

# مادختساب RA-VPNaaS ل ن م آ ل ل و ص و ل ا ن ي و ك ت ISE مادختساب Posture م ي ي ق ت و ي ئ ا ن ث SSO

## تاي و ت ح م ل ا

---

[ق م د ق م ل ا](#)

[ق ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ق م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ق ي س ا س ا ت ا م و ل ع م](#)

[ق ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ن ي و ك ت ل ا](#)

[ي ئ ا ن ث ل ا ن ي و ك ت ل ا](#)

[ن م آ ل ل و ص و ل ا ن ي و ك ت](#)

[IP ت ا ع م ج ت ي ل ع RADIUS ق م و م ج م ن ي و ك ت](#)

[ISE م ا د خ ت س ا ل VPN ف ي ر ع ت ف ل م ن ي و ك ت](#)

[ق م ا ع ل ا ت ا د ا د ع ل ا](#)

[ق ب س ا ح م ل ا و ل ي و خ ت ل ا و ق ق د ا ص م ل ا](#)

[ر و ر م ل ا ق ك ر ح ه ي چ و ت](#)

[Cisco ن م ن م ا ل ي م ع ن ي و ك ت](#)

[ISE ت ا ن ي و ك ت](#)

[ق ك ب ش ل ل ا ق م ي ا ق ن ي و ك ت](#)

[ق م و م ج م ن ي و ك ت](#)

[ي ل ح م م د خ ت س م ن ي و ك ت](#)

[چ ه ن ل ا ق م و م ج م ن ي و ك ت](#)

[ت ا س ا ي س ل ا ق م و م ج م ض ي و ف ت ن ي و ك ت](#)

[Active Directory ي م د خ ت س م و ا ن ي ي ل ح م ل ا RADIUS ي م د خ ت س م ن ي و ك ت](#)

[ISE ق ي ع ض و ن ي و ك ت](#)

[ع ض و ل ا ط و ر ش ن ي و ك ت](#)

[ع ض و ل ا ت ا ب ل ط ت م ن ي و ك ت](#)

[ع ض و ل ا چ ه ن ن ي و ك ت](#)

[ل ي م ع ل ا د ا د م ل ن ي و ك ت](#)

[ل ي م ع ل ا ر ي ف و ت چ ه ن ن ي و ك ت](#)

[ل ي و خ ت ل ا ت ا ف ي ص و ت ع ا ش ن ا](#)

[ع ض و ل ا چ ه ن ق م و م ج م ن ي و ك ت](#)

[ق ح ص ل ا ن م ق ق ح ت ل ا](#)

[ع ض و ل ا ن م ق ق ح ت ل ا](#)

[ز ا ه ج ل ا ي ل ع ل ا ص ت ل ا](#)

[ISE ي ف ت ا ل ح س ل ا ن م ق ق ح ت ل ا ق ي ف ي ك](#)

[ا د ا ي ق ن ا](#)

[ل ا ث ت م ل ا م د ع](#)

[ISE ل م ا ك ت و ن م آ ل ل و ص و ل ا ع م ي ل و ا ل ا ت ا و ط خ ل ا](#)

[ا ه ج ا ل ص ا و ع ا ط خ ا ل ا ف ا ش ك ت س ا](#)

[ISE ق ي ع ض و ع ا ط خ ا ح ي ح ص ت ت ا ل ح س ل ي ز ن ت ق ي ف ي ك](#)

[ن م آ ل ا د ع ب ن ع ل و ص و ل ا ت ا ل ح س ن م ق ق ح ت ل ا ق ي ف ي ك](#)

## ةمدقملا

نع لوصولل VPN ةكبش يمدختسمل عضول مبيقت نيوكت ةيفي كدنتسمل اذه حضوي Duo مادختساب نمآل لوصولل او (ISE) ةيوهلا ةمدخ كرحم مادختساب دع

## ةيساسال تابلطتملا

- نمآل لوصولل لىل ع [مدختسمل ريفوت نيوكت](#)
- ةيچراخ ةهجل IDP وأ ةقداصملا لىل ك و مادختساب يئانثال [SSO](#) نيوكت
- قف نل ربع Cisco نم نمآل لوصولل ةلصت م ISE

## تابلطتملا

ةيلال عيضاوملاب ةفرعم كيدل نوكت نأب Cisco ي صوت:

- [ةيوهلا ةمدخ كرحم](#)
- [نمآل لوصولل](#)
- [Cisco Secure Client](#)
- [يئانثال نامأل - لىل ةيوهلا ةقداصملا لىل](#)
- ISE Posture
- ةبساحملا لىل وختلا و ةقداصملا

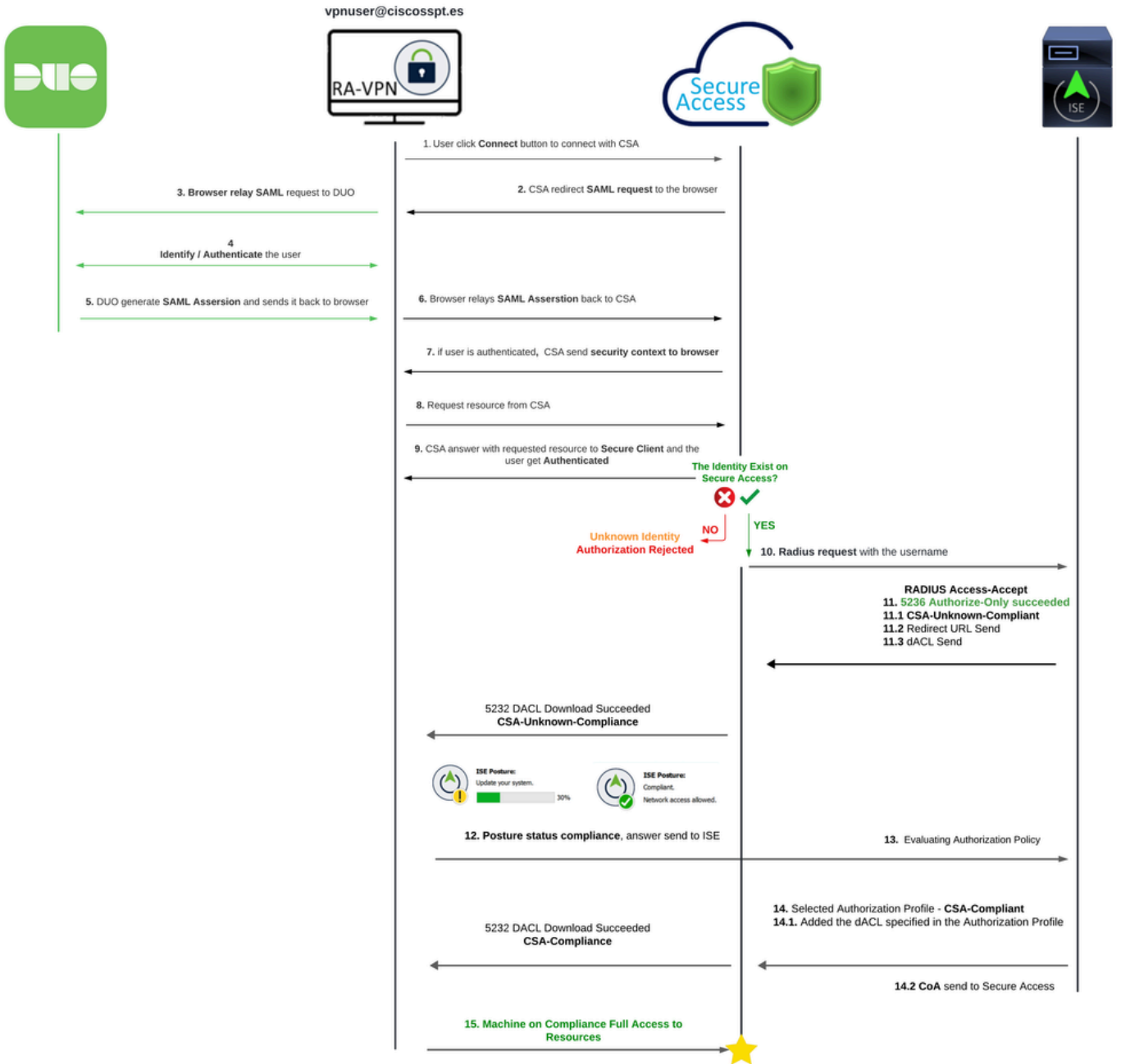
## ةمدختسمل تانوكملا

لىل دنتسمل اذه ي ةدراول تامولعملا دنتست:

- Identity Service Engine (ISE)، رادصلال 3.3 Patch 1
- نمآل لوصولل
- Cisco Secure Client - AnyConnect VPN، رادصلال 5.1.2.42

ةصاخ ةيلمعم ةئيىب ي ةدوجوملا ةزهجال نم دنتسمل اذه ي ةدراول تامولعملا عاشنا مت ت ناك اذ. (يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ةمدختسمل ةزهجال عيچ تادب رما يأل لمحتملا ريثأتلل كمهف نم دكأتف، لىل غشتلا دي ق ك تكبش

## ةيساسال تامولعم



، قداصلما ةيلم نيسحت ل Cisco ن (ISE) ةيوه ل تامدخ كرحم عم Duo SAML جم دي دؤي ةيناكمإ Duo SAML ةزيم رفوت Cisco. نم نمالا لوصول لولح لىل رخأ ناما ةقبط ةفاضوا عم مدختسمل لوخد ليجست ةيلم ع طيسبت لىل عمعت يتلا (SSO) يدالحال لوخدلا ليجست تقولا سفن يف نامال ةيلع ريعام نامض

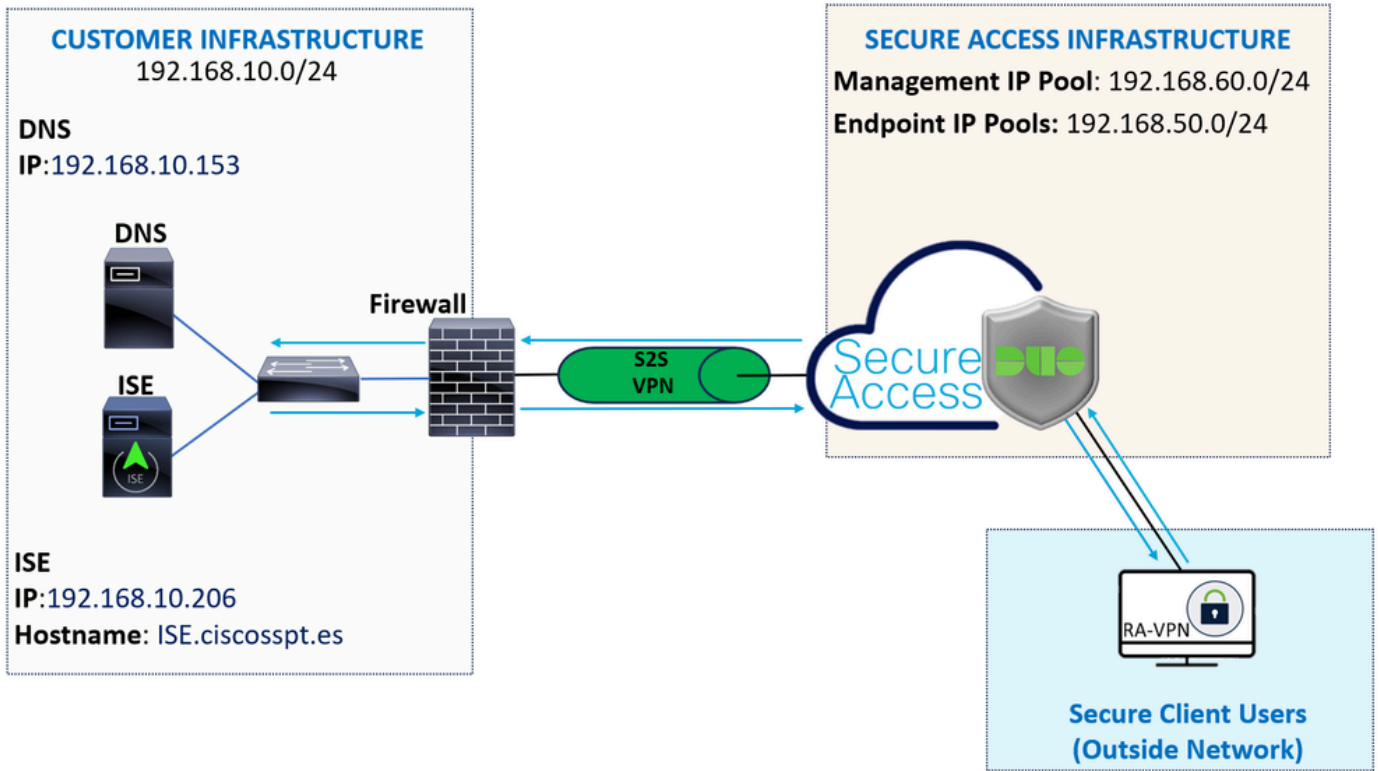
ISE Cisco ةطساوب ليوختلا ةيلم ع ةلعم متت ، Duo SAML لالحنم اهيلع قداصلما درجمبو مدختسمل ةيوه لىل اذانتسا يكيما نيدلا لوصولا يف مكحتلا تارارق داختاب حمسي اذهو نكمي يتلا دراوملا يلمت ةيلصفت تاسايس ISE ضرفي نأ نكمي. زاهال عضوو ةزهجأ يا نمو ، اهيل لوصول مدختسمل



نېماظننلا الك نېب لاصتا دوجو نم دكأتلا كمزلي، RADIUS لمكت نيوكتل: ةظحالم  
نېيساسألا.

---

ةكبشلل يطيختلا مسرلا



نيوكتلا

---

مادختساب ىل واولا تاوطلخ لىا لامك ا كىل ع ب جى ، نىوكتلا ةىلم ع ادب لبق :ةظحال م  
[ISE لىم ا ك ت و "نم ا ل ل و ص و ل ا"](#).

---

## ىئانثلا نىوكتلا

ةىلاتلا تاوطلخ لىا عبتا ، RA-VPN قىبب طت نىوكتلا

ىلا لقتنا [Duo ةرادا ةحول](#) ىلا لقتنا

- Applications > Protect an Application ىلا لقتنا
- Generic SAML Service Provider ن ع شحب لىا
- Protect رقتنا

# Protect an Application

Generic SAML Service Provider

Application

Protection Type



Generic SAML Service Provider

2FA with SSO hosted by Duo  
(Single Sign-On)

[Documentation](#)

Protect

VPN نيوكتل قيبتتال مساركذت، ةشاشلالىلع قيبتتال ضرعي نأ بجي



Successfully added Generic SAML Service Provider - Single Sign-On to protected applications.  
[Add another.](#)

Dashboard > Applications > Generic SAML Service Provider - Single Sign-On

## Generic SAML Service Provider - Single Sign-On

[Authentication Log](#) | [Remove Application](#)

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

### Metadata

Entity ID	<a href="https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/metadata">https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/metadata</a>	Copy
Single Sign-On URL	<a href="https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/sso">https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/sso</a>	Copy
Single Log-Out URL	<a href="https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/slo">https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/slo</a>	Copy
Metadata URL	<a href="https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/metadata">https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DI9818G01ZNKK5L9LR7Z/metadata</a>	Copy

### Certificate Fingerprints

SHA-1 Fingerprint	05:76:95:6B:E1:7C:F7:D1:79:12:2C:23:B6:1A:63:59:32:01:88:B1	Copy
SHA-256 Fingerprint	CF:CB:25:7C:41:0D:81:49:E5:83:48:79:EA:6B:45:C9:9F:4A:9A:21:A9:72:32:D3:C1:7F:86:4	Copy

Generic SAML Service Provider ةلجال هذه في

نمآلال لوصول نيوكتل

IP تاعمجت لىع RADIUS ةومجم نيوكتل

ةلالتال تاوطخال لمكأ، RADIUS مادختساب VPN فيرعت فلم نيوكتل

كب ةصخال نمآلال لوصول. تامول عم ةحول لىل لقتنا



- [Connect > Enduser Connectivity > Virtual Private Network](#) قوف رقنا
- [Manage](#) قوف رقنا، [\(Manage IP Pools\)](#) عمجتال نيوكتل تحت

## Manage IP Pools

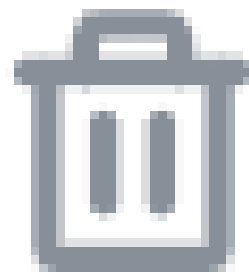
Manage

2 Regions mapped

- رادىوس سرڤر لى تىل كىش و IP Pool Region لى تىرتىخاً

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	 

- هر ىرتىل صاصر لى ملق لى رقىنا





- **Radius Group (Optional)** نمض IP عمجت مسق نيوكت لفسأ، نآلا
- Add RADIUS Group رقنا

## RADIUS Groups (optional)

Associate one RADIUS group per AAA method to this IP pool.



**No RADIUS groups created**

[Add RADIUS Group](#)

# ← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings

## RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE\_CSA ×

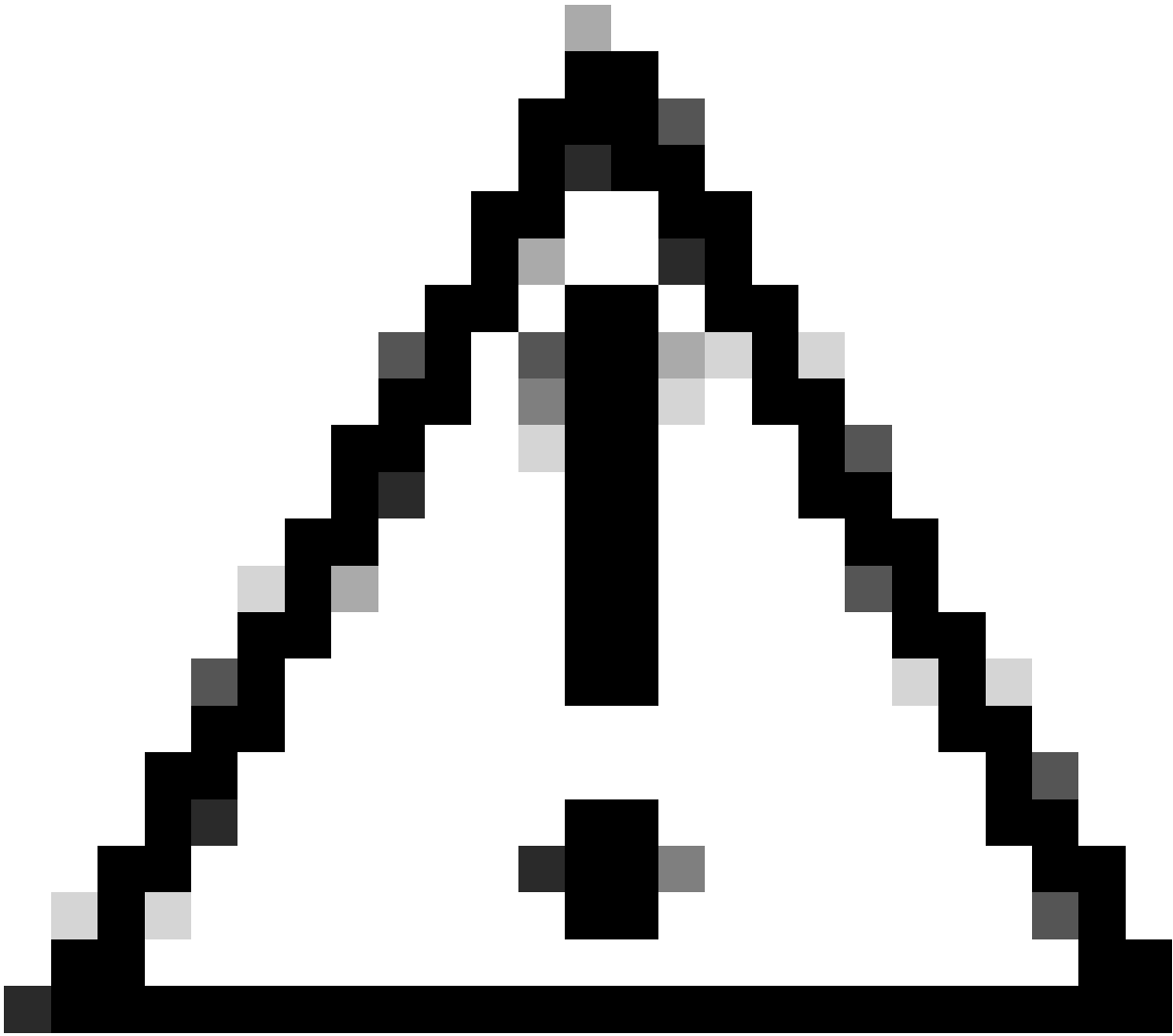
+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

## نمآلا لوصولا يف

### ◦ AAA method

- **Authentication:** وه، يضارتفا لكشب، هديحتو **Authentication** ذفنم لل رايتخالالا ةناخ ىلع ةمالع عضو 1812
- قداصملا **Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)** بلطت ةلاحي يف رايتخالالا ةناخ ىلع ةمالع عضو
- **Authorization:** ذفنملا اذه هديحتو ذفنم لابل **Authorization** ةصاخلا رايتخالالا ةناخ ىلع ةمالع عضو 1812 وه، يضارتفا لكشب
- **Authorization mode Only Change of Authorization (CoA)** تاريغيغتو ةيعضوب حامسلاو **mode** رايتخالالا ةناخ ىلع ةمالع عضو
- **Accounting:** 1813 وه، يضارتفا لكشب، ذفنملا هديحتو ليوختلل رايتخالالا ةناخ ىلع ةمالع عضو
- دحاو مداخ ىلا ةبساحملا تانايب لاسرا متي، درفملا عضو لا يف) **Single or Simultaneous** رتخأ (ةومجمملا يف مداوخلال عي مجل ةبساحملا تانايب ريفوت متي، نمازتملا عضو لا يف. طقف
- ةتقؤملا **RADIUS** لئاسرل يرودل عاشنإلا نيكم تمل **Accounting update** رايتخالالا ةناخ ددح **Accounting-Update**.



ذفنم لاسفن ، اهديدحت دنع ، بيلاسأل او بيلاسأل ال **Authorization** نم لك مدختست Authentication أن بجي : ريذحت

- 
- **RADIUS** مسقلا لىل ع AAA ربع قداصل ملل هم ادختسا متي يذلا **RADIUS Servers (ISE)** نيوكت لىل جاتحت ، كلذ دعب **RADIUS Servers:**
  - Add + قوف رقنا

## RADIUS Servers

You can add up to 8 servers in each group

Assign servers

**+ Add**

#	Server Name	IP Address
---	-------------	------------

- في التواريخ التي نيوكتب مق، كذد دع ب:

## Add RADIUS Server

Server name

IP Address

Password type

Secret Key

 [Show](#)

Password

 [Show](#)

**Cancel**

**Save & Add server**

**Save**

- **Server Name:** مداخل فيرعتل مسانويك تپ مق ISE.
- **IP Address:** نمال لوصول لالغ نم هيل لوصول وانكمي يذلا Cisco ISE زاهل IP نويك ت
- **Secret Key:** یرسل ال RADIUS حاتفم نويك ت
- **Password:** كب ةصاخ ال RADIUS رورم ةم لك نويك تپ مق
- **ك ب صاخ ال ISE مداخل ددحو رايخ ال Assign Server نمض ك ب صاخ ال RADIUS مداخل ددحو Save رقنا**

## RADIUS Servers

You can add up to 8 servers in each group

### Assign servers

^

ISE\_CSA

[+ Add](#)

---

- **مت يذلا نويك تال طافحل یرخأ ةرم Save رقنا**

# ← Edit RADIUS Group



Add group of RADIUS servers, which will be used to control access to your VPN profiles

Change of authorization (CoA) mode ⓘ

CoA Port: 1700

Accounting

Port

1813

Accounting mode

Single

Simultaneous

Accounting update

Interim accounting update

Update interval

1

hour(s)

Settings

## RADIUS Servers

You can add up to 8 servers in each group

Assign servers

ISE\_CSA ×

+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

◦ **Protocols: رتخا SAML**

- رقنا Download Service Provider XML file
- لىكشرت duo، ةوطخلال ي ف لكشي قيبتلالي ف ةمولعملال تلدبتسا

- ه موقت يذل لمالكالاب قلعتم عيش لى لى انثال مسا ريغت ب مق، تامولعملال هذه نيوكت درجم

## Settings

Type Generic SAML Service Provider - Single Sign-On

Name

Duo Push users will see this when approving transactions.

- رقنا Save لىل عملال
- رزلا قوف رقنالا SAML Metadata لىزنن ب جي، ظفح قوف رقنالا درجم



# ISE - SAML

See the [Generic SSO documentation](#) to integrate Duo into your SAML-enabled service provider.

## Metadata

Entity ID	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadata</code>	Copy
Single Sign-On URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/sso</code>	Copy
Single Log-Out URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/slo</code>	Copy
Metadata URL	<code>https://sso-5ed0a388.sso.duosecurity.com/saml2/sp/DIGN1FGK2GW6MVKFB45F/metadata</code>	Copy

## Certificate Fingerprints

SHA-1 Fingerprint	<code>53:0E:25:4F:29:3A:B5:DF:09:A2:0D:BB:08:C7:F6:E8:D9:DB:DE:6B</code>	Copy
SHA-256 Fingerprint	<code>C5:6F:35:44:F8:FC:74:C6:E6:2B:C1:8F:92:9C:E2:80:91:B1:61:C9:75:0B:F9:C5:4B:81:B8:F</code>	Copy

## Downloads

Certificate	<a href="#">Download certificate</a>	<a href="#">Copy certificate</a>	Expires: 01-19-2038
SAML Metadata	<a href="#">Download XML</a>		

- **Next** قوف رقن او **Upload IdP security metadata XML file** 3. رايخ ال تحت ن مآلا لوصولو **SAML Metadata** لي محتب مق

VPN Profile name

ISE\_CSA\_SAML

- ✓ General settings  
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IPsec (IKEv2)
- 2 Authentication, Authorization, and Accounting SAML
- ✓ Traffic Steering (Split Tunnel)  
Connect to Secure Access | 1 Exceptions
- ✓ Cisco Secure Client Configuration

**Authenticate with CA certificates**  
Select to use CA certificates to authenticate this VPN profile.

SAML Configuration

SAML Metadata XML Configuration

1. **Download Service Provider XML file**  
This XML file contains metadata required to configure your IdP.

[Download service provider XML file](#)

2. **Generate IdP Security Metadata XML File**  
a. Upload the Service Provider XML file to your IdP.  
b. From your IdP, create and download an IdP Security Metadata XML file.

3. **Upload IdP security metadata XML file**

✓ File 'ISE - SAML - IDP Metadata.xml' uploaded. [Replace](#) [Delete](#)

Manual Configuration

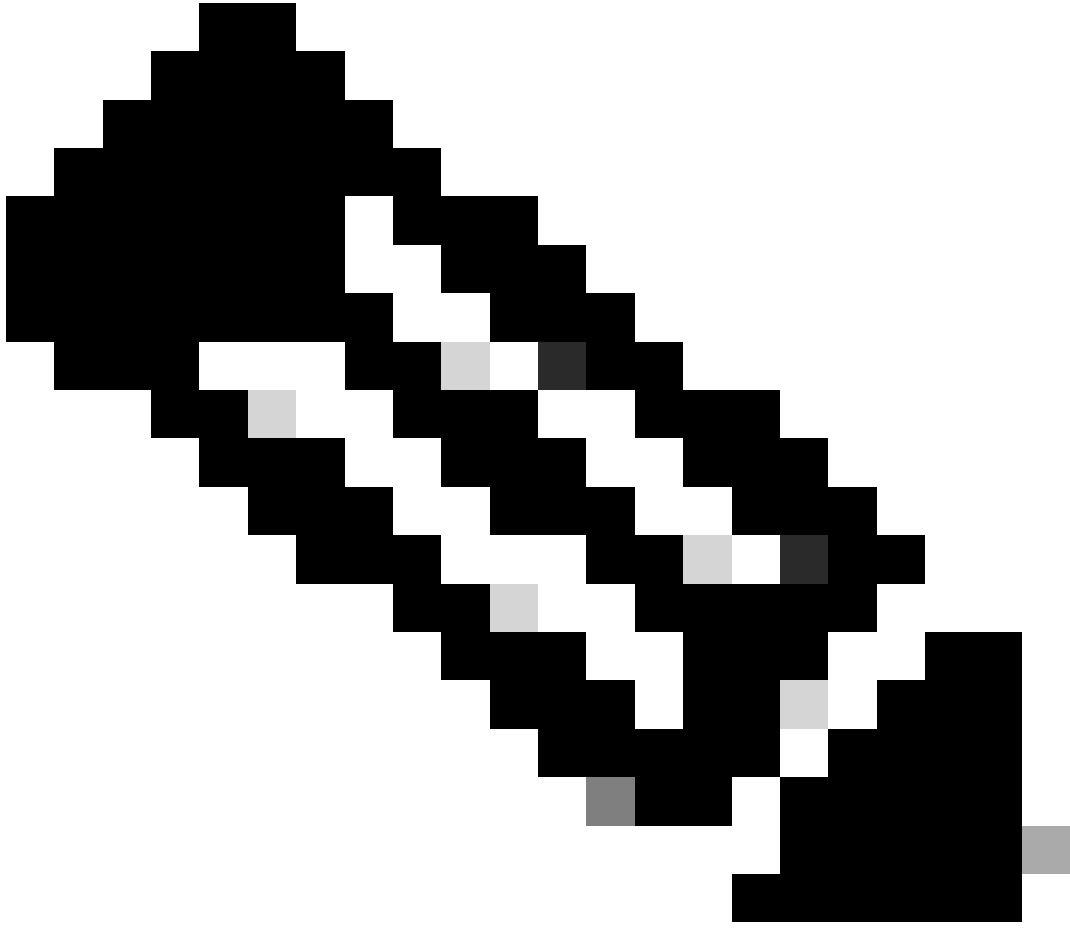


Cancel

Back

Next

ضيوفتلا مادختساب ةعباتملاب مق.



يتمثل RADIUS مزجاً يُنعَى أمم، ISE لالخ نم اهلي وخت متيس، SAML مادخت ساب ةقداصل مال نيوكت درجمب: ةظحالم  
انه دوجوم ريغ رورملا ةملك ل قح. طاقف مدختس مال مسا يلع يوتحت فوس Secure Access ةطساوب اهلا سرا متي

- ✓ **General settings**  
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**  
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**  
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

## Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication **Authorization** Accounting

**Enable Radius Authorization**  
Use defaults or customize groups to map to regions

Select one group for all regions + Group

ISE\_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

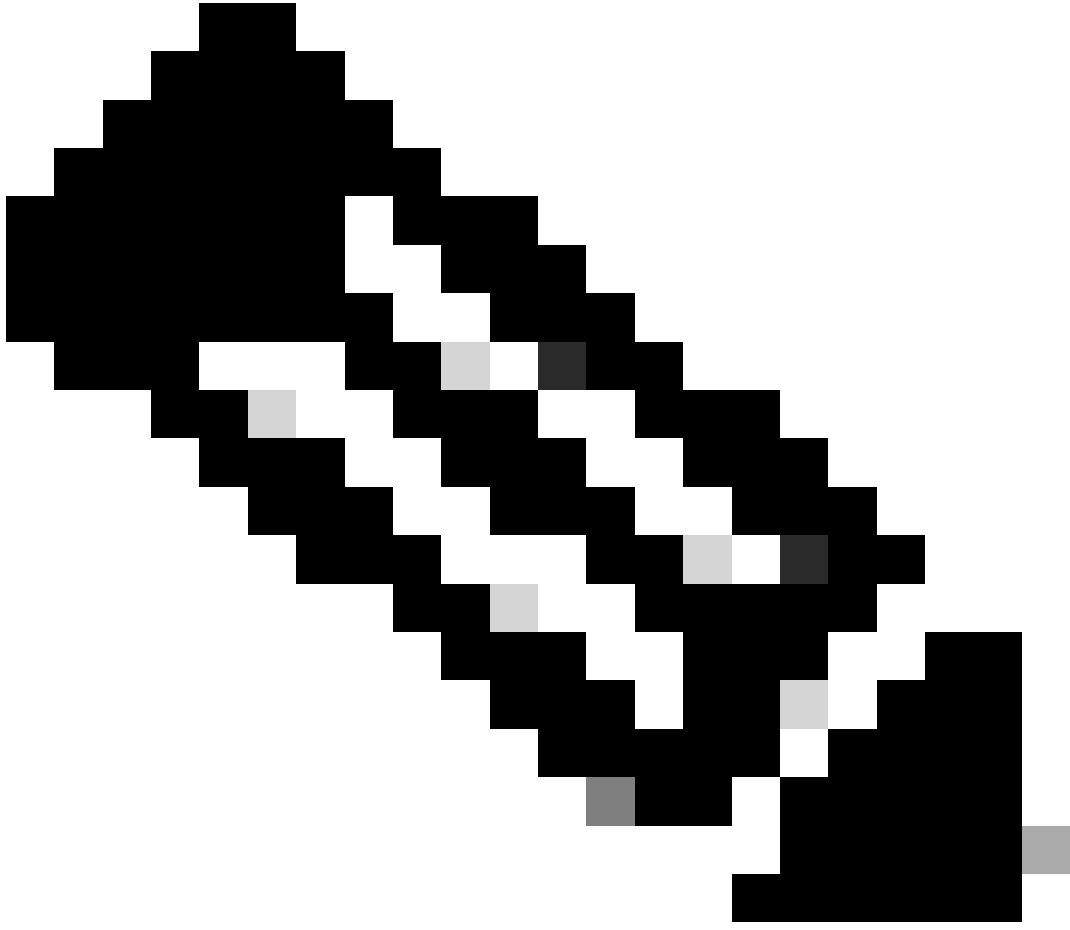
### • Authorization

◦ **Enable Radius Authorization:** RADIUS ضيوفت نيكمتل رايتخاله اناخ يلع عمال ع عضو

• نع لوصول تا عمت عي مجل ددحم دحاو RADIUS مداخ مادخت سالا رايتخاله اناخ ددح: قطنملا عي مجل ددحاو عومجم ددح  
لصفنم لكش ب عمت لكلا اه في رعت ب مق وأ، (RA-VPN) ةيره اظلاله صخاله كة بشال - دعب

### • Next رقنا

Accounting مادخت ساب ةعباتملا عاجرلا، عجال Authorization لك نيوكت دعب



لمعت نلف ،ةفيطول Radio Authorization نيكمتب مقتم مل اذا :تظالم

- ✓ **General settings**  
Default Domain: ciscospt.es | DNS Server: House (192.168.10.153) | Protocol: TLS / DTLS, IKEv2
- 2 Authentication, Authorization, and Accounting**  
RADIUS
- ✓ **Traffic Steering (Split Tunnel)**  
Connect to Secure Access | 2 Exceptions
- ✓ **Cisco Secure Client Configuration**

## Authentication, Authorization, and Accounting

Choose a configuration method to complete the SAML authentication process for this VPN profile. [Help](#)

Authentication Authorization **Accounting**

### Enable Radius Accounting

Use defaults or customize groups to map to regions

Select one group for all regions

+ Group

ISE\_CSA

Region	Management IP pools	Groups
RA VPN 2	192.168.80.0/24	ISE_CSA
RA VPN 1	192.168.60.0/24	ISE_CSA (default)



Cancel

Back

Next

- **Accounting**

- **Map Authorization groups to regions:** راي ت خ او ق ط ان م ل ا راي ت خ | **Radius Groups**

- **Next** ر ق ن ا

After you have done configured the Authentication, Authorization and Accounting Traffic Steering ة ع ب ا ت م ا ج ر ل ا ة ع ب ا ت م ا ج ر ل a

رورم ل ا ة ك ر ه ي ج و ت

ن م آ ل ا ل و ص و ل ا ل ا ل خ ن م ل ا ص ت ا ل ا ع و ن ن ي و ك ت ك م ز ل ي ، رورم ل ا ة ك ر ه ي ج و ت ت ح ت



- كِب صاخلا تنرتنإلا رفوم ربع رمت كب ةصاخلا تنرتنإلا رورم ةكرح لك نإف **Bypass Secure Access** كلذ تترق اذا (تنرتنإة يامح دجوت ال) Secure Access لالغ نم سېلو

### Tunnel Mode

Bypass Secure Access ▾

All traffic is steered outside the tunnel.



### Add Exceptions

Destinations specified here will be steered **INSIDE** the tunnel.

+ Add

Destinations

Exclude Destinations

Actions



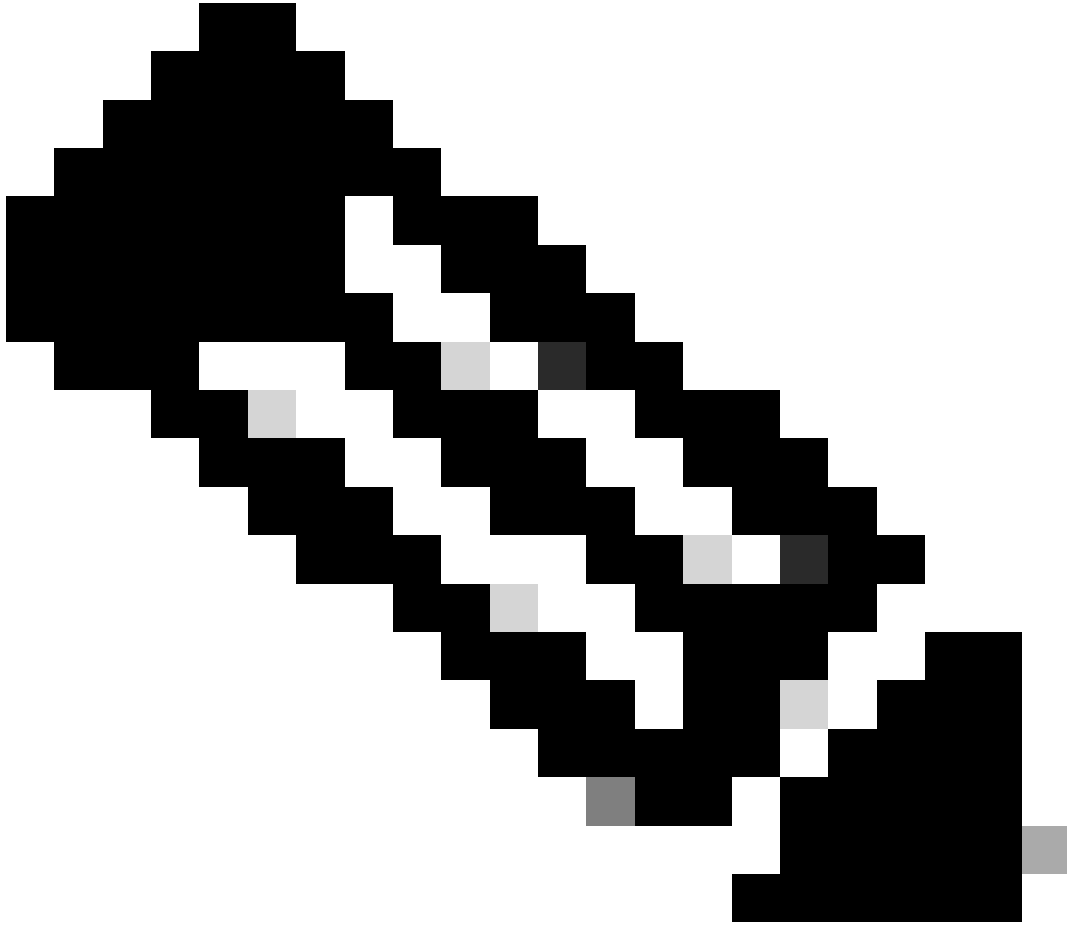
No matches found

Cancel

Back

Next





**Bypass Secure Access** كرايخ| دنع (ISE) ةيوهال تامدخ كرحم ةيعضو ISE Posture [enroll.cisco.com](https://enroll.cisco.com) ةفاضل اءارلا :ءظالم

---

+ رقنا ،كلذب مايقلل VPN ةكبش لالغ نم اهليل لوصولا ديرت يتل ةصاخلا ةكبشلا دراوم عيمج ددحت ،ةوطخلل هذه يف دراوملا ةفاك ةفاضل دنع **Next** رقنا مءء **Add**.

Cisco نم نم آ ليمع نيوكت

### Cisco Secure Client Configuration

Select various settings to configure how Cisco Secure Client operates. [Help](#)

Session Settings **3** Client Settings **13** Client Certificate Settings **2** [Download XML](#)

**Banner Message**  
Require user to accept a banner message post authentication

**Session Timeout**  
 days

**Session Timeout Alert**  
 minutes before

**Maximum Transmission Unit** ⓘ

[Cancel](#) [Back](#) [Save](#)

ك ب صاخال نيوكتال صيصخت ديرت تنك اذا نكلو، Save رقنللاو يضارتفاك عيش لك ىلع ظافحلل كنكمي، ةوطخلل هذه يف [Cisco](#) نم نمالا لي عمل للوؤسم ليلد نم ققحتللا عاجرلاف، رثكأ

Name	General	Authentication, Authorization & Accounting	Traffic Steering	Secure Client Configuration	Profile URL
ISE_CSA_SAML	ciscospt.es TLS, IPsec (IKEv2)	SAML RADIUS	Connect to Secure Access 1 Exception(s)	13 Settings	vpn.sse.cisco.com/ISE_CSA_SAML

ISE تانويكت

ةكبشللا ةزهجأ ةمئاق نيوكت

Cisco ISE ىلع تامالعلسا عاجرل اهنكمي يتللا اهب حومسمللا ةزهجال نيوكت كمزلي، Cisco ISE لالخل نم ةقداصلل نيوكتل لك:


- Administration > Network Devices ىللا لقتنا
- Add + قوف رقنا

## Network Devices

Name CSA

Description \_\_\_\_\_

\_\_\_\_\_

IP Address  \* IP : 192.168.60.0 / 24 


Device Profile  Cisco  

RADIUS Authentication Settings

### RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret ..... [Show](#)

Use Second Shared Secret 

Second Shared Secret \_\_\_\_\_ [Show](#)

CoA Port 1700 [Set To Default](#)

- **Name:** نم آلا لوصول دي دحتل مسا مادختسا
- **IP Address:** ةوطخال Management Interface نيوكت، [IP عمجت ةقطنم](#)
- **Device Profile:** رتخأ Cisco
  - **Radius Authentication Settings**
    - **Shared Secret:** ةوطخال يلع هنيوكت مت يذلا كرتشمل رسال سفن نيوكت، [يرسل احاتفملا](#)
    - **CoA Port:** "نم آلا لوصول" ةزيم يف اضيأ 1700 زارطال مادختسا متي شيح، ةيضارتفا ةميقك اهعد

لم اكلتال نم ققحتلل يلحم مدختسم عاشنال ةعباتملاب مق، حيحص لكشب لم اكلتال لمع نم ققحتلل **Save** رقنلا كلذ دعب

ةومجم نيوكت

ةيلاتال تاوطخال عبتا، نييحلحمل ني مدختسمل عم مادختسالل ةومجم نيوكتل:

- **Administration > Groups** يف رقنا
- **User Identity Groups** رقنا
- **Add** + رقنا
- **Submit** قوف رقناو ةومجملل Name ةومجم عاشناب مق

The screenshot displays the 'Identity Groups' configuration page. On the left, the 'Administration' menu is open, with 'Identities' > 'Groups' selected (marked with a red '2'). The main content area shows the 'User Identity Groups' page with a 'New User Identity Group' form. The form includes a 'Name' field containing 'CSA-ISE' (marked with a red '5') and a 'Description' field. Below the form is a 'Submit' button (marked with a red '6'). To the right, a list of existing groups is shown, including 'ALL\_ACCOUNTS (default)', 'CSA-ISE' (with a 'GROUP CREATED' status), and 'Employee'. The 'Add' button in the top left of the form area is marked with a red '4'.

يحلح م دختسم نيوكت

ك: صاخلا لم اكلال نم ققحتلل يحلح م دختسم نيوكتل

- Administration > Identities لى لقتنا
- Add + قوف رقتنا

## Network Access User

\* Username

Status  Enabled ▼

Account Name Alias  ⓘ

Email

### Passwords

Password Type: Internal Users ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

	Password	Re-Enter Password	
* Login	<input type="password"/>	<input type="password"/>	Generate Password ⓘ
Enable	<input type="password"/>	<input type="password"/>	Generate Password ⓘ

## ▼ User Groups

⋮ CSA-ISE ▼ 🗑️ +

- **Username:** ةوطخلال ىل اذه دنن سسي Secure Access: يف فورعم UPN ريفوت مادختساب مدختسملا مسان يوكت [ةيساسالاب لطلت مل او](#)
- **Status:** طشن
- **Password Lifetime:** كل اقفو، Never Expires، و With Expiration اهن يوكت كنكم مي
- **Login Password:** مدختسملل رورم ةملك عاشن |
- **User Groups:** ةوطخلال ىل ع اهواشن | مت يتللا ةومجملا رتخ [ةومجم نيوكت ب مق](#)

---

Secure Access نم ةمداقلا تارادصإلإ يف اهريريغتل UPN إلى ةدنتسمل ةقداصملا نييعت مت :تظالم

---

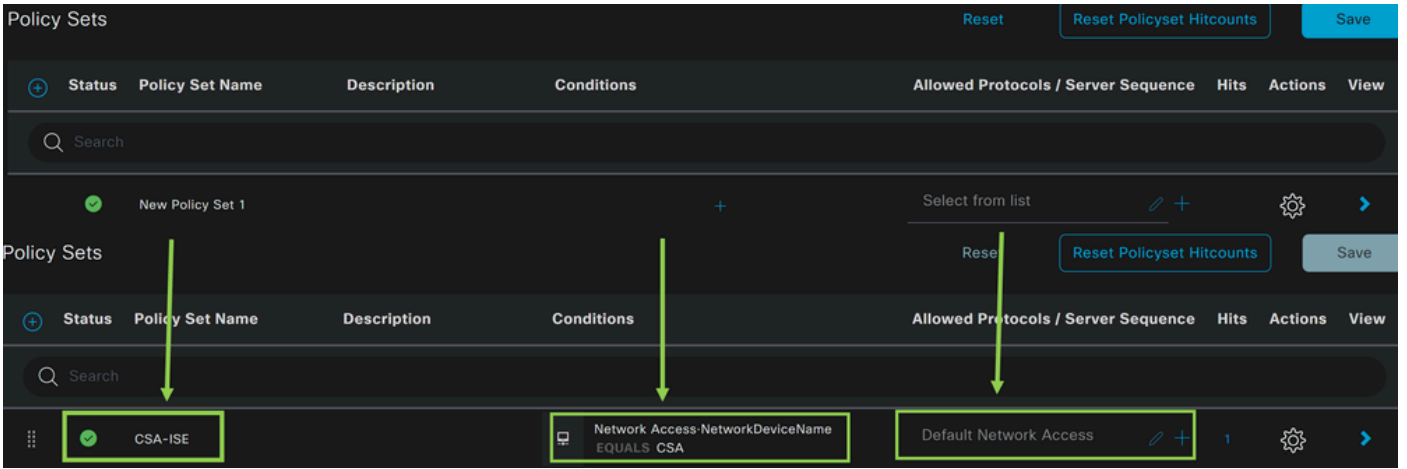
Configure Policy Set. ةوطخالاب ةعباتملاو نيوكتل Save كنكمي ،كلذ دعب

جهنلا ةعومجم نيوكت

ةلاح ويرانيسل اذح ضوي .ضيوفتل او ةقداصملا اناثا هذاختاب ISE موقوي يذلا ءارجال نيوكتب مق ،جهنلا ةعومجم راطا يف اذا امم ققحتي و RADIUS ةقداصم لصأ نم ISE ققحتي ،الوا .مدختسمل لوصول ريفوتل ةطيسب ةسايس نيوكتل مادختسال لوصول ريفوتل ISE مدختسم تانايب ةدعاق يف ةدوجوم تايوهلا تناك

Cisco ISE تامولعم ةحول إلى لقتنا ،جهنلا اذح نيوكتل

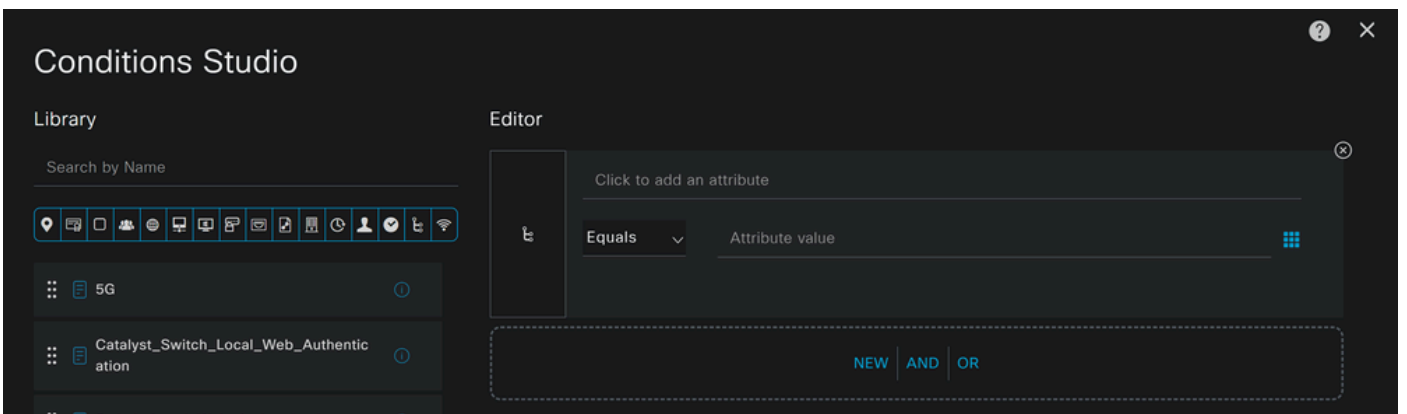
- Policy > Policy Sets قوف رقنا
- ةديج جهن ةعومجم ةفاضال + قوف رقنا



ةقداصملا نيوكتب مق ،كلذ دعب .ةيضارتفالا ةعومجملا تحت لمعلال نم ال دب ةديج جهن ةعومجم عاشناب مق ،ةالجال هذه يف ةوطخلال يف فرعملال ةكبشلال زاهج ىلا لوصولاب هنيوكت مت يذلال جهنلال حمسي .هذه جهنلال ةعومجم ىلا ادا نسا ضيوفتلاو ك جهنلال يف لوخدلال مث CSA Network Device List نم يتأت ةقداصملا هذه نأ نم ققحتلل [ةكبشلا ةزهجأ ةمئلا نيوكت](#) **Default Network Access** لثم ،اهب حومسملا تالوكوتورربلا ،اربخأو **Conditions**.

ةيلا تاملال ةمادختساب ةعباتملا ب مق ،جهنلال ةعومجم قباطت يتلا **condition** تاميلعلتلا عاشنال

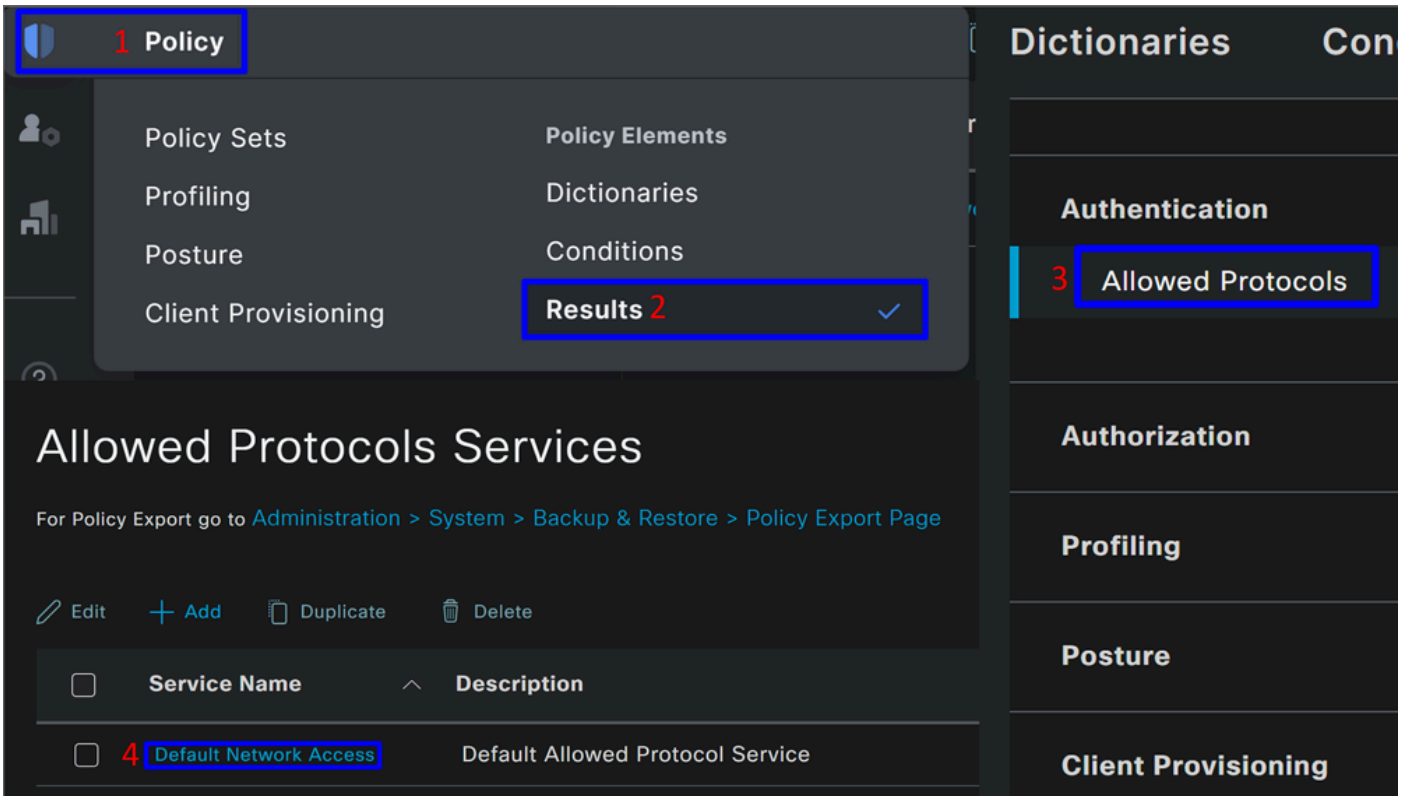
- + قوف رقنا
- ةيلا ام هاندا **Condition Studio** ةحاتملا تامولعملال نمضتتو



- Click to add an attribute قوف رقنا ،طورشلا عاشنال
- رزلا **Network Device** ىلع رقنا
- رايخ **Network Access - Network Device Name** قوف رقنا ،ةيفلخلال تارايخلال تحت





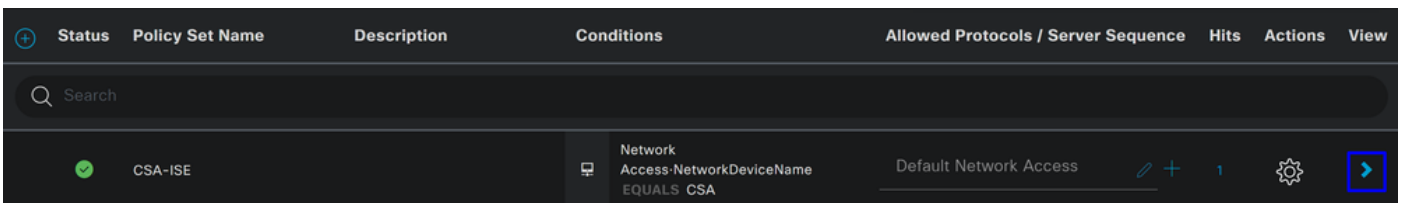


- **Default Network Access** ىلع اه ب حوم س م ل ا ل و ك و ت و ر ب ل ا ع ي م ج ى ل ع ع ا ل ط ا ل ا ك ن ك م ي ، ك ل ذ د ع ب

تاسايس ل ا ة و م ج م ض ي و ف ت ن ي و ك ت

ة: ل ل ا ت ل ا ت ا و ط خ ل ا ب م ق ، **Policy Set** ن م ض ج ه ن ل ا **Authorization** ء ا ش ن ا ل

- > ق و ف ر ق ن ا



- ة: و ر ع م ت ا س ا ي س ل ا **Authorization** ى ر ت ، ك ل ذ د ع ب

Policy Sets → CSA-ISE Click here to do visibility setup [Do not show this again.](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	27
<a href="#">&gt; Authentication Policy(2)</a> <a href="#">&gt; Authorization Policy - Local Exceptions</a> <a href="#">&gt; Authorization Policy - Global Exceptions</a> <span style="border: 1px solid blue; padding: 2px;">&gt; Authorization Policy(7)</span>					

ةوطخل نيوكت جهن ةعومجم نمض ددحمل اسفن وه جهنلا

ليوختلا ةسايس

نيوكت ةوطخل ي ةدحمل ةعومجملا ي ني مدختسمل ليوختب مق، ةالجال هذه ي قرط ةدعب ليوختلا جهن نيوكت كنكمي  
 ك صاخلا ليوختلا جهن نيوكتل لالاتلا لامل اعجار ةعومجم:

Authorization Policy(2)

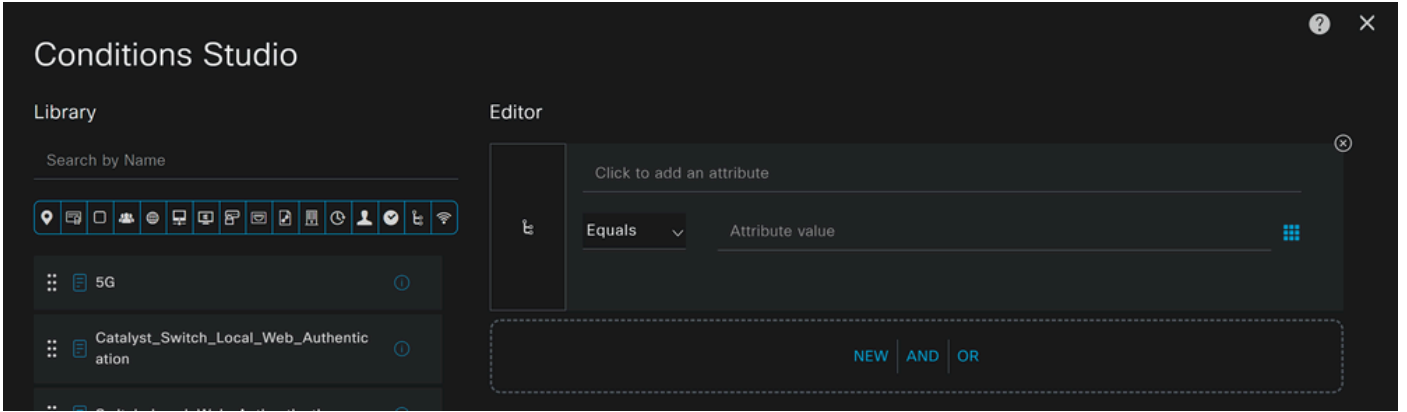
			Results		
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Authorization Rule 1		Select from list	Select from list
+	+	+	+	+	+
+	+	+	+	+	+
+	✓	Authorization Secure Access	InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE	PermitAccess	Select from list

- Authorization Policy قوف رقنا
- لثمل ليوختلا جهن ديحتل + قوف رقنا:

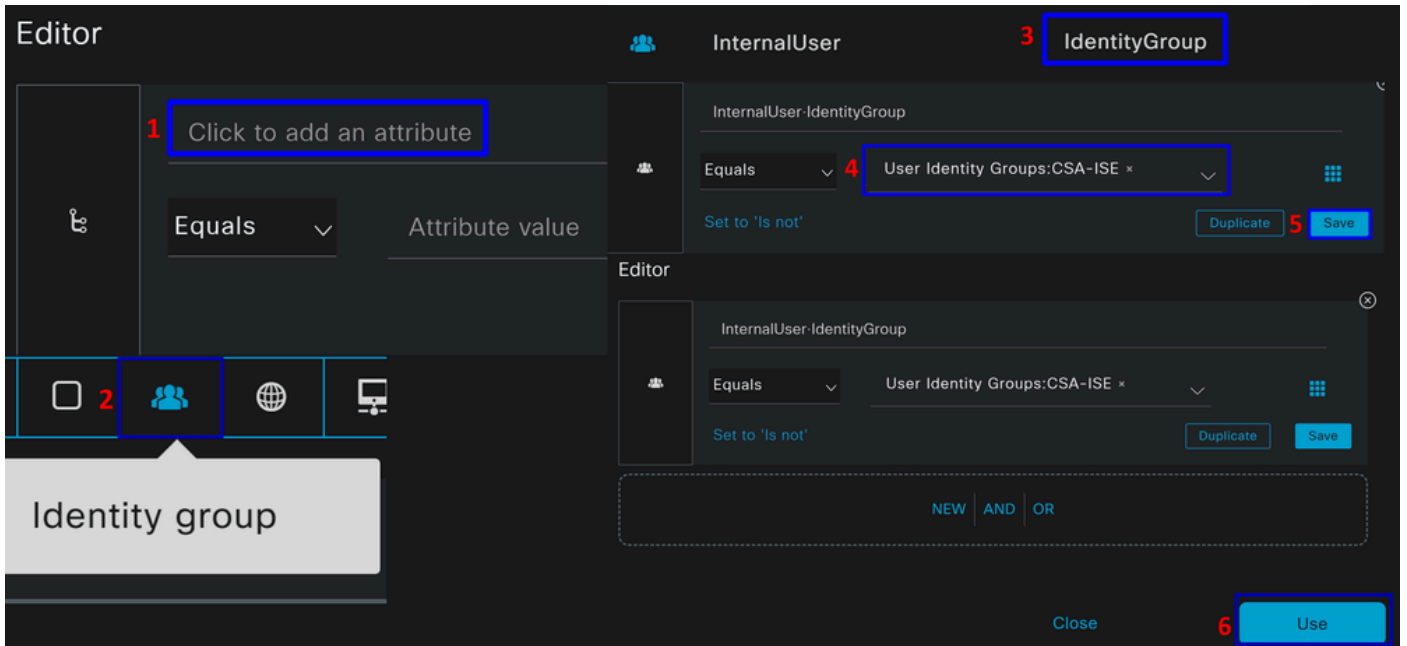
Authorization Policy(2)

			Results		
+	Status	Rule Name	Conditions	Profiles	Security Groups
+	✓	Authorization Rule 1		Select from list	Select from list

- Profiles و Rule Name، ريغيغت ب مق، ةليلال ةوطخلل
- ةلوهسب ليوختلال جهن ديحتل مسان يوكت Name نييعت دنع
- + قوف رونا، مكحتلال رصنع Condition نيوكتل
- تامولعمل دجت Condition Studio، اهتحت



- Click to add an attribute قوف رونا، طورشل ءاشنال
- رزل Identity Group ىلع رونا
- راىخ IdentityGroup - يلخاد مدختسم قوف رونا، هاندأ تاراىخال تحت
- نيوكتب مق، ةوطخلال يف ةقداصلل دمتعمل Group ىلع روثلل ةلدسنملا ةمئاقلا مدختسأ، راىخال Equals تحت [ةعومجم](#)
- Save رونا
- Use رونا



Profiles، which help approve user access under the authorization policy once the user authentication matches the group selected on the policy.

- Profiles قوف رونا لدرسنملا رزلا Authorization Policy تحت
- جي رصت ن ع شحبالا
- PermitAccess دي دحت
- Save رونا

InternalUser-IdentityGroup  
EQUALS User Identity  
Groups:CSA-ISE

Select from list 1

InternalUser-IdentityGroup  
EQUALS User Identity  
Groups:CSA-ISE 2 permit

Profiles

3 PermitAccess

PermitAccess x

DenyAccess

Reset 4 Save

ةلكشم ثودح نود لصتې مدختسملناك اذا امم ققحتلل ةقداصملااب مق .كتسايس Authorization فيرعتب تمق ،كلذ دعب ISE و Secure Access ىلع تالجسلا ةيؤركنكمي ناك اذا امو .

لاصتال او Secure Access ىلع هؤاشنن مت يذلا فيرعتلا فلم مادختس كنكمي ،(VPN) ةيره اظلا ةصاخلا ةكبشلاب لاصتال ل ISE فيرعت فلم مادختساب Secure Client لالخنم .

- ةقداصملا ىلع ةقفاوملا دنع Secure Access يفلجسلا ضرع متي فيكي
  - [نمألا لوصول تامولعم ةحول](#) ىل لقتنا
  - Monitor > Remote Access Log قوف رونا

## 28 Events

User	Connection Event	Event Details	Internal IP Address	Public IP Address	VPN Profile
vpn user (vpnuser@ciscospt.es)	Connected		192.168.50.2	151.248.21.152	ISE_CSA

- ةقداصملا ىلع ةقفاوملا دنع ISE يف لجسلا ضرع متي فيك

◦ Cisco ISE Dashboard ىلا لقتنا

- Operations > Live Logs قوف رقنا

Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles
▼		Identity	Authentication Policy	Authorization Policy	Authorization Profiles
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess
		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> Authorization CSA	PermitAccess

ةقداصملا ىلع ةقفاوملا دنع Duo يف لجسلا ضرع متي فيك

- [يئانثلا قرادا ةجول](#) ىلا لقتنا
- Reports > Authentication Log قوف رقنا

Timestamp (UTC) ▼	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
10:02:34 14 DE ABR. DE 2024	<b>Granted</b> User approved	vpnuser	ISE - SAML	N/A	▼ iOS 17.4.1 AnyConnect 5.0.05207 Flash Not installed Java Not installed Krakow, 12, Poland 83.29.26.111 Endpoint trust is unknown because there are no active Trusted Endpoints Configurations.	▼ Duo Push Apple iPhone 15 Pro Max DPFK77EPVMXGJ7H7TMD3 Krakow, 12, Poland 83.29.26.111

Active Directory يف مدختسم وأ نيي لحملا RADIUS يف مدختسم نيوكت

ISE ةيعضو نيوكت

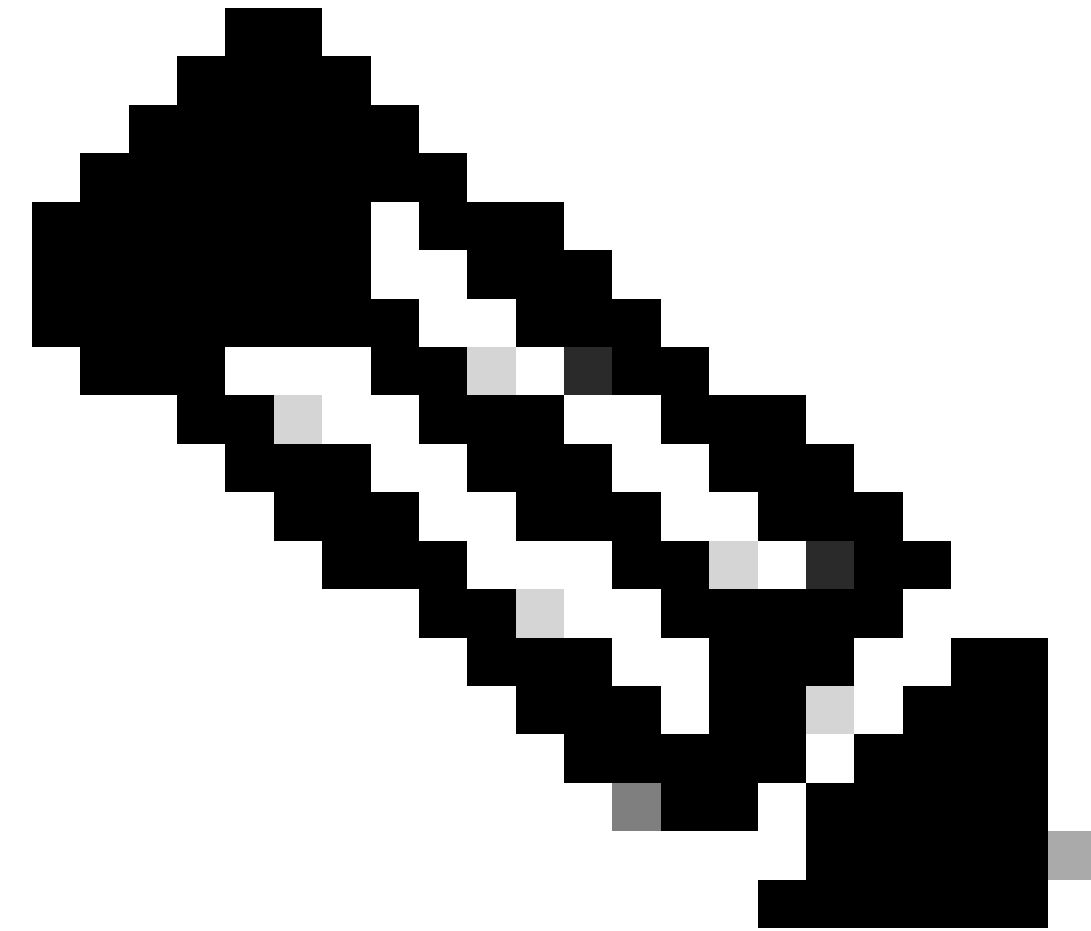
وأ ةيلخادلا دراوملا ىلا لوصولا حنم لبق ةياهنلا ةطقن قفاوت نم ققحتلل نيوكتلا عاشناب مق ،ويرانيسلا اذه يف

هضفر.

ةيلالال تاوطلال لال لقتنا ،هنوكتل

عضولا طورش نوكتل

- ISE تامولعم ةحول لال لقتنا
- **Work Center > Policy Elements > Conditions** قوف رقتنا
- **Anti-Malware** قوف رقتنا





---

ك. ب. ةصاخ لة ي ل خ اد ل ا

---

## Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource

File

Firewall

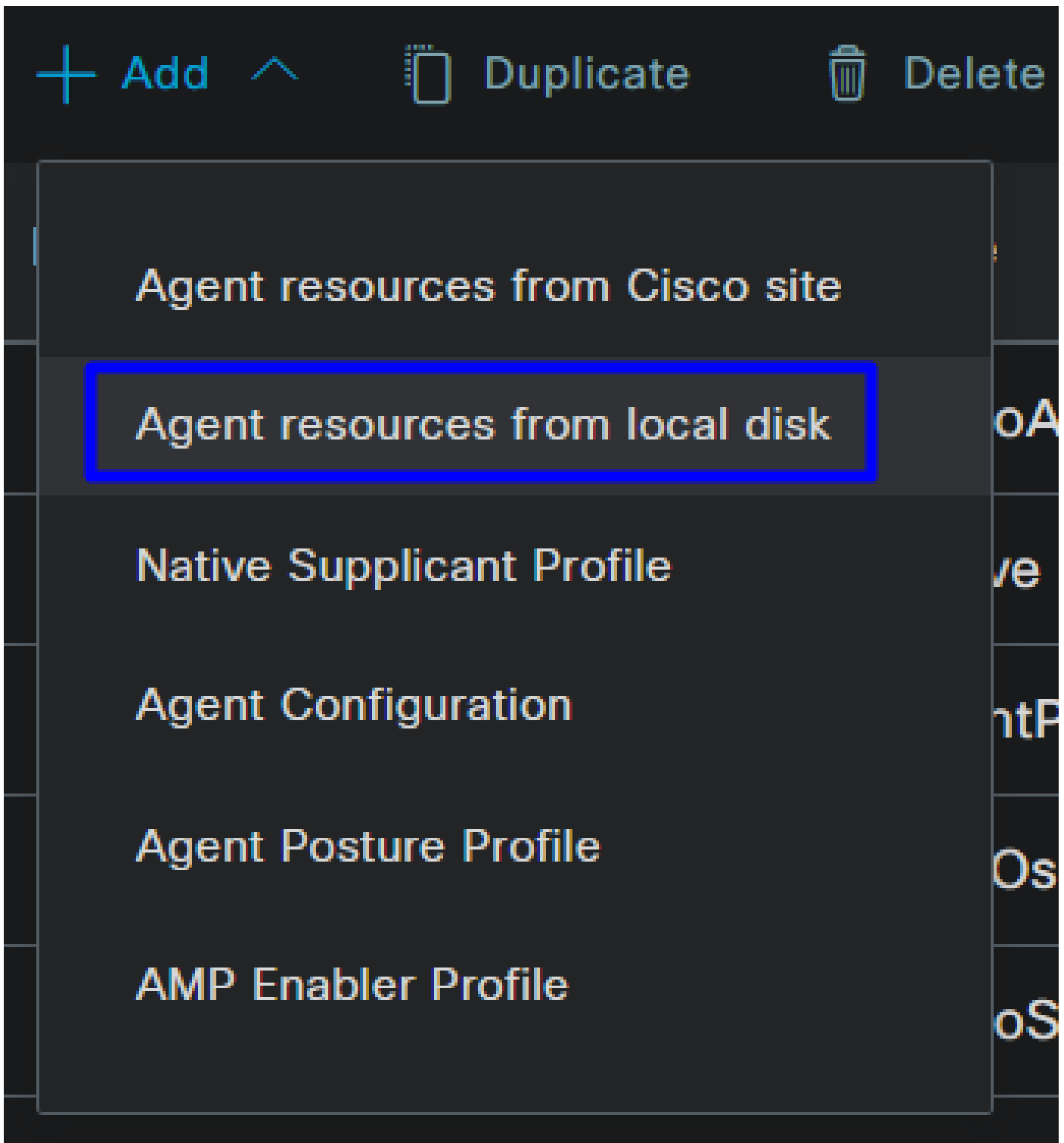
1. Agent Resources	ليعمل لة نم آل بيولا دادