C7224F3A A9B0426A FDCC50E6 8A04583E
    Fingerprint SHA1: 9B31C319 A515AC41 0114EA43 33716E8B 472A4EF5
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
%

Certificate successfully imported
```

Device Base64 ةداهش ةقداصم 5: ةوطخل

ةتبتثمل قداصم ل عجرم ل ةداهش ل باقم زاهل ل ةعقوم ل ةداهش ل ةقداصم

```
<#root>
device(config)#
crypto pki trustpoint webadmin-TP
device(ca-trustpoint)#
chain-validation stop
device(ca-trustpoint)#
crypto pki authenticate webadmin-TP
```

زاهل ةداهش ي ف قصل، ةبلاطم ل دن ع

```
<#root>
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
Certificate has the following attributes:
Fingerprint MD5: DD05391A 05B62573 A38C18DD CDA2337C
Fingerprint SHA1: 596DD2DC 4BF26768 CFB14546 BC992C3F F1408809
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Catalyst 9000 switch ل وحم ل ل ع زاهل نم ةعقوم ةداهش داريتس 6: ةوطخل

TrustPoint ل Base64 ل عقوم ل زاهل ةداهش داريتس

```
<#root>
```

```
device(config)#
```

```
crypto pki import webadmin-TP certificate
```

اهب ل ط دن ع ةداهش ل ق صل

```
<#root>
```

Enter the base 64 encoded certificate.

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

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

```
< 9300 device certificate >
```

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

```
% Router Certificate successfully imported
```

ت اذ (CA) ةق دصم ل عجارم ل عي م ع ل و ح م ل ل زاه ل ةداهش ل اري ت س ل م ت ي ، ة ط ق ن ل ه ذ ه دن ع م د خ ت س م ل ة ه ج ا و ل ل ل و ص و ل ك ل ذ ي ف ا م ب ، م ا د خ ت س ل ل ة ز ه ج ة د ا ه ش ل ن و ك ت و ، ة ل ص ل ل ة م و س ر ل ل (HTTPS).

ة د ي د ج ل ة د ا ه ش ل م ا د خ ت س ل : 7 ة و ط خ ل

ل و ح م ل ل ل ع HTTPS ل و ص و ن ي ك م ت و ن م آ ل HTTP م د ا خ ب TrustPoint ن ا ر ق ا ب م ق

```
<#root>
```

```
device(config)#
```

```
ip http secure-trustpoint webadmin-TP
```

```
<#root>
```

```
device(config)#
```

```
no ip http secure-server
```

```
<#root>
```

```
device(config)#
```

```
ip http secure-server
```

بېيولا تاضرعتسم لبق نم اه ب قوټوم ةداهشلا نأ نم دكأتلا ةيفيك: 8 ةوطخلا

- ناوئع عم (SAN) ليدبلا عوضوملا مسا وأ (CN) ةداهشلل عئاشلا مسالا قباطتي نأ بجي .
ضرعتسملا لبق نم هيلا لوصولا مت يذلا URL
- اهتيخالص هدم نمض هداشلا نوكت نا .
- (قدصملا عجرملا ةلسلس وأ) (CA) قدصملا عجرملا لبق نم ةداهشلا رادصا متي نأ بجي
لوحمل رفوي نأ بجي .ضرعتسملا لبق نم هب اقوټوم هب صاخلا رذجل نوكي يذلا
ادوجوم ةداع نوكي يذلاو، رذجل قدصملا عجرملا ءانثتساب) ةلماكلا تاداهشلا ةلسلس
(ضرعتسملا نزخم ي ف لعفلاب
- اهليزنت هنكمي ضرعتسملا نأ نم دكأت ف ،لاطبإ مئاقو ىلع يوتحت ةداهشلا تناك اذا
لاطبإ مئاق يا ي ف ةداهشلل CN چاردا مدع نمو

ةحصللا نم ققحتلا

ةيلاحلا ةلاحلاو ةداهشلا نيوكت نم ققحتلل رماوالا هذه مادختسا كنكمي

ةقثلا ةطقنل اهتلاحو ةتبٲملا تاداهشلا ضرع

<#root>

device#

show crypto pki certificate webadmin-TP

چاخاللا لاثم

<#root>

Certificate Status:

Available

Certificate Serial Number (hex): 4700000129584BB4BAFA13EABB000000000129

Certificate Usage: General Purpose

Issuer:

cn=mitch-DC02-CA dc=mitch dc=local

Subject: Name:

C9300.cisco.com

Serial Number: XXXXXXXXXX

cn=

myc9300.local-domain

ou=LANSW

o=TAC

l=CA
st=CA
c=SJ

hostname=C9300.cisco.com

Validity Date:

start date: 05:09:42 UTC Jun 12 2025

end date: 07:25:06 UTC Dec 16 2026

Associated Trustpoints:

webadmin-TP

CA Certificate Status: Available

Certificate Serial Number (hex): 101552448B9C2EBB488C40034C129F4A

Certificate Usage: Signature

Issuer: cn=mitch-DC02-CA dc=mitch dc=local

Subject: cn=mitch-DC02-CA dc=mitch dc=local

Validity Date:

start date: 07:15:06 UTC Dec 16 2021

end date: 07:25:06 UTC Dec 16 2026

Associated Trustpoints: webadmin-TP RootCA

ةنرتقم لاة قث لاة طقنو HTTPS م داخ ة لاه نم ققحت:

<#root>

device#

show ip http server secure status

ج ا ر خ ا ل ل ا ث م :

<#root>

HTTP secure server status: Enabled

HTTP secure server port: 443

HTTP secure server ciphersuite: rsa-aes-cbc-sha2 rsa-aes-gcm-sha2

dhe-aes-cbc-sha2 dhe-aes-gcm-sha2

ecdhe-rsa-aes-cbc-sha2

ecdhe-rsa-aes-gcm-sha2 ecdhe-ecdsa-aes-gcm-sha2

HTTP secure server TLS version: TLSv1.2 TLSv1.1

HTTP secure server client authentication: Disabled

HTTP secure server PIV authentication: Disabled

HTTP secure server PIV authorization only: Disabled

HTTP secure server trustpoint: webadmin-TP

HTTP secure server peer validation trustpoint:
HTTP secure server ECDHE curve: secp256r1
HTTP secure server active session modules: ALL

اهال صإو ءاطخأل فاشك تسإ

تاكرح حيحصت نيكم تل رم اوأل هذه مدختسأ ، ءداهشلإ تيبتت ءي لمع ءانثأ لكاشم تهجاو اذا
اهل ي جست وأ ءداهشلإ داري تسإ ءانثأ لشفلإ تالاح صيخشتل صاخ لكشب دي فم اذهو . PKI

<#root>

device#

debug crypto pki transactions

حجان ويراني س ءاطخأ حيحصت جارخا دلع لاثم

<#root>

*Jun 12 05:16:03.531: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named C9300.cisco.com has been generated or
*Jun 12 05:16:03.534:

%CRYPTO-6-AUTOGEN: Generated new 2048 bit key pair

*Jun 12 05:16:03.556: CRYPTO_PKI: unlocked trustpoint RootCA, refcount is 0
*Jun 12 05:16:03.556: CRYPTO_PKI: using private key C9300.cisco.com for enrollment
*Jun 12 05:16:04.489: CRYPTO_PKI: Adding myc9300.local-domain to subject-alt-name field
*Jun 12 05:16:17.463: CRYPTO_PKI: using private key csr-key for enrollment
*Jun 12 05:18:32.378: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:19:15.464: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:19:15.470: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0
*Jun 12 05:19:15.472: CRYPTO_PKI: (A018E) Session started - identity not specified
*Jun 12 05:19:15.473: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a subject match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Check for identical certs
*Jun 12 05:19:15.473: CRYPTO_PKI: Found a issuer match
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Suitable trustpoints are: RootCA,
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E) Attempting to validate certificate using RootCA policy
*Jun 12 05:19:15.473: CRYPTO_PKI: (A018E)

Using RootCA to validate certificate

*Jun 12 05:19:15.474: CRYPTO_PKI(make trusted certs chain)
*Jun 12 05:19:15.474: CRYPTO_PKI:

Added 1 certs to trusted chain.

*Jun 12 05:20:05.555: CRYPTO_PKI: locked trustpoint webadmin-TP, refcount is 1
*Jun 12 05:20:25.734: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0
*Jun 12 05:20:25.735: CRYPTO_PKI(Cert Lookup)

issuer="cn=mitch-DC02-CA,dc=mitch,dc=local"

serial number= 10 15 52 44 8B 9C 2E BB 48 8C 40 03 4C 12 9F 4A
*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_get_cert_record_by_cert()

*Jun 12 05:20:25.735: CRYPTO_PKI:

Found a cert match

*Jun 12 05:20:25.735: CRYPTO_PKI: crypto_pki_authenticate_tp_cert()

*Jun 12 05:20:25.735: CRYPTO_PKI: trustpoint webadmin-TP authentication status = 0

*Jun 12 05:20:32.094: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing

*Jun 12 05:20:32.096: CRYPTO_PKI:

Notify subsystem about new certificate.

*Jun 12 05:20:32.097: CRYPTO_PKI: unlocked trustpoint webadmin-TP, refcount is 0

*Jun 12 05:21:50.789: CRYPTO_PKI:

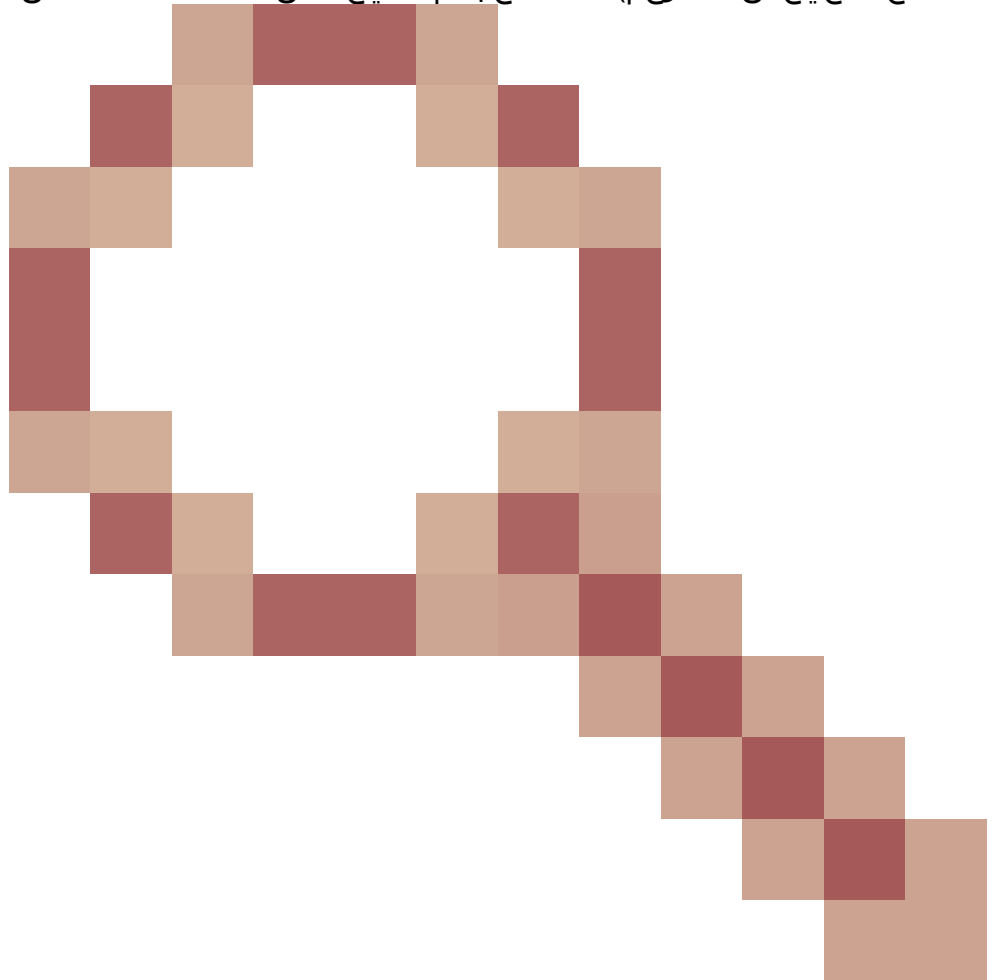
using private key csr-key for enrollment

