

IOS زاھج ىلع TLS 1.3 ربع TACACS+ نىوكت ISE مادختساب XR

تايوتحمل

[قمدملا](#)

[قماع قرظن](#)

[لىلدلا اذه مادختسا](#)

[قيساسال تابلطتملا](#)

[تابلطتملا](#)

[قمدمتسملا تانوكملا](#)

[صيخرتلا](#)

[قزھجالا قراڊال ISE نىوكت - 1 عزجلا](#)

[TACACS+ مڊاخ ققڊاصمل قڊاھشلل عىقوت بىلط عاشنا](#)

[TACACS+ مڊاخ ققڊاصمل بڭجلا قڊصملا عجرملا قڊاھشلل عىقوت](#)

[ISE ب \(CSR\) عقمول قڊاھشلل عىقوت بىلط طبر](#)

[TLS 1.3 نىكمت](#)

[ISE ىلع قزھجالا قراڊال نىكمت](#)

[TLS ربع TACACS نىكمت](#)

[قكبشلل قزھجاو قكبشلل قزھجاو تاعومجم عاشنا](#)

[ConfigureIdentity رجاتم](#)

[TACACS+ فىرعت تافل م نىوكت](#)

[لوؤسملا فىرعت فلم - IOS XR RW](#)

[لغشملا فىرعت فلم - IOS XR RO](#)

[configureTACACS+ رماوا تاعومجم](#)

[Cisco IOS XR RW - رماوا قعومجم](#)

[Cisco IOS XR RO لغشملا رماوا قعومجم](#)

[زاھجالا لوؤسم جھت تاعومجم نىوكت](#)

[TLS 1.3 ربع Cisco IOS XRfor TACACS+ نىوكت - 2 عزجلا](#)

[قيلوالا قئىھتلا تايلمع](#)

[TrustPoint نىوكت](#)

[TLS مادختساب TACACS & AAA نىوكت](#)

[قڊاھشلل ڊيڭت](#)

[ققحتلا](#)

[اھجال صاوا طاخلال افاشكتسا](#)

قمدملا

مڊاخك (ISE) Cisco Identity Services Engine عم TLS ربع TACACS+ ل الاثم دنتسملا اذه فصى
للمعك Cisco IOS® XR زاھجو.

ةماع ةرطن

ةيفرطال ةطحمل الى لوصول م كحت ةدحو الى لودل ةبقارم ماظن لوكوتورب حيتي ةكبش الى لوصول مداوخو تاهجوم لل زاهجل ةيزكرم ال ةرادال ةيناكم [RFC8907] (TACACS+) تامدخ رفوي وهو. رثكأ وأ دحاو TACACS+ مداخ لال خ نم ةكبش لاب ةلصت ال ىرخال ةزهجال او ةزهجال ةرادا مادختسا تالاحل اصيصخ ةممصم ال، (AAA) ةبساحم ل او ضيوفت ل او ةقداصم ال.

لقن ةقبط لال خ نم لوكوتورب ال نيسحت ىلع [RFC8446] TLS 1.3 ربع TACACS+ لمعي ةهازنل او ةيرسل لمكتل اذه نمضي. ةيساسحل ةديش تانايل ال ةيامح ىلع لمعي امم، ةنم مداوخال او TACACS+ ءالمع نيب ةكبش ال رورم ةكرحو لاصلت ال ةقداصم ال.

ليلدل اذه مادختسا

ةكبش ال ةزهجال يرادل لوصول ةرادا نم ISE نيكمتل نيئزج الى ةطشنال ليلدل اذه مسقي Cisco IOS XR الى ةدنتسم ال.

- زاهجل لوؤسم ل ISE نيوكت - 1 ءزجل
- TLS ربع TACACS+ ل Cisco IOS XR نيوكت - 2 ءزجل

ةيساسال تابلطتم ال

تابلطتم ال

TLS ربع TACACS+ نيوكت تابلطتم:

- عيقوتل TLS ربع TACACS+ لبق نم ةمدختسم ال ةداهش ال عيقوتل (CA) قدصم عجرم ةكبش ال ةزهجال ISE تاداهش.
- (CA) ةداهش ال حنم ةهج نم رزجل ةداهش ال.
- ءامسأ ل ح اهنكمي و DNS الى لوصول ةيناكم الى ل ISE و ةكبش ال ةزهجال يوتحت فيضم ال.

ةمدختسم ال تانوكم ال

ةيلات ال ةيدام ال تانوكم ل او جمارب ال تارادصل الى دنتسم ال اذه في ةدراول تامولعمل دنتست:

- ISE VMware، يرهاظل زاهجل 3.4 Patch 2 رادصل ال
- 25.3.1 رادصل ال، Cisco 8201 ءجوم ال

ةصاخ ةيلمعم ةئيبي في ةدوچوم ال ةزهجال نم دنتسم ال اذه في ةدراول تامولعمل ءاشنإ م تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسم ال اذه في ةمدختسم ال ةزهجال عيمج تأب رمأ يال لمحتم ال ريثأتلل كمهف نم دكأتف، ليغشتل دي قكتكبش.

صيخرت ال

في. ةسايس ال ةمدخ ةدقع ىلع TACACS+ تامدخ مادختساب ةزهجال ةرادا صيخرت كل حمسي تامدخ مادختساب ةزهجال ةرادا صيخرت كل حمسي، رفوتل ةيلاع (HA) ةلقنسم رشن ةيلمع

HA. جوزي فة دح او ةسايس ةمدخ ةدقع ىلع TACACS+.

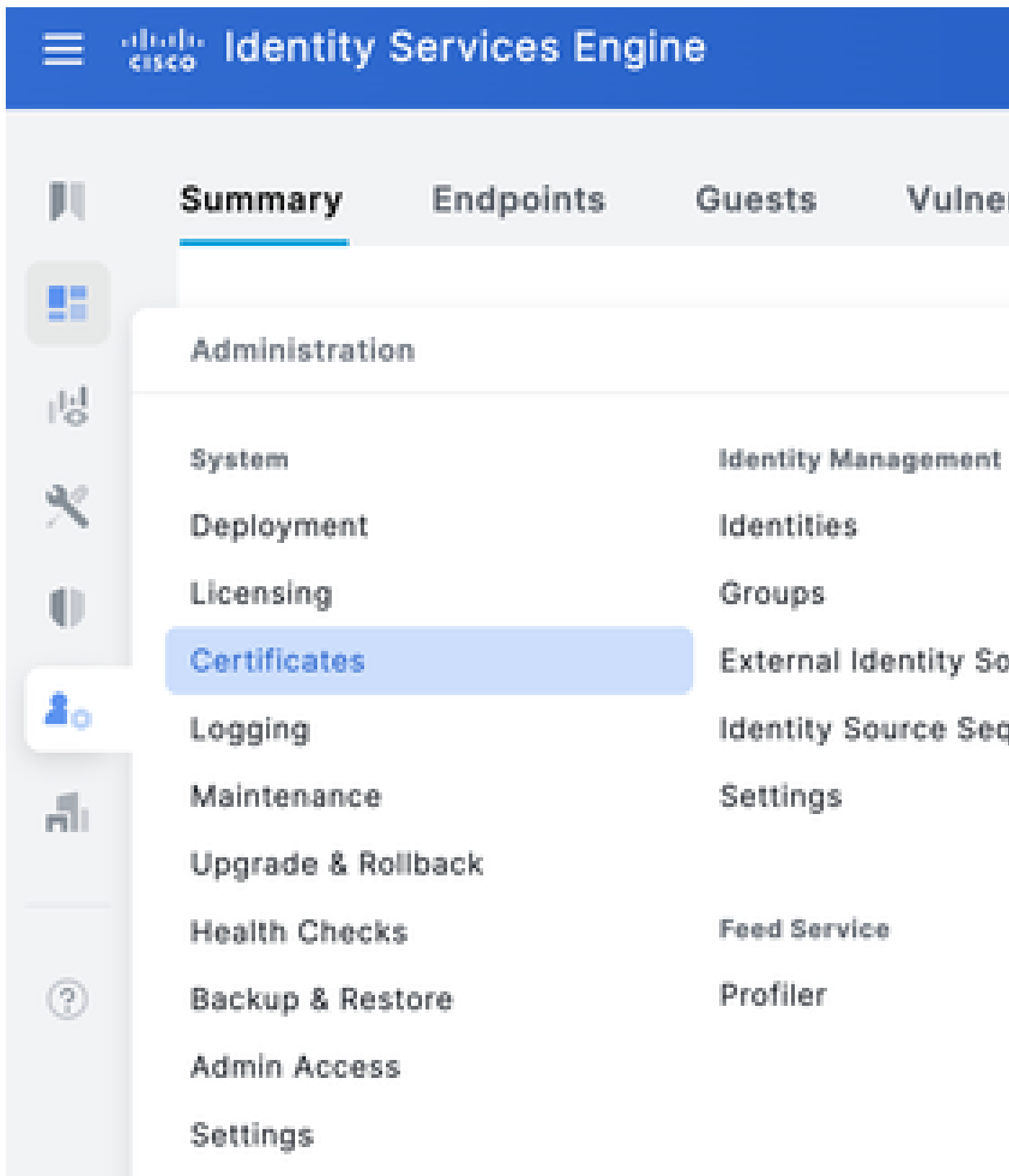
ةزهجالا ةرادال ISE نيوكت - 1 ءزجالا

TACACS+ مداخ ةقداصل ةداهشلا عيقوت بلط عاشنإ

ةم و ةدملا تاضرعت سمل دحأ مادختساب بيولا ىلع ISE ةرادا ةباوب ىلإ لوخدلا لفس . 1 ةوطخل

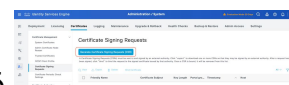
ىلوالا ةوطخل لثمتت . تامدخل اعيمجل ايتاذ ةعقوم ةداهش ISE مدختسي ، يضارتفا لكشبو (CA) قءصملا عفرملا لبق نم هعيقوتل (CSR) ةداهش عيقوت بلط عاشنإ ف

تاداهشلا > ماظنلا > ةرادال ىلإ لقتنا . 2 ةوطخل



3. عوطخل عيقتو بلط عاشن| رقنا ،ةداهشلا عيقتو تابلط تحت .

4. عوطخل مادتسالا ديقت TACACS دح .



Usage

Certificate(s) will be used for **TACACS** 

Allow Wildcard Certificates ☐ 

أهـل TACACS+ نـي كـمـت مـت يـت الـا PSN تـا كـبـش دـدح 5. ةـوطـخـال

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☒ ISE1	ISE1#TACACS

ةـبـسـانـمـال تـامـولـعـمـلـاب عـوضـومـال لـوقـح أـلمـا 6. ةـوطـخـال

Subject

Common Name (CN)
\$FQDN\$



Organizational Unit (OU)
CX



Organization (O)
Cisco



City (L)
Raleigh

State (ST)
North Carolina

Country (C)
US

(SAN) ليدب مسا عوضوم ال تحت IP ناونعو DNS مسا فضا 7. ةوطخل

Subject Alternative Name (SAN)

⋮	DNS Name	✓	ISE1.lab	-	+	
⋮	IP Address	✓	10.225.253.209	-	+	①

ريدصتال قوف مٹ عاشنل قوف رقنا 8. ةوطخل



Successfully generated CSR(s)

Certificate Signing request(s) generated:

ISE2#TACACS

Click Export to download CSR(s) or OK to return to list of CSR(s) screen

OK

Export

(CA) قدصم ال عجرم ال نم ةعقوم (CRT) ةداهش ال عل لوصح ال كنكمي ،نآل

TACACS+ م داخ ةق داصم ل رذل ال قدصم ال عجرم ال ةداهش ليمحت

جاردا رقنا ،ةنومضم ال صيخار ال تحت .تاداهش ال > ماطن ال > ةرادإل ال إل لقتنا.1 ةوطخل

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / System page. The 'Certificates' tab is selected in the top navigation bar. On the left, the 'Certificate Management' sidebar is visible, with 'Trusted Certificates' selected. The main content area displays a table titled 'Trusted Certificates' with a warning icon and text: 'For disaster recovery it is recommended to export and backup all your trusted certificates.' The table has columns: Friendly Name, Trusted For, Serial Number, Issued To, Issued By, Valid From, Expiration Date, and Status. The 'Import' button is highlighted in the top left of the table area. The table lists several certificates, including Amazon root CA, Cisco ECC Root CA 2099, Cisco Licensing Root CA, Cisco Manufacturing CA SHA2, Cisco Root CA 2048, Cisco Root CA 2099, Cisco Root CA M1, Cisco Root CA M2, and Cisco RXC-R2.

