

IOS زاهج ىلع TLS 1.3 ربع TACACS+ نيوكت XE مادختساپ ISE

تاي وتحمل

[قىدقملا](#)

[قىماع قرطن](#)

[لييلدلا اذه مادختسا](#)

[قيس اس الاتاب طتملا](#)

[تاب طتملا](#)

[قىمدىخس ملابات نوكملما](#)

[صىيخرتلا](#)

[قىزچىلا قرادال 1- عزجل](#)

[مدادخ ئوق داصمل ئاداھش لىا عىقوقت بىل طعاش نا TACACS+](#)

[مدادخ ئوق داصمل رذچ لىا قدص ملابات عىرملابا ئاداھش لىيمەت TACACS+](#)

[ISE ب \(CSR\) عقۇمۇلا ئاداھش لىا عىقوقت بىل طېپر](#)

[نېيكەت TLS 1.3](#)

[ISE ىلەع قىزچىلا قرادانىكەت](#)

[نېيكەت TACACS ربۇغ TLS](#)

[فەكىش لىا قىزچىلار ئەتكىش لىا قىزچىلات اۋامەجم عاش نا](#)

[رجاتم ConfigureIdentity](#)

[TACACS+ فيرىعت تافارىم نېوكت](#)

[IOS XE RW - لوقۇس ملابا فيرىعت فارم](#)

[IOS XE RO - لغۇش ملابا فيرىعت فارم](#)

[رماؤت اۋامەجم configureTACACS+](#)

[Cisco IOS XE RW - لوقۇس ملابا رماؤت اۋامەجم](#)

[Cisco IOS XE RO - لغۇش ملابا رماؤت اۋامەجم](#)

[زاهجلا لوقۇس ملابا اۋامەجم نېوكت](#)

[Cisco IOS XE J TACACS+ ربۇغ Cisco IOS XE نېوكت - 2 عزجل](#)

[زاهجلا ۋەتس اوب مۇاشنامەت حىيت افم جوز - 1 نېوكتلىبا بولسا](#)

[مدادخ نېوكت TACACS+](#)

[نېوكت TrustPoint](#)

[TACACS & AAA عەم TLS](#)

[ۋەتس اوب مۇاشنامەت حىيت افم جوز - 2 نېوكتلىبا بولسا CA](#)

[TACACS & AAA عەم TLS](#)

[قىقحتلى](#)

قىدقملا

مدادخ لالاڭىم دنتسىملا اذه فصىي TLS ربع TACACS+ مع Cisco Identity Services Engine (ISE) زاهج و Cisco IOS® XE لىيەمەك.

ةماع ةرظن

ةيفرطلا ةطحملالا ىلإ لوصولالا مكحـت ةـدـحـوـىـلـا لـوـخـدـلـا ةـبـقـارـمـ مـاظـنـ لـوـكـوتـورـبـ حـيـتـيـ ةـكـبـشـلـاـ ىـلـاـ لـوـصـوـلـاـ مـداـوـخـوـ تـاهـجـوـمـلـلـ زـاهـجـلـلـ ةـيـزـكـرـمـلـاـ ةـرـادـإـلـاـ ةـيـنـاـكـمـاـ [TACACS+] [RFC8907] تـامـدـخـ رـفـوـيـ وـهـوـ رـثـكـأـ وـأـ دـحـاوـ TACACS+ مـدـاخـلـاـلـخـ نـمـ ةـكـبـشـلـابـ ةـلـصـتـمـلـاـ ةـزـهـجـأـلـاـ وـأـ ةـزـهـجـأـلـاـ ةـرـادـإـ مـادـخـتـسـاـ تـالـاحـلـاـ اـصـيـصـخـ ةـمـمـصـمـلـاـ ،ـ ةـبـسـاحـمـلـاـوـضـيـوـفـتـلـاـوـقـدـاصـمـلـاـ.

لـقـنـ ةـقـبـطـ لـاـلـخـ نـمـ لـوـكـوتـورـبـلـاـ نـيـسـحـتـ ىـلـعـ [TLS 1.3 [RFC8446] TACACS+] ربـعـ لـمـعـيـ ةـهـاـزـنـلـاـوـ ةـيـرـسـلـاـ لـمـاـكـتـلـاـ اـذـهـ نـمـضـيـ .ـ ةـيـسـاسـحـلـاـ ةـدـيـدـشـ تـانـاـيـبـلـاـ ةـيـاـمـحـ ىـلـعـ لـمـعـيـ اـمـمـ ،ـ ةـنـمـآـ مـداـوـخـلـاـوـ تـامـدـخـتـسـاـ تـالـاحـلـاـ اـصـيـصـخـ ةـمـمـصـمـلـاـ ،ـ ةـبـسـاحـمـلـاـوـضـيـوـفـتـلـاـوـقـدـاصـمـلـاـ.

ليـلـدـلـاـ اـذـهـ مـادـخـتـسـاـ

ةـكـبـشـلـاـ ةـزـهـجـأـلـ يـرـادـإـلـاـ لـوـصـوـلـاـ ةـرـادـإـ نـمـ ISEـ نـيـكـمـتـلـ نـيـئـزـجـ ىـلـاـ ةـطـشـنـأـلـاـ لـيـلـدـلـاـ اـذـهـ مـسـقـيـ Cisco IOS XEـ.

- زـاهـجـلـاـ لـوـفـسـمـلـ ISEـ نـيـوـكـتـ - 1ـ عـزـجـلـاـ
- Cisco IOS XEـ لـ TACACS+ـ ربـعـ نـيـوـكـتـ - 2ـ عـزـجـلـاـ

ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ

تابـلـطـتـمـلـاـ

تابـلـطـتـمـلـاـ تـامـدـخـتـسـمـلـاـ نـيـوـكـتـ TLSـ ربـعـ:

- عـيـقـوـتـلـ TLSـ ربـعـ لـ بـقـ نـمـ ةـمـدـخـتـسـمـلـاـ ةـدـاهـشـلـاـ عـيـقـوـتـلـ (CA)ـ قـدـصـمـ عـجـرمـ ةـكـبـشـلـاـ ةـزـهـجـأـلـ ISEـ تـادـاهـشـ.
- ةـدـاهـشـلـاـ حـنـمـ ةـهـجـ نـمـ رـذـجـلـاـ ةـدـاهـشـلـاـ (CA).

- ءـامـسـأـ لـحـ اـهـنـكـمـيـوـ DNSـ ىـلـاـ لـوـصـوـلـاـ ةـيـنـاـكـمـاـ ىـلـعـ ISEـ وـ ةـكـبـشـلـاـ ةـزـهـجـأـ يـوـتـحـتـ فـيـضـمـلـاـ.

ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ

ةـيـلـاتـلـاـ ةـيـدـامـلـاـ تـانـوـكـمـلـاـوـجـمـاـرـبـلـاـ تـارـادـصـاـ ىـلـاـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـراـوـلـاـ تـامـوـلـعـمـلـاـ دـنـتـسـتـ:

- رـادـصـإـلـاـ 3.4 Patch 2ـ ISE VMwareـ يـرـهـاظـلـاـ زـاهـجـلـاـ
- رـادـصـإـلـاـ 17.15+ـ Cisco IOS XEـ جـمـانـرـبـ

ةـصـاخـ ةـيـلـمـعـمـ ةـيـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ عـاـشـنـاـ مـتـ تـنـاكـ اـذـاـ .ـ (ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـ لـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ

صـيـخـرـتـلـاـ

يـفـ .ـ ةـسـايـسـلـاـ ةـمـدـخـ ةـدـقـعـ ىـلـعـ TACACS+ـ تـامـدـخـ مـادـخـتـسـابـ ةـزـهـجـأـلـاـ ةـرـادـإـ صـيـخـرـتـ كـلـ حـمـسـيـ تـامـدـخـ مـادـخـتـسـابـ ةـزـهـجـأـلـاـ ةـرـادـإـ صـيـخـرـتـ كـلـ حـمـسـيـ ،ـ رـفـوـتـلـاـ ةـيـلـاعـ (HA)ـ ةـلـقـتـسـمـ رـشـنـ ةـيـلـمـعـ

TACACS+ حوز يف ڏدحاو ڦس اي س ڦم دخ ڏدقع ىلع HA.

ڙهڙ جا ڦرادايل ISE نيوكت - 1 ڦنجل

ڦداخ ڦق دا ص مل ڦداهش لـا عي قوت بل ط ٽاشنـا TACACS+

ڦم وع دملـا تا ضرعت سـمـلـا دـحـا مـادـخـتـسـابـ بـيـولـاـ ىـلـعـ ISEـ ڦـراـدـاـ ڦـبـاـوبـ ىـلـاـ لـوـخـدـلـاـ لـجـسـ 1ـ ڦـوـطـخـلـاـ.

ىـلـوـأـلـاـ ڦـوـطـخـلـاـ لـلـثـمـتـتـ .ـ تـاـمـدـخـلـاـ عـيـمـجـلـ اـيـتـاـذـ ڦـعـقـوـمـ ڦـداـهـشـ ISEـ ڦـدـخـتـسـيـ ،ـ ڦـضـاـرـتـفـاـ لـكـشـبـ وـ ڦـدـصـمـلـاـ عـجـرـمـلـاـ لـبـقـ نـمـ ڦـعـيـقـوـتـلـ (CSRـ)ـ ڦـداـهـشـ عـيـقـوـتـ بلـطـ ٽـاشـنـاـ ـيـفـ.

ـ تـاـدـاـهـشـ لـاـ >ـ ڦـرـادـاـلـاـ ىـلـاـ لـقـتـنـاـ 2ـ ڦـوـطـخـلـاـ.



Administration



System

Identity Management



Deployment

Identities



Licensing

Groups



Certificates

External Identity Sources



Logging

Identity Source Sequence



Maintenance

Settings



Upgrade & Rollback

Feed Service



Health Checks

Profiler



Backup & Restore

Admin Access



Admin Access

Settings



Settings

ة. داهش لـ عيقوت بلط عاشنـا رقـنا ، داهـش لـ عيـقوـت تـابـلـط تـحـتـ 3ـةـ وـطـخـلـا.

Identity Services Engine Administration / System Evaluation Mode 28 Days

Bookmarks Deployment Licensing Certificates Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management System Certificates Admin Certificate Node Restart Trusted Certificates OCSP Client Profile

Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

مادختس الـ TACACS ددح 4. ۋە طخلى.

Usage

| | | |
|---------------------------------|--------------------------|---|
| Certificate(s) will be used for | TACACS | ▼ |
| Allow Wildcard Certificates | <input type="checkbox"/> |  |

نيكىم ت مەتىيىس يېتلا PSN تاكبىش ددح 5. ۋە طخلى.

Node(s)

Generate CSR's for these Nodes:

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

ۋە سانملا تامولۇملاپ عوضۇملا لوقىح ألمى. 6. ۋە طخلى.

Subject

Common Name (CN)

\$FQDN\$



Organizational Unit (OU)

CX



Organization (O)

Cisco



City (L)

Raleigh

State (ST)

North Carolina

Country (C)

US

لېدب مسا عوضوملا نمض IP ناونعو DNS مسا فضأ 7. ۋەتەخلى.

Subject Alternative Name (SAN)



DNS Name



ISE1.lab



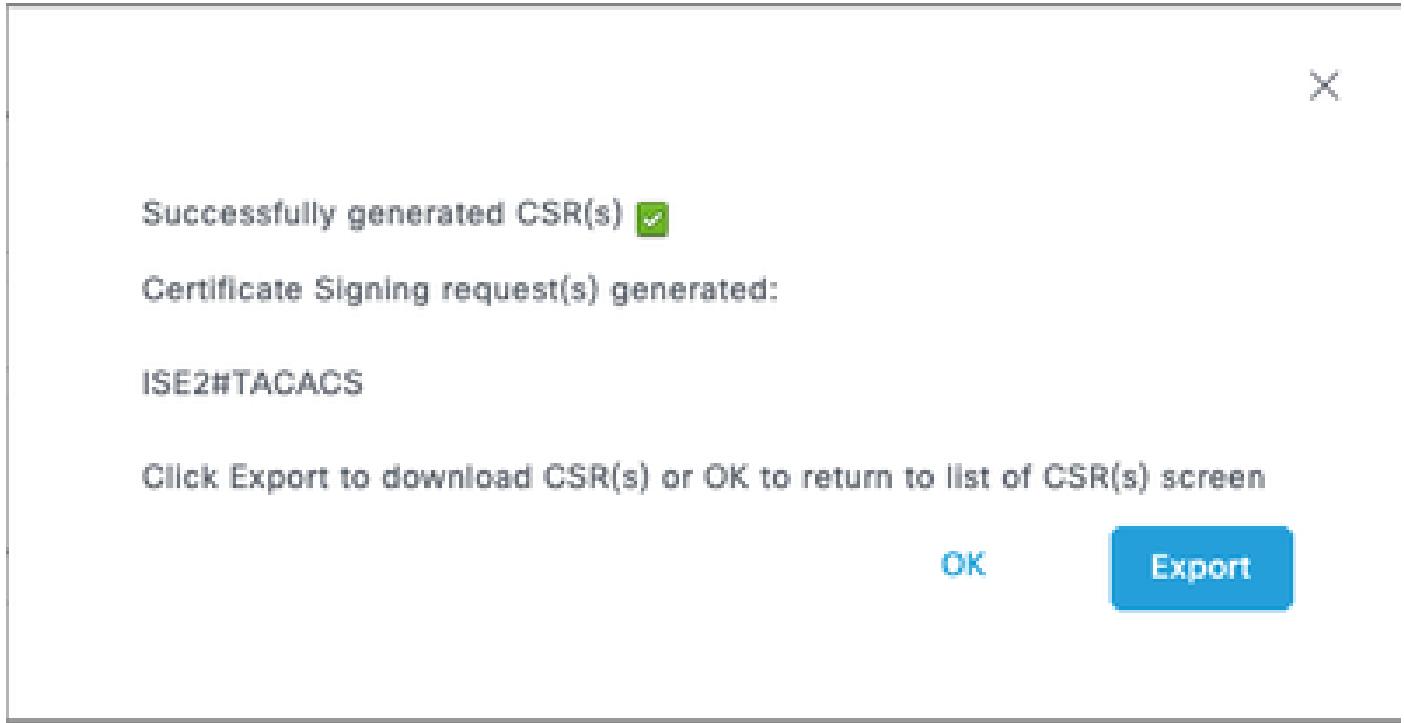
IP Address



10.225.253.209



رېدصىت مىڭ ئاشنە قوف رقنى 8. ۋەتەخلى.



صيخرتلا ةئيه نم ١عقوم (CRT) ١داهشلا ىلع لوصحلا كنكمي ،نآلـا

مداخ ١قـداصـمل رـذـجـلـا عـجـرـمـلـا ١ـدـاهـشـ لـيـمـحـتـ TACACS+

جارـدا رـقـنـا ،ـةـنـوـمـضـمـلـا صـيـخـارـتـلـا تـحـتـ .ـتـادـاهـشـلـا > مـاظـنـلـا لـقـتـنـا 1ـ. ١ـوـطـخـلـا

| 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 2025 | Ena |
| Cisco ECC Root CA 2099 | Cisco Services | 03 | Cisco ECC Root CA | Cisco ECC Root CA | Thu, 4 Apr 2013 | Mon, 7 Sep 2023 | Ena |
| Cisco Licensing Root CA | Cisco Services | 01 | Cisco Licensing R... | Cisco Licensing R... | Thu, 30 May 2013 | Sun, 30 May 2023 | Ena |
| Cisco Manufacturing CA SHA2 | Endpoints Infrastructure | 02 | Cisco Manufactur... | Cisco Root CA M2 | Mon, 12 Nov 2012 | Thu, 12 Nov 2022 | Ena |
| 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 2024 | 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 2026 | Ena |
| 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 2020 | Ena |
| Cisco Root CA M2 | Infrastructure Endpoints | 01 | Cisco Root CA M2 | Cisco Root CA M2 | Mon, 12 Nov 2012 | Thu, 12 Nov 2022 | Ena |
| Cisco RXC-R2 | Cisco Services | 01 | Cisco RXC-R2 | Cisco RXC-R2 | Wed, 9 Jul 2014 | Sun, 9 Jul 2034 | Ena |

١ـدـاهـشـ عـيـقوـتـ بـلـطـ عـقـوـيـذـلـا (CA) ١ـقـدـاصـمـلـا نـعـ ١ـرـادـاـصـلـا ١ـدـاهـشـلـا دـدـحـ .ـعـيـقوـتـ بـلـطـ عـقـوـيـذـلـا (CSR) ١ـلـخـادـ ١ـقـدـاصـمـلـابـ ١ـقـثـلـانـأـ نـمـ دـكـأـتـ .ـكـبـ صـاخـلـا TACACS (CSR) ١ـنـكـمـ رـايـخـلـا ISE

Import a new Certificate into the Certificate Store

* Certificate File [Examinar...](#) ISE SVSLab CA.crt

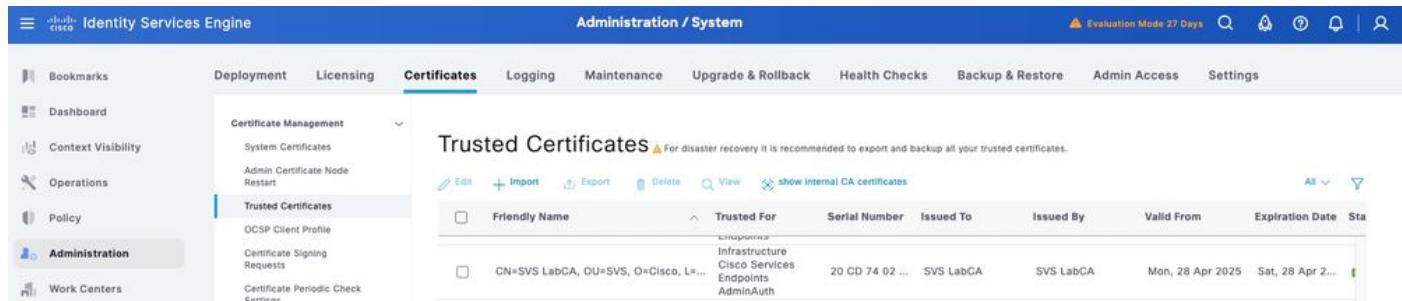
Friendly Name

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](#)

اھب قوچومل ا تاداهشل ا نممض نآل ا ۋەدەشل ا رەھەت نأ بجى .لاسرا قوف رقنا 3. ۋەطخىل.

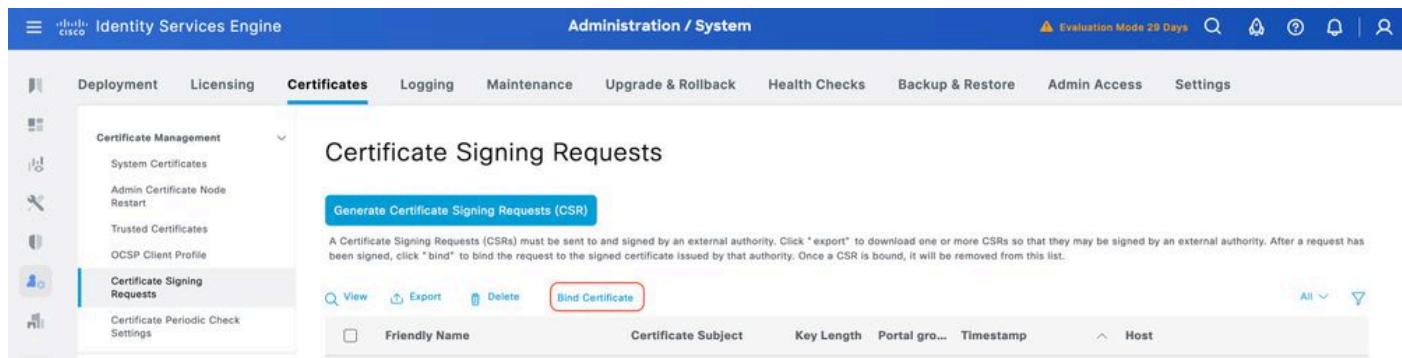


| Friendly Name | Trusted For | Serial Number | Issued To | Issued By | Valid From | Expiration Date | Sta |
|---|--|-----------------|-----------|-----------|------------------|------------------|--------|
| CN=SVS LabCA, OU=SVS, O=Cisco, L=, C=US | Infrastructure, Cisco Services, Endpoints, AdminAuth | 20 CD 74 02 ... | SVS LabCA | SVS LabCA | Mon, 28 Apr 2025 | Sat, 28 Apr 2025 | Active |

ISE ب (CSR) عوقومل ا ۋەدەشل ا عيقوت بلط طبر

اىلۇع ۋەعوقومل ا ۋەدەشل ا تىبىتت كىنكمى ، (CSR) ۋەدەشل ا عيقوت بلط عيقوت درجمب.

دەح ، ۋەدەشل ا عيقوت تابلىق تەخت .تاداهشل ا > ماظنل ا > ۋەرادىل ا > ماظنل ا > ۋەردىل ا > 1. ۋەطخىل TACACS ۋەدەشل ا طبر قوف رقنا او ۋەقاباسل ا ۋەطخىل ا يىف ھواشنى مەت يىذل ا CSR.



| Friendly Name | Certificate Subject | Key Length | Portal gro... | Timestamp | Host |
|---|---|------------|---------------|----------------------|-----------|
| CN=SVS LabCA, OU=SVS, O=Cisco, L=, C=US | CN=SVS LabCA, OU=SVS, O=Cisco, L=, C=US | 2048 | Default | 2025-04-28T14:00:00Z | SVS LabCA |

مادختىسىلا تەخت ۋەعوقومل ا TACACS رايىتىخالا ۋەناخ نأ نم دكأت و ۋەعوقومل ا ۋەدەشل ا دەح .2. ۋەطخىل ۋەدەم لۆتسىس.

Identity Services Engine Administration / System Evaluation Mode 20 Days

Deployment Licensing Certificates Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests**
- Certificate Periodic Check Settings
- Certificate Authority

Bind CA Signed Certificate

* Certificate File: Examiner...

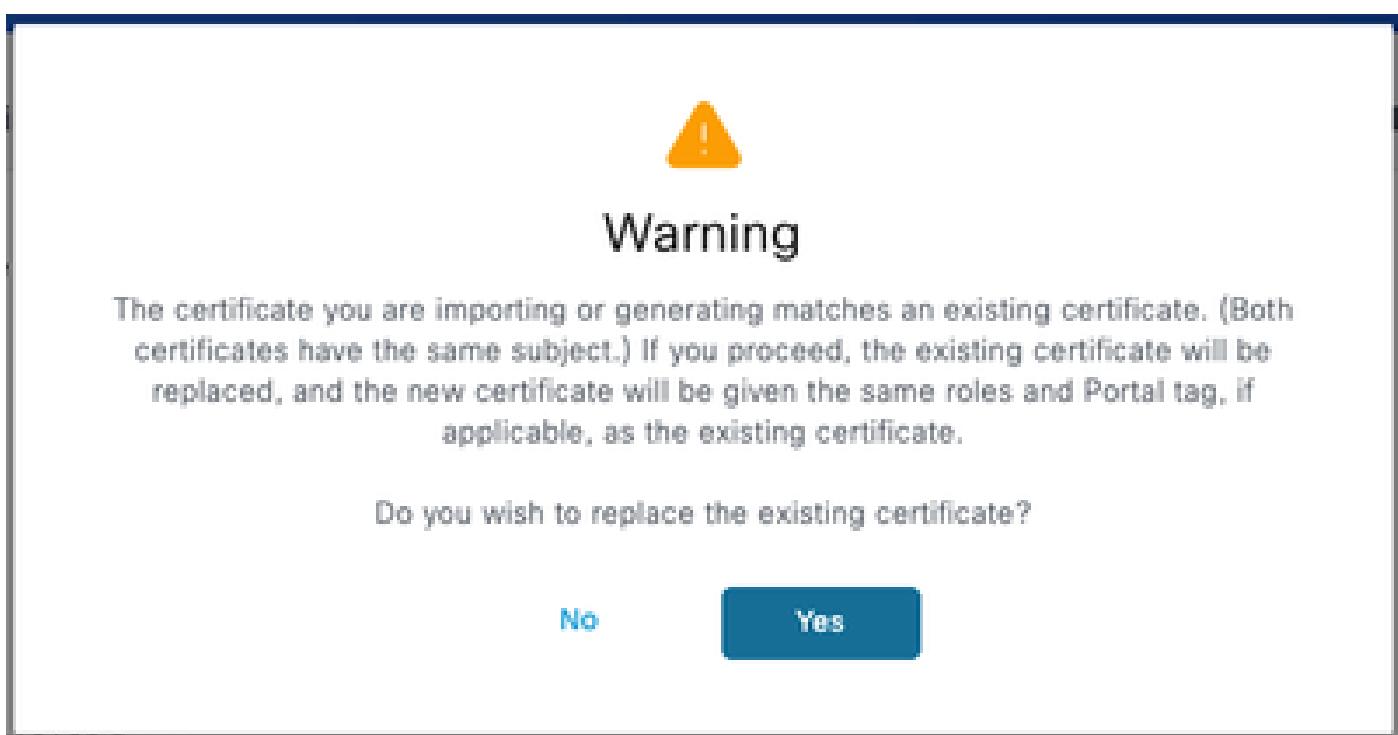
Friendly Name:

Validate Certificate Extensions:

Usage: TACACS: Use certificate for TACACS Server

Submit Cancel

معن قوف رقنا، ڈوجوملا ڈاہشل ادبتسا لوح اریذحت تیقلت اذا. لاسرا قوف رقنا 3. ڈوٹخلا عباتملل.



Identity Services Engine Administration / System Evaluation Mode 20 Days

Deployment Licensing Certificates Logging Maintenance Upgrade & Rollback Health Checks Backup & Restore Admin Access Settings

Certificate Management

- System Certificates**
- Admin Certificate Node Restart
- Trusted Certificates
- OCSP Client Profile
- Certificate Signing Requests
- Certificate Periodic Check Settings
- Certificate Authority

System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

| Friendly Name | Used By | Portal group tag | Issued To | Issued By | Valid From | Expiration Date | Status |
|---------------|---------|------------------|---|-----------|------------------|------------------|-------------------------------------|
| ISE1 | | | ISE1.lab | ISE1.lab | Wed, 10 Sep 2025 | Fri, 10 Sep 2027 | <input checked="" type="checkbox"/> |
| | | | C=US, ST=NC, L=Raleigh, O=Cisco, OU=SVS, CN=ISE1.lab!ISE1.lab!00010 | | | | Active |

TLS 1.3 نیکمٹ

ايوهدي اهنيلكمت بجي TLS 1.3 نيكمنت متي ال ISE 3.4.x.

تادادع إلأ > ةرادالا إلأ لقتنا 1. ووطخل.

cisco 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 ✓

مث ، رادصا تادادع| نممض TLS1.3 راوجب رايتحالا ئناخ ددحو ،نامألا تادادع| قوف رقنا.2. ئوطخل ظفح قوف رقنا.

Client Provisioning

FIPS Mode

Security Settings

Alarm Settings

General MDM / UEM Settings

Posture >

Profiling

Protocols

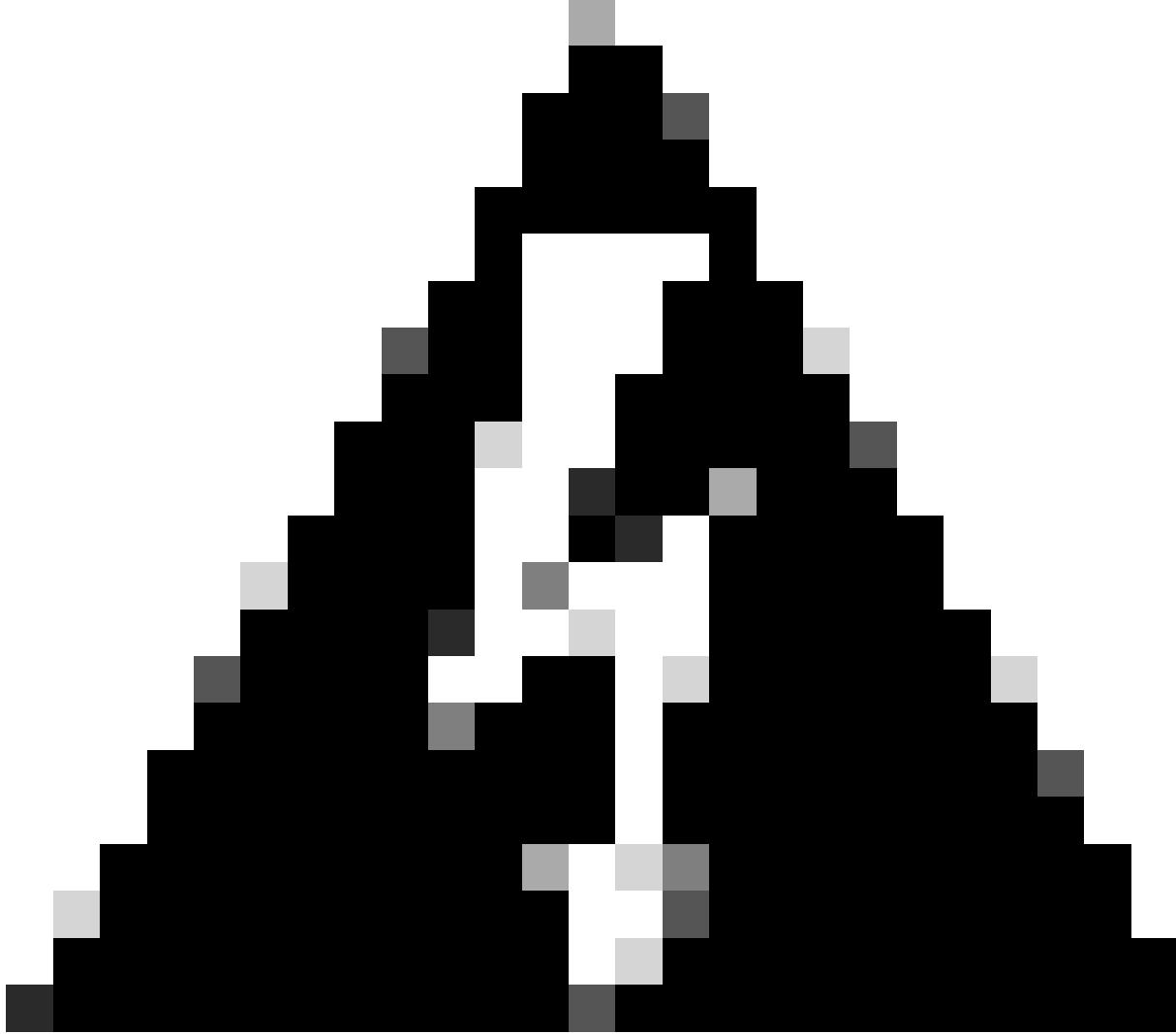
Security Settings

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 ⓘ

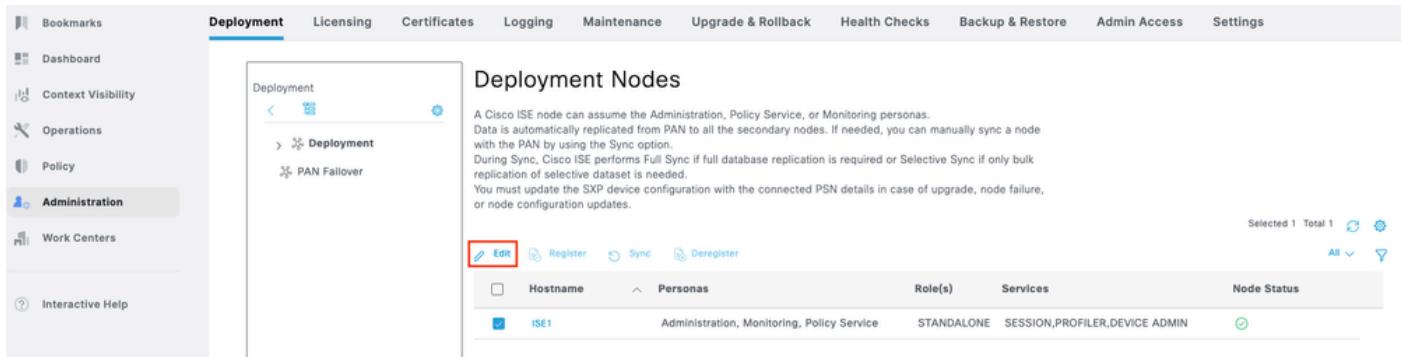


عيمج ىلע Cisco ISE قيي بطت مداخ ليغشت ئداع| مدت ، رادصا رىيغت دنع :ريذحت Cisco ISE. رشنللا ئزهجأ.

ىلع ۆزهجألا ۆرادا نیکمەت ISE

نیکمەت مق ISE ۆدقع ىلع يضارتفا لکشپ (TACACS+) ۆزهجألا ۆرمدەخ نیکمەت مەتىي ال TACACS+ ۆدقع ىلع PSN.

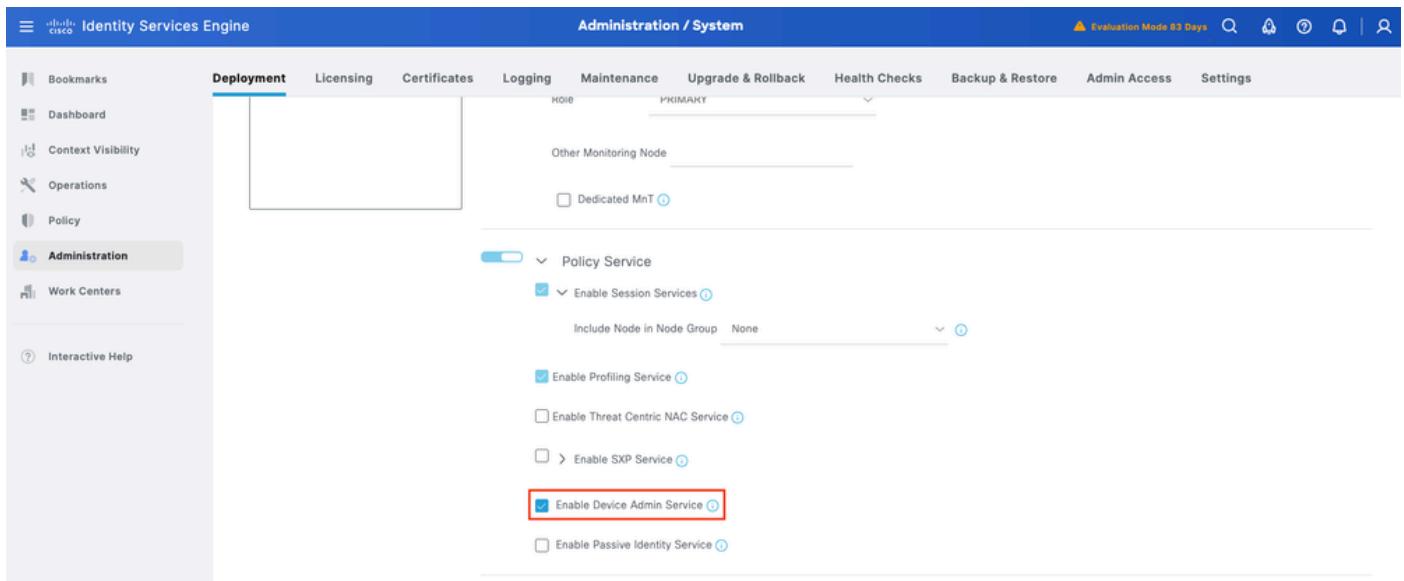
رقن او ISE ۆدقع ۆرەجەلە رايىت خالا ۆناخ دەح. رشنلە > ماظنلە > ۆرادا لىلىقتنى. 1. ۆوطخىلارىحەت قوف.



The screenshot shows the 'Deployment Nodes' section of the Cisco ISE interface. It displays a table with one node entry: 'ISE1'. The node details are as follows:

| Hostname | Personas | Role(s) | Services | Node Status |
|----------|----------|--|--|-------------|
| ISE1 | | Administration, Monitoring, Policy Service | STANDALONE SESSION,PROFILER,DEVICE ADMIN | OK |

نیکمەت ل ۆرەجەلە رايىت خالا ۆناخ دەح و لفس اىلى رىرمەتلىپ مق، ىلەن تەختىتى. 2. ۆوطخىلارىحەت قوف.



The screenshot shows the 'Administration / System' configuration page. Under the 'Policy Service' section, the 'Enable Device Admin Service' checkbox is checked and highlighted with a red box.

ىلع نآللا "زاهىللا لەۋەسىم ۆرمدەخ" نیکمەت مەت. نیوكتىلا ظەفحىا. 3. ۆوطخىلارىحەت قوف.

رابع TLS نیکمەت TACACS

ۆماع ۆرەظن > ۆزهجألا ۆرادا > لەمعلە زكارم لىلىقتنى. 1. ۆوطخىلارىحەت قوف.

The screenshot shows the Cisco Identity Services Engine (ISE) interface under the 'Work Centers / Device Administration' section. On the left, there's a navigation sidebar with links like Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Help. The main content area is titled 'Device Administration Overview'. It features a '1. Prepare' section for 'Authorization Roles' and a '2. Define' section for 'Configure Devices'. A '3. Go Live & Monitor' section includes 'Real-time Monitoring' and 'Auditing' sub-sections. The 'Configure Devices' section has a dropdown menu for 'Device Administration' with 'Overview' selected.

رابع ددح TACACS نيكمت ديرت ثيچ PSN رشنلا قوف رقنا.2. ۋەطخا

The screenshot shows the 'Device Administration Deployment' page in the Cisco ISE interface. Under the 'Deployment' tab, it lists 'ISE Nodes' (ISE1.lab and ISE2.lab) and sets up 'TACACS Ports' (Port 49) and 'TACACS Over TLS Port' (Port 6049).

رابع TCP ذفنم ددح وأ 6049 يضارتفالا ذفنملاب ظفتحا.3. ۋەطخا ظفح قوف رقنا مىث.

ۋەتكىشلار ئۆزىجىڭىز ئۆتكىشلار ئۆزىجىڭىز ئاشنى

لەك لىثمىي. ئۆزىجىڭىز ئاتاومىجىل ئەددۇتىم ئۆيمىرە تالىسىلىنىڭ ئۆزىجىڭىز اىچىمىجىت ISE رفويي. ئۆتكىشلار ئۆزىجىڭىز ئۆتكىشلار ئۆزىجىڭىز ئاشنى.

ئۆزىجىڭىز ئاتاومىجىم قوف رقنا. ئۆتكىشلار دراوم > زاھىجا ئۆرەن > لەمعەلە زەكارەم ئىلى لەقتىنامىنى. 1. ۋەطخا ئۆتكىشلار iOS XE مەساب ئەپلەپ ئۆزىجىڭىز ئاشنى.

cisco Identity Services Engine

Work Centers / Device Administration

Add Group

Name*
IOSXE

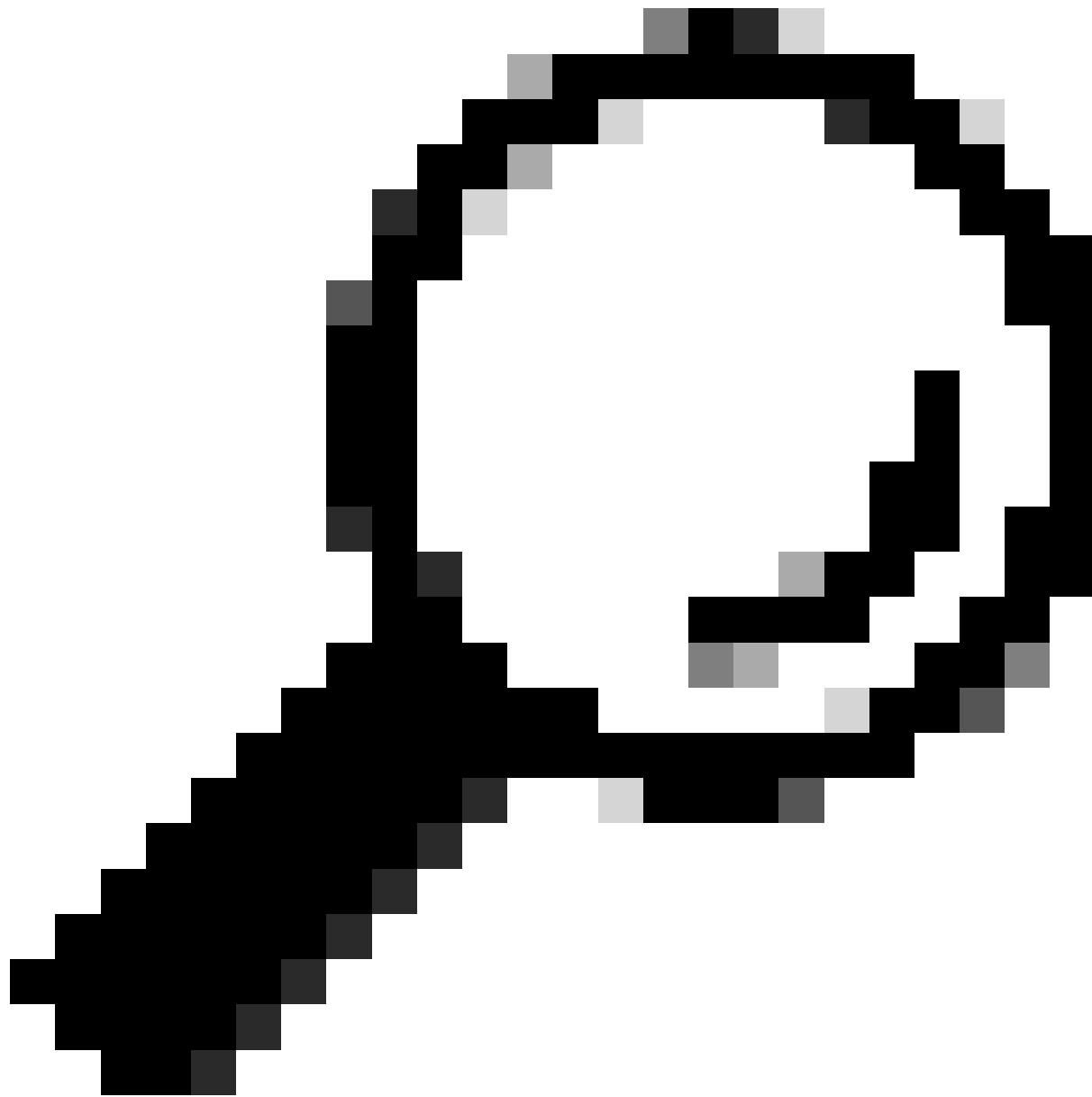
Description

Parent Group*
Select Group or Add as root group

Cancel Save

IOSXR

The screenshot shows a modal dialog titled "Add Group" from the Cisco Identity Services Engine. The "Name" field is populated with "IOSXE". The "Description" field is empty. The "Parent Group" dropdown menu is open, showing the option "Select Group or Add as root group". At the bottom right of the dialog are "Cancel" and "Save" buttons. The background of the dialog shows the "Network Device Groups" section of the interface, which includes icons for Network Devices, Network Device Groups, Default Devices, TACACS External Servers, and TACACS Server Sequence. The "Network Device Groups" item is currently selected. The overall interface has a dark theme with blue highlights for selected items.



متي ئيضا تالسلست عقاوملا ئفاك و ئزهجانا عاونا عيمج دعت : حيملىت
فيروعتوكب ئصالخلا ئيمرهلا تاجردىلا ئفاضا كنكمي ISE. ئطساوب اهريفيوت
ئلاح يف اقحال ھمادختسإ نكمي يذلا ئكبشلا زاهج فيروعت يف ئفلت خملاتانوكملا
ئس ايسلما

> زاهجلارادا > لمعلا زكارم ىلارقتنا. ئكبش زاهج فضأ ،نآل 2. ئوطخلارابتخالا اذهل .ديدج ئكبش زاهج ئفاضال ئفاضا ىلعرقنا. ئكبشلا ئزهجانا > ئكبشلا دراوم SVS_BRPASR1K.

Identity Services Engine Work Centers / Device Administration

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

Network Devices List > SVS_BRPASR1K

Network Devices

| | |
|----------------------|----------------------------|
| Name | SVS_BRPASR1K |
| Description | |
| IP Address | * IP : 10.225.253.180 / 32 |
| Device Profile | Cisco |
| Model Name | |
| Software Version | |
| Network Device Group | |
| Location | All Locations |

Set To Default

مق، اريخأ. زاهج لـ (IOS XE) زاهج لـ عون و عقولا نيعت نم دكأت و زاهج لـ IP ناونع لـ خـ 3. ـ و طـ خـ لـ تـ اـ دـ اـ دـ اـ عـ رـ بـ نـ يـ كـ مـ تـ بـ TACACS+.

Identity Services Engine Work Centers / Device Administration

Evaluation Mode 67 Days

- Bookmarks
- Dashboard
- Context Visibility
- Operations
- Policy
- Administration
- Work Centers**
- Interactive Help

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)*

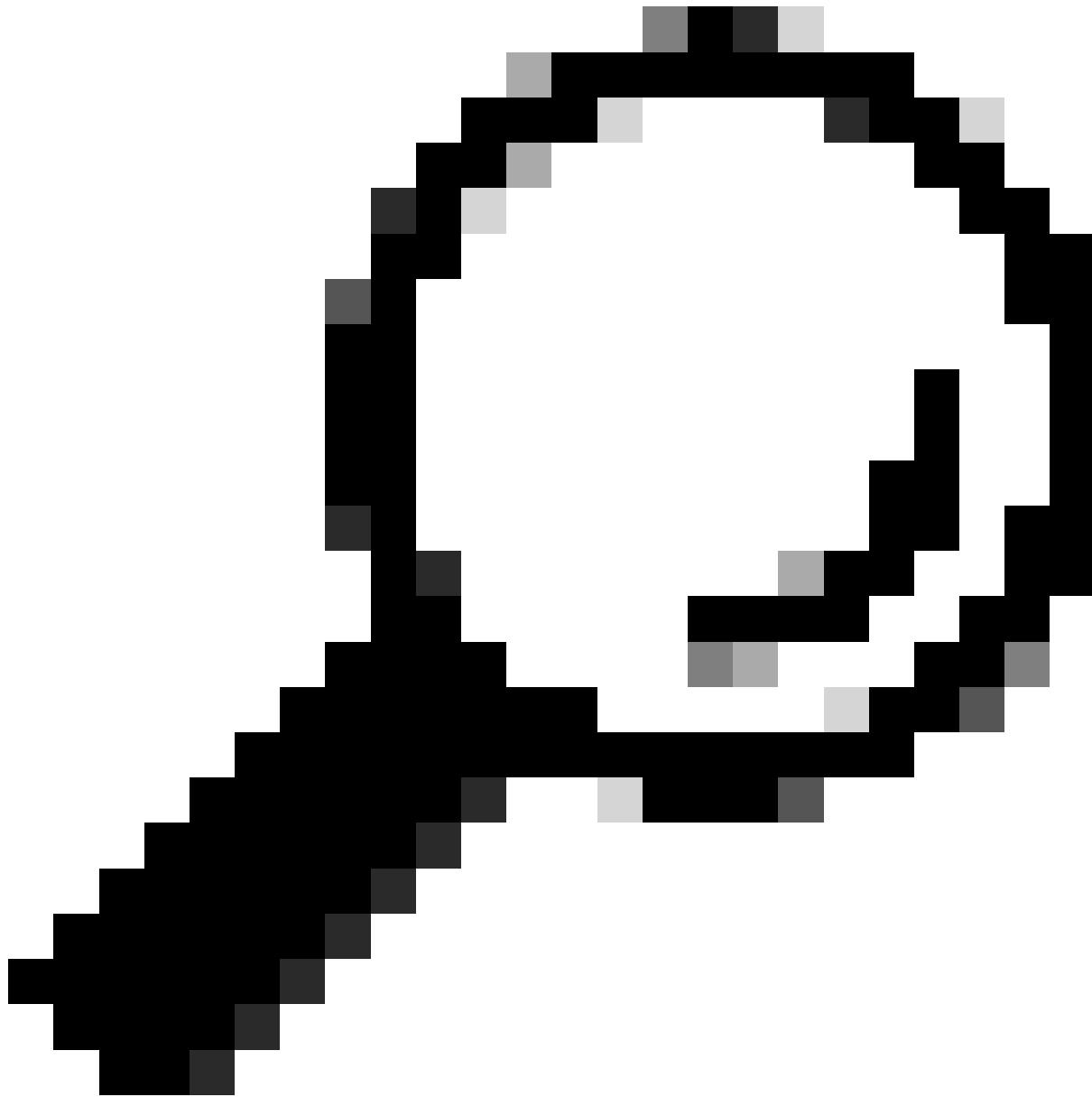
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When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



لەم ئەسلىج لىيغشت ئەداعا بىنچتلى دىفەرمانلا لاصىتالا عضۇنىكىمتب ئىصوئى :حېيملىت
زاهىجا ئىلإ اهىف رەمأ لاسرا مەتى ئەرم لىك يەف TCP.

رجاتم ConfigureIdentity

نېيىلخادىلا ISE يىمدىختىسىم نوکىي نأ نكەمىي يىذلار، ئەزەجألا يىلۋۇسىملى ئېيۇھ نىزخە مىسىقىلا اذە دەھىي
يىجراخ ئېيۇھ رەدصىم، Active Directory (AD)، مەدىختىسىي انە . ئەمۇعدم ئېيىجراخ ئېيۇھ رەداصىم يىأو

رقنالا > ئېيىجراخلا ئېيەھلە نىزاخىم > ئەرادىدا > ئەرادىلا ئىلإ لىقتىنا. 1. ئەوطخلە
ئەدىدەج ئەكىرتىشىم AD ئەطقۇن دىدەختلى ئەفاضا قوف.

Identity Services Engine Administration / identity Management Evaluation Mode 70 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources

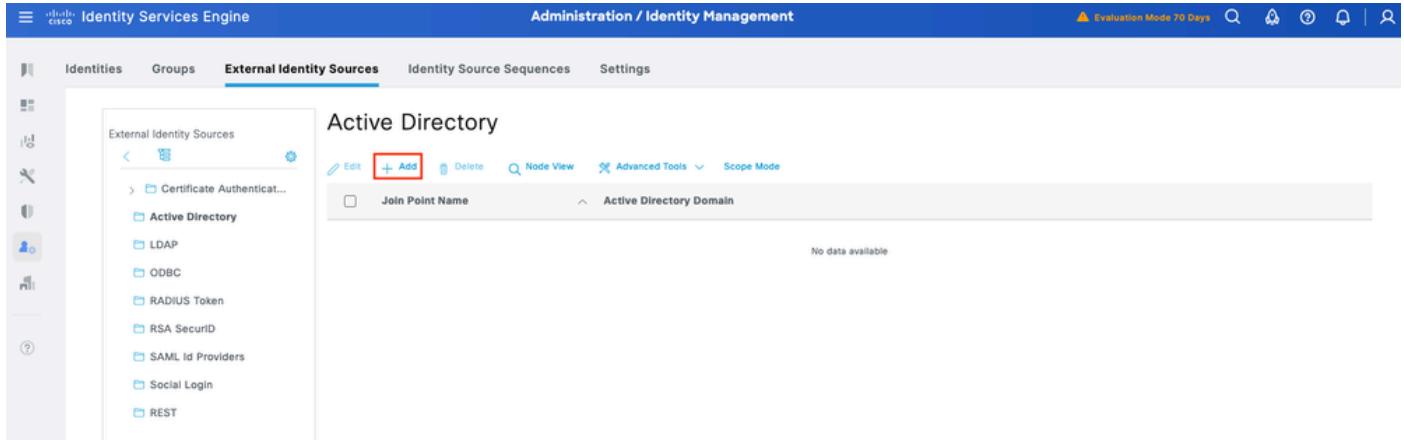
- Certificate Authentication
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

Active Directory

Edit **Add** Delete Node View Advanced Tools Scope Mode

Join Point Name Active Directory Domain

No data available



ل اسرا رقنا او AD لاجم مس او طبرلا ةطقن مسا ددح . 2. ۋوطخلار

Identity Services Engine Work Centers / Device Administration Evaluation Mode 29 Days

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

External Identity Sources

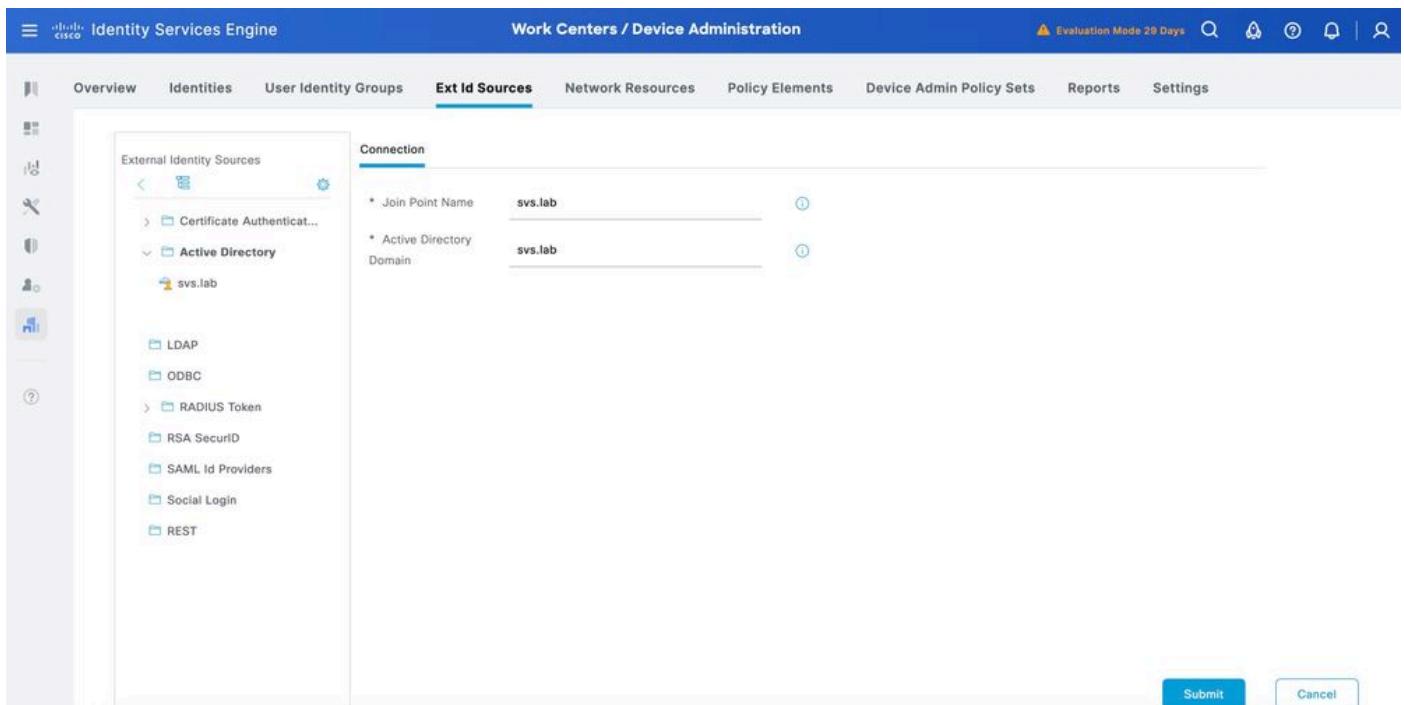
- Certificate Authentication
- Active Directory
 - svs.lab
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

Connection

* Join Point Name: svs.lab

* Active Directory Domain: svs.lab

Submit Cancel



ل اجمنىل ا ISE دقعنىم يىف بغرت لە ئېلەطىلدا دىنۇ معن قوف رقنا . 3. ۋوطخلار ئاده ؟

Silabs Cisco Identity Services Engine Administration / Identity Management Evaluation Mode 70 Days

Identities Groups External Identity Sources Identity Source: tmo.svs

External Identity Sources Connection Allowed Domains

* Join Point Name: tmo.svs
* Active Directory Domain: tmo.svs

Information Would you like to Join all ISE Nodes to this Active Directory Domain?

No Yes

+ Join + Leave Test User Diagnostic Tool Refresh Table

| ISE Node | ISE Node R... | Status | Domain Controller | Site |
|------------------|---------------|------------|-------------------|------|
| ISE2.tmo.svs.com | STANDALONE | Not Joined | | |

Save Reset

وًلأجلـا نـم قـقـحـتـ .ـىـلـاـ ISEـ مـضـنـ اوـ ADـ تـازـيـتـمـاـبـ دـامـتـعـاـلـاـ تـانـاـيـبـ لـخـاـدـأـ .ـ4ـ وـطـخـلـاـ
لـمـعـتـ اـهـنـأـ نـم قـقـحـتـلـلـ.

X

Join Domain

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

* AD User Name

* Password

Specify Organizational Unit

Store Credentials

Cancel OK

Join Operation Status

Status Summary: Successful.

ISE Node

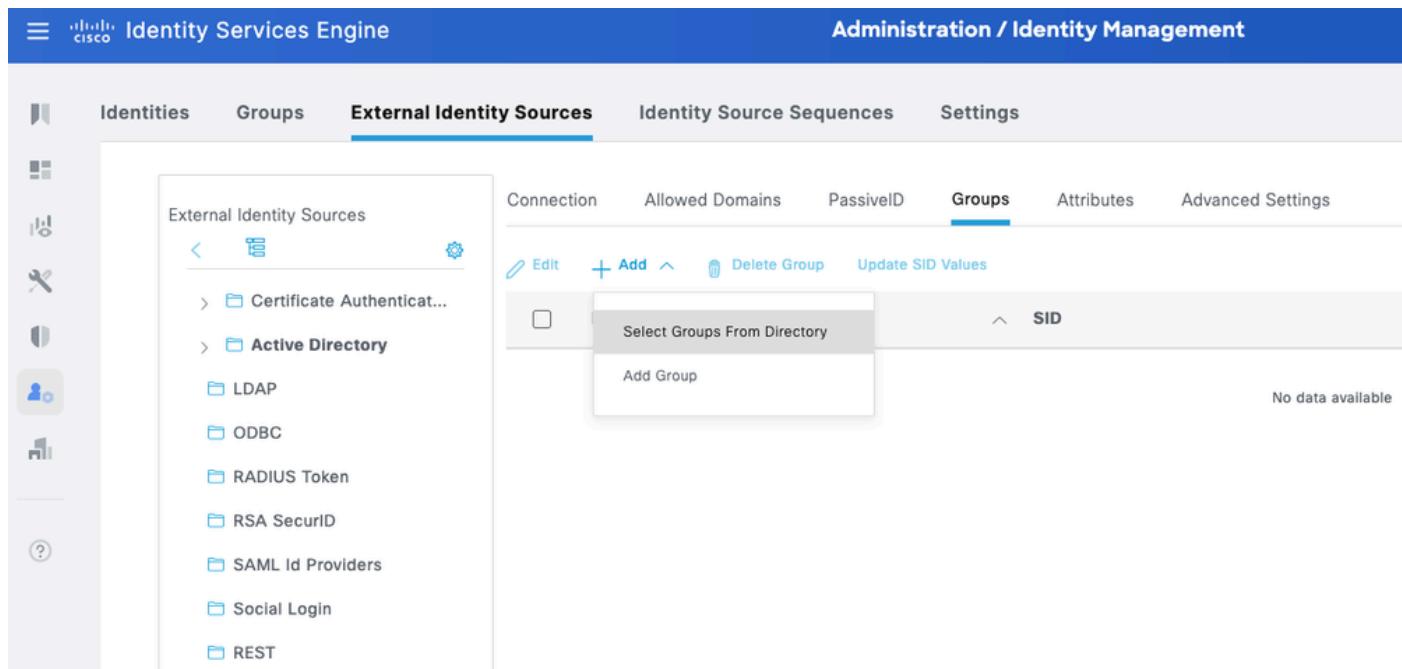
Node Status

ISE1.lab

Completed.

[Close](#)

عيمج ىلع لوصحلل ةفاضا قوف رقناو ،تاعومجم بيوبتل ا ئممالع ىلا لقتنا .5. ۋوطخلما
اده حضوي .زاهجلا ىلا لوصولل نيلوخم نيمدختسملا نم يأ ىلا ادانتسا ئبولطملا تاعومجم ملا
لىلدلا ادھ يف ليوختلا جھن يف ئمددختسملا تاعومجم ملا لاثم ملا

The screenshot shows the Cisco Identity Services Engine (ISE) Administration / Identity Management interface. The top navigation bar includes 'Administration / Identity Management' and tabs for 'Identities', 'Groups', 'External Identity Sources' (which is selected), 'Identity Source Sequences', and 'Settings'.

On the left, a sidebar lists various identity sources: Certificate Authentication, Active Directory, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, Social Login, and REST. Active Directory is currently selected.

The main panel displays the 'Groups' tab under 'External Identity Sources'. It has columns for 'Connection', 'Allowed Domains', 'PassiveID', 'Groups' (which is selected), 'Attributes', and 'Advanced Settings'. A sub-menu for 'Groups' is open, showing options 'Select Groups From Directory' and 'Add Group'. The status message 'No data available' is visible at the bottom right of this panel.

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain svs.lab

| Name Filter | Device * | SID Filter | Type Filter | ALL |
|---|--|------------|-------------|------------|
| <button>Retrieve Groups...</button> 2 Groups Retrieved. | | | | |
| <input type="checkbox"/> Name | Group SID | | | Group Type |
| <input type="checkbox"/> svs.lab/Users/Device Admin | S-1-5-21-4125682916-2670386087-26956193... | | | GLOBAL |
| <input type="checkbox"/> svs.lab/Users/Device RO | S-1-5-21-4125682916-2670386087-26956193... | | | GLOBAL |

Identity Services Engine Administration / Identity Management

Evaluation Mode 70 Days

Identities Groups External Identity Sources Identity Source Sequences Settings

External Identity Sources

- Certificate Authentication
- Active Directory
- LDAP
- ODBC
- RADIUS Token
- RSA SecurID
- SAML Id Providers
- Social Login
- REST

Connection Allowed Domains PassiveID Groups Attributes Advanced Settings

Edit Add Delete Group Update SID Values

| <input type="checkbox"/> Name | SID |
|---|--|
| <input type="checkbox"/> svs.lab/Users/Device Admin | S-1-5-21-4125682916-2670386087-2695619305... |
| <input type="checkbox"/> svs.lab/Users/Device RO | S-1-5-21-4125682916-2670386087-2695619305... |

Save Reset

فیرعت تافلم نیوکت TACACS+

ۆزهجأ ىلع نییسیئر نیم دختسەم نیرود ىلإ تاپەاد تەنأ Cisco IOS XE:

- راھجلا یف تازایتما رەڭلە رودلە وە اذە - (یرۇچىلا ماظنلىرى دەم) ىلە لەمەكلىا يېرادىلە لەوصولە قىچىب يېرۇچىلا ماظنلىلۇ ئۆفسەم رود بەحاص مەختىمىنىيەتىنەتكەنلىكما او ماظنلىلارما ئۆسۈچىمەج.
- ەئارقىللىلە لەوصولە نىچەتەنەم دختسەملە ىلە رودلە اذە فەدەي - لېغشتىلە لەماعاھالىسى او ئەپقەرمەلە ضارغۇلە ماظنلىلە طقىف.

IOS XE_RW و IOSXR_RO نەم نافىصوت تافىصوتلا ھەذە نىب ھەنأ ىلإ راشىو.

IOS XE_RW - فەلم فەرعت لەوصىمەلە

تافلم > جئاتنلا > ةسايسل رصانع > ةزهجلأا ةرادا > لمعل زكارم ىلإ لقتن 1 ةوطخلأا IOS XE_RW هتيمستب مقوا ديوج TACACS فيرعت.

15. ك زايتما يصقلأا دحلاو زايتما ريصقتلا تبنيعو تصحف. 2. ةوطخ

ظفحلاو نيوكتلا نم دكأت. 3. ةوطخلأا

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', 'Work Centers / Device Administration', and search/filter icons. The main menu bar has tabs: Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (which is currently selected), Device Admin Policy Sets, and More. On the left, there's a sidebar with icons for Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements (selected), Device Admin Policy Sets, and More. Below the sidebar, a tree view shows 'TACACS Profiles > IOSXE_RW'. The main content area displays the 'TACACS Profile' configuration for 'IOSXE_RW'. It includes fields for 'Name' (set to 'IOSXE_RW') and 'Description' (empty). Under 'Task Attribute View', there are sections for 'Common Tasks' and 'Common Task Type' (set to 'Shell'). Two dropdown menus for 'Default Privilege' and 'Maximum Privilege' both show the value '15'.

IOS XE_RO - فلم فيرعت شملأا

تافلم > جئاتنلا > ةسايسل رصانع > ةزهجلأا ةرادا > لمعل زكارم ىلإ لقتن 1 ةوطخلأا IOS XE_RO هتيمستب مقوا ديوج TACACS فيرعت.

1. ك زايتما يصقلأا دحلاو زايتما ريصقتلا تبنيعو تصحف. 2. ةوطخ

ظفحلاو نيوكتلا نم دكأت. 3. ةوطخلأا

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

Name: IOSXE_RO

Network Conditions

Results

- Allowed Protocols
- TACACS Command Sets
- TACACS Profiles**

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

رماؤ اتعوّمجم configureTACACS+

رماؤ اتعوّمجم اهنأ يل رصانعلا هذه فيرعت متىو TACACS+: Cisco_IOS_XE_RW وCisco_IOS_XE_RO.

لوفسمل رماؤ اتعوّمجم Cisco_IOS_XE_RW -

رماؤ اتعوّمجم > جئاتنلا > ئاسيل رصانع > ئازهجلأا ئرادا > لمعلا زكارم ىلإ لقتنا 1. ۋوطخل تACACS. اهتيمستب مقوّة ديدج Cisco_IOS_XE_RW.

(لوفسمل رودل رمأ يأب حمسى اذهو) ھاندأ جردم ريغ رمأ يأب حامسلا رايتحالا ۋناخ ددح 2. ۋوطخل ظفح قوف رقناو.

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

TACACS Command Sets > CISCO_IOSXE_RW

Command Set

Name: CISCO_IOSXE_RW

Results

- Allowed Protocols
- TACACS Command Sets**
- TACACS Profiles

Commands

Permit any command that is not listed below

Add Trash Edit Move Up Move Down

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

Cisco_IOS_XE_RO - لغش ملا رمأوأ ئاعومجم

> ئاسايسلار رصانع > زاهجلا ئرادا > لمعلا زكارم ئلا لقتنا، ISE، مدخلتسىم ئهجانم 1 ئوطخلا
مق مث ئيديج TACACS، رمأوأ ئاعومجم ئفاصاب مق. جئاتنلا Cisco_IOS_XE_RO.

دييچ رمأ فضا، رمأوأ مسق يف 2. ئوطخلا.

رقن او؛ رمألا دومع يف ضرعلا لخدأو ئاحنملا دومعل ئلدىسنملار ئامئاقلا نم حامسلار ددح. 3. ئوطخلا
كىشلا مەس قوف.

ظفح قوف رقن او تانايبلار نم دكأت. 4. ئوطخلا.

The screenshot shows the Cisco Identity Services Engine (ISE) interface under the 'Work Centers / Device Administration' tab. On the left, there's a sidebar with various icons. The main area is titled 'Policy Elements' and shows a 'TACACS Command Sets' section. A command set named 'CISCO_IOSXE_RO' is selected. The 'Name' field contains 'CISCO_IOSXE_RO'. The 'Description' field is empty. Under the 'Commands' section, there's a checkbox for 'Permit any command that is not listed below'. Below this, there's a table with two rows. The first row has columns for 'Grant' (checkbox), 'Command' (text input), and 'Arguments' (text input). The second row has columns for 'PERMIT' and 'show'. At the bottom right of the table, there are three icons: a pencil, a magnifying glass, and a plus sign.

زاهجلا لەۋىسمەن تاعومجم نىوكت

تاعومجم مسقىت نأ نكمى. ئازەجألا ئرادا يضارتفا لىكشب جەنلار تاعومجم نىكىمت مەتى
TACACS فيىرعت تافلم قىبلىتلىيەستل ئازەجألا عاونا ئىلا ادانتسا تاسايسلار.

ئازەجأ ئفاصىا. ئازەجألا ئرادا تاسايىس تاعومجم > زاهجلا ئرادا > لمعلا زكارم ئلا لقتنا. 1. ئوطخلا
عاونا لىك يواسى زاهجلا عون: ئادا ددح طرش تتحت. تاسايسلار تاعومجملى ئيديجلا IOS XE
يضارتفا لەۋىسمەن ددح، اھب حومسملار تالوكوتوربىلا تتحت. IOS XE# ئازەجأ.

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

Reset Reset Policy Set Hit Counts Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|-----------------|-------------|---|-------------------------------------|------|---------|------|
| Green | IOS-XE devices | | DEVICE:Device Type EQUALS All Device Types#IOS-XE | Default Device Admin | 0 | | |

ذه جهـنـلـا ـعـوـمـجـمـ نـيـوـكـتـلـ نـمـيـأـلـا قـوـفـ رـقـنـاـ وـظـفـحـ قـوـفـ رـقـنـاـ 2ـ وـطـخـلـاـ.

كرـتـأـ. فـرـعـمـلـا نـزـخـمـكـ ADـ مـدـخـتـسـتـ . قـدـاصـمـلـا ـسـاـيـسـ عـاـشـنـابـ مـقـ. 3ـ وـطـخـلـاـ
تـلـشـفـ اـذـاـ وـمـدـخـتـسـمـلـا رـثـعـيـ مـلـ اـذـاـ ، قـدـاصـمـلـا تـلـشـفـ اـذـاـ تـاـرـاـيـخـلـاـ
ةـيـلـمـعـلـاـ.

Identity Services Engine Work Centers / Device Administration Evaluation Mode 28 Days

Bookmarks Dashboard Context Visibility Operations Policy Administration Work Centers Interactive Help

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

Policy Sets → IOS-XE devices

Reset Reset Policy Set Hit Counts Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits |
|--------|-----------------|-------------|---|-------------------------------------|------|
| Green | IOS-XE devices | | DEVICE:Device Type EQUALS All Device Types#IOS-XE | Default Device Admin | 0 |

Authentication Policy(1)

| Status | Rule Name | Conditions | Use | Hits | Actions |
|--------|-----------|------------|---------|------|---------|
| Green | Default | | svs.lab | 0 | |

Options

- If Auth fail REJECT
- If User not found REJECT
- If Process fail DROP

ضـيـوـفـتـلـا ـسـاـيـسـ دـيـدـجـتـ 4ـ وـطـخـلـاـ.

يـفـ نـيـمـدـخـتـسـمـلـا تـاعـوـمـجـمـ لـاـ إـدـانـتـسـاـ لـيـوـخـتـلـاـ جـهـنـاـ عـاـشـنـابـ مـقـ.

لـاـثـمـلـاـ لـيـبـسـ ىـلـعـ:

فـلـمـ وـRـOـ رـمـاـوـلـاـ ـعـوـمـجـمـلـ ADـ ـعـوـمـجـمـلـ Cisco_IOSXR_ROـ نـيـيـعـتـ مـتـيـ
فـيـرـعـتـ Cisco_IOSXR_RO_Shellـ.

رـمـاـوـلـاـ ـعـوـمـجـمـلـ ADـ ـعـوـمـجـمـلـ Cisco_IOSXR_RWـ زـاهـجـ يـفـ نـيـمـدـخـتـسـمـلـا نـيـيـعـتـ مـتـيـ
فـيـرـعـتـ Cisco_IOSXR_RWـ.

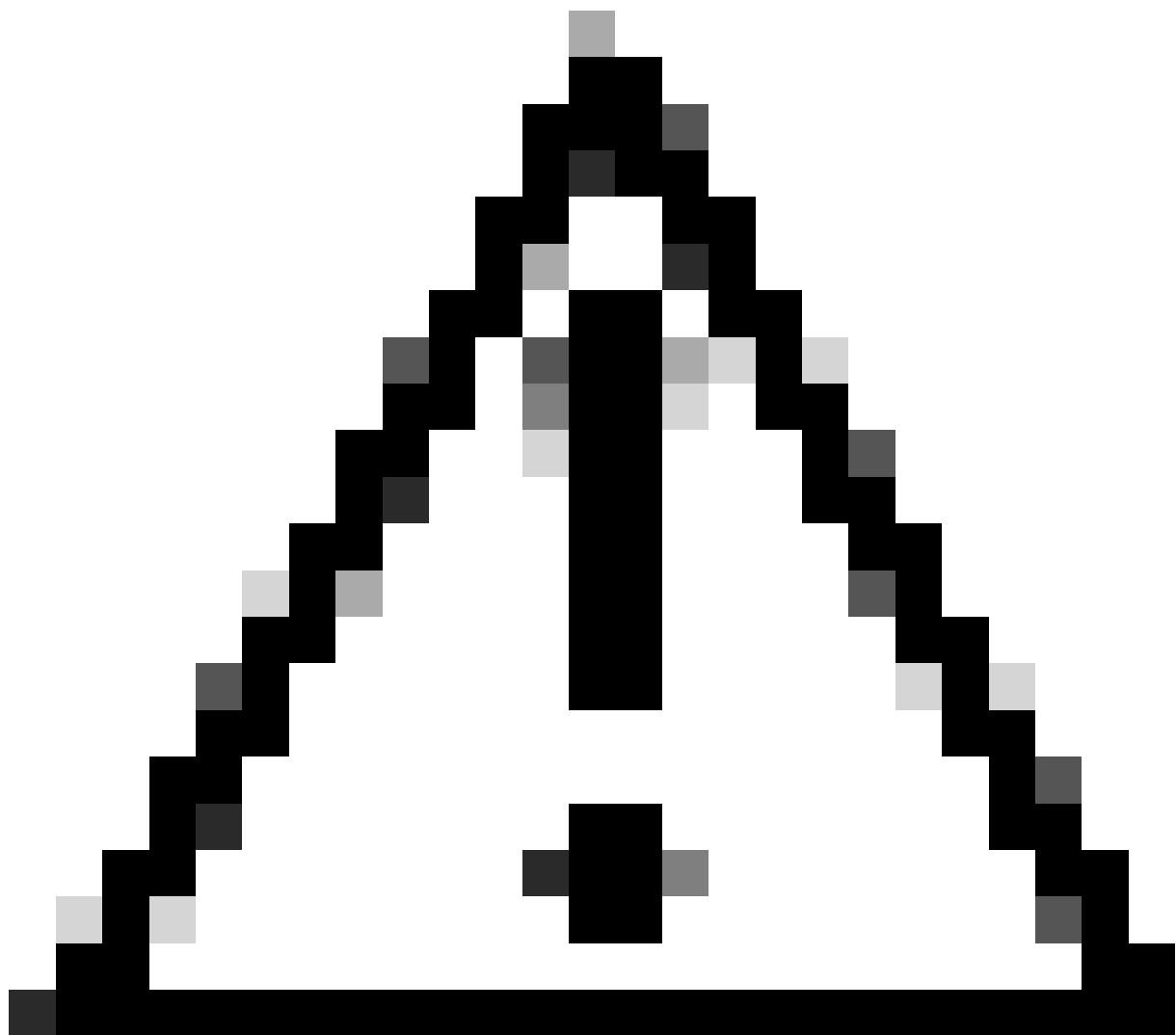
Identity Services Engine Work Centers / Device Administration

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

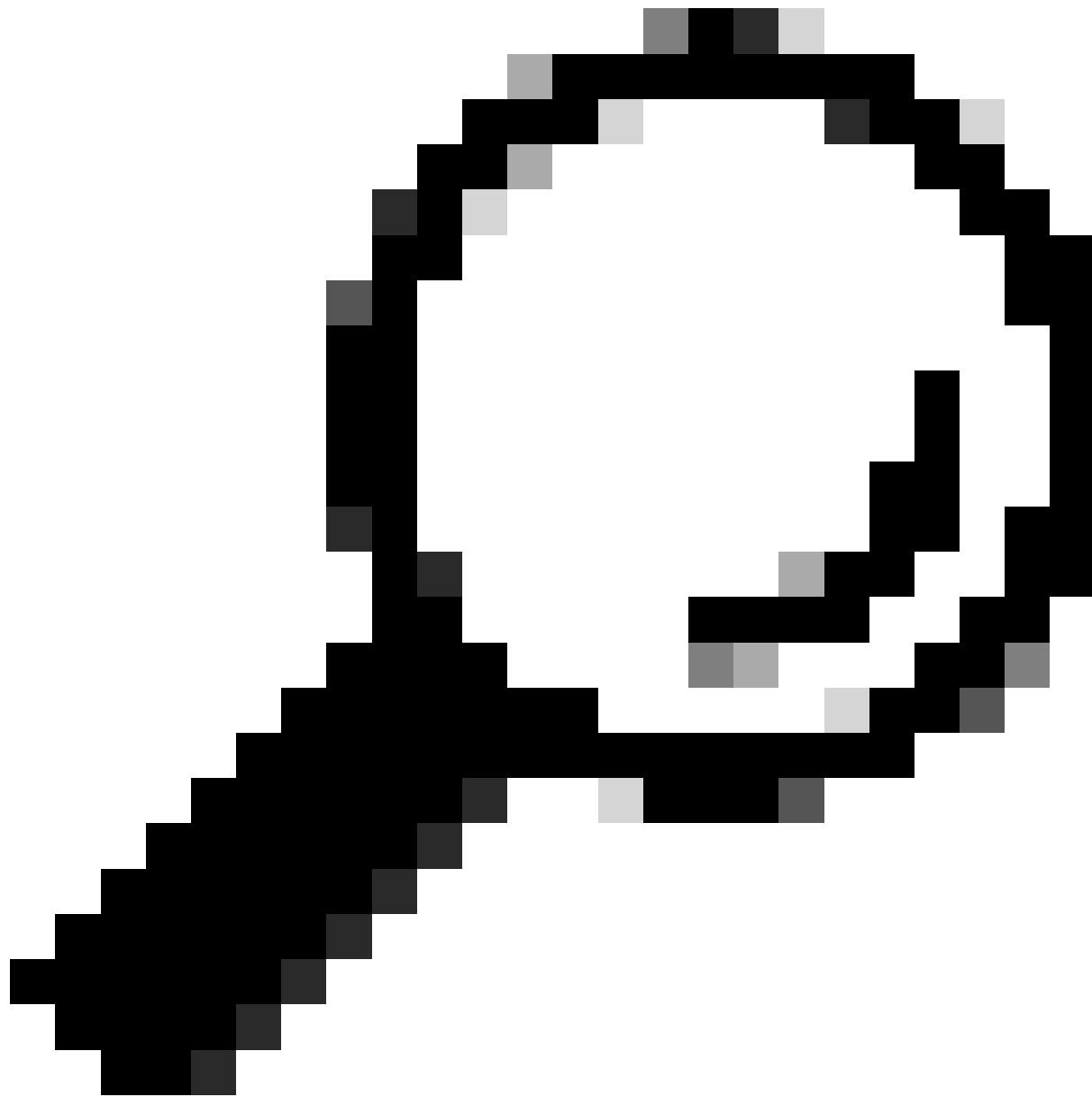
Policy Sets → IOS-XE devices Reset Reset Policy Set Hit Counts Save

| Status | Policy Set Name | Description | Conditions | Allowed Protocols / Server Sequence | Hits | | |
|--|-----------------------|--|---|-------------------------------------|------------------------|---------|--|
| | IOS-XE devices | | DEVICE:Device Type EQUALS All Device Types#IOS-XE | Default Device Admin | 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 | |
| | | | | | | | |
| | Authorization Rule RO | svs.lab:ExternalGroups EQUALS svs.lab/Users/Device RO | CISCO_IOSXE_RO | | IOSXE_RO | 0 | |
| | Authorization Rule RW | svs.lab:ExternalGroups EQUALS svs.lab/Users/Device Admin | CISCO_IOSXE_RW | | IOSXE_RW | 0 | |
| | Default | | DenyAllCommands | | Deny All Shell Profile | 0 | |

Cisco IOS XE J TACACS+ رب ع TLS 1.3 نیوکت - 2 عزجا



حیحص لکشب هلمع و مکحتلا ۃدحو لاصتا یل الوصولا ۃیناکم ا نم دکأت :ریذحت



ضيوفتل او AAA ۋىرقىچىم قىرط رىيغەت و تىقۇم مىخىتسىم نىيوكىتپ ئىصوئى : حىيملىت
، نىيوكىتلا تارىيغەت ئارجا ئانىثا TACACS نىم الدب ئىلەحەملە دامىتىعالا تانايىب مادختىسىل
زاهجىلا جراخ ھباسح لفوق بىنجلە.

زاهجىلا ۋە طاساوب ھۋاشنى مەت حىيتا فىم جوز - 1 نىيوكىتلا بولسأ

مداخ نىيوكىت TACACS+

Router TrustPoint. مىخىتسىي حىيتا فىم جوز ئاشنى او لاجەملە مىسا نىيوكىتپ مۇق 1 ۋە خەللا

```
ip domain name svs.lab
```

```
crypto key generate ec keysize 256 label svs-256ec-key
```

نويوكت TrustPoint

حياتاً ملا جوز نارق أو هجوم لـ قـث طـقـن يـشـنـا 1 وـطـخـلـا.

```
crypto pki trustpoint svs_cat9k
    enrollment terminal pem
    subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
    serial-number none
    ip-address none
    revocation-check none
    eckeypair svs-256ec-key
```

ـدـاهـشـ تـيـبـثـتـبـ CAـ ـقـدـاصـمـ 2ـ وـطـخـلـا.

```
<#root>
cat9k(config)#
crypto pki authenticate svs_cat9k
```

Enter the base 64 encoded CA certificate.

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

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

```
MIIF1DCCA3ygAwIBAgIIIM10AsTa.../UwDQYJKoZIhvcNAQELBQA...jELMAKGA1UE
BhMCVVMxFzAVB...gNDk5vcnRoIEhcm9sa...5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMR...IwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAw...hcmNMzUwNDI4MTcwNTAw...jBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xp...bmExEDAOBgNVBAcTB1JhbGVpZ2gx...DjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTV1MxEjAQBgNVBAMTCVN...UyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEB...BQADggIPADCCAg...cggIBAJvZUO...n2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kks...iFD33GyHQepk7vfp4NFU50tQ4HC7t/A0v9grDa3QW
VvvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLbo0kXEiKjPLat...kXojB8FVrhLF30
jMBSqwa4/Wlniy5S+7s4FFxscf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmj1bBjMmgsp0bULo/wxMHdTbtPBF11HRHTkNIo3qy04UADL2
WpoGhgT/FaxxB...o2UBcnYVaP+jjRE0NYT973MCbVA...xtNVU6bEBR0z+LwniACzupm
+qh23SL43u...w5A3iSw/BuU1E9p7B0e8oDNKU6gXlojKyLP/gC7j8AeP03ir+KZui8
b8X4iYn/67SbzFhw...xn3chkW4JYhQ4AI...mW1An2Q1+DMoZL7zRtS...qQ3g9ZqRIMzQN
gj+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIKB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTA01xh60I4QnK+MNQKpTjt/E4
ydH10rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVL1783nTc9wYptQEPi5sw
```

```
83g9EMgKV0ARIiVuA/q1AgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAyB4
QgEBBAQDAGAHMBkGCWCGSAGG+EIBDQQMFgpTV1MgTGFiIENBMA0GCSqGSiB3DQEBC
CwUAA4ICAQAIT308oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oK0dGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
0+ja6zTQqj061qJhmrSkyFbYf/ZTpe4d10zJsZjNsN0r8bF9nOA/7qNZLp3Z3cpU
PU0KdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazo1VBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIE0f5ay1PKURO/8aj/B7a1uJapXkmnj5qPeGhN0pB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eu/1X7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggz1P0ds/i6Lo7ypYX0eB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4172a6K18CR3U2Cr4wsuvndPEq/qd2NRSBWfffFOXE/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. ۋەطخىل ئاشنە ئىقتۇشلا ئەداھىل (CSR).

<#root>

cat9k(config)#

crypto pki enroll svs_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-----

```
MIIBfdCCASMCQAwgYQxGjAYBgNVBAMTEWNhdD1rLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTV1MxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSiB3DQEJAhYRY2F00WsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrt14ddevCh3UgxjYi
4N4oBGWrpbJbctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXV0DE1wtTAHHBrIXqoDww
OgYJKoZIhvNAQkOMS0wKzAcBgNVHREEFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIZj0EAwQRDwAwRAIgZqP2QTwm3ZZrmIphJ7+jSTER
40kTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----
```

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

Redisplay enrollment request? [yes/no]:

no

cat9k(config)#

٤. ٥ و ط خ ل ا ع ج ر م ل ا ن م ٦ ع ق و م ل ا ٧ دا ه ش ل ا دار ي ت س ا . ق دص م ل ا

<#root>

```
cat9k(config)#
crypto pki import svs_cat9k certificate
```

Enter the base 64 encoded certificate.

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

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

```
MIID8zCCAdugAwIBAgIIKfdYwg5WpskwDQYJKoZIhvcNAQELBQAjELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWx1aWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRlwEAYDVQQDEw1TV1MgTGFi
Q0EwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F00WsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ21zY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTA1VTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay50bW8uc3ZzLmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEH
A0IAB01gTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFy0rLiyjxXmLpFcO3uQeA/0
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCCSAGG+EIBDQQRFg94Y2EgY2Vv
dG1maWNhdGUwHAYDVR0RBBUwE4IRY2F00WsudG1vLnN2cy5jb20wCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUA4ICAQB0bgKVkeyVC9Usvuu0AUUsGaZHgwy2H9Yd
m5vIaui6PJczkCzIoAIghHPCQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHltifPayxv9juDu0ZRx+wYR2PIQ5eLv1bafg7K8E82sq0Cf0tcPr
Oc0NU8UCxq0bd0gu4XsdBN1+wcWFqeQSDLmP7nxvh00m/LXwCWUHwgVio0AuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
1xCSoLtY0dUxFIpJyK2MOZBY2zq2cNSc8Xbs05/0EQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqfq4mGh/A08T4iXfWDwfNezh7ZxMsCSCK/ZR1ELZ2hj60fzwX1H27UF8XU
ecr0Wx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VvRPitwN3Zb09poZyWiRLTnBsb42xNaWiL9bjQznA0iTDFmFFFourBsaAioz7ouY
2r1Mh+OpE83Uu+410TMawDgGiEv7iaiJ6xWc95EC+Adm0x3FvBXMtIM9qr7WwHW6
3C2hVYHJH254e1V5+H8iiz7rovEPm8ZDs nvYpJn4Km3iDvBNqp/vvAH0FcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----
```

% Router Certificate successfully imported

cat9k(config)#+

TACACS & AAA نیوکت ع TLS

١. ٥ و ط خ ل ا ع ج ر م ل ا ج و م (TrustPoint) TACACSS و AAA نارق او، تاعومج و اش نا داخ م.

```

tacacs server svs_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client svs_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
server name svs_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request

```

بىلاساً نىوكت 2. ۋەطخلا AAA.

```

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

```

CA ۋەطساوب ھۋاشنە مەت حىتافم جۈز - 2 نىوكتلا بولسأ

قىسىنتب ۋەطساوب CA و زاهىلە تاداھش كىلدىكىرەتلىك دارىتىساب موقۇت تىنك اذى ئەقىرىتلىكا ھەذە مادختىسا كىنكمىي CSR، ۋەطساوب ھۋاشنە ئەپلىكىشن PKCS#12.

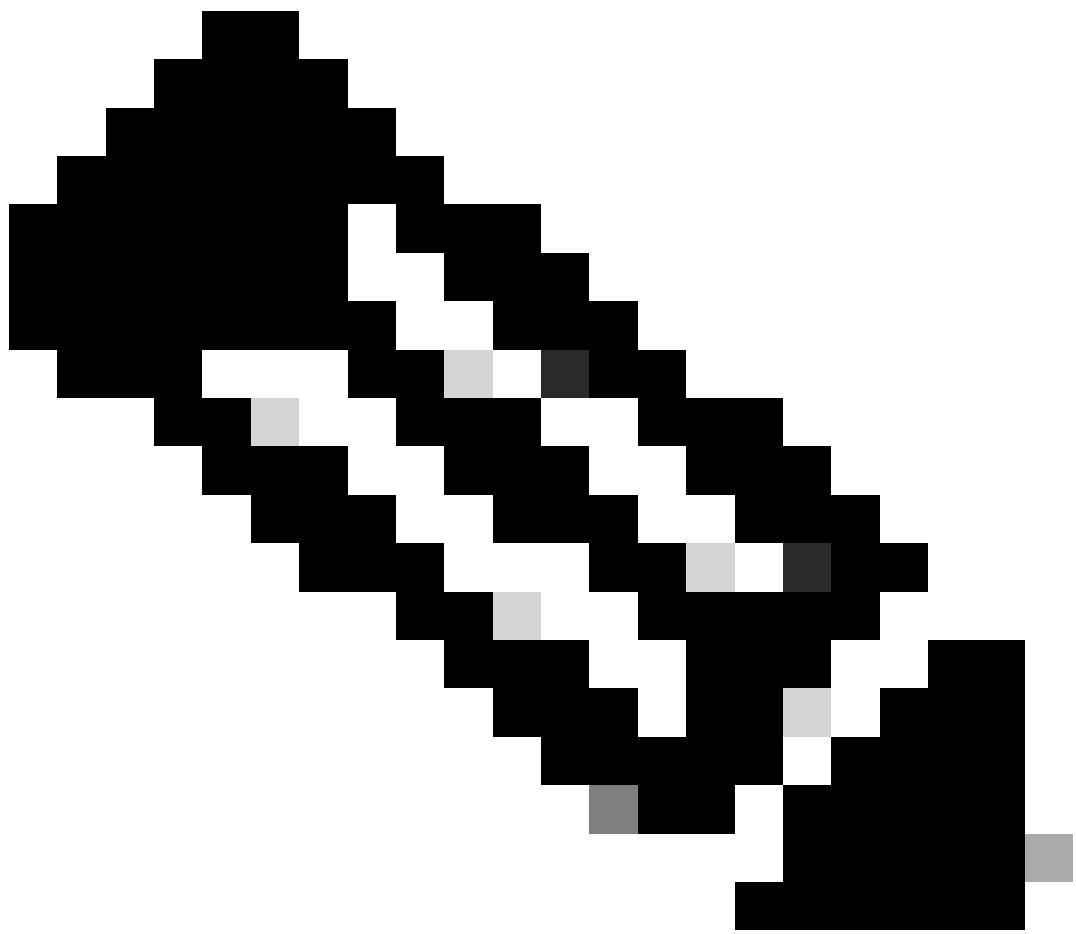
لېمۇع لىل ئەپلىكىشن TrustPoint 1. ۋەطخلا.

```

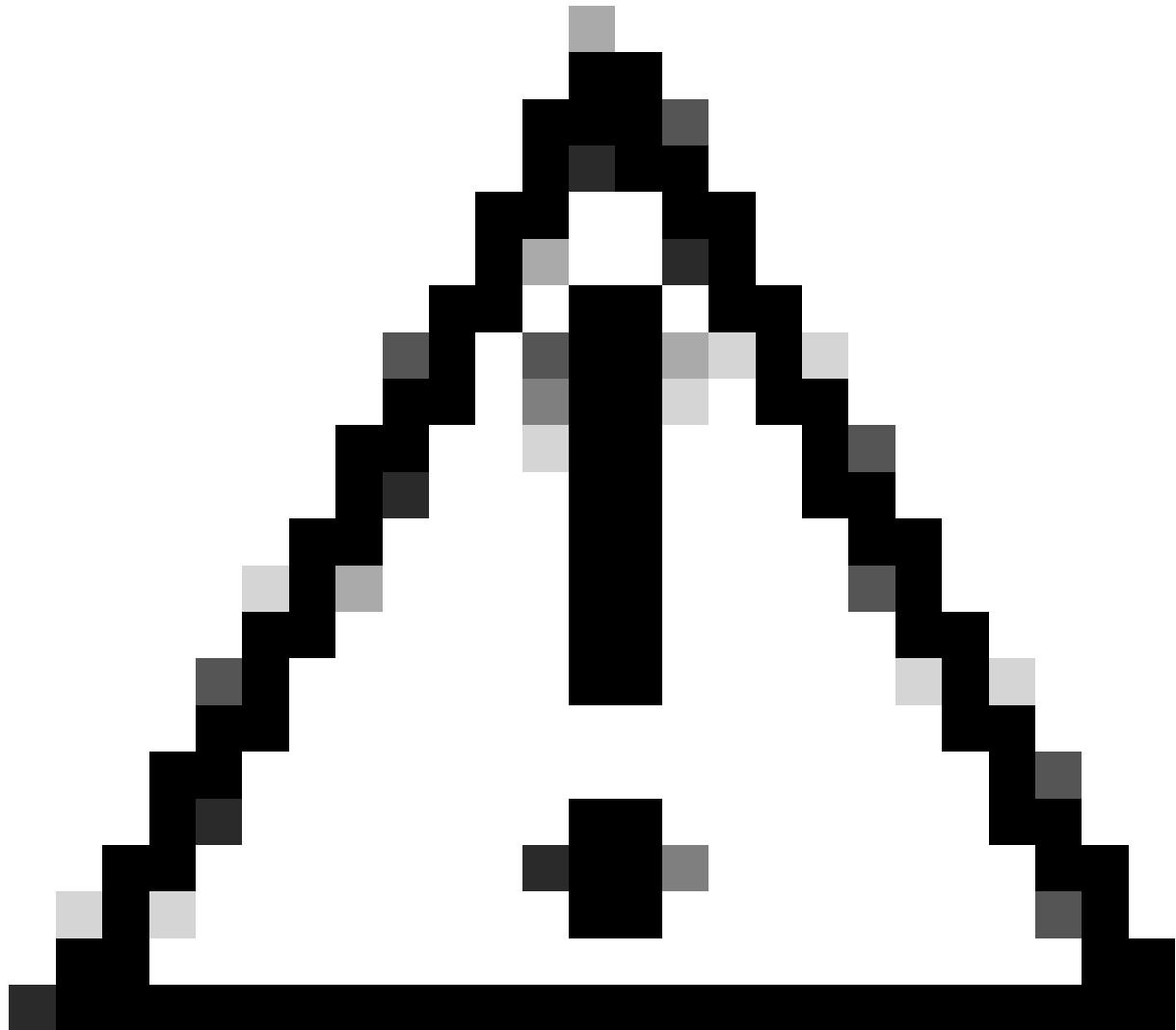
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none

```

ئىلى PKCS#12 فلم خسنا 2. ۋەطخلا.



حاتفملاو ۋەلماكلا تاداھشلار ئىلىم يىوتىجى PKCS#12 فلم نا نم دكأت: ئەظحالىم رفشم فلمك صاخلا.



ىلع) RSA نم ۋەرىتەسەملە PKCS#12 يف ۋەچۈرۈشلە حېتافمەل نوکت نأ بجى: رىذحت سىل، RSA 2048، عونلۇ لاثمەلە ليبس ECC.

```
<#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)
```

دارىتسا رمألا مادختىساب PKCS#12 فلم دروتىسا 3. ۋەطخىلا.

```
<#root>

cat9k#
crypto pki import svs_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 svs_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: svs_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: svs_cat9k_25jun17 svs_cat9k
```

Storage: nvram:SVSLabCA#37F5CA.cer

TACACS & AAA نیوکت ع TLS

نارقاو، AAA تاعومج و TACACS م داخ عاشنا 1. ۋوطخلانى.

```
tacacs server svs_tacacs
address ipv4 10.225.253.209
single-connection
tls port 6049
tls idle-timeout 60
tls connection-timeout 60
tls trustpoint client svs_cat9k
tls ip tacacs source-interface GigabitEthernet0/0
tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
server name svs_tacacs
ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

بىلاساً نیوکت 2. ۋوطخلانى.

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

ققحتلما

نیوکتلى نم ققحتلما.

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

ةبساحمل او ضيوفتل او ةقداصمل اءاطخأ حيحصت و AAA+TACACS.

```
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
```

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).