*Jun 12 05:22:12.947: CRYPTO_PKI:

make trustedCerts list for webadmin-TP

دويقلو تاطحال مل

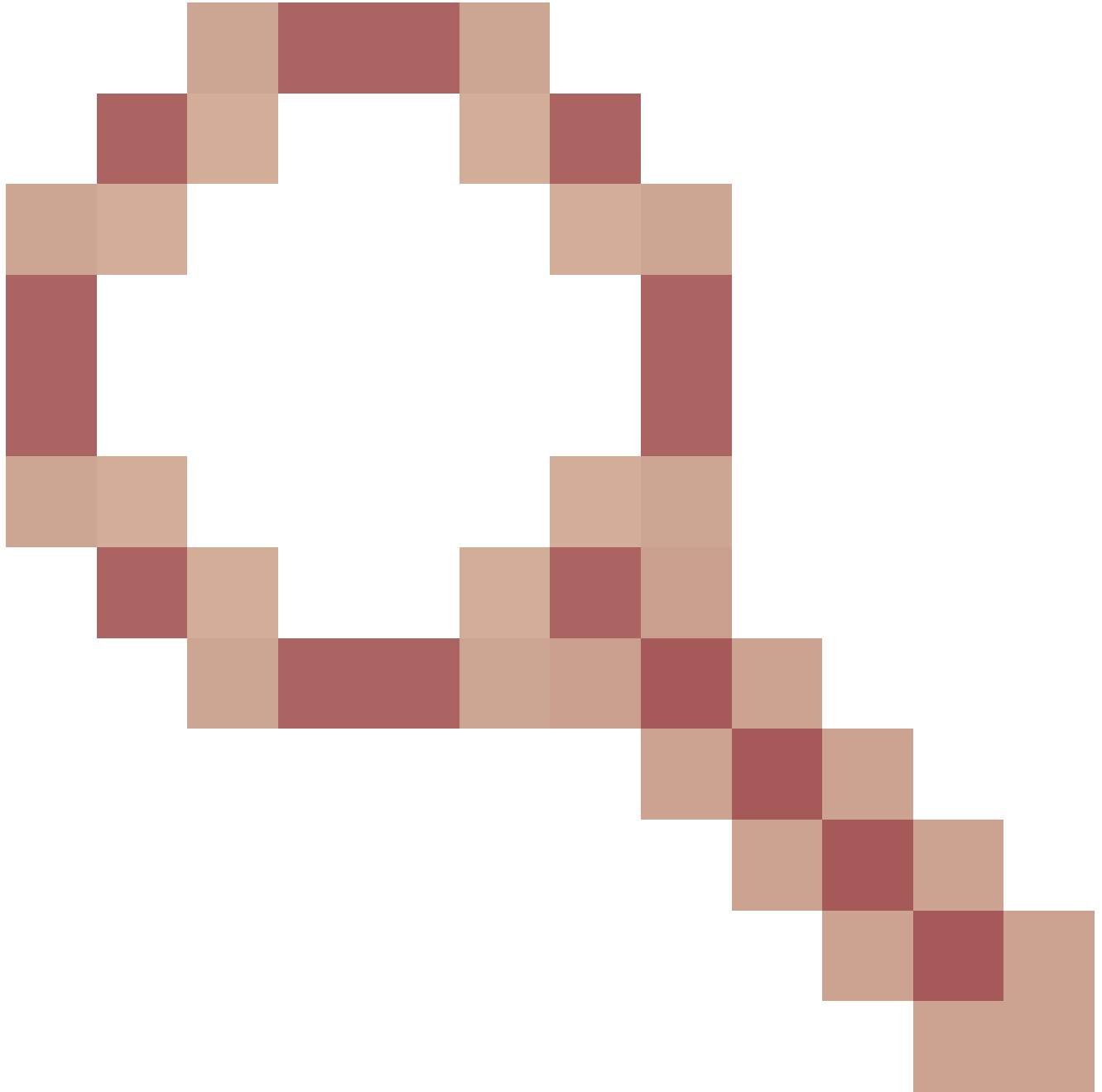
- عا طخال حي حصت فرعم (2099 دعب امل ةي حال صلا تاذا CA تادامش Cisco IOS® XE م عدي ال



نم Cisco [CSCvp64208](#)

).

- ةم و عدم ةم و جم SHA256 (ةم و جم SHA256 PKCS 12 ةل اسر صخلم Cisco IOS® XE م عدي ال ةم و جم SHA256 عم ةع قوم اه سفن PKCS12 ةم زح تناك اذا سيل نكل نم عا طخال فرعم) Cisco [CSCvz41428](#)



17.12.1 رادصإلا يف اذه حالصإ مت .)

ةلص تاذا تامولعم

- [Cisco نم تاليزنت لاويفن فلإ مع دلإ](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط 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 م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا