

# IOS زاهج ىلع TLS 1.3 ربع TACACS+ نيوكت ISE مادختساب XE

## تايوتحمل

---

[قمدملا](#)

[قماع قرظن](#)

[لىلدلا اذه مادختسا](#)

[قيساسلا تابلاطت](#)

[تابلاطت](#)

[قمدمتسملا تانوك](#)

[صيخرت](#)

[قزوجل افرادل ConfigureISE-1 عزجلا](#)

[TACACS+ مداخ ققداصل قداهشل ا عي قوت بلط عاشنا](#)

[TACACS+ مداخ ققداصل رنجل ققداصل ا عجرملا قداهشل ا عي قوت بلط عاشنا](#)

[ISE ب \(CSR\) عوملا قداهشل ا عي قوت بلط طبر](#)

[TLS 1.3 نيوكت](#)

[ISE ىلع قزوجل افرادل نيوكت](#)

[TLS ربع TACACS نيوكت](#)

[قكبشلا قزوجل ا عكبشلا قزوجل ا عومم عاشنا](#)

[ConfigureIdentity رجات](#)

[TACACS+ فيرعت تافل نيوكت](#)

[IOS XE RW - فلم - لوؤسملا فيرعت](#)

[IOS XE RO - فلم - لغشملا فيرعت](#)

[configureTACACS+ رماوا تاعومم](#)

[Cisco IOS XE RW - قعومم - لوؤسملا رماوا](#)

[Cisco IOS XE RO - قعومم - لغشملا رماوا](#)

[زاهجلا لوؤسم جهت تاعومم نيوكت](#)

[TLS 1.3 ربع TACACS+ ل Cisco IOS XE نيوكت - 2 عزجلا](#)

[زاهجلا قطس اوپ هؤاشنا مت حيتافم جوز - 1 نيوكتلا بولسا](#)

[TACACS+ مداخ نيوكت](#)

[TrustPoint نيوكت](#)

[TLS نيوكت عم TACACS & AAA](#)

[CA قطس اوپ هؤاشنا مت حيتافم جوز - 2 نيوكتلا بولسا](#)

[TLS نيوكت عم TACACS & AAA](#)

[ققحتلا](#)

---

## قمدملا

مداخك Cisco Identity Services Engine (ISE) عم TLS ربع TACACS+ ل الاثم دنتسملا اذه فصلي  
ليممعك Cisco IOS® XE زاهجو

## ةماع ةرطن

ةيفرطال ةطحمل الى لوصول مكحت 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 XE الى ةدنتسم ال.

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

## ةيساسال تابلطتم

### تابلطتم

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

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
- Cisco IOS XE، جم انرب 17.15+ رادصل 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 عيجم تادب رماي ال لمحتم ال ريثأتلل كمهف نم دكأتف، ليغشتل ديقت ككبش.

### صيخرت

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 دحاة وة سايس ة مدخ ة دق ع ىل ع TACACS+

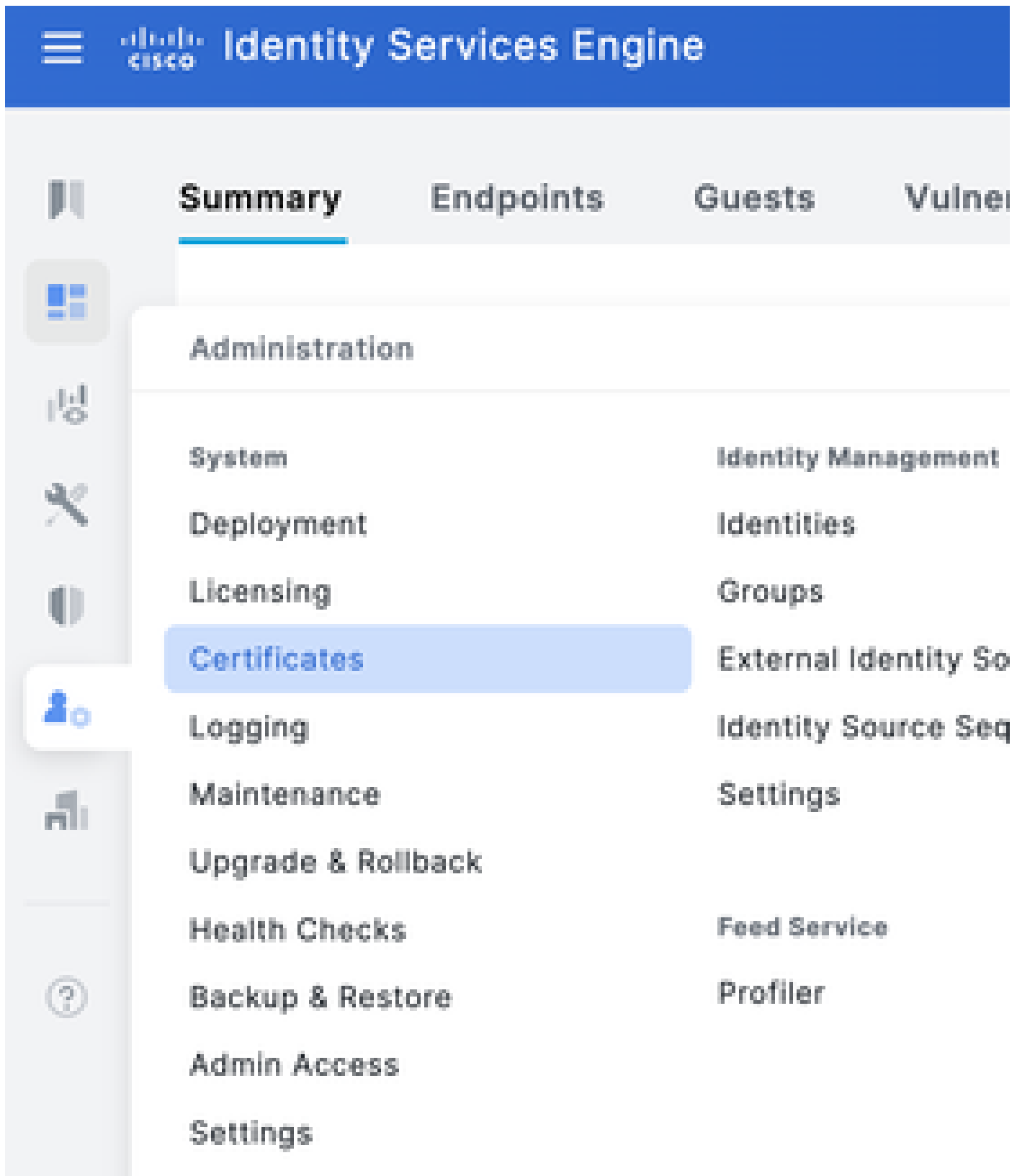
## ةزهجالا ةرادال ISE نيوكت - 1 ءزجالا

TACACS+ مداخ ة قداصل ة داهشلل عي قوت بل ط ءاشنل

.ةم وءملا تا ضرعت سمل دحأ مادختساب بيلولا ىل ع ISE ةرادل ة باب ىل ل لوخدل ل جس . 1 ة وطلال

ىل وائل ة وطلال ل ثمتت . تامدخال عي مجل ايتاذ ة ع قوم ة داهش ISE مدختسي ، يضا رتفا لكش بو  
(CA) ق دصملا ع رملال لبق نم ه عي قوتل (CSR) ة داهش عي قوت بل ط ءاشنل ي ف

.تاداهشلل > ماظنل > ةرادال ىل ل لقتنل . 2 ة وطلال



3. عودتك إلى صفحة إعدادات النظام، انقر على "إعدادات النظام" في القائمة الجانبية. انقر على "إعدادات النظام" في القائمة الجانبية.



مادختسالا دي ق TACACS ددح.4 ةوطخل

## Usage

Certificate(s) will be used for TACACS 

Allow Wildcard Certificates ☐ 

اهل TACACS+ ني كم ت متيس يتال PSN تاكبش ددح.5 ةوطخل

## Node(s)

Generate CSR's for these Nodes:

| Node                                     | CSR Friendly Name |
|------------------------------------------|-------------------|
| <input checked="" type="checkbox"/> ISE1 | ISE1#TACACS       |

ةبسانملا تامولعملاب عوضوملا لوقح ألما .6 ةوطخل

## 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 عوضومال نامض IP ناونعو DNS مسا فضا.7 ةوطخلال

### Subject Alternative Name (SAN)

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

ريدصت مٹ عاشن| قوف رقنا.8 ةوطخلال



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) صيخرتلا ةئيه نم ةعقوم (CRT) ةداهشلا ىلع لوصحلا كنكمي ،نآلا

TACACS+ مداخ ةقداصم ل رذجلا قداصم ل عجرم ل ةداهش ليمحت

جاردا رقنا ،ةنومضم ل صيخارلا تحت .تاداهشلا > ماطنلا > ةرادإلا ىلإ لقتنا 1. ةوطخلا

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' highlighted. 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.

| <input type="checkbox"/> | Friendly Name               | Trusted For                      | Serial Number    | Issued To            | Issued By            | Valid From       | Expiration Date   | Status |
|--------------------------|-----------------------------|----------------------------------|------------------|----------------------|----------------------|------------------|-------------------|--------|
| <input type="checkbox"/> | Amazon root CA              | Infrastructure<br>Cisco Services | 06 6C 9F CF ...  | Amazon Root CA 1     | Amazon Root CA 1     | Tue, 26 May 2015 | Sun, 17 Jan 2...  | Enr    |
| <input type="checkbox"/> | 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    |
| <input type="checkbox"/> | Cisco Licensing Root CA     | Cisco Services                   | 01               | Cisco Licensing R... | Cisco Licensing R... | Thu, 30 May 2013 | Sun, 30 May 2...  | Enr    |
| <input type="checkbox"/> | Cisco Manufacturing CA SHA2 | Endpoints<br>Infrastructure      | 02               | Cisco Manufactur...  | Cisco Root CA M2     | Mon, 12 Nov 2012 | Thu, 12 Nov 2...  | Enr    |
| <input type="checkbox"/> | Cisco Root CA 2048          | Endpoints<br>Infrastructure      | 5F F8 7B 28 2... | Cisco Root CA 20...  | Cisco Root CA 20...  | Fri, 14 May 2004 | Mon, 14 May ...   | Dis    |
| <input type="checkbox"/> | 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    |
| <input type="checkbox"/> | 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    |
| <input type="checkbox"/> | Cisco Root CA M2            | Infrastructure<br>Endpoints      | 01               | Cisco Root CA M2     | Cisco Root CA M2     | Mon, 12 Nov 2012 | Thu, 12 Nov 2...  | Enr    |
| <input type="checkbox"/> | Cisco RXC-R2                | Cisco Services                   | 01               | Cisco RXC-R2         | Cisco RXC-R2         | Wed, 9 Jul 2014  | Sun, 9 Jul 2034   | Enr    |

ةداهش عي قوت بلط عقو يذلا (CA) قداصم ل عجرم ل نع ةرداصل ةداهشلا دح 2. ةوطخلا  
نكمم راخلا ISE لخاد ةقداصم ل اب ةقتلانا نم دكأت .كب صاخلا (CSR) TACACS

### Import a new Certificate into the Certificate Store

\* Certificate File **Examiner...** 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

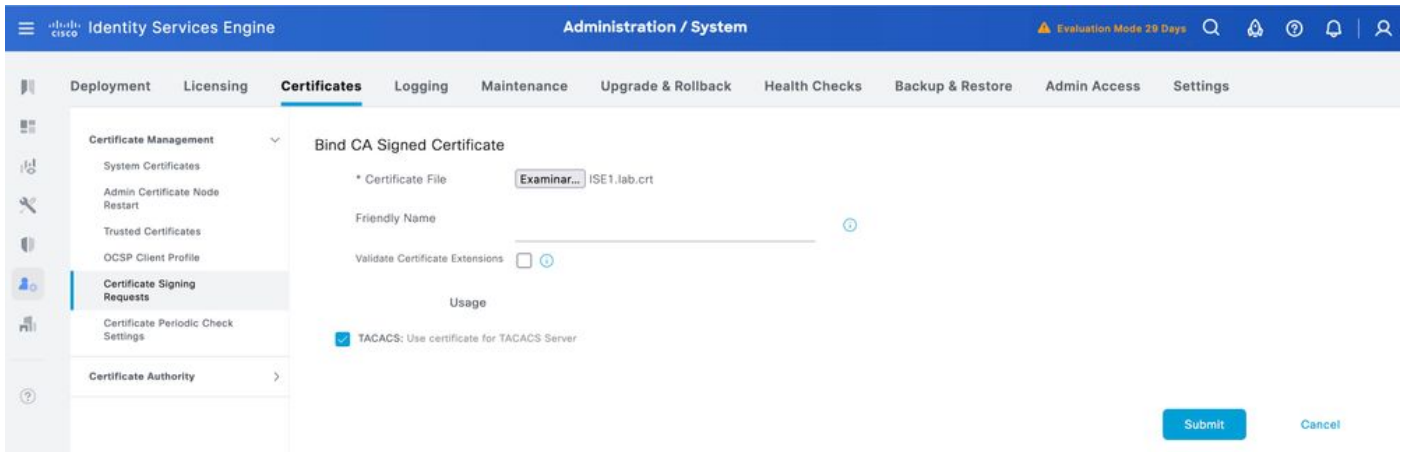
امب قوٹومل تاداهشل نمض نآل اءداهشل رهظت نأ بجي .لاسرا قوف رقنا 3. ةوطخل

ISE ب (CSR) عقوقملا ةداهشل عي قوت بلط طبر

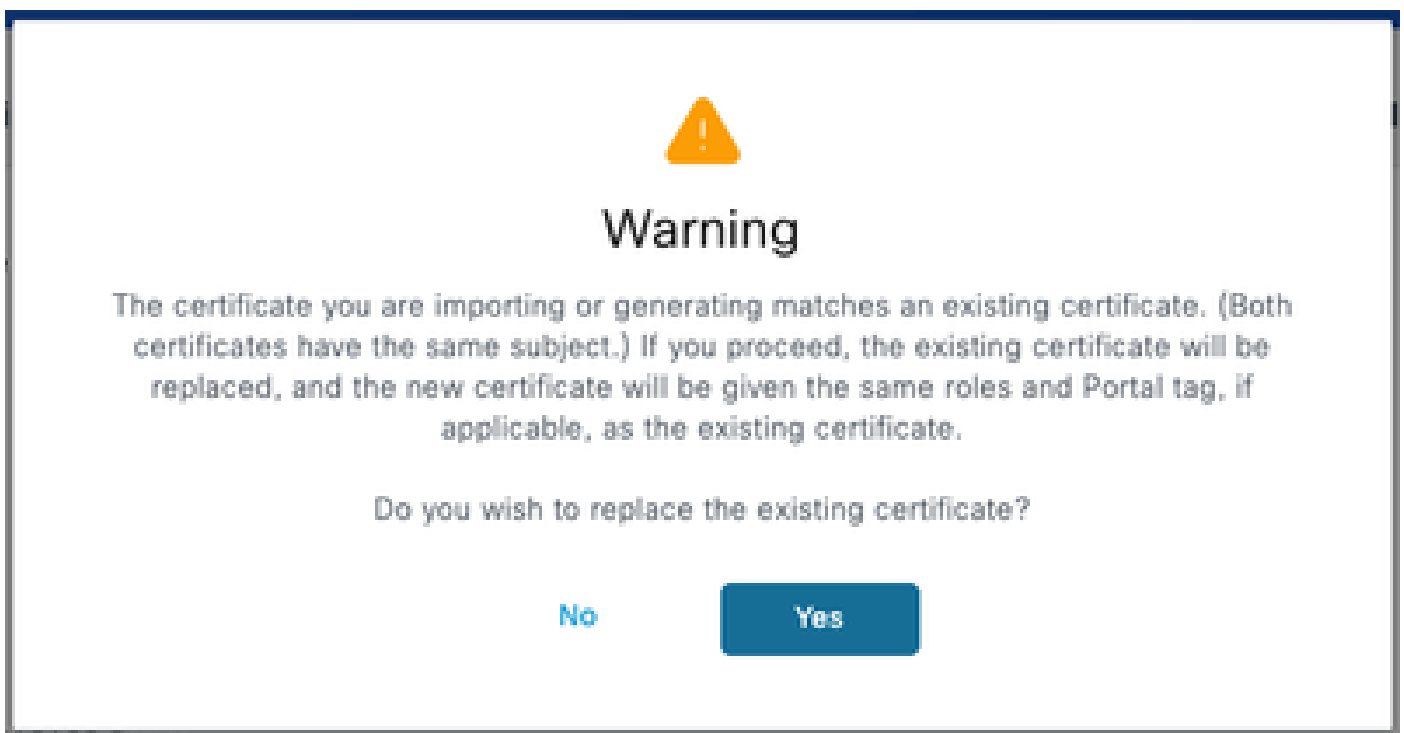
ISE. ىلع ةعقوملا ةداهشل تي بثت كنكمي ، (CSR) ةداهشل عي قوت بلط عي قوت درجم ب

TACACS دح ، ةداهشل عي قوت تابلط تحت . تاداهشل > ماظنل > ةرادإل ىلإ لقنتنا 1. ةوطخل ةداهشل طبر قوف رقناو ةقباسل ةوطخل ي ف هؤاشن مت يذل CSR.

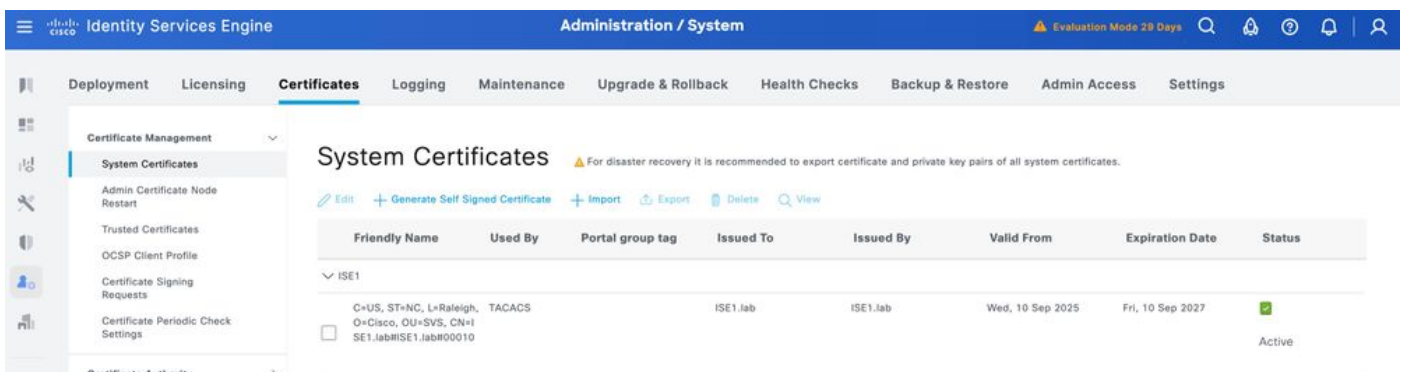
مادختسال تحت ةدوجومل TACACS راي تخال ةناخ نأ نم دكأتو ةعقوملا ةداهشل دح 2. ةوطخل ةددم لظتس.



معن قوف رقنا ،ةدوجومال ةداهشل لادبتسا لوح اريذحت تيقلت اذا .لاسرا قوف رقنا.3 ةوطخل ةعباتملل



مماظنل تاداهش نمض كلذ نم ققحتلا كنكمي .حيحص لكشب نآل ةداهشل تيبتت بجي



نكمت TLS 1.3

ايودي اهنى كم ت ب جي ISE 3.4.x ي ف يضارت فا لك ش ب TLS 1.3 نى كم ت م تي ال

تاداع ال > مازن ال > ةراد ال ال لوقت نا. 1. ةوطخ ال

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

مٹ، TLS رادصل تادادع نمض TLS1.3 راوجب راي تخالال ةناخ ددحو، نامأل تادادع قوف رقنا 2 ةوطخلال ظفح قوف رقنا.

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

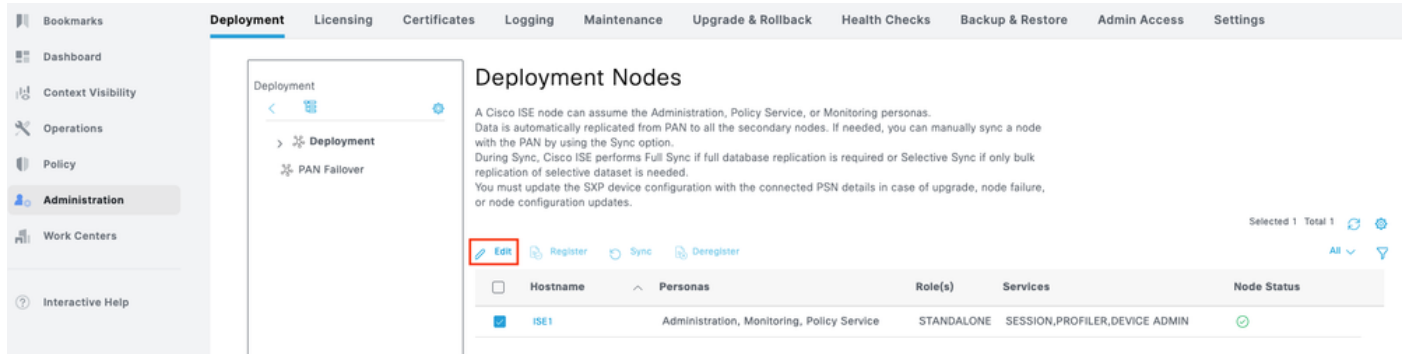


عيمج ىلع Cisco ISE قيبطت مداخ ليغشت ةداع ممت، TLS رادصل ريغت دنع: ريذخت Cisco ISE رشنللا ةزهجأ.

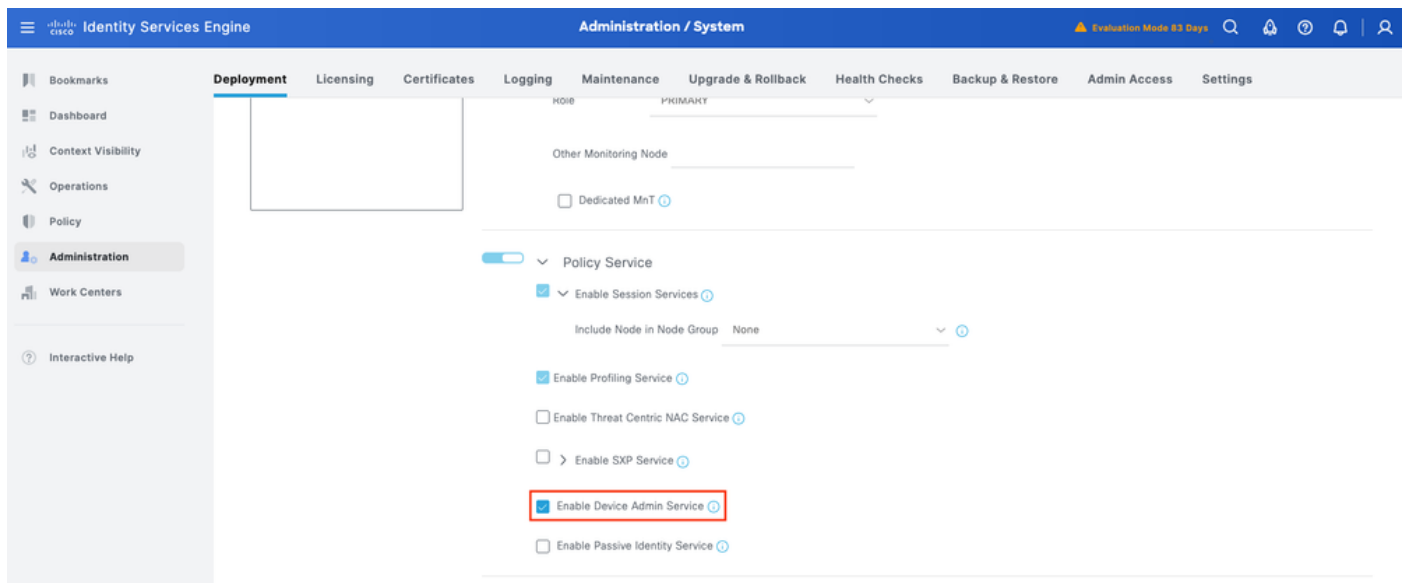
## ISE ىل عزهجالا ةرادا نيكمت

نيكمت ب مق ISE. ةدق ىل ع يضارتفا لكشب (TACACS+) عزهجالا ةرادا ةمدخ نيكمت متي ال PSN. ةدق ىل ع TACACS+.

رقن او ISE ةدق ل ةرواجم ال راي تخالالا ةناخ دح. رشن ال > ماظن ال > ةرادال ال ال لقتنا. 1. ةوطخل ريرحت قوف.



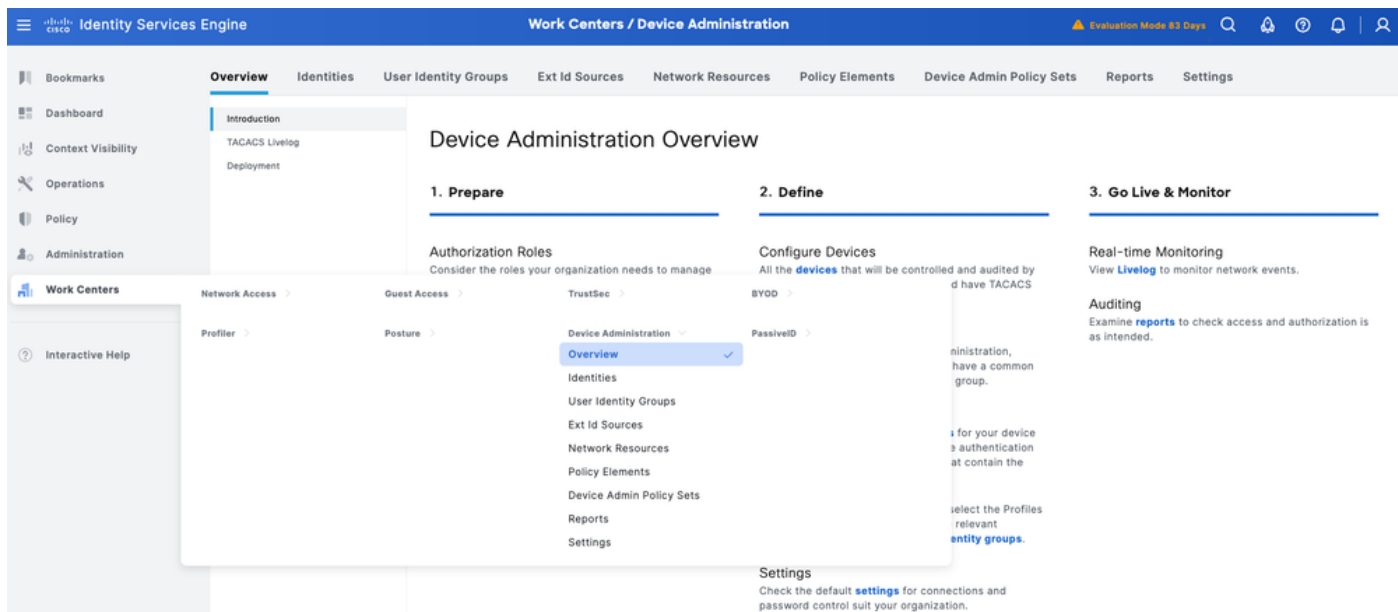
نيكمت ل ةرواجم ال راي تخالالا ةناخ دحو لفسا ال ريرمت للاب مق GeneralSettings تحت. 2. ةوطخل ةزهجالا ةرادا ةمدخ.



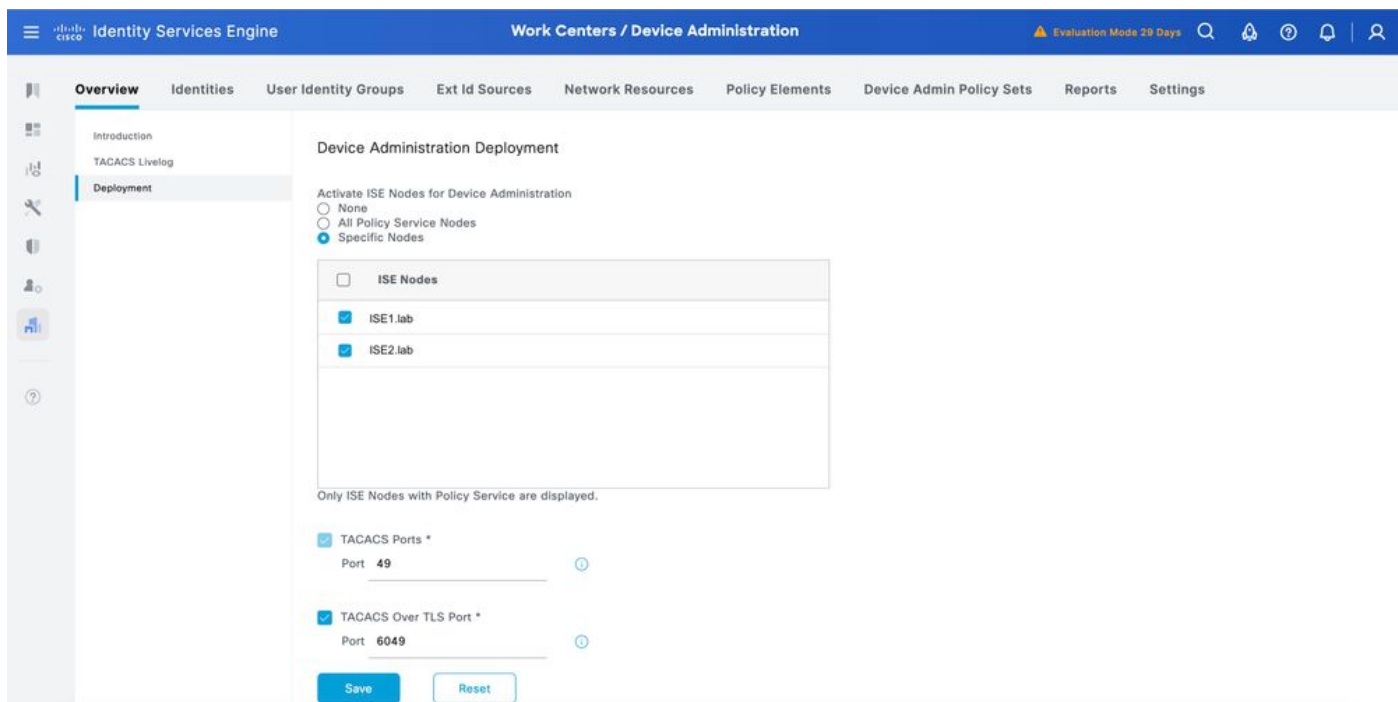
ISE. ىل ع نالال "زاهجالا لوؤسم ةمدخ" نيكمت مت. نيوكتال ظفح. 3. ةوطخل

TLS ربع TACACS نيكمت

ةماع ةرطن > عزهجالا ةرادا > لمعال زكارم ال 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 يلكيه لسلست

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

Identity Services Engine

Work Centers / Device Administration

Evaluation Mode

OverviewIdentitiesUsers

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

×

Add Group

Name\*

IOSXE

Description

Parent Group\*

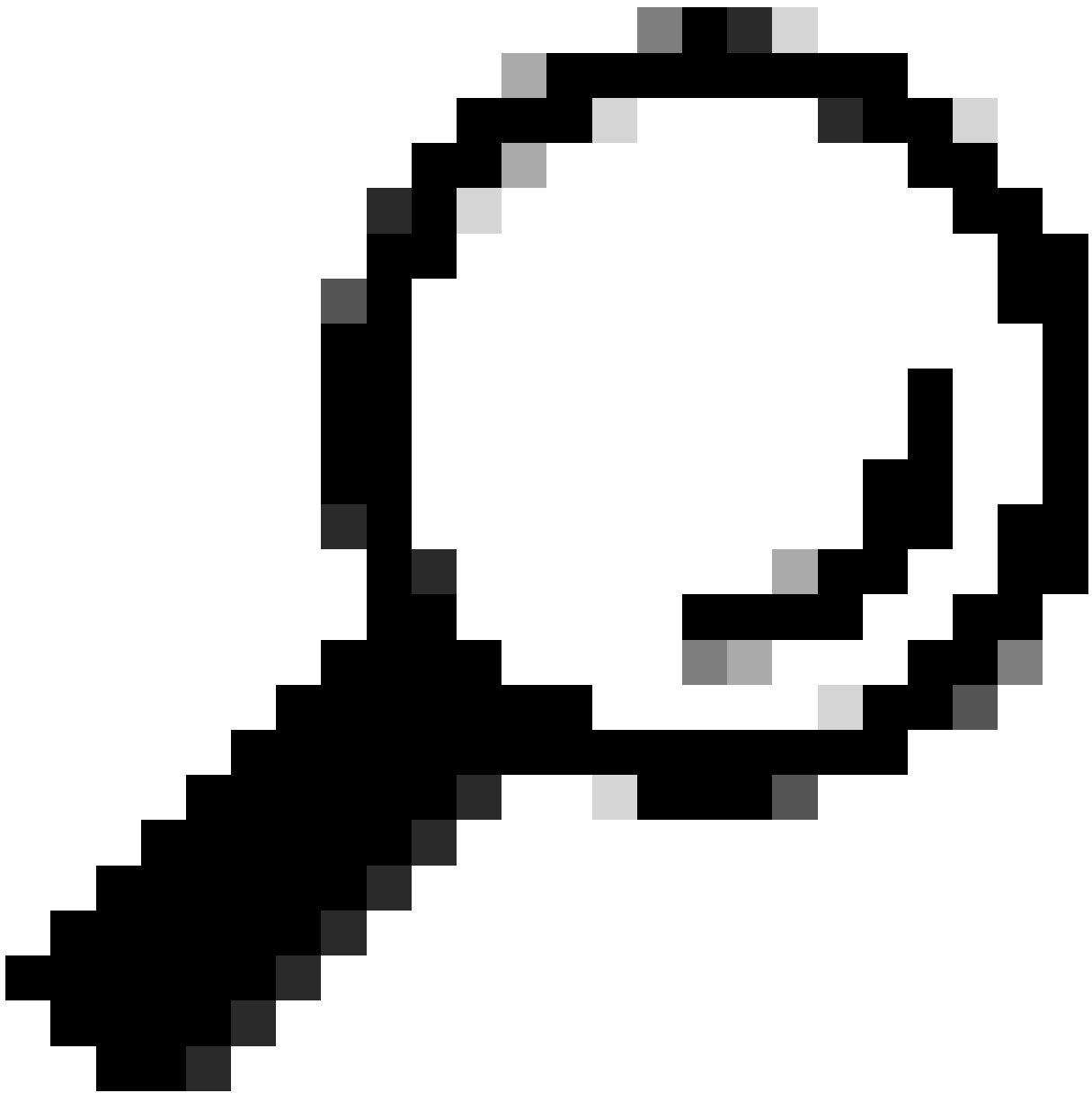
Select Group or Add as root group

Cancel

Save

☐

IOSXR

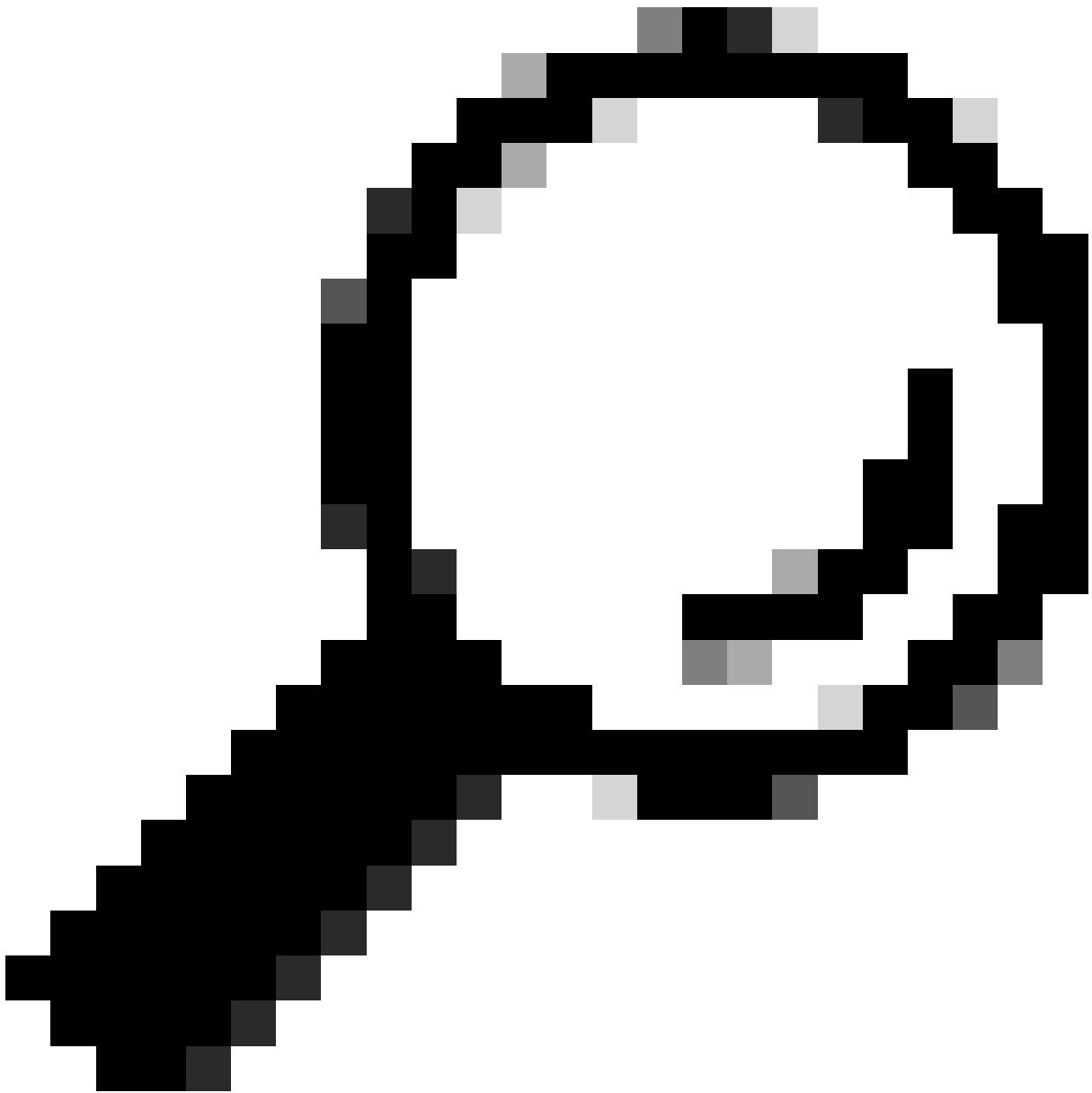


م تي ةيضا رتفا ةي مره تالسلست عقاومل ةفاكو ةزهجالا عاونأ عي مج دعت :خيملت  
في رعتو كب ةصاخلا ةي مرهلا تاجردتلا ةفاضل كنكمي . ISE ةطساوب اهري فوت  
ةلاح في اقحال همادختس كنكمي يذلا ةكبشل زاهج في رعت في ةفلتخملا تانوكملا  
ةسايسلا

---

> زاهجال ةرادا > لمعل زكارم ىلإ لقتنا . ةكبش زاهجك Cisco IOS XE زاهج فضا ، نآلا . 2 ةوطخل  
رابتخالا اذهل . ديدج ةكبش زاهج ةفاضلا ةفاضلا ىل عرقنا . ةكبشلا ةزهجا > ةكبشلا دراوم  
SVS\_BRPASR1K. نوكيس





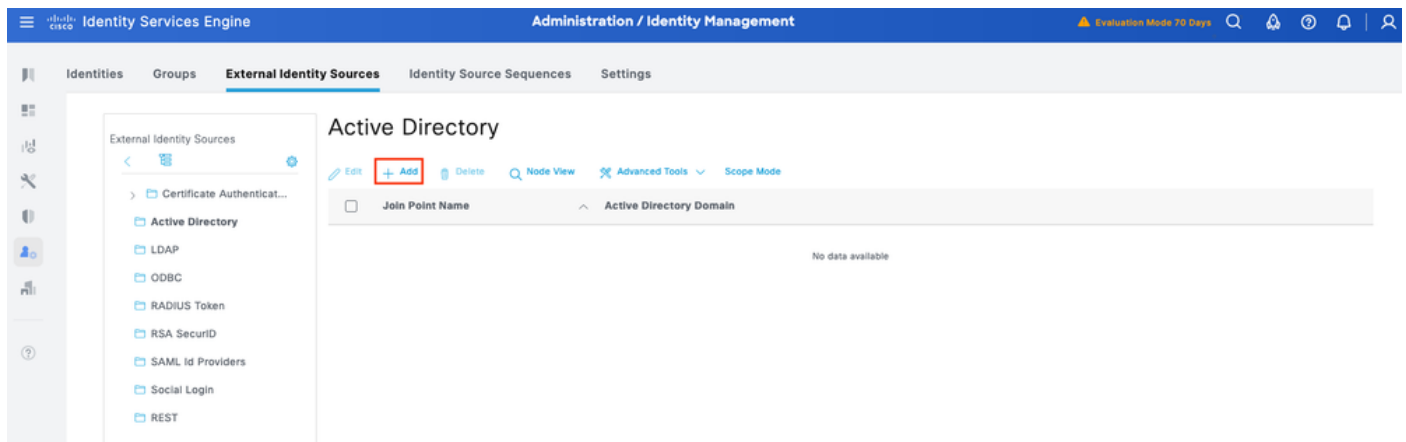
لمع ةسلج ليغشت ةداعإ بنجتل درفملا لاصتالا عضو نيكم تب ي صوي :خملت زاهجلا ىلإ اهيف رمأ لاسرا متي ةرم لك في TCP.

---

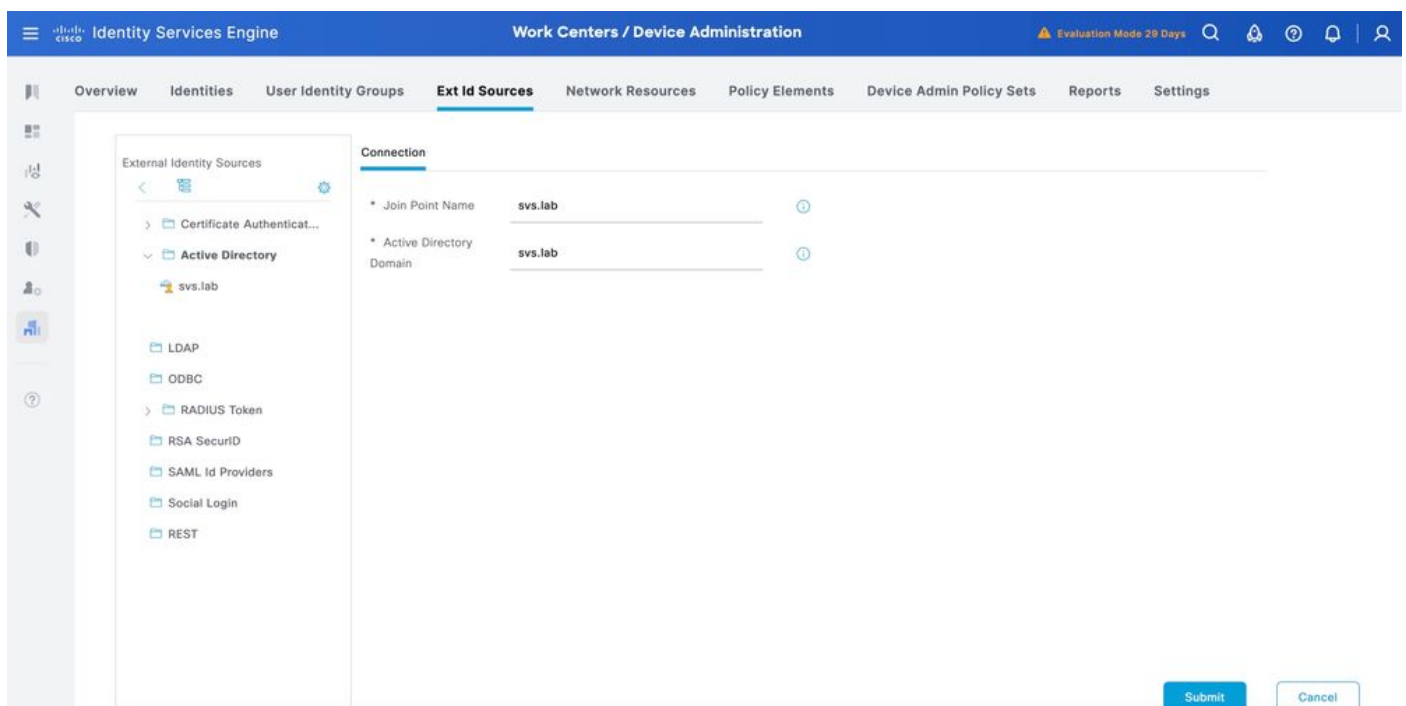
## Configured Identity رجاتم

نبي لخدال ISE يمدختسم نوكي نأ نكمي يذلاو، ةزهجال يل ووؤسم ةي وه نزخم مسقلا اذه ددحي جراح ةي وه ردصم، Active Directory (AD) ممدختسمي انه. ةم و عدم جراح ةي وه رداصم يأو.

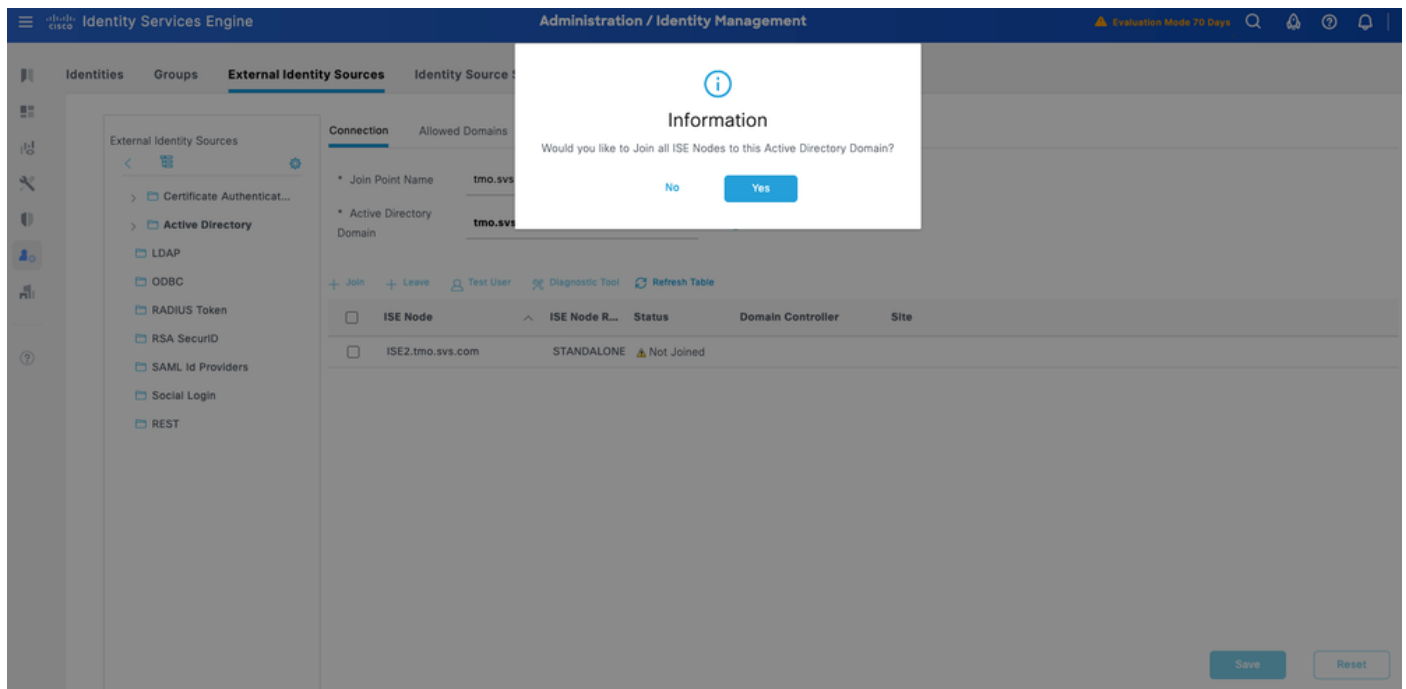
رقنا. Active Directory > جراحال ةي وهال نزاخم > ةي وهال ةرادإ > ةرادإلا ىلإ لقتنا. 1. ةوطخلا ةديج ةكرتشم AD ةطقن ديدحتل ةفاضل قوف.



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



Active Directory لاجم إلى ISE دقع عي مج مض يف بغرت له ةبالاطم ال دنع معن قوف رقن. 3 ةوطخل  
أذه؟



ةلإاحل نم ققحت AD إلى ISE مضمن او AD Join تا زايتم اب دامت عال اناي ب لخدأ 4. ةوطخل 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 ⓘ

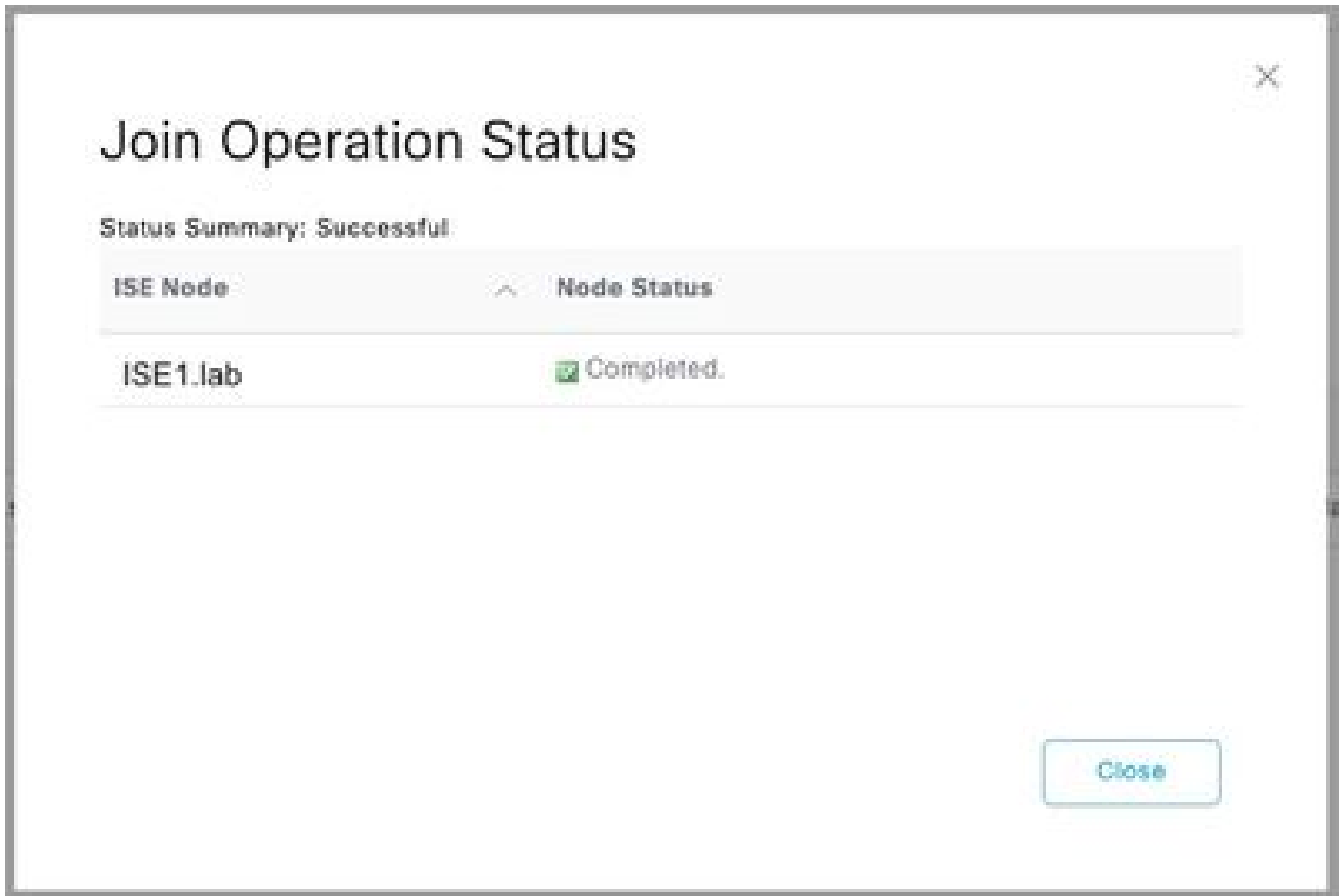
.....

☐ Specify Organizational Unit ⓘ

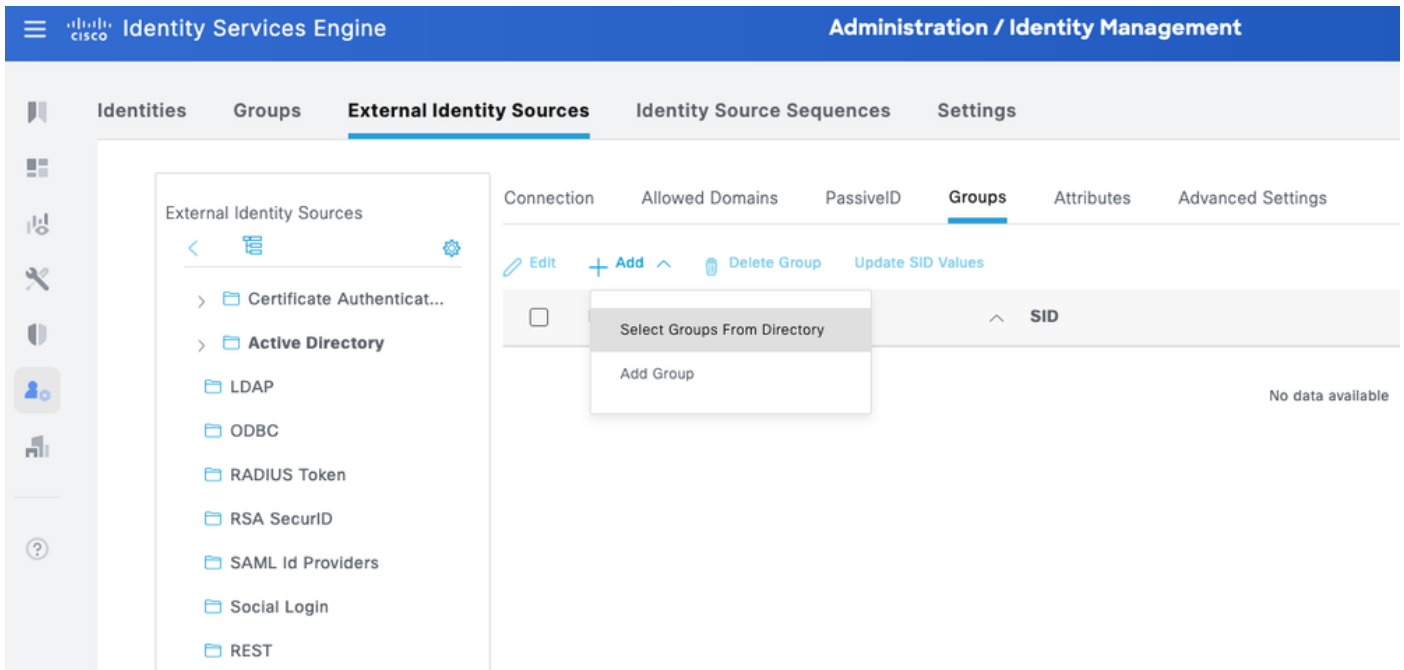
☒ Store Credentials ⓘ

Cancel

OK



عيج يلى لوصحلل ةفاضل قوف رقناو ،تاعومجم بيوبتلة مالع ىل لقتنا 5. ةوطخل اذه حضوي .زاهل الى لوصولل نيلوخم نيمدختسمل نم ي الى ادانستسا ةبولطملم تاعومجملم ليلدل اذه في ليلوختل جهن في ةمدختسمل تاعومجملم لاثمل



# Select Directory Groups

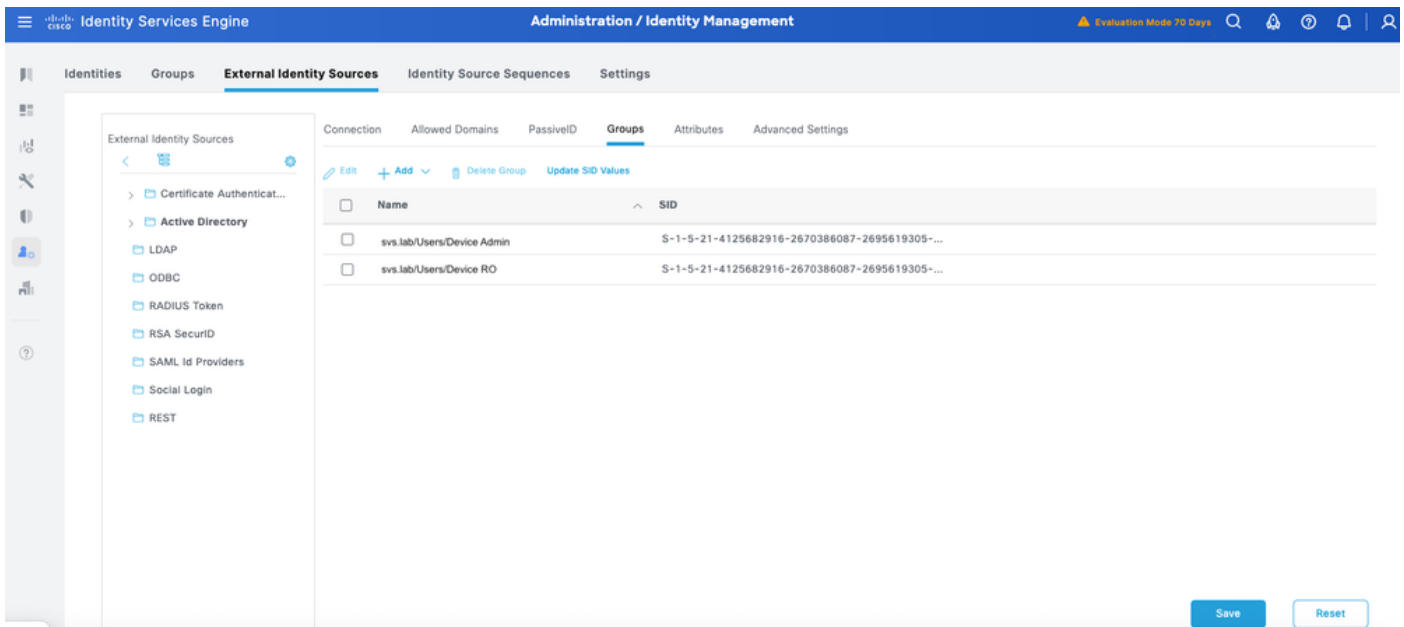
This dialog is used to select groups from the Directory.

Domain svcs.lab

Name Device \* SID \* Type ALL  
Filter Filter

Retrieve Groups... 2 Groups Retrieved.

| <input type="checkbox"/> | Name                        | Group SID                                  | Group Type |
|--------------------------|-----------------------------|--------------------------------------------|------------|
| <input type="checkbox"/> | svcs.lab/Users/Device Admin | S-1-5-21-4125682916-2670386087-26956193... | GLOBAL     |
| <input type="checkbox"/> | svcs.lab/Users/Device RO    | S-1-5-21-4125682916-2670386087-26956193... | GLOBAL     |



## TACACS+ في رعت تافل م ني وكت

زهجأ ىل ع نيي سيئر ني مدختسم ني رود ىل TACACS+ تافيصوت نيي عت ىل ب هاذ تنأ Cisco IOS XE:

- زاهج ال ي ف تازايتما رثكأل رودل وه اذه - (يرذجال ماطنل ريدم) Root System Administrator ىل لمكأل يرادلل لوصول قح بيرذجال ماطنل لوؤسم رود بحاص مدختسم ال عتمتي ني وكتل تاناكمل ماطنل رماو اعيمج.
- ةارقلل لوصول ىل نوجاتحي نيذل ني مدختسم ال ىل رودل اذه فدهي - ليغشتل لماع اهجالص او عاخال فاشكتساو عبقارملا ضارغل ماطنل ىل طقف.

TACACS+: IOS XE\_RW و IOSXR\_RO. نم نافيصوت تافيصوتل هذه ني ب هنأ ىل راشيو

لوؤسم ال في رعت فلم - IOS XE\_RW

تافلم > جئاتنل > ةسايسل رصانع > ةزهجأل ةرادإ > لمعلل زكارم ىلإ لقتنا 1 ةوطخل  
IOS XE\_RW هتيمستب مقو اديج TACACS فيرعت فلم فضا. TACACS فيرعت

15. ك زايتما ىصقأل دحلل او زايتما ريصقتل تنيعو تصحف 2. ةوطخل

ظفحلل او نيوكتل نم دكأت. 3. ةوطخل

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Device Administration'. The left sidebar contains a navigation menu with options like Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, and More. The main content area is titled 'TACACS Profiles > IOSXE\_RW' and 'TACACS Profile'. It shows the 'Name' as 'IOSXE\_RW' and a 'Description' field. Below this, there are tabs for 'Task Attribute View' (selected) and 'Raw View'. Under 'Task Attribute View', there is a section for 'Common Tasks' with a 'Common Task Type' dropdown set to 'Shell'. Two checkboxes are visible: 'Default Privilege' and 'Maximum Privilege', both checked. Each checkbox has a value of '15' and a dropdown menu with the text '(Select 0 to 15)'.

لغشملل فيرعت فلم - IOS XE\_RO

تافلم > جئاتنل > ةسايسل رصانع > ةزهجأل ةرادإ > لمعلل زكارم ىلإ لقتنا 1 ةوطخل  
IOS XE\_RO هتيمستب مقو اديج TACACS فيرعت فلم فضا. TACACS فيرعت

1. ك زايتما ىصقأل دحلل او زايتما ريصقتل تنيعو تصحف 2. ةوطخل

ظفحلل او نيوكتل نم دكأت. 3. ةوطخل

Identity Services Engine Work Centers / Device Administration

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

Conditions > Network Conditions > Results > Allowed Protocols > TACACS Command Sets > **TACACS Profiles**

Name: IOSXE\_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)

☐ Access Control List

☐ Auto Command

## configure TACACS+ رماو اتاعومجم

TACACS+: Cisco\_IOS XE\_RW و Cisco\_IOS XE\_RO رماو اتاعومجم انا ىلع رصانعال هذه فيرعت متيو XE\_RO.

لوؤسمال رماو ةعومجم - Cisco\_IOS XE\_RW

رماو اتاعومجم > جئاتنل > ةسايسل رصانع > ةزهجال ةرادا > لمعال زكارم ىلإ لقتنا 1. ةوطخل TACACS. Cisco\_IOS XE\_RW اهتي مستب مقو ةديج TACACS رماو ةعومجم فضا.

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

Identity Services Engine Work Centers / Device Administration

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

Conditions > Network Conditions > Results > Allowed Protocols > **TACACS Command Sets** > TACACS Profiles

TACACS Command Sets > CISCO\_IOSXE\_RW

Command Set

Name: CISCO\_IOSXE\_RW

Description:

Commands

Permit any command that is not listed below ☒

Add Trash Edit Move Up Move Down

| Grant | Command | Arguments |
|-------|---------|-----------|
|-------|---------|-----------|

## لغشمل رماوأةومجم Cisco\_IOS XE\_RO

> ةسايسال رصانع > زاهال ةرادا > لمعل زكارم ىلإ لقتنا، ISE مدختسم ةهجاو نم 1 ةوطخل مق مثةديج TACACS رماوأةومجم ةفاضاب مق. TACACS رماوأةومجم > جئاتنل Cisco\_IOS XE\_RO اهتيمستب

ديج رما فضا، رماوالا مسق ي ف. 2. ةوطخل

رقناو؛ رمالا دومع ي ف ضرعل لخدأو ءحنملا دومعل ءلدسنملا ءمئاللا نم ءامسال ددح. 3. ةوطخل كيشلال مهس قوف

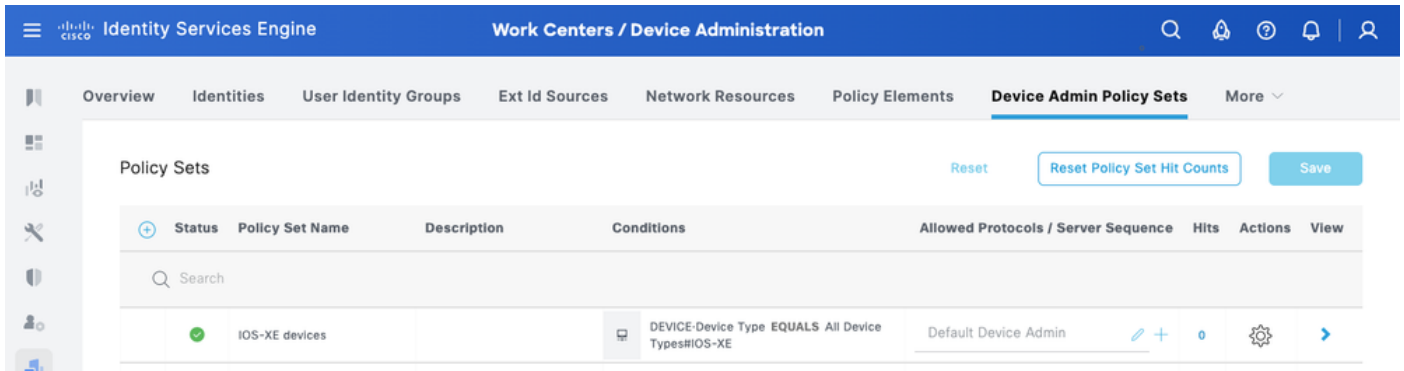
ظفح قوف رقناو تانايبلا نم دكأت. 4. ةوطخل

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Work Centers / Device Administration'. The left sidebar has a menu with 'Policy Elements' selected. The main content area is titled 'TACACS Command Sets > CISCO\_IOSXE\_RO Command Set'. It contains a 'Name' field with 'CISCO\_IOSXE\_RO', a 'Description' text area, and a 'Commands' section with a checkbox for 'Permit any command that is not listed below'. Below this is a table with columns 'Grant', 'Command', and 'Arguments'. The table has one row with 'PERMIT' in the 'Grant' column and 'show' in the 'Command' column. At the bottom right of the table are icons for edit, delete, and add.

## زاهال لوؤسم ءهن تاعومجم نيوكت

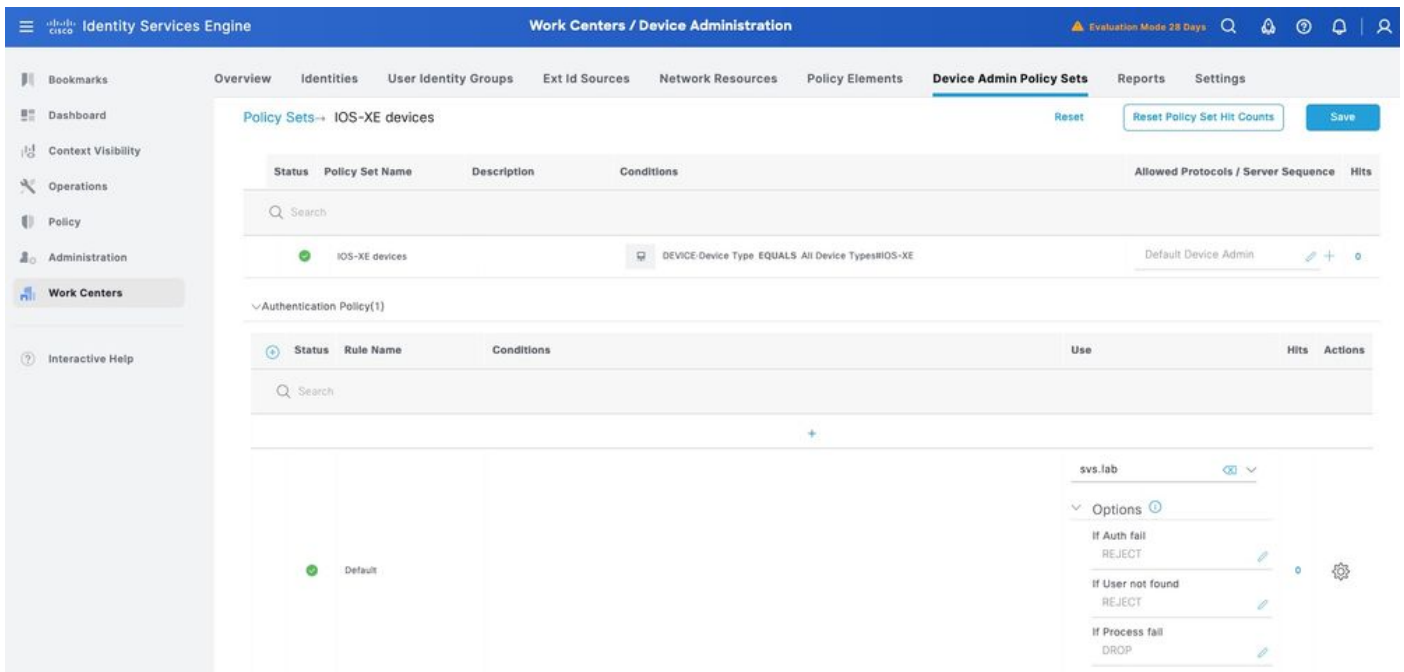
تاعومجم مسقت نا نكمي. ءزهال ةرادال يضارتفا لكشب ءهنل تاعومجم نيكمت متي TACACS فيرعت تافل مقببط ليهستل ءزهال عاونأ ىلإ اءانتسا تاسايسال

ءزهأةفاضل. ءزهال ةرادا تاسايس تاعومجم > زاهال ةرادا > لمعل زكارم ىلإ لقتنا. 1. ةوطخل عاونأ لك يواسي زاهال عون:ءادأ ددح طرش تحت. تاسايسال ءومجمل ءيديل IOS XE يضارتفال زاهال لوؤسم ددح، اءب ءومسمل تالوكوتوربلا تحت. #IOS XE ءزهال



هذه جهنلا ةعومجم نيوكتل نميألا مهسلا قوف رقناو ظفح قوف رقنا. 2 ةوطخل

كرتأ. فرعما نزمك AD مدختست، ةقداصم لل. ةقداصم لا ةسايس عاشناب مق. 3 ةوطخل  
تلشف اذاو مدختسم لا رثعي مل اذا، ةقداصم لا تلشف اذا تحت ةيضارتفالا تاراخيلا  
ةيلعمل.



ضيوفتلا ةسايس ديحت. 4 ةوطخل

Active Directory (AD) في نيمدختسم لا تاومجم لا اذانتسا ليوختلا جهن عاشناب مق

لالم لا لبس لا

فلمو Cisco\_IOSXR\_RO رماوالا ةعومجم لا AD ةعومجم وا زاه في نيمدختسم لا نييعت متي  
IOSXR\_RO Shell فيرت.

Cisco\_IOSXR\_RW رماوالا ةعومجم لا AD ةعومجم زاه لوؤسم في نيمدختسم لا نييعت متي  
IOSXR\_RW ةقبط فيرت فلمو.

**Identity Services Engine**

## Work Centers / Device Administration

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

[Policy Sets → IOS-XE devices](#) [Reset](#) [Reset Policy Set Hit Counts](#) [Save](#)

| Status                               | Policy Set Name | Description | Conditions                                        | Allowed Protocols / Server Sequence    | Hits |
|--------------------------------------|-----------------|-------------|---------------------------------------------------|----------------------------------------|------|
| <span style="color: green;">✔</span> | IOS-XE devices  |             | DEVICE:Device Type EQUALS All Device Types#IOS-XE | Default Device Admin <a href="#">+</a> | 0    |

> Authentication Policy(1)

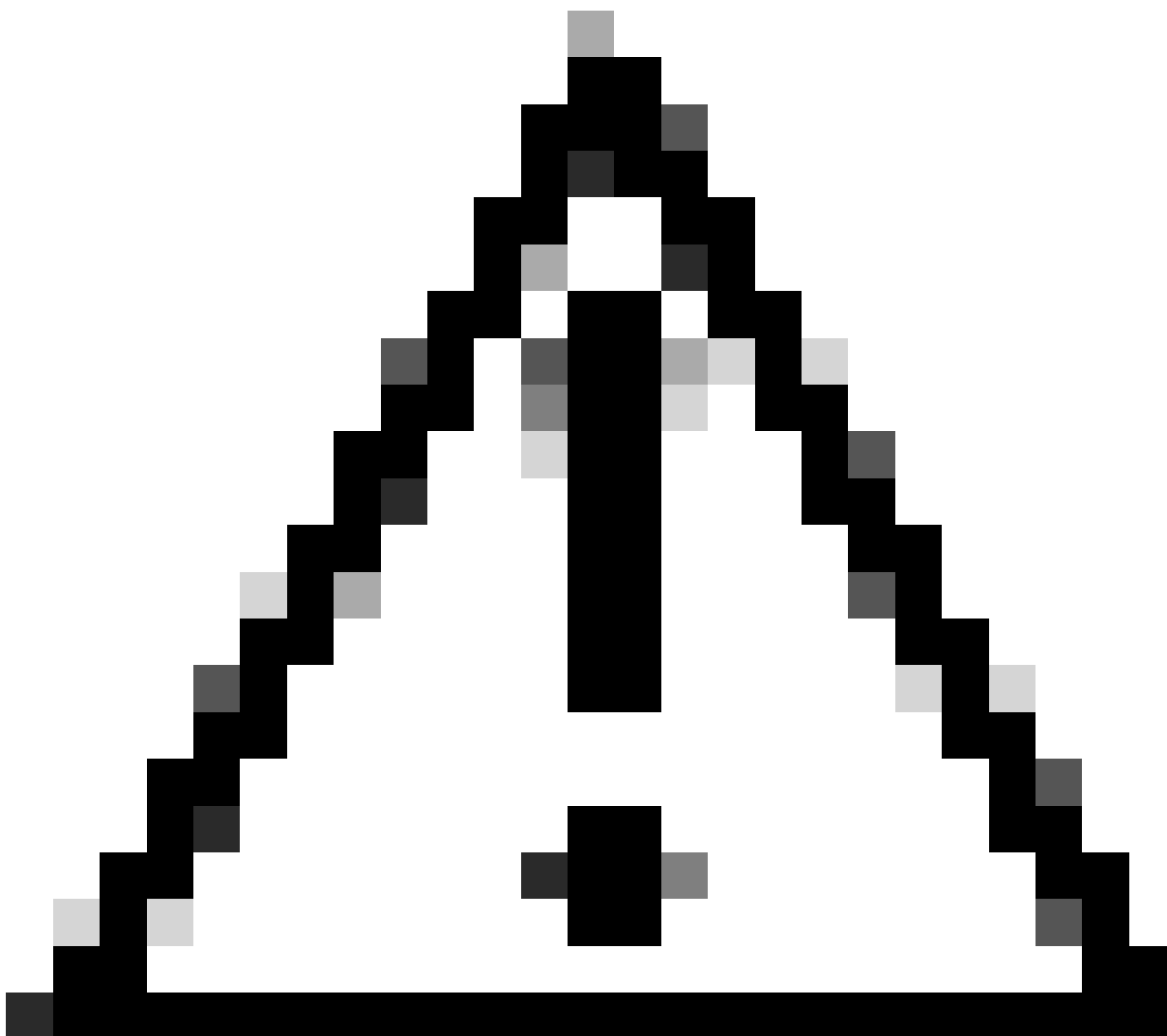
> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

∨ Authorization Policy(3)

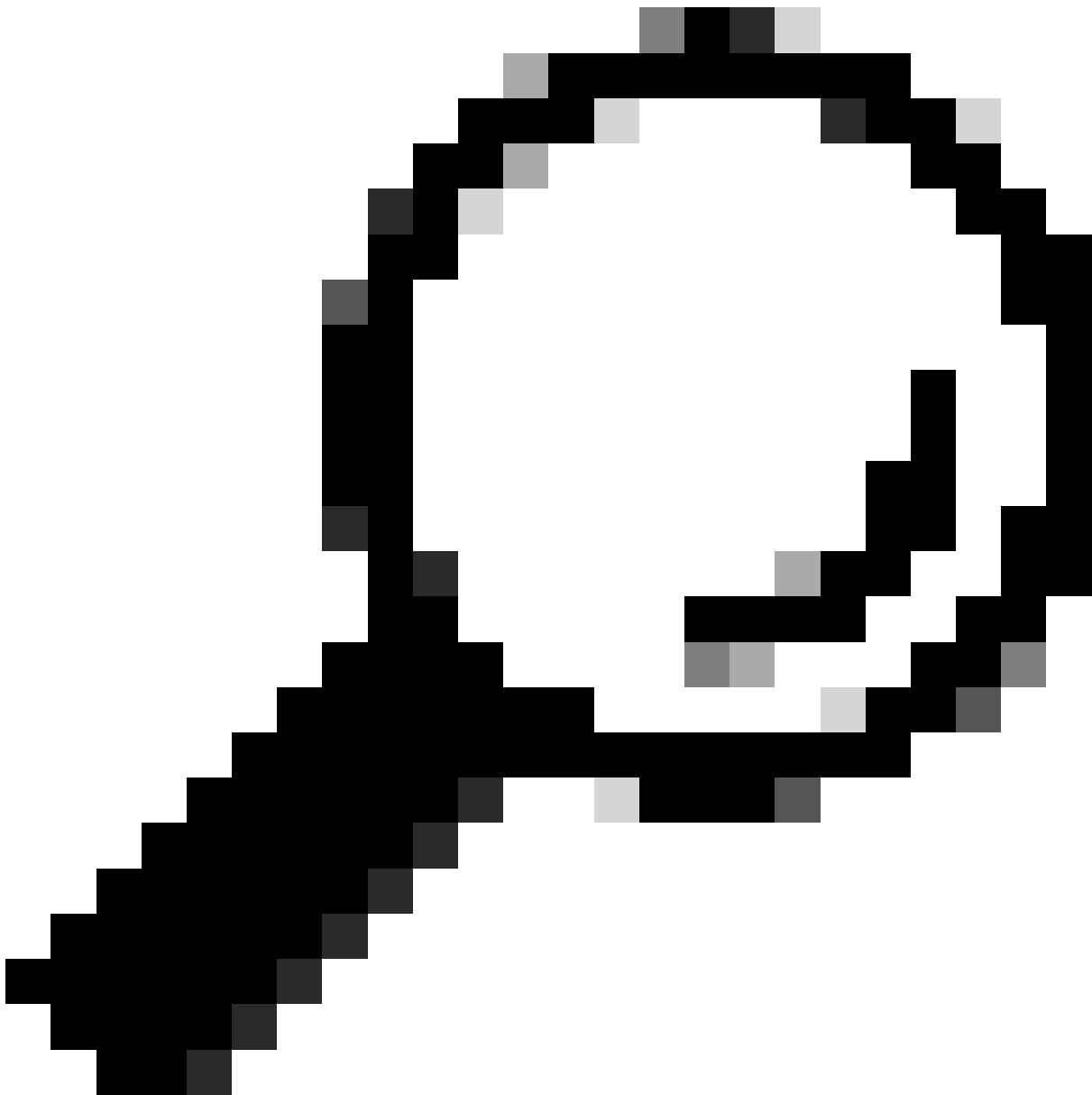
|                                      |                       |                                                             |  | Results                           |                                          |      |         |
|--------------------------------------|-----------------------|-------------------------------------------------------------|--|-----------------------------------|------------------------------------------|------|---------|
| + Status                             | Rule Name             | Conditions                                                  |  | Command Sets                      | Shell Profiles                           | Hits | Actions |
| <span style="color: green;">✔</span> | Authorization Rule RO | svs.lab ExternalGroups<br>EQUALS svs.lab/Users/Device RO    |  | CISCO_IOSXE_RO <a href="#">+</a>  | IOSXE_RO <a href="#">+</a>               | 0    |         |
| <span style="color: green;">✔</span> | Authorization Rule RW | svs.lab ExternalGroups<br>EQUALS svs.lab/Users/Device Admin |  | CISCO_IOSXE_RW <a href="#">+</a>  | IOSXE_RW <a href="#">+</a>               | 0    |         |
| <span style="color: green;">✔</span> | Default               |                                                             |  | DenyAllCommands <a href="#">+</a> | Deny All Shell Profile <a href="#">+</a> | 0    |         |

## 1.3 TLS ربيع Cisco IOS XE نيوكت - 2 عجل



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

---



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

## زاهجل ةطساوب هؤاشنإ مت خيتافم جوز - 1 نيوكتلتا بولسا

TACACS+ مداخ نيوكت

Router TrustPoint ل مدختسي خيتافم جوز ءاشنإو لاجملا مسا نيوكتب مق 1 ةوطخل

```
ip domain name svcs.lab
```

```
crypto key generate ec keysizes 256 label svcs-256ec-key
```

حیاتیات اور جیولوجی کے شعبوں میں 1 ویں درجہ

## CA. شهادة TrustPoint 2.0

```
Enter the base 64 encoded CA certificate.

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

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

MIIFDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UEBhMCVVMxZmFzAVBgNVBAGTdk5vcnRoIENhcn9saW5hMRAwDgYDVQQHEwdSYWx1aWdoMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECXMdu1ZTMRIwEAYDVQQDEw1TV1MgTGF1Q0EwHhcnMjUwNDI4MTcwNTAwWhcnMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJVUzEXMBUGA1UECBMTm9ydGggQ2Fyb2xpbmExEDAOBgNVBACTB1JhbGVpZ2gxZjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVNWUyBYWJJDQTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZU0yn2vIn6gKbx3M7vaRq2YjwZlZSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QWVvwV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLbo0kXEiKjPLatkXojB8FVrhLF30jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4mutNo7IhbJSrgAFXmj1bBjMmgspObULo/wxMHDtbtPBf11HRHTkNIo3qy04UADL2WpoGhgT/FaxxBo2UBcnYVaP+jjREONYT973MCbVAAxtNVU6bEBR0z+LWniACzupm+qh23SL43uw5A3iSw/BuU1E9p7B0e8oDNKU6gX1ojKyLP/gC7j8AeP03ir+kZui8b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQNgJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTixy9hpKZIKB86t2ZA3JX8CLsbCa13sAz1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4ydH10rrurXsZummj9QBnkX4pgY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw

```
83g9EMgKV0ARIiVUa/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQMFgptV1MgTGF1IENBMAOGCSqGSib3DQEB
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLFINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqj06lqJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9n0A/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8v1oI7YZmjFmem+5rT6Gnk
eU/1X7nV61SYG5W5K+I8uaKuyBHOmN7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0dsS/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgDRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWffFOXe/AJHQG7STT
HaXLU9r2Ko603oecu8ysGTwL1It/9T1/F0b0xZRugWcpJrVoTgDGuA==
```

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

Certificate has the following attributes:

Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D

Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 9A854A95 C83AC737

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

yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

cat9k(config)#

3. إعداد شهادة CSR.

<#root>

cat9k(config)#

crypto pki enroll svcs\_cat9k

% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab

% The subject name in the certificate will include: cat9k.svs.lab

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

yes

Certificate Request follows:

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

```
MIIBfDCCASMAQAwgYQxGjAYBgNVBAMTEWdhD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLewNTV1MxDjAMBGNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAXCzAJBgNVBAGT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCsqGSib3DQEJAhyRY2F0OWsudG1vLnN2cy5j
b20wWTATBgcqhkiJOPQIBggqhkiJOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQKOMS0wKzAcBgNVHREFTATghFjYXQ5ay50bw8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTWm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
```

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

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

Redisplay enrollment request? [yes/no]:

no

cat9k(config)#

ق.دصملا عجرملا نم ةعقوملا ةداهشلا داري تسلا 4. ةوطخل

<#root>

cat9k(config)#

crypto pki import svcs\_cat9k certificate

Enter the base 64 encoded certificate.

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

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

```
MIID8zCCAduGAWIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxZzAVBgNVBAGTDk5vbnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECjMDU1ZTMRIwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTEOMTUxMjAwWhcNMjUwNTEOMTUxMjAwWjCBhDEaMBGGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAStA1NWUzEOMAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUEELMAkGA1UECBMCTkMxZzA1BgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IAB01gTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiYjXmLpFc03uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQRRFg94Y2EgY2Vy
dG1maWNhdGUwHAYDVRORBBUwE4IRY2F0OWsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMAOGCSqGSIb3DQEBGwUAA4ICAQB0bgKVykeyVC9Usvuu0AUsGaZHGwy2H9Yd
m5vIau16PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAHzY
RtmIM5KIojiDHLtiFpayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLP7nxvh00m/LXwCWUhwgVio0AuU2Fe
k5NthtvdXNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyZCsTBb6RvL+HsXqBgXGc5
1xCSolTYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvj4rSPUHQSY+4m
Qq2Sn3iqf4mGh/A08T4iXfWdWfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27Uf8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVRpitwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDfmmFFourBsaAioz7ouY
2r1Mh+OpE83Uu+41OTMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXmtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAH0FcyXrvG6
3i/1b9erGQ==
```

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

% Router Certificate successfully imported

cat9k(config)#

## TACACS & AAA نيوكت عم TLS

(هجوم) ليمع لل TrustPoint نارق او، AAA تاعومجومو TACACSS م داخ عاشنلا 1. ةوطخل

```

tacacs server svcs_tacacs
  address ipv4 10.225.253.209
  single-connection
  tls port 6049
  tls idle-timeout 60
  tls connection-timeout 60
  tls trustpoint client svcs_cat9k
  tls ip tacacs source-interface GigabitEthernet0/0
  tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svcs_tls
  server name svcs_tacacs
  ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request

```

AAA بېلگىسىنىڭ 2. قىسمىنىڭ.

```

aaa authentication login default group svcs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svcs_tls enable
aaa authorization config-commands
aaa authorization exec default group svcs_tls local if-authenticated
aaa authorization commands 1 default group svcs_tls local if-authenticated
aaa authorization commands 15 default group svcs_tls
aaa accounting exec default start-stop group svcs_tls
aaa accounting commands 1 default start-stop group svcs_tls
aaa accounting commands 15 default start-stop group svcs_tls
aaa session-id common

```

## CA قىسمىنىڭ 2 - قىسمىنىڭ بېلگىسى

PKCS#12 قىسمىنىڭ قىسمىنىڭ CA ۋە زامانلىق تەدۈرلەش كىلىدىغان بېلگىسىنىڭ قىسمىنىڭ مۇددەتلىك بولسا، CSR قىسمىنىڭ بىر قىسمىنىڭ بولسا.

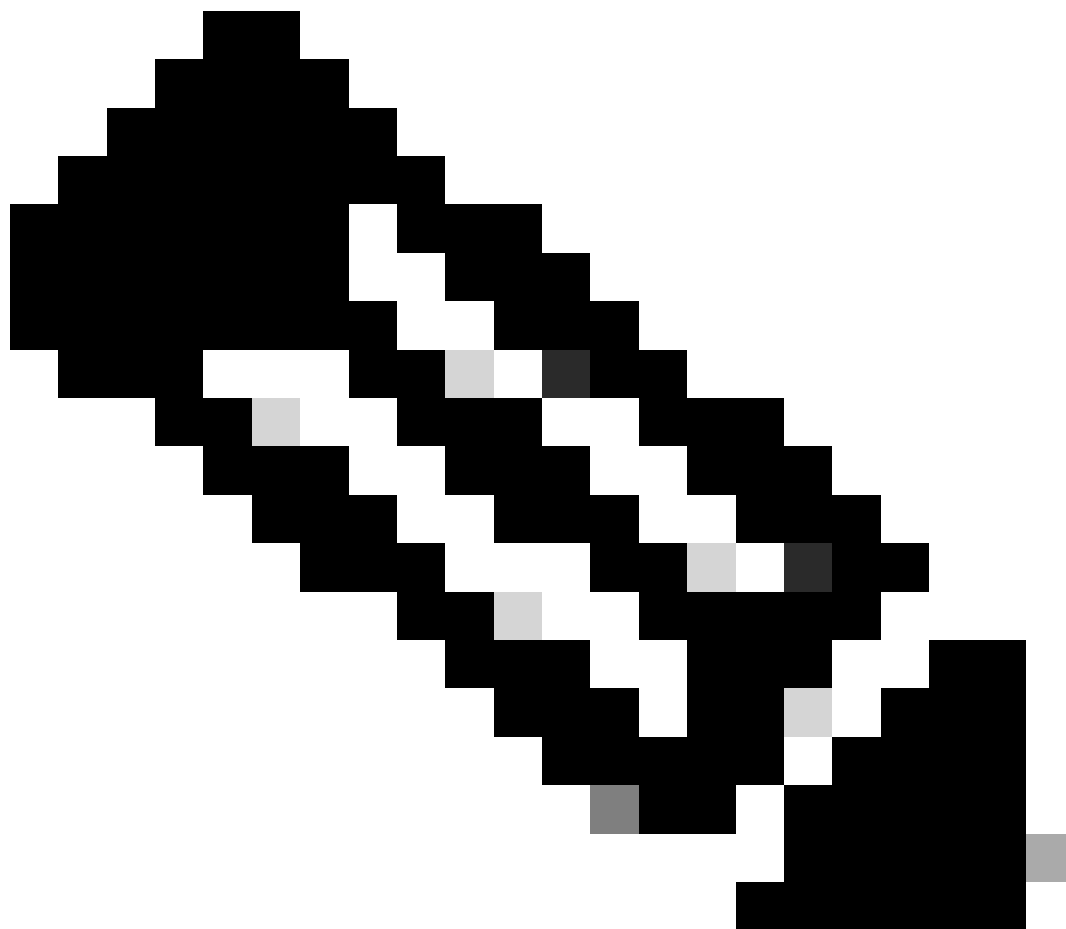
TrustPoint قىسمىنىڭ 1. قىسمىنىڭ.

```

cat9k(config)#crypto pki trustpoint svcs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none

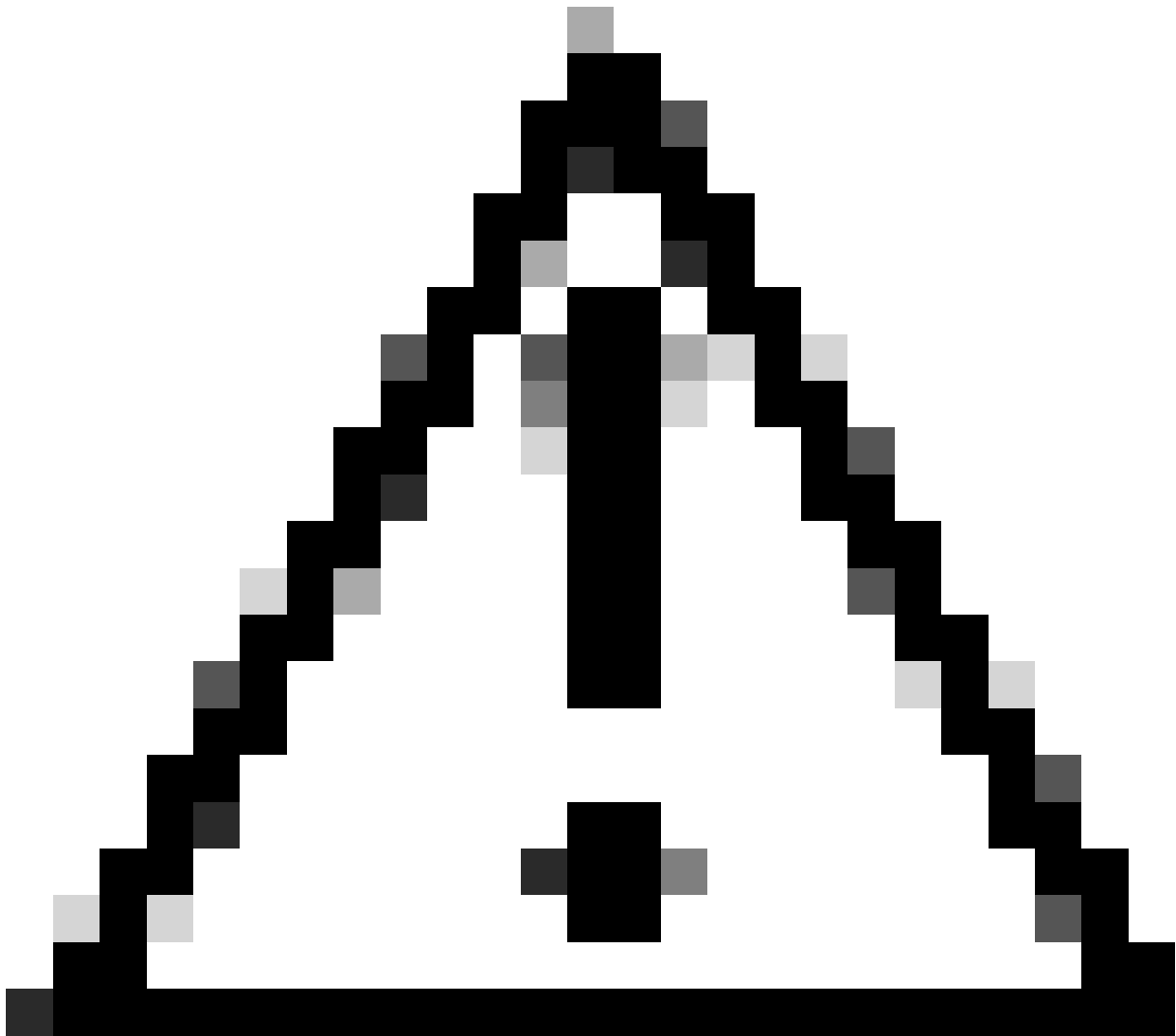
```

bootflash ۋە PKCS#12 قىسمىنىڭ 2. قىسمىنىڭ.



حاتفملاو ةلماكلا تاداهشلا ةلسلس ىلع يوتحي PKCS#12 فلم نأ نم دكأت :ةظحالم  
رفشم فلمك صاخلا

---



ىل ع) RSA نم ةدروت سملا PKCS#12 ي ةدوجوملا حيتافملا نوكت نأ بجي :ريذحت  
ECC سېل ،(RSA 2048 عونلا :لا ثمل لېبس

<#root>

cat9k#

**copy sftp bootflash: vrf Mgmt-vrf**

Address or name of remote host [10.225.253.247]?  
Source username [svs-user]?  
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx  
Destination filename [cat9k-25jun17.pfx]?  
Password:  
!  
2960 bytes copied in 3.022 secs (979 bytes/sec)

داريتسا رمالا مادختسا اب PKCS#12 فلم دروتسا 3. ةوطخلا

<#root>

cat9k#

**crypto pki import svc\_cat9k\_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx**

password C1sco.123

% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx

CRYPTO\_PKI: Imported PKCS12 file successfully.

cat9k#

cat9k#

**show crypto pki certificates svc\_cat9k\_25jun17**

#### Certificate

Status: Available

Certificate Serial Number (hex): 5860BF33A2033365

Certificate Usage: General Purpose

##### Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

##### Subject:

Name: cat9k.svs.lab

e=pkalkur@cisco.com

cn=cat9k.svs.lab

ou=svs

o=cisco

l=rtp

st=nc

c=us

##### Validity Date:

start date: 17:56:00 UTC Jun 17 2025

end date: 17:56:00 UTC Jun 17 2026

Associated Trustpoints: svc\_cat9k\_25jun17

#### CA Certificate

Status: Available

Certificate Serial Number (hex): 20CD7402C4DA37F5

Certificate Usage: General Purpose

##### Issuer:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

##### Subject:

cn=SVS LabCA

ou=SVS

o=Cisco

l=Raleigh

st=North Carolina

c=US

##### Validity Date:

start date: 17:05:00 UTC Apr 28 2025

end date: 17:05:00 UTC Apr 28 2035

Associated Trustpoints: svc\_cat9k\_25jun17 svc\_cat9k

Storage: nvram:SVSLabCA#37F5CA.cer

## TLS نېوكټ عم AAA & TACACS

(هجوم ل) لېم عمل TrustPoint نارق او، AAA تاعومجمو TACACS م داخ عاشن. 1. ؤوطخل

```
tacacs server sv_s_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint cli_s_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ sv_s_tls
server name sv_s_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

AAA بې لاساً نېوكټ 2. ؤوطخل

```
aaa authentication login default group sv_s_tls local enable
aaa authentication login console local enable
aaa authentication enable default group sv_s_tls enable
aaa authorization config-commands
aaa authorization exec default group sv_s_tls local if-authenticated
aaa authorization commands 1 default group sv_s_tls local if-authenticated
aaa authorization commands 15 default group sv_s_tls
aaa accounting exec default start-stop group sv_s_tls
aaa accounting commands 1 default start-stop group sv_s_tls
aaa accounting commands 15 default start-stop group sv_s_tls
aaa session-id common
```

## ققحت ل

نېوكټ ل نم ققحت ل.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

TACACS+ و (AAA) ةبساحم ل او ضي وف ت ل او ةق د اص م ل اء اط خ اء ح ص ت

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure
```

! Below debugs will be needed only if there is any issue with SSL Handshake

```
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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 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