☐	Friendly Name	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Status
☐	Amazon root CA	Infrastructure Cisco Services	06 6C 9F CF ...	Amazon Root CA 1	Amazon Root CA 1	Tue, 26 May 2015	Sun, 17 Jan 2...	Enr
☐	Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2...	Enr
☐	Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing R...	Cisco Licensing R...	Thu, 30 May 2013	Sun, 30 May 2...	Enr
☐	Cisco Manufacturing CA SHA2	Endpoints Infrastructure	02	Cisco Manufactur...	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enr
☐	Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2...	Cisco Root CA 20...	Cisco Root CA 20...	Fri, 14 May 2004	Mon, 14 May ...	Dis
☐	Cisco Root CA 2099	Cisco Services	01 9A 33 58 7...	Cisco Root CA 20...	Cisco Root CA 20...	Tue, 9 Aug 2016	Sun, 9 Aug 20...	Enr
☐	Cisco Root CA M1	Cisco Services	2E D2 0E 73 4...	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20...	Enr
☐	Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2...	Enr
☐	Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 2034	Enr

ةداهش عي قوت بل ط ع ق و ي ذل ا (CA) قدصم ال عجرم ال نع ةرداصل ةداهش ال دح .2 ةوطخل
نكمم رايل ال ISE لخاد ةق داصم ال ب ةق ث ال نأ نم دكأت .كب صاخ ال (CSR) TACACS

Import a new Certificate into the Certificate Store

* Certificate File **Examinar...** ISE SVSLab CA.crt

Friendly Name

Trusted For:

- ☒ Trust for authentication within ISE
- ☐ Trust for client authentication and Syslog
 - ☐ Trust for certificate based admin authentication
- ☐ Trust for authentication of Cisco Services
- ☐ Trust for Native IPSec certificate based authentication
- ☐ Validate Certificate Extensions

Description

Submit

Cancel

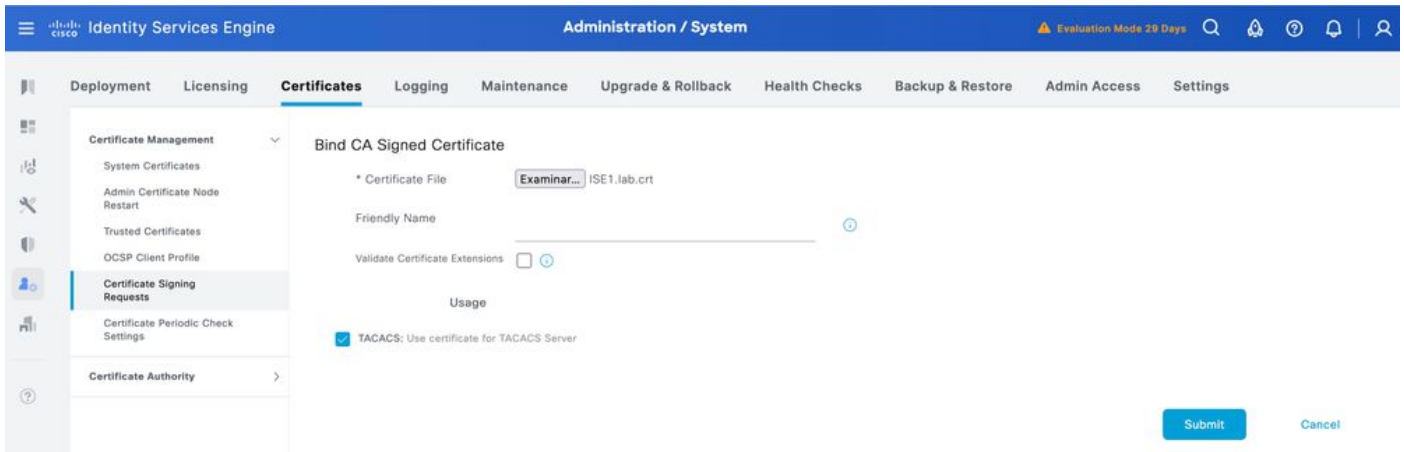
امب قوٹوم تاداهش تحت نآال عدهاشل رهظت نأ بجي . لاسرا قوف رقنا

ISE ب (CSR) عقوقم ال عدهاشل عي قوت ب ل ط طبر

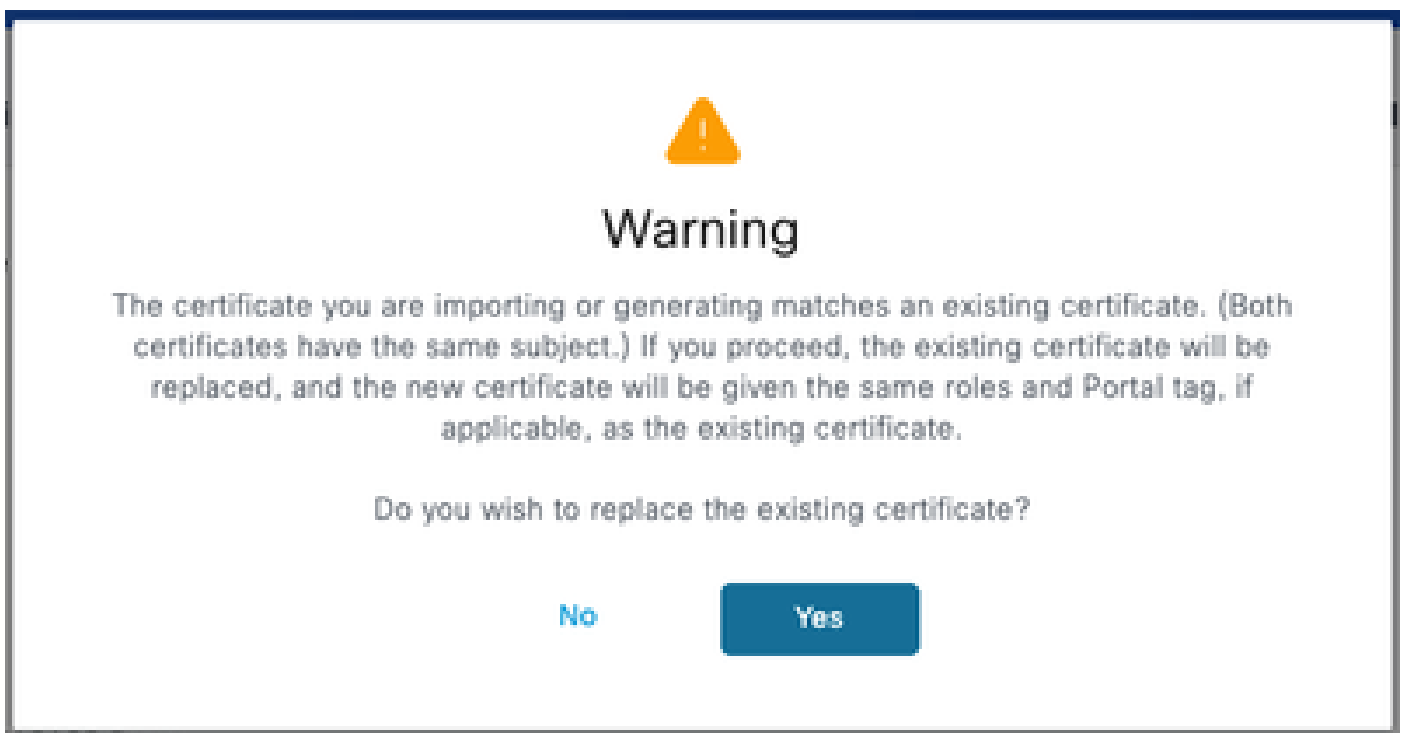
ISE. ىلع ةعقوقم ال عدهاشل تي بثت كنكمي ، (CSR) عدهاشل عي قوت ب ل ط عي قوت درجم ب

TACACS دح ، عدهاشل عي قوت تابل ط تحت . تاداهشل > ماظنل > ةرادال ىل لقتن. 1. ةوطخل عدهاشل طبر قوف رقناو ةقباسل ةوطخل ي ف ؤاشن مت يذل CSR.

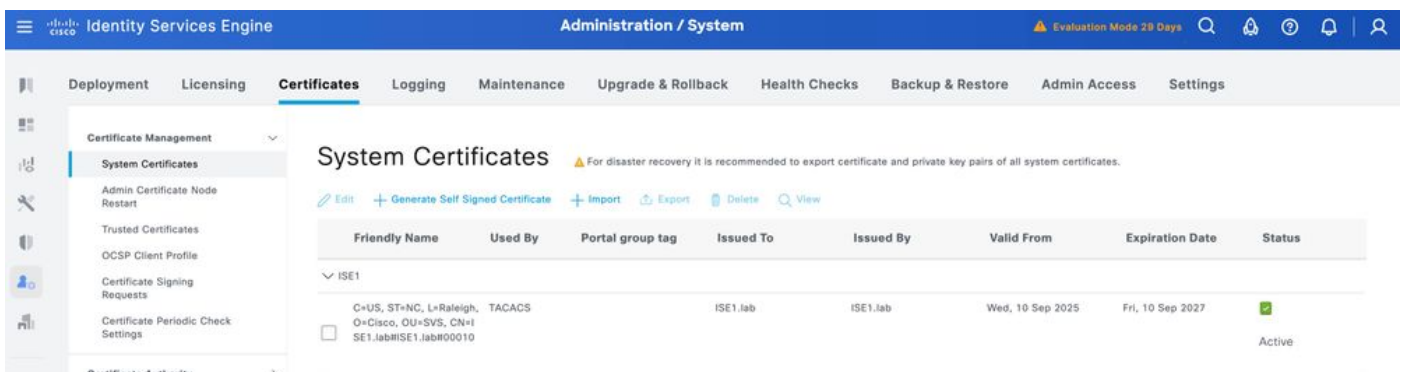
ال مادختسال تحت ةدوجوم ال TACACS راي تخال ةناخ نأ نم دكأتو ةعقوقم ال عدهاشل دح. 2. ةوطخل ةدحمت لازت.



معن قوف رقنا ،ةدوجومال ةداهشلا لادبتسا لوح اريذحت تيقلت اذا .لاسرا قوف رقنا 3. ةوطخلل ةعباتملل



م.اظنل تاداهش نمض كلذ نم ققحتلا كنكمي .حيحص لكشب نآلا ةداهشلا تيبتت بجي



نيكمت TLS 1.3

ايودي هنيكمت بحجي و ISE 3.4.x ي ف يضارتفا لكشب TLS 1.3 نيكمت متي ال

تادادعال > مازنل > ةرادلإا لىل لقتنا.1 ةوطخال



Identity Services Engine



Bookmarks



Dashboard



Context Visibility



Operations



Policy



Administration



Work Centers



Interactive Help

Deployment

Licensing

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

System

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade & Rollback

Health Checks

Backup & Restore

Admin Access

Settings ✓

رادصا تادادعإ نمض TLS1.3 ل ةرواجملا رايثخالا ةناخ ددحو، نامألا تادادعإ قوف رقنا 2. ةوطخل
ظفح قوف رقنا مث، TLS.

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture

Profiling

Protocols

Security Settings

Choose the security settings you want to enable to ensure safe communications across your network.

TLS Versions Settings

TLS 1.2 is enabled by default and can't be deselected. Choose one or a range of consecutive TLS versions.

☐ TLS 1.0

☐ TLS 1.1

☒ TLS 1.2

☒ TLS 1.3

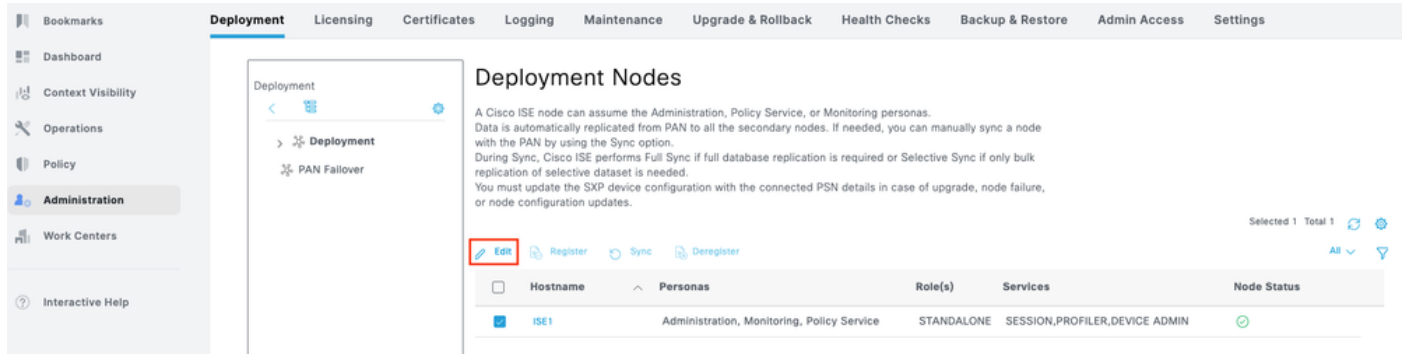


عيمج ىلع Cisco ISE قيبطت مداخل ليغشت ةداعإ متت، TLS رادصا رييغت دنع: ريذخت
Cisco ISE رشنلا ةزهجأ.

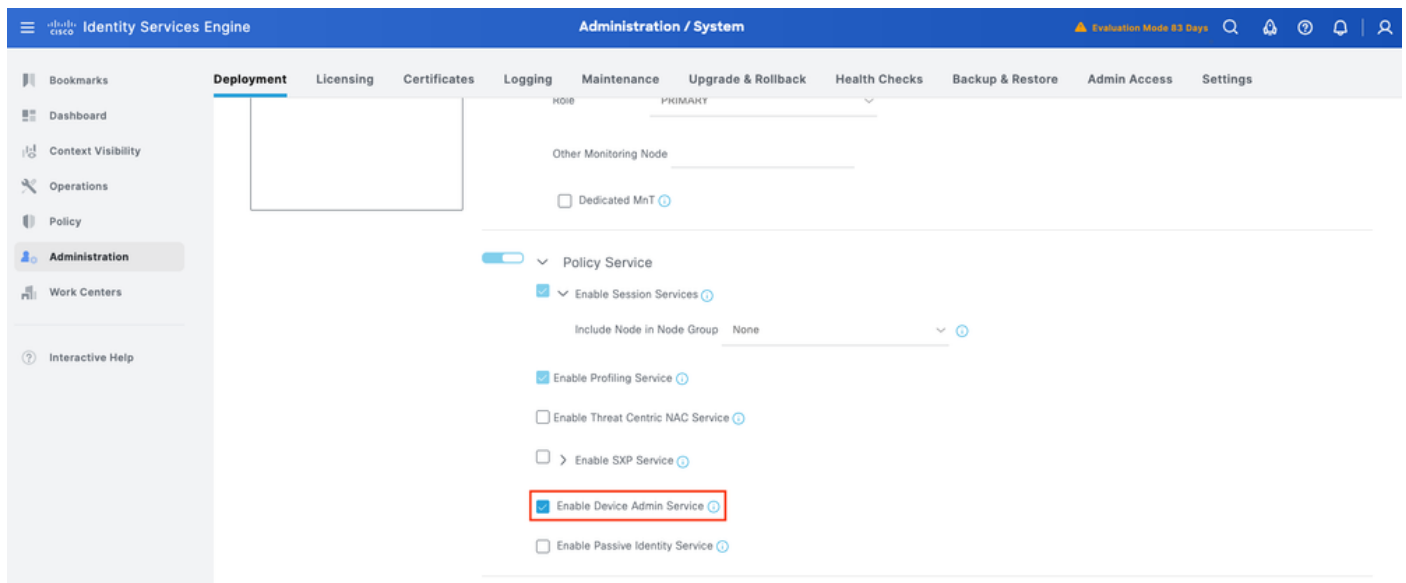
ISE ىل عزهجالا ةرادا نيكمت

نيكمتل ISE ةدقع ىل ع يضارتفا لكشب (TACACS+) عزهجالا ةرادا ةمدخ نيكمت متي ال PSN ةدقع ىل ع TACACS+:

رقناو ISE ةدقعل ةرواجملا رايخالا ةناخ دح .رشنل > ماظنل > ةرادال ىل لقتنا 1. ةوطخل ريرحت قوف.



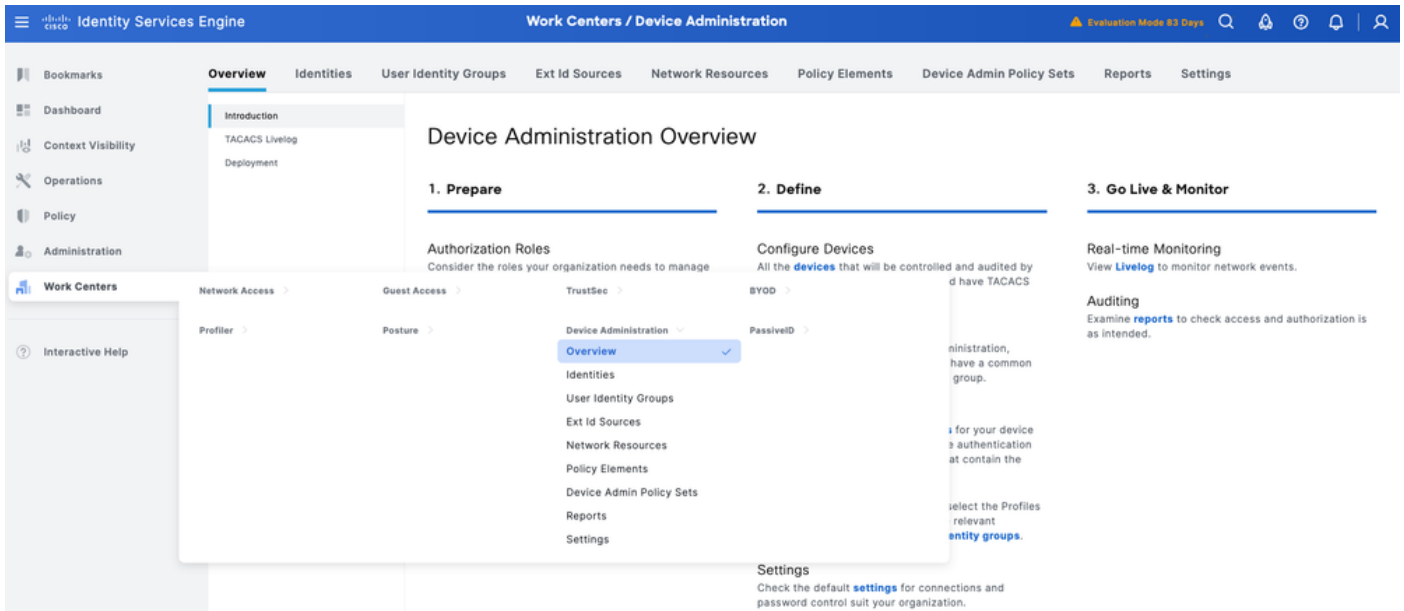
نيكمتل ةرواجملا رايخالا ةناخ دحو لفسا ىل ريرمتلاب مق ،GeneralSettings تحت 2. ةوطخل ةزهجالا ةرادا ةمدخ.



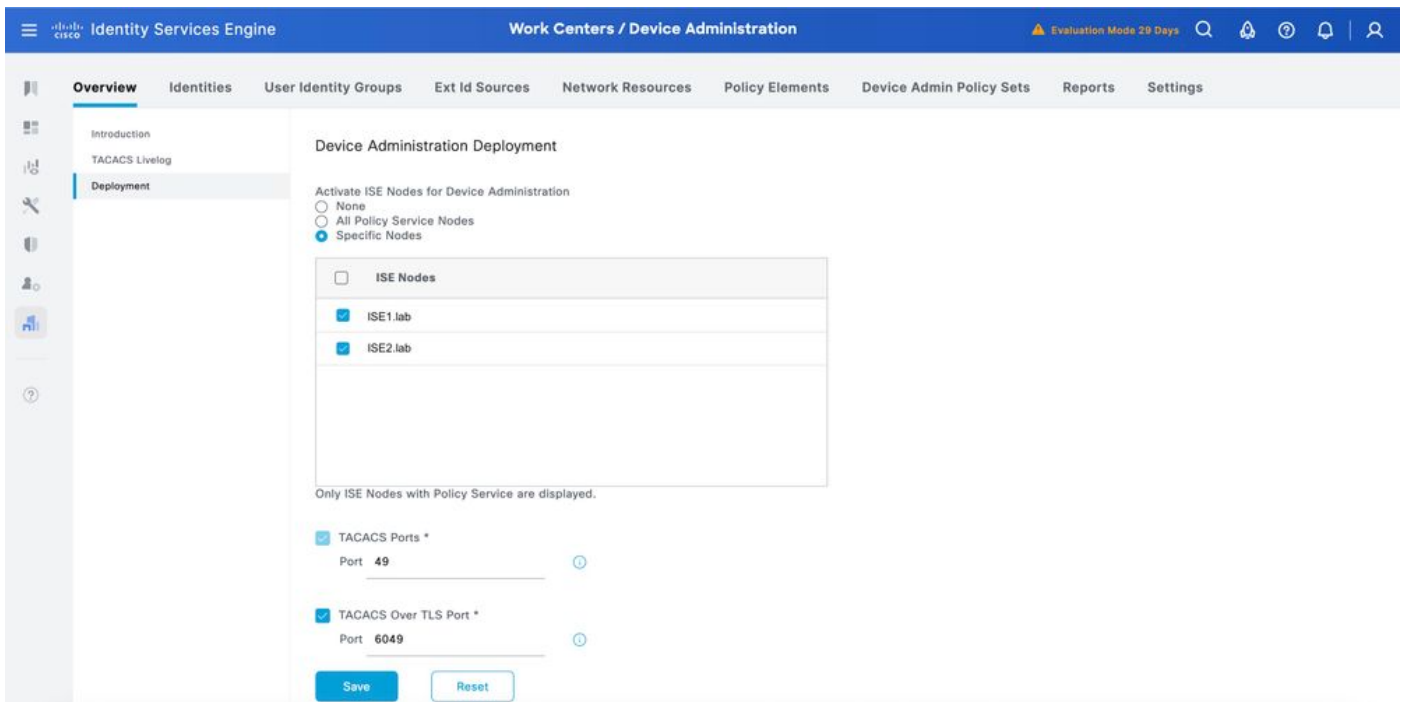
ISE ىل نآال "زاهجالا لوؤسم ةمدخ" نيكمت مت .نيوكتلا ظفح 3. ةوطخل

TLS ربع TACACS نيكمت

ةماع ةرطن > عزهجالا ةرادا > لمعل زكارم ىل لقتنا 1. ةوطخل



TLS. ربع TACACS نيكمت ديتر شيح PSN دقع دح .رشنللا قوف رقنا.2 ةوطخل



TLS. ربع TACACS ل فلتخم TCP ذفنم دح وأ 6049 يضرارفاللا ذفنم لابل طفتحا.3 ةوطخل
ظفح قوف رقنا م

ةكبشللا ةزهجأو ةكبشللا ةزهجأ تاعومجم عاشنإ

لك لثمي .ةزهجالا تاعومجمل ةددعتم ةيمره تالسلستب ةزهجالا ايوق اعيمجت ISE رفوي
ةكبشللا ةزهجالا لقتسم وازيتمتم افينصت يللكيه لسلست

ةزهجأ تاعومجم قوف رقنا.ةكبشللا دراوم > زاهجالا ةرادإ > لمعلال زكارم ىلإ لقتنا.1 ةوطخل
م ساب ةعومجم ئشنأو ةكبشللا

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 93 Days

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Admin Policy Sets

More

✕

Edit Group

Name*

IOS-XR

Description

Group Hierarchy

Device Type > All Device Types > IOS-XR

Cancel

Save

☐ ADVA

ADVA SyncDirector Network Time Monitoring

No. of Network Device

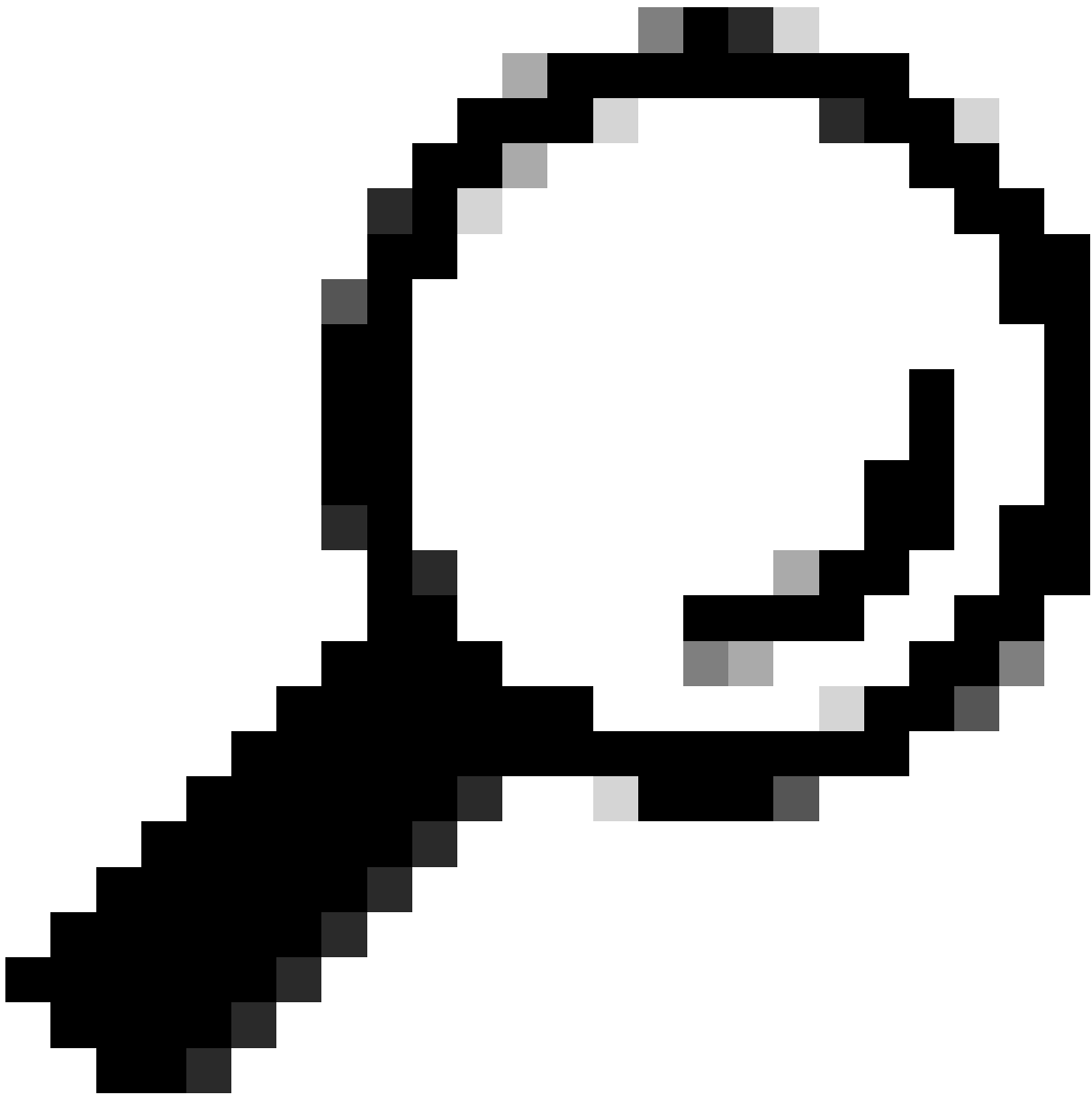
--

702

0

11

243



م تي ةيضا رتفا ةي مره تالسلست عقاومل ةفاكو ةزهجالا عاونأ عي مج دعت :خيملت
في رعتو كب ةصاخلا ةي مرهلا تاجردتلا ةفاضل كنكمي . ISE ةطساوب اهري فوت
ةلاح في اقحال همادختس كنكمي يذلا ةكبشل زاهج في رعت في ةفلتخملا تانوكملا
ةسايسلا

> زاهجالا ةرادا > لمعل زكارم ىلا لقتنا . ةكبش زاهجك Cisco IOS XR زاهج فضا ، نآلا . 2. ةوطخل
ديدج ةكبش زاهج ةفاضلا ةفاضلا ىل عرقنا . ةكبشلا ةزهجا > ةكبشلا دراوم

Identity Services Engine Administration / Network Resources

Network Devices

Network Devices List > BRC-8201-1

Network Devices

Name BRC-8201-1

Description

IP Address * IP: 10.225.253.167 / 32

IP Address * IP:

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type IOS-XR Set To Default

مق، اريخاً. زاهجلل (IOS XR) عونو عقومل ننيي عت نم دكأت و زاهجلل IP اونو ع لخدأ. 3 ةوطخل
 TLS. ربع TACACS+ ةق داصم تادادع ننيكمتب

Identity Services Engine Work Centers / Device Administration

Network Resources

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

☐ RADIUS Authentication Settings

☐ TACACS Authentication Settings

☒ TACACS over TLS Authentication Settings

This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.

Subject Alternative Name (SAN)*

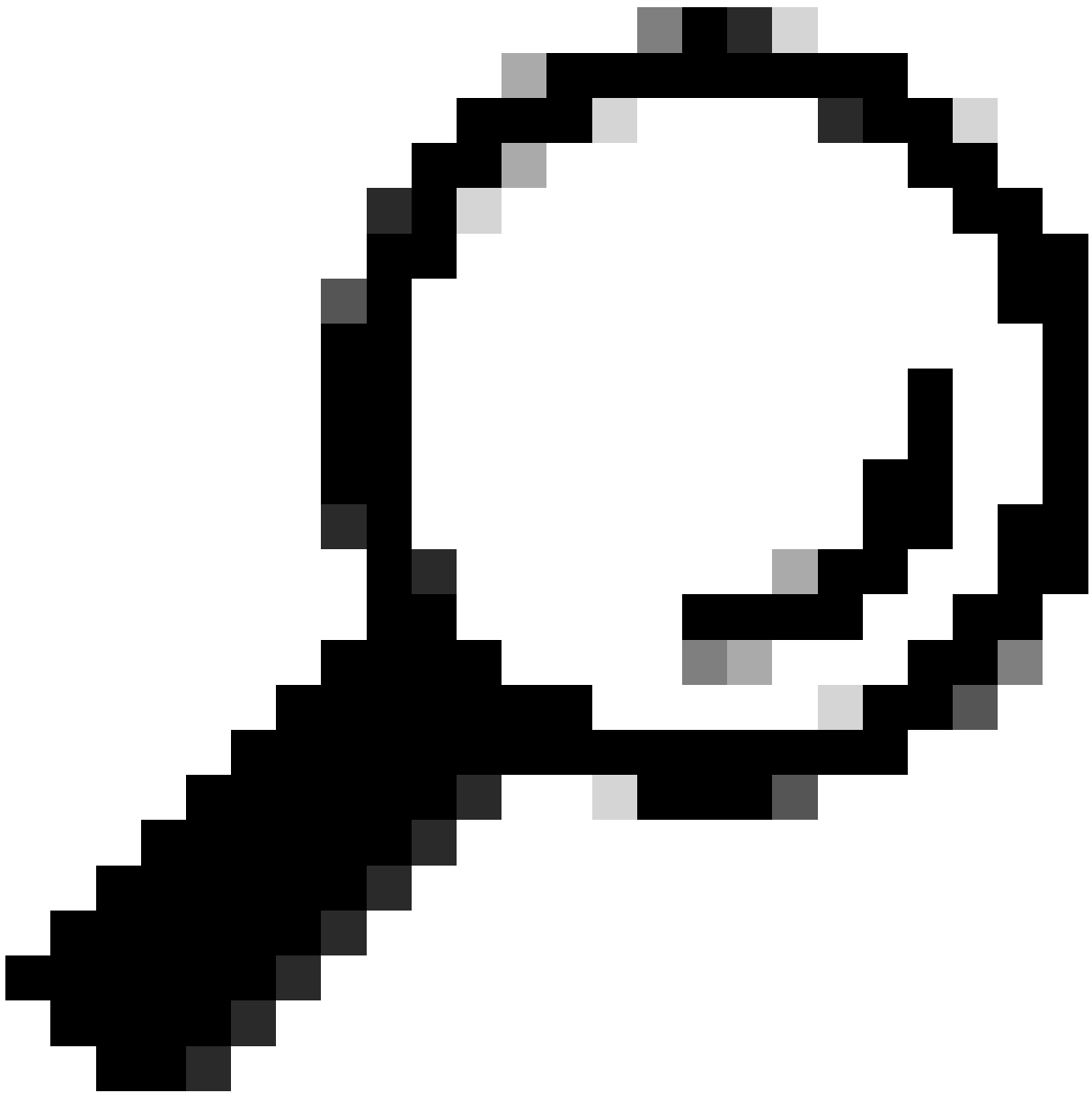
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.

☐ IP Address

The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.

Additional SAN attribute details Show

Additional SAN Attributes

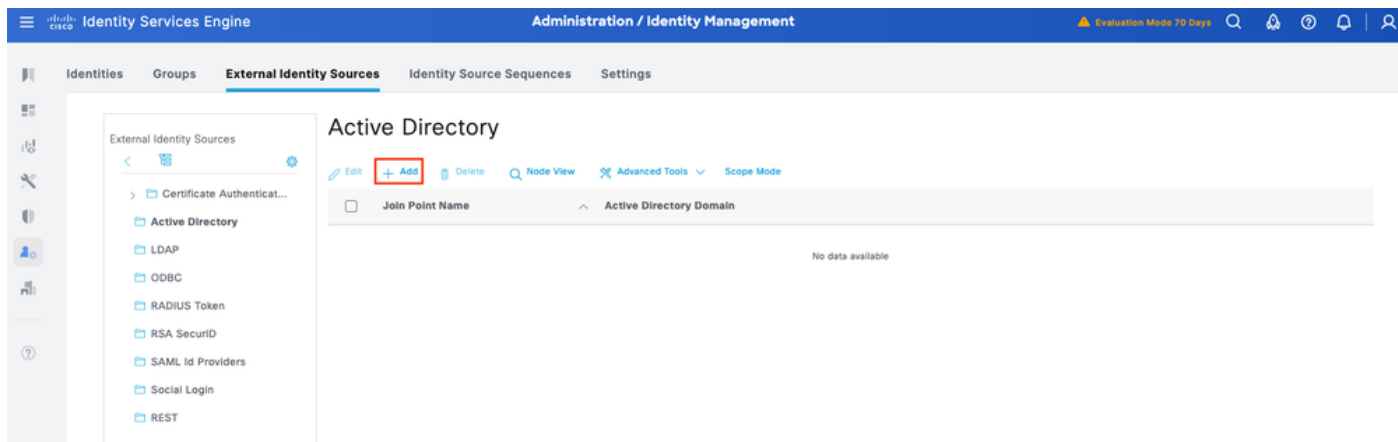


لمع ةسلج ليغشت ةداع| بنجتل درفملا لاصتالا عضو نيكم تب ىصوي :خملت
زاهجلا ىلا اهي رمأ لاسرا متي ةرم لك في TCP.

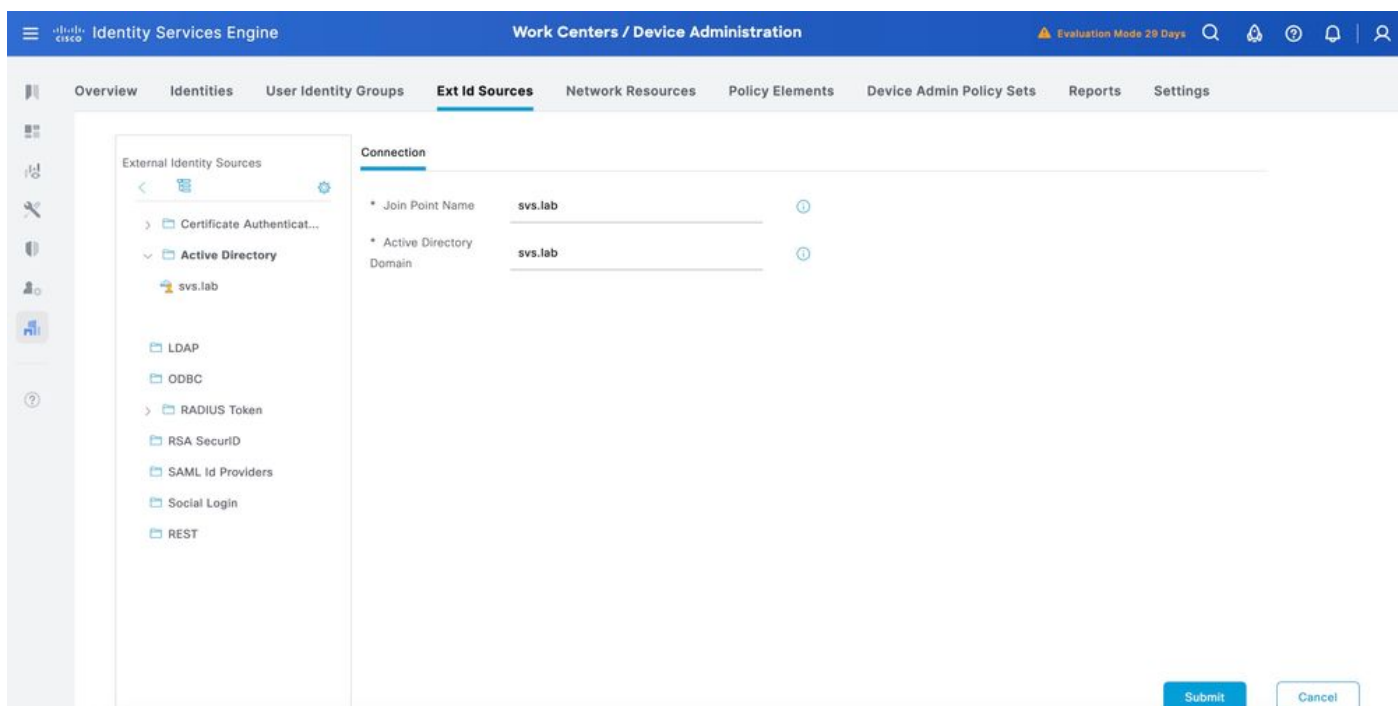
Configured Identity رجاتم

نبي لخدال ISE يمدختسم نوكي نأ نكمي يذلاو، ةزهجال يلوؤسم ةيوه نزخم مسقلا اذه ددحي
يجراخ ةيوه ردصم، Active Directory (AD) ممدختسمي انه. ةمومدم ةيجراخ ةيوه رداصم يأو

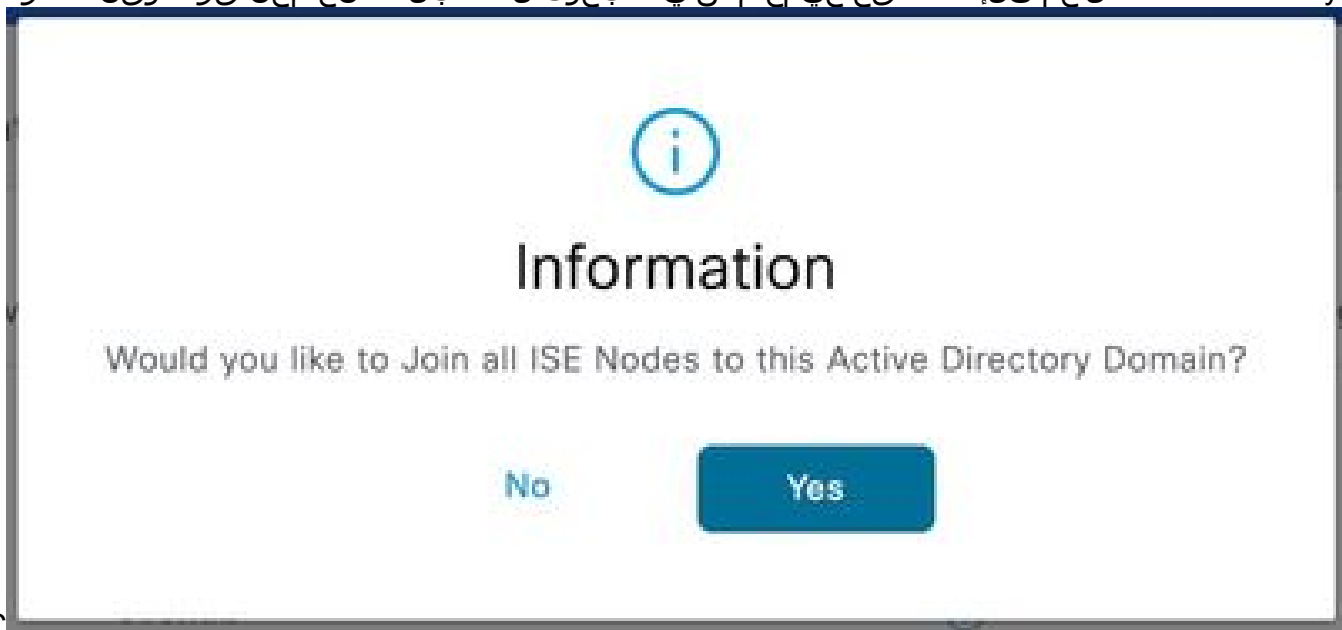
رقنا. Active Directory > ةيجراخال ةيوهال نزاخم > ةيوهال ةرادا > ةرادالال ىلا لقتنا. 1. ةوطخال
ةديج ةكرتشم AD ةطقن ديحتل ةفاضل قوف.



لإسراء رقن او AD لاجم مساو طبرلا ةطقن مسا دح. 2. ةوطخل



Active Directory لاجم إلى ISE دقع عيمج مضيف بغرت له، اهبلط دنع معن قوف رقن. 3. ةوطخل



ةلاحال نم ققحت AD إلى ISE مضمن او AD Join تازايت ماب دامت عال تانايب لخدأ. 4. ةوطخلل لمعت اهنأ نم ققحتلل

×

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name ⓘ administrator

* Password
.....

☐ Specify Organizational Unit ⓘ

☒ Store Credentials ⓘ

Cancel OK

×

Join Operation Status

Status Summary: Successful

ISE Node	Node Status
ISE1.lab	✔ Completed.

Close

عيمي جىل ع لوصحلل ةفاضل قوف رقناو ،تاعومجم بيوبتل ةمالع لىل لقتنا. 5 ةوطخل اذه حضوي .زاهل لىل لوصولل نىل وخم نىم دختسمل نم يلىل اذانتسا ةبولطملم تاعومجملم لىل وختل جهن في ةمدختسمل تاعومجملم لاثملم

Identity Services Engine

Administration / Identity Management

IdentitiesGroupsExternal Identity SourcesIdentity Source SequencesSettings

External Identity Sources

Certificate Authentica...Active DirectoryLDAPODBCRADIUSTokenRSASecurIDSAMLI d ProvidersSocial LoginREST

ConnectionAllowed DomainsPassiveIDGroupsAttributesAdvanced Settings

EditAddDelete GroupUpdate SID Values

Select Groups From DirectoryAdd Group

SID

No data available

Select Directory Groups

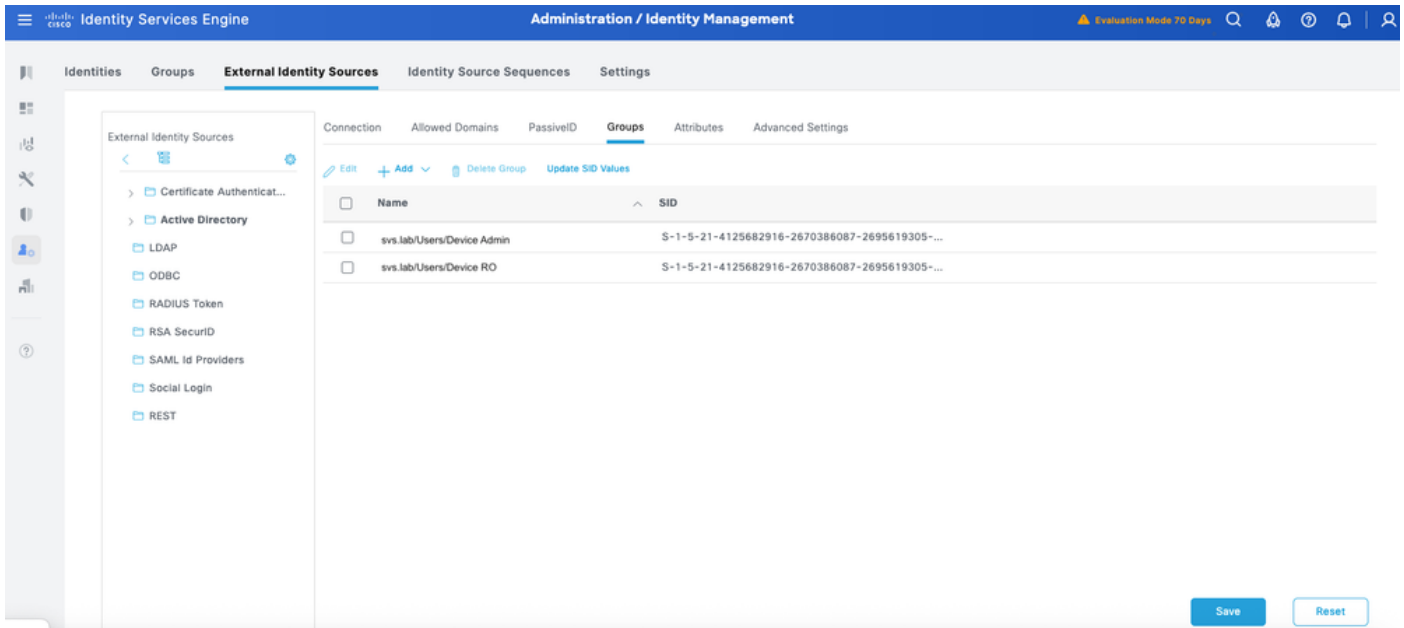
This dialog is used to select groups from the Directory.

Domain svslab

Name Device *SID *Type ALL
Filter Filter Filter

Retrieve Groups... 2 Groups Retrieved.

☐	Name	Group SID	Group Type
☐	svslab/Users/Device Admin	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL
☐	svslab/Users/Device RO	S-1-5-21-4125682916-2670386087-26956193...	GLOBAL



TACACS+ تافيصوت نيوكت

لثاملا اذه في Cisco IOS XR ةزهجأ ىلع نيمدختسملا راودأل TACACS+ تافيصوت طيطخت
يلي ام فيرعت متي:

- زاهجلا في تازايتما رثكأل رودلا وه اذه - (يرذجلا ماظنلا ري دم) Root System Administrator
ىلإ لماكلا يرادإلا لوصول قح بيرذجلا ماظنلا لوؤسم رود بحاص مدختسملا عتمتي
نيوكتلا تاناكمإو ماظنلا رماوأ عيمج.
- ةءارقلا لوصول ىلإ نوجاتحي نيذل نيمدختسملا ىلإ رودلا اذه فدهي - ليغشتلا لماع
اهحالصإو عاطخألا فاشكتساو ةبقارملا ضارغلأ ماظنلا ىلإ طقف.

TACACS+: IOSXR_RW و IOSXR_RO فيفيصوت ديدحت

لوؤسملا فيرعت فلم - IOS XR_RW

تافلما > جئاتنلا > ةسايسلا رصانع > ةزهجألا ةرادإ > لمعل زكارم ىلإ لقتنا 1. ةوطخلا
IOSXR_RW هتيمستو ديدج TACACS فيرعت فلم ةفاضاب مق. TACACS فيرعت

15. ك زايتمأ صقألا دحلأو زايتمأ ريصقتلا تنيعو تصحف 2. ةوطخ

ظفحلأو نيوكتلا دكأ 3. ةوطخلا

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Conditions > TACACS Profiles > IOSXR_RW
TACACS Profile

Network Conditions >

Results > Allowed Protocols
TACACS Command Sets
TACACS Profiles

Name
IOSXR_RW

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

☒ Default Privilege 15 (Select 0 to 15)
☒ Maximum Privilege 15 (Select 0 to 15)
☐ Access Control List
☐ Auto Command
☐ No Escape (Select true or false)

لغش الم فيرنت فلم - IOS XR_RO

تافلم > جئاتنل > ةسايسل رصانع > ةزهجالأ ةرادا > لمعل زكارم ىلإ لقتنا 1. ةوطخل
IOSXR_RO هتيمستب مقو اديج TACACS فيرنت فلم فضا. TACACS فيرنت

1. ك زايتم اى صقألا دحل او زايتم اري صقتال تنيعو تصحف 2. ةوطخل

ظفحل او نيوكتال نم دكأت. 3. ةوطخل

Identity Services Engine Work Centers / Device Administration Evaluation Mode 62 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Conditions > TACACS Profiles > New
TACACS Profile

Network Conditions >

Results > Allowed Protocols
TACACS Command Sets
TACACS Profiles

Name
IOSXR_RO

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

☒ Default Privilege 1 (Select 0 to 15)
☒ Maximum Privilege 1 (Select 0 to 15)

رم اوأ تاعومجم TACACS+ configure

ىلع تاقىب طتل هذه ديدحت متي، لاثملا اذه في TACACS+ رم اوأ تاعومجم فيرنت

Cisco_IOSXR_RW و Cisco_IOSXR_RO.

لوؤسمل رماوأة وومجم - Cisco IOS XR RW

رماوأة وومجم > جئاتنل > ساسل رصانع > زاهال ةرادل > لمعل زكارم لىل لقتنا 1. ةوطخل Cisco_IOSXR_RW اهتيمستب مقو ةديج TACACS رماوأة وومجم فضا. TACACS.

(لوؤسمل رودل رماوأة حمسي اذهو) هاندأ جردم ريغ رماوأة ياب حامسل رايتخال ةناخ دح 2. ةوطخل (ظفح قوف رقاو).

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar has a menu with 'Overview', 'Identities', 'User Identity Groups', 'Ext Id Sources', 'Network Resources', 'Policy Elements' (selected), 'Device Admin Policy Sets', 'Reports', and 'Settings'. The main content area is titled 'TACACS Command Sets > CISCO_IOSXR_RW Command Set'. It contains fields for 'Name' (CISCO_IOSXR_RW) and 'Description'. Below these is a 'Commands' section with a checkbox 'Permit any command that is not listed below' which is checked. At the bottom, there is a table with columns 'Grant', 'Command', and 'Arguments'. The table is currently empty, showing 'No data found.' There are 'Cancel' and 'Save' buttons at the bottom right.

Cisco IOS XR RO لغشمال رماوأة وومجم

> ساسل رصانع > زاهال ةرادل > لمعل زكارم لىل لقتنا 1. ةوطخل ISE مدختسم ةهجاو نم 1. ةوطخل اهتيمستب مقو ةديج TACACS رماوأة وومجم ةفاضاب مق. TACACS رماوأة وومجم > جئاتنل Cisco_IOSXR_RO.

ديج رماوأة فضا ، رماوأة مسق ي ف 2. ةوطخل.

رقناو ؛رماوأة دومع ي ضرعل لخدأو ةحنمل دومعل ةلدسنمل ةمئاقلا نم حامسل دح 3. ةوطخل لكيشل مهس قوف.

ظفح قوف رقاو تانايبلا نم دكأت 4. ةوطخل.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Command Sets > CISCO_IOSXR_RO
Command Set

Name
CISCO_IOSXR_RO

Description

Commands

Permit any command that is not listed below ☐

Add Trash Edit Move Up Move Down

Grant	Command	Arguments
☐	PERMIT	show

Cancel Save

زاهجال لوؤسم جهن تاعومجم نيوكت

تاعومجم مسقت نأ نكمي. ةزهجالا ةرادال يضارتفا لكشب جهنل تاعومجم نيكمت متي TACACS فيرعت تافلم قيبطت ليهستل ةزهجالا عاونأ إل ادانتسا تاسايسلا

ةزهجالا ةرادال تاسايس تاعومجم > زاهجالا ةرادال > لمعلل زكارم إلال لقتنا. 1. ةوطخل عاونأ لك يواسي زاهجالا عون: ةادأ ددح طارش تحت. تاسايسلا ةعومجمل ةديجل IOS XR يضارتفال زاهجالا لوؤسم ددح، اهب حومسمل تالوكوتوربل تحت. #IOS XR ةزهجالا

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets More

Policy Sets Reset Reset Policy Set Hit Counts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	IOS-XR devices		DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73		

هذه جهنل ةعومجم نيوكتل نميال مهسلال قوف رقناو Saved قوف رقنا. 2. ةوطخل

تارايلال كرتأ. فرعلال نزخمك AD مدختست، ةقداصلل. ةقداصلال ةسايس عاشنإ. 3. ةوطخل ةي لمعلال ي ف مدختسمل لشفي مل اذا، ةقداصلال تلشف اذا تحت ةيضارتفال

Identity Services Engine Work Centers / Device Administration Evaluation Mode 63 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** More

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	IOS-XR devices		DEVICE-Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	73

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default			85	svs.lab Options If Auth fail REJECT If User not found REJECT If Process fail DROP

ضيفو التالاسايس ديحت 4. ةوطخل

Active Directory (AD) في نيمدختسمل تاعومجم إلى ادا نسا لي وختال جهن عاشناب مق

لالم لي بس إلى:

- رماوأل ةعومجم زاهلل تالال ةعومجم في نيمدختسمل نيي عت متي cisco_iosxr_ro IOSXR_RO Shell في رعت فلمو
- رماوأل ةعومجم مل تالال ةعومجم زاهل لوؤسم في نيمدختسمل نيي عت متي CISCO_IOSXR_RW IOSXR_RW Shell في رعت فلمو

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode 62 Days

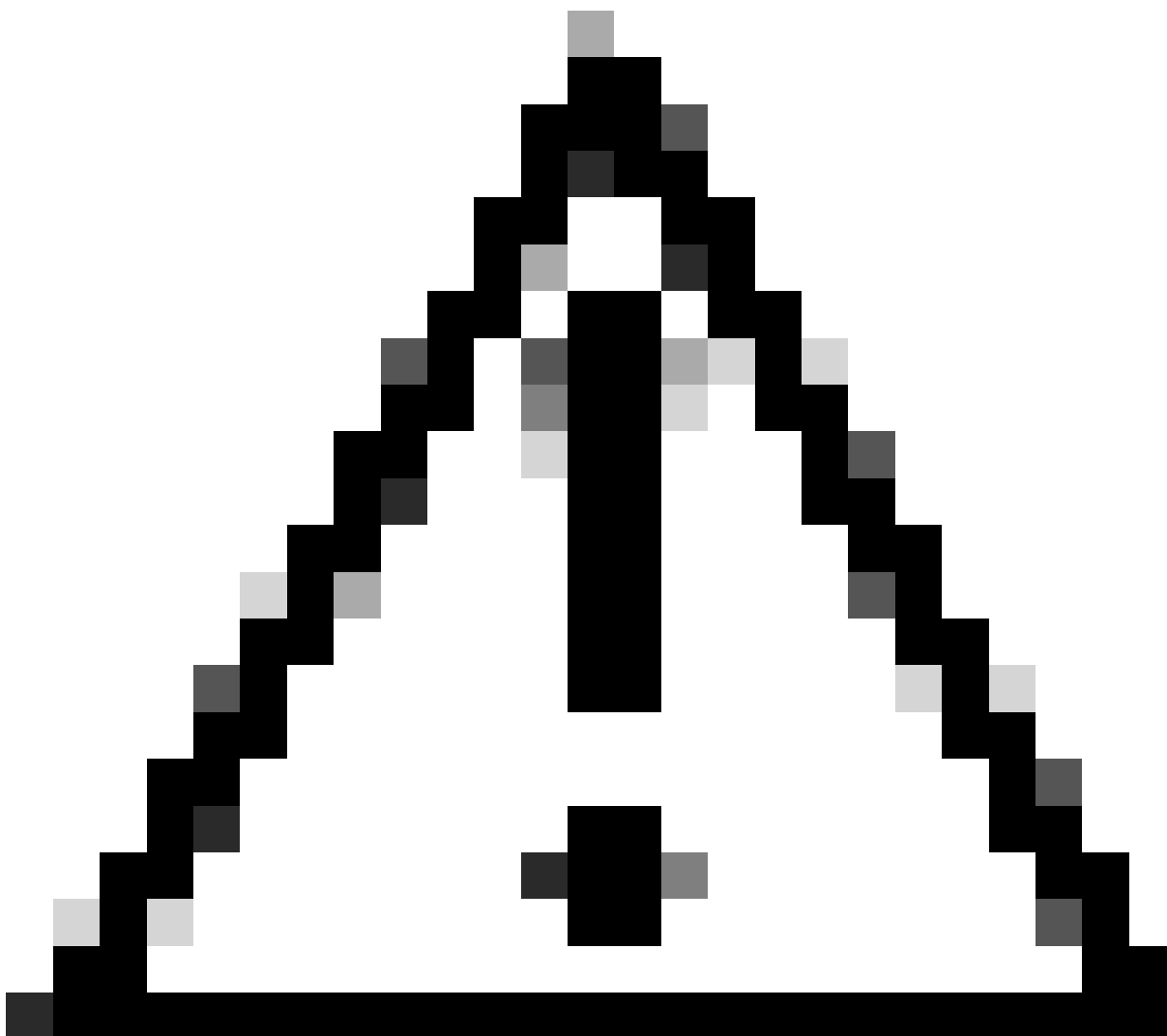
Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets → IOS-XR devices

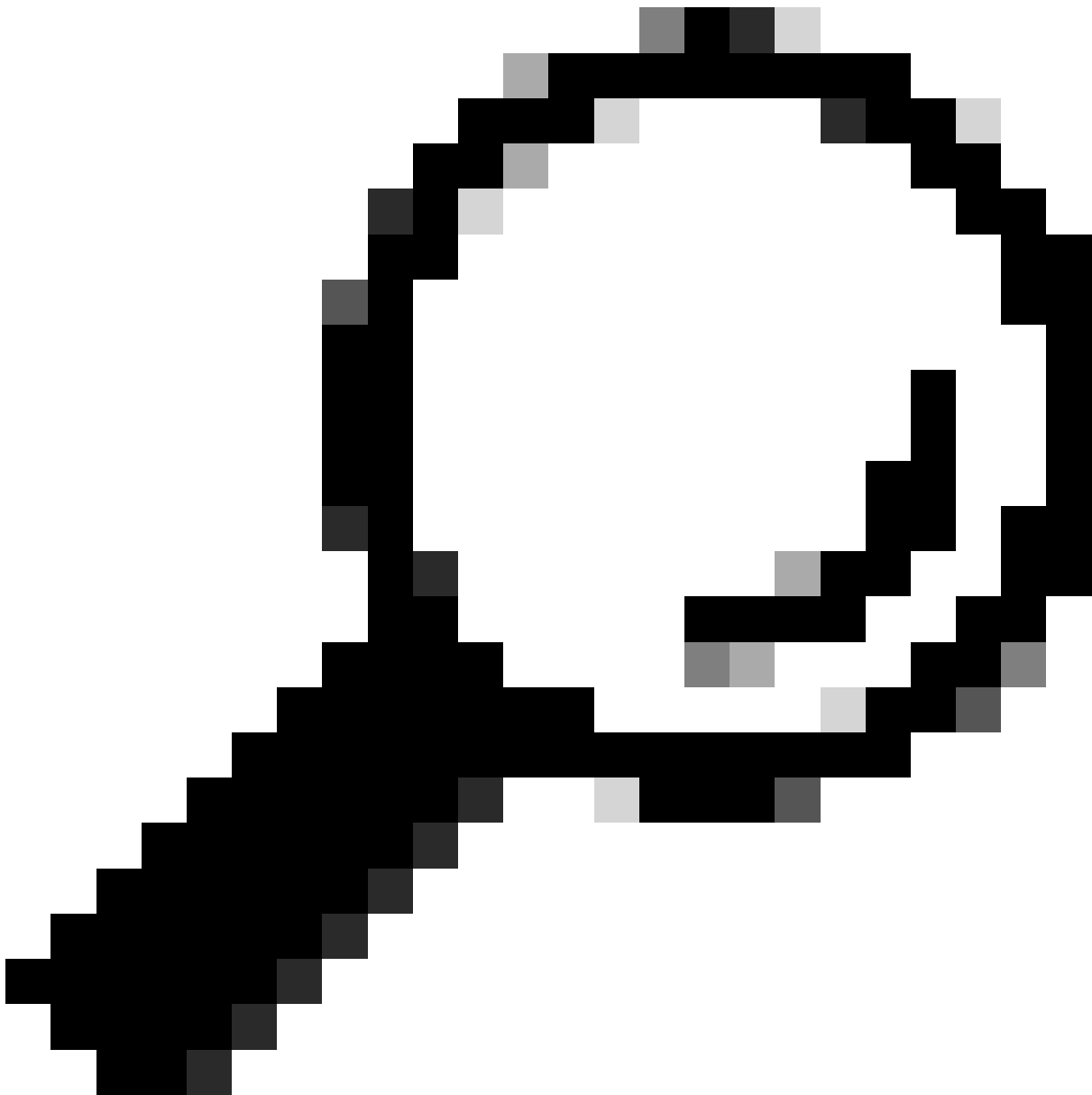
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
🔍 Search					
✔️	IOS-XR devices		DEVICE=Device Type EQUALS All Device Types#IOS-XR	Default Device Admin	77
> Authentication Policy(1)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
∨ Authorization Policy(3)					

				Results			
+ Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions	
🔍 Search							
✔️	Authorization Rule RO	svs.lab - ExternalGroups EQUALS svs.lab /Users/Device RO	CISCO_IOSXR_RO	IOSXR_RO	0	⚙️	
✔️	Authorization Rule RW	svs.lab - ExternalGroups EQUALS svs.lab /Users/Device Admin	CISCO_IOSXR_RW	IOSXR_RW	77	⚙️	
✔️	Default		DenyAllCommands	Deny All Shell Profile	0	⚙️	

1.3 TLS ربيع Cisco IOS XR J TACACS+ نيوكت - 2 عجل



حيحص لكشب هلمعو مكحتلا ةدحو لاصتا ىلإ لوصولا ةيناكمإ نم دكأت :ريذحت



ضيوفتالو AAA ةقداصم قرط ريغتو تقؤم مدختسم نيوكتب ىصوي :خيملت
،نيوكتلتا ريغت ارجا اناثا TACACS نم الدب ةيلحلم دامتعالا تانايب مادختسال
زاهجل جراخ هباسح لفق بنجل

ةيلوالا ةئيहतلا تايلمع

ةلهؤملا تالاجملا امسأ لىل عجوملا ةردق نمو (DNS) مسالا مداخ نيوكت نم دكأت 1. ةوطخل
ISE. مداخل FQDN ةصاخو ،حاجنب (FQDNs) رركتم لكشب

```
domain vrf mgmt name svls.lab  
domain vrf mgmt name-server 10.225.253.247  
no domain vrf mgmt lookup disable
```

```
RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svls.lab
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:

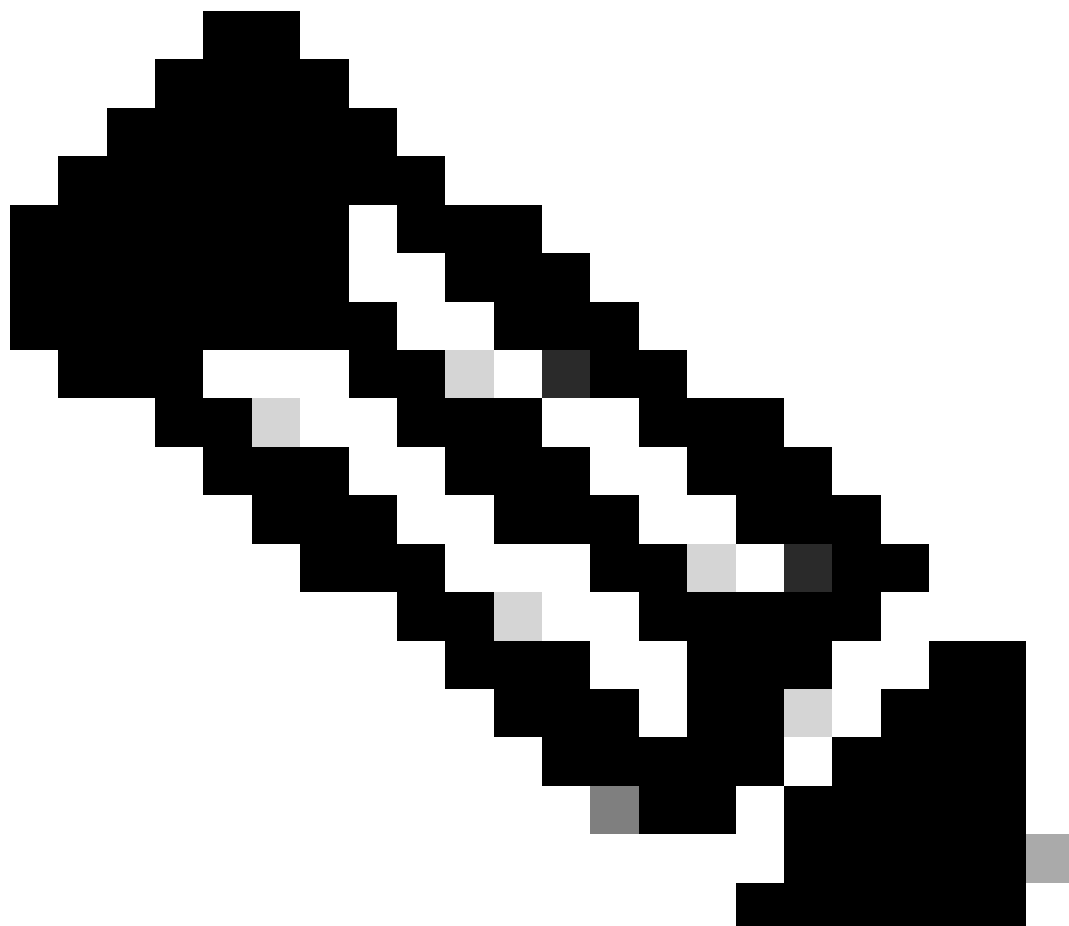
!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

طاقن دوجو مدع نم دكأت. ةمدختسم ريغ/ةميدق تاداهش و ةقث طاقن يأ حسمب مق 2. ةوطخلا
اهحسم/اهتلازاب مقف، ةميدق تالاخدا يأ ىرت تنك اذا. ةميدق تاداهش و ةقث

```
show crypto ca trustpoint
show crypto ca certificates
```

```
(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



مل اذا TrustPoint. تحت هقافراو ايودي ديج RSA حيتافم جوز عاشنإ كنكمي :ةطحالم

دامتعا ايلاح متي ال .يضا رتفالال حيتافملا جوز مادختسا متيس ،دحاو عاشن اب مقت
TrustPoint نمض ECC حيتافم جوز فيرعت

TrustPoint نيوكت

(يرايتخا) حيتافملا جوز نيوكت 1. ةوطخلا

```
<#root>
```

```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto key generate rsa
```

```
4096
```

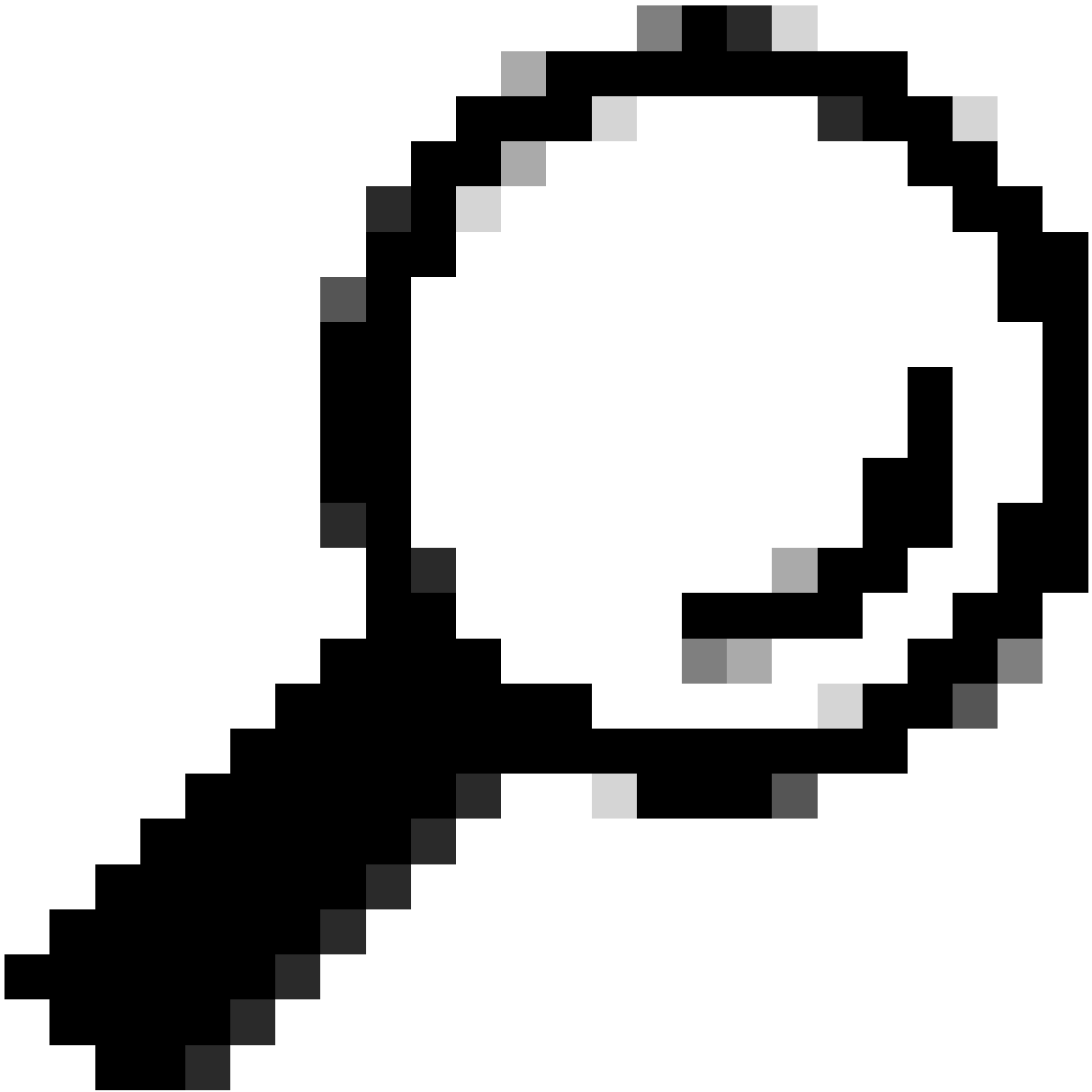
```
RP/0/RP0/CPU0:BRC-8201-1(config)#
```

```
crypto ca trustpoint
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
rsakeypair
```

ةقت ةطقن عاشن ا 2. ةوطخلا



ISE) ىلع هنېكم تةلاحي (ف) يرايتخا ليدبال عوضومال مسال DNS نيوك ت: حيملت
ه ب ى صوي نكلو.

<#root>

RP/0/RP0/CPU0:BRC-8201-1(config)#

crypto ca trustpoint sv

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#

vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#

crl optional

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

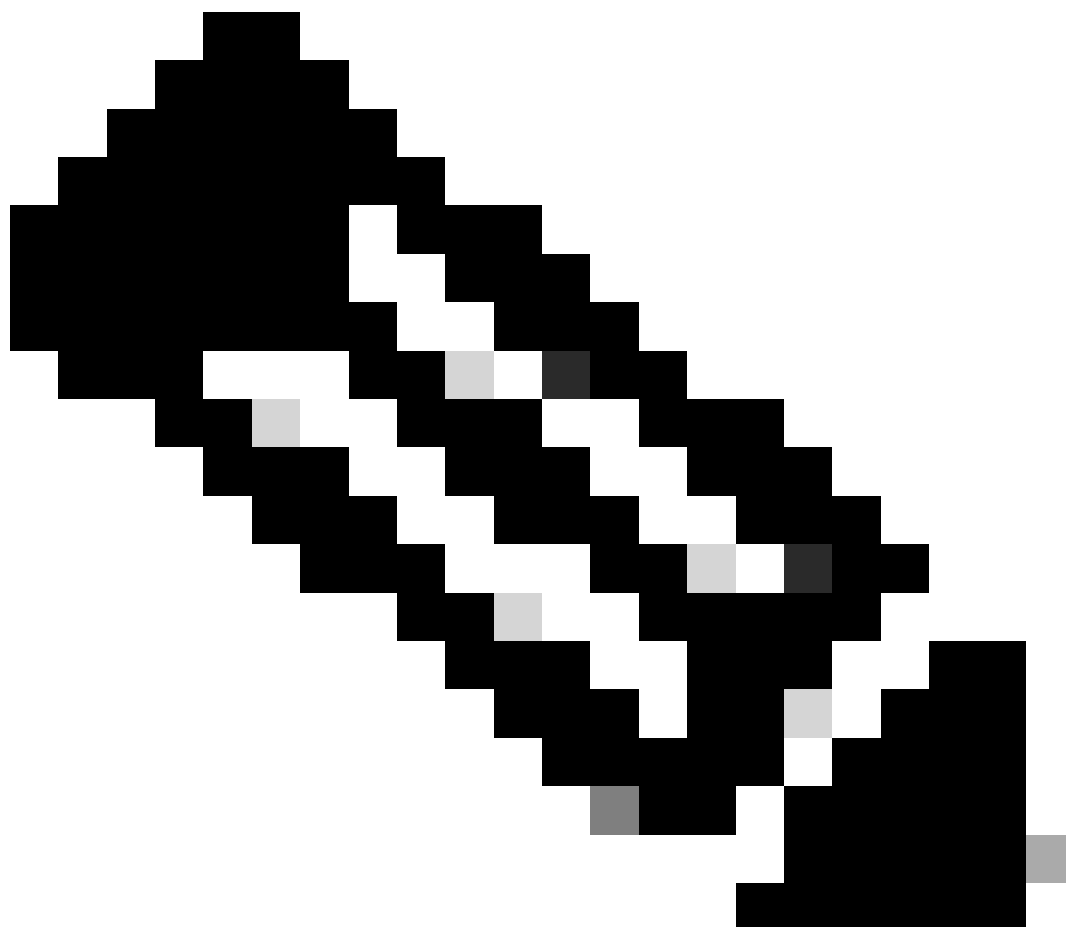
```
enrollment url terminal
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
rsakeypair sv-4096
```

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
```

```
commit
```



قوائم طرش اءءءس اءنكمي O و O ي ؤلصاف مءءءس ال ءءءا اءا :ءظءال م
o=Cisco Systems\, Inc. :الءم ال لى بس لى لى . ؤلصاف ال لى بى (\) ؤسك

CA. ؤءاءش ءىبءءب ءrustPoint ؤءءاصم 3. ؤوطءال

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svcs

Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

```
MIIFDCCA3yqAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMjUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLLEwNTV1MxEjAQBgNVBAMTCVNWUyBYWJJDQTC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZ1zSH6EkEvxnJTty+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLbo0kXEiKjPLatkXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qy04UADL2
WpoGhGT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBROz+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpl334rTixy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XC0NX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCSAGG+EIBDQQMFGpTV1MgTGFiIENBMAOGCSqGSIb3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyflFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
0+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TFITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIE0f5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpiYtprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPPSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOX/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTWl1It/9T1/F0b0xZRugWcpJrVoTgDGUA==
```

-----END CERTIFICATE-----

quit

Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5

Subject:

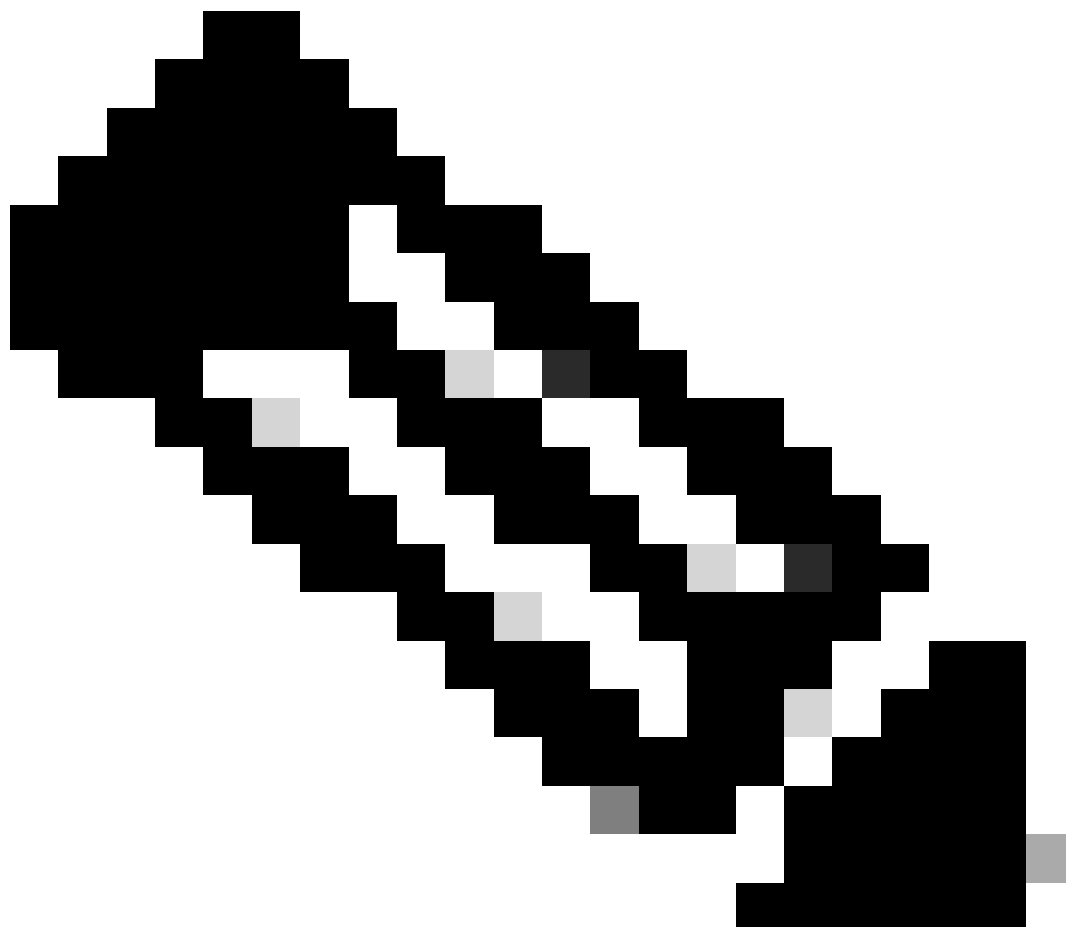
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Issued By :

CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
yes

RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated



عج رمل تاداهش نم لك داريتس ال جاتحت ،عبات قدصم عج رمل ماظن كي دل ناك اذا :ةظحال م
عج رمل عم هسفن رمل المدختسأ .ةيعرف ال قدصم ال عج رمل تاداهش و رذل ال قدصم ال
ل.فسأل ال ف رصم ال اول عال ال ف يعرف ال قدصم ال

(CSR). ةداهش ال عي قوت بلط عاشنإ 4. ةوطخال

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca enroll svcs

Fri May 9 14:52:44.030 UTC

% 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 make a note of it.

Password:

Re-enter Password:

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167

% The subject name in the certificate will include: BRC-8201-1.svs.lab

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

yes

% The serial number in the certificate will be: 4090843b

% Include an IP address in the subject name? [yes/no]:

yes

Enter IP Address[]

10.225.253.167

Fingerprint: 36354532 38324335 43434136 42333545

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

yes

Certificate Request follows:

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

MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5DMQwwCgYDVQQQH
DANSVFAXDjAMBGNVBAoMBUNpc2NmMQwwCgYDVQQQLDANTVlMxZzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTYzMRUwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtr1oDH9iOZxPvEDARwN0t4WrPEjaQc1ZUA
6ax6Cqx/0JlQiUf2+eQv+4rKZqAZ1xDhiaIMGqETn00LKpwmtx10IqXL7UYMHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQChmTVFz3M5fBt86xx4t1nxTFU/4lRwMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkKwI0cb1X2HgtbVQdCXTAwJDmr209
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAACBiTAYBgqhkiG
9w0BCQcxCMJQzFzY28uMTIzMG0GCSqGSIb3DQEJJDJFgMF4wDgYDVROPAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCSGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBOX0eWF5ZUZ701GFjuQHBBdgYb+3lhF0xbYm9psIWfv1uwjKkOL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswj1YpO+IxxUM971Ejwg2rj+jABDR7I8SU
06Y06mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTI1jdgVxB+Xyz0FJMckI05US3j
T/3aw/115RcXerdrh360MUHEepUjIx/15u9s1c7e1mxACoQE6f90A+fdg2zYt0ME
Z6VAw64cY+YF6iLbYv7c41iz05Zj2NJBuKpeqijkFAKY/1rIXTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZN00

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

no

قدصم ال عجرم ال نم ةعقوم ال ةداهش ال داريتس ا 5 ةوطخل

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

crypto ca import svcs certificate

Fri May 9 15:00:35.426 UTC

Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsEgAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZmZAVBgNVBAGTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDAxNjBzEMMAoGA1UECXMdU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTA5MTQ1NzAwWWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTMxMDDAKBgNVBACMA1JUUEDEOMAwGA1UECgwFQ2lZy28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAUMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOd02uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXE0GJ
qIwaoR0c7QsqnCa3HXQipcvrtRgwcFAx29EgjnboiARyDxrdbHrpSQTfpeh5dp/k
eQuio07rxfdztss+8x7WwzC+artGbLYMC7fQcH879iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdR0v1h0okuMykFPa00TemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTajRxvVfYeC1tVB0JdMDAK0avY73N3Zkjr16dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAyb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0
ZTA0BgNVHQ8BAf8EBAMCBaAwIAyDVR01AQH/BBYwFAYIKwYBBQUHAWEGCCsGAQUF
BwMCMAMGA1UdEwQCMAAwHwYDVR0RBBGwFoIOMTAUMjI1LjI1My4xNjcxETAPBgNV
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+oj012106WxedDQ8Vdu0bBtrn0H+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTzrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8Y007HR/2jf7gfhovwR5QN0EHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvo1tx1k9AeLjzb2syv5/fG6QuOZdWwTaaQh0Y2h/cVDiV97wg
ODlmeFdv6QrxQSujZr22RzVykKH1tuiV2B74pthUuGRBtFHS5Xfy7uTTbfGX8M6
ZJw8rX1SADr8tDp1rf1ZIrPmv3ZPP7woTB22yWzyd0use+5Ia1b0w70twN4t/Iiw
8CJu6HfnDXLDPZ0jsC8stefrSlopwGccp3j6aZKPFz+I/Purb44a9WxEwa2TA7H
+rloynBcGMet0HxVlnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF5370w+uNHok8Bdt8mqadUT40oUSqY8ArV0Bom05tzbemreVPmQAZ/IahZ7TqKo
3dGNontAFTTESM1iujQ81iRKsikdHysnwcCM2ni1CKZrhVq5IB8NK6jKRJZ0eQAX
vMt1
-----END CERTIFICATE-----

quit

Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US

Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792

هجوم لايوه ةداهش ليجست نم ققحت

<#root>

RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca trustpoint svcs detail

Trustpoint :svs-new
=====

KeyPair Label:	the_default
CRL:	optional
enrollment:	terminal
subject name:	C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#

show crypto ca certificates svcs

Wed May 14 14:55:58.173 UTC

Trustpoint : svcs-new
=====

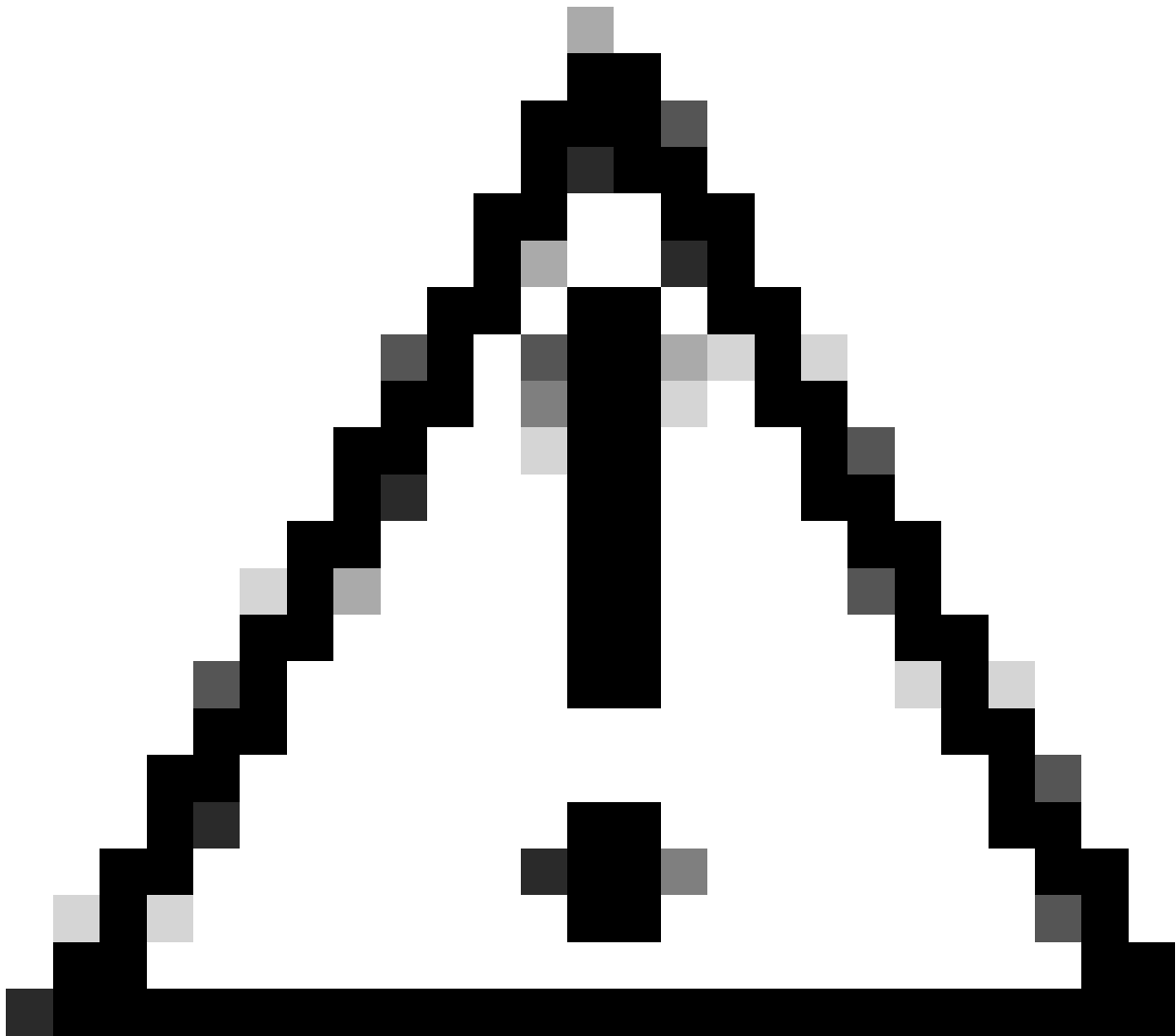
CA certificate
Serial Number : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
Subject:
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 17:05:00 UTC Mon Apr 28 2025
Validity End : 17:05:00 UTC Sat Apr 28 2035
SHA1 Fingerprint:
0EB181E95A3ED7803BC5A8059A854A95C83AC737

Router certificate

Key usage : General Purpose
Status : Available
Serial Number : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
Subject:
serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
Validity Start : 19:59:00 UTC Fri May 09 2025
Validity End : 19:59:00 UTC Sat May 09 2026
SHA1 Fingerprint:
AC17E4772D909470F753BDBFA463F2DF522CC2A6

Associated Trustpoint: svcs

TLS مَادخَت سَاب AAA & TACACS ني وكت



دامت عال تانايب مادختساب مكحتال دحووالال خ نم نيوكتالت تاريغت اارجاب مق ريذحت
ةلحمل.

TACACS+ م داخ نيوكتب مق 1. ةوطخال

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
key 7 072C705F4D0648574453
```

```
aaa group server tacacs+ tacacs2
server 10.225.253.209
vrf mgmt
```

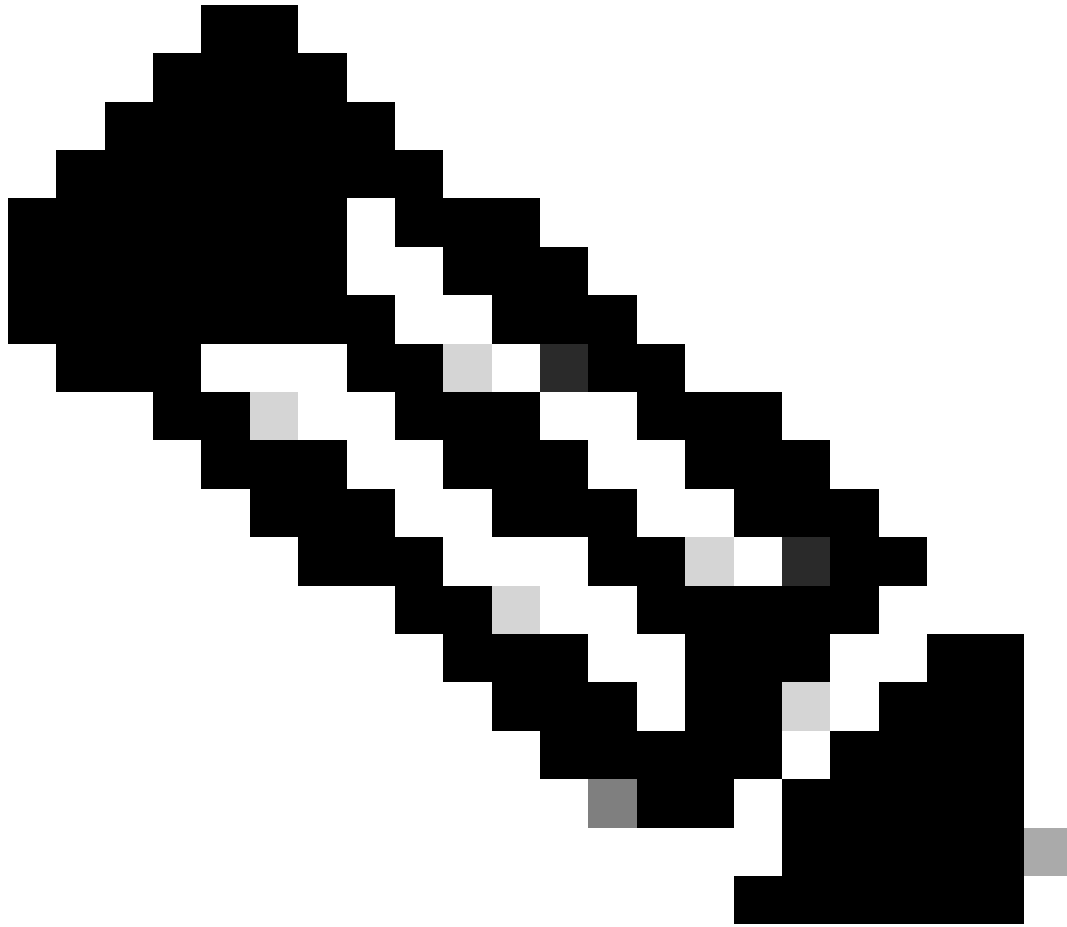
AAA ةومجم نيوكت 2. ةوطخال

```
aaa group server tacacs+ tac_tls_sc
vrf mgmt
server-private 10.225.253.209 port 6049
timeout 10
tls
trustpoint sv
!
single-connection
```

AAA نيوكت 2. ةوطخا

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

ةداهشا دي دجت



ديدجتالءانثأ TACACS+ نيوكت نم ةقثال ةطقن ةلازا مزلي ال :ةظحال

ةيلالجال ةداهشال ةيحالص خيراوت نم ققحت 1. ةوطخال

RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svcs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svcs-new

=====

CA certificate

Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B

Subject:

CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Issued By :

CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US

Validity Start : 22:13:17 UTC Thu Jun 26 2025

Validity End : 22:13:16 UTC Tue Jun 25 2030

CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM

SHA1 Fingerprint:
EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
Subject:
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Sun Jun 24 2035
SHA1 Fingerprint:
E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
Key usage : General Purpose
Status : Available
Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
Subject:
CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 16:38:36 UTC Wed Jul 30 2025
Validity End : 16:38:35 UTC Thu Jul 30 2026
CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY

SHA1 Fingerprint:
B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svb-new

2. TrustPoint ةداهش فذح ةوطخل

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database updated
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

نيوكت تحت تاوطخل ي فضوم وه امك اهليجستو ةقثال ةطقن ةقداصم ةداعا 3. ةوطخل ةقثال ةطقن

ةداهشال ةيخالص خيراوت ثيذحت نم دكأت 4. ةوطخل

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC
```

Trustpoint : KF_TP

=====

CA certificate

Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Tue Jun 25 2030

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uB1QsZDYy6wxomiFWB5Gv0AZM>
SHA1 Fingerprint:
EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2

Trusted Certificate Chain

Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
Subject:
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Issued By :
CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 22:13:17 UTC Thu Jun 26 2025
Validity End : 22:13:16 UTC Sun Jun 24 2035
SHA1 Fingerprint:
E225647FF9BDA176D2998D5A3A9770270F37D2A7

Router certificate

Key usage : General Purpose
Status : Available
Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
Subject:
CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
Validity Start : 15:17:29 UTC Thu Aug 14 2025
Validity End : 15:17:28 UTC Fri Aug 14 2026

CRL Distribution Point

<http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4Qg1Qa8g1xoH8GY>
SHA1 Fingerprint:
D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP

ققحتلا

نېوكتلا نم ققحتلا

```
show crypto ca certificates [detail]  
show crypto ca trustpoint detail  
show tacacs details
```

TACACS+ ءاطخأ حيحصت

```
debug tacacs tls
```

```
debug TLS
```

```
debug ssl error  
debug ssl events
```

AAA. ةقداصم نيوكت لبق ديغبلا مدختسملا ربتخا

```
<#root>
```

```
test aaa group tacacs2
```

```
user has been authenticated
```

اهحالصإو ءاطخألا فاشكتسا

(ةقث ةطقنب ةطبترملا تاداهشلا لك فذح ىلإ اذه يدؤي) تاداهشلا حسم

```
clear crypto ca certificate <trustpoint name>
```

(رمألا مزل اذا) TACACS ةيلمع ليغشت ةداعإ

```
process restart tacacsd
```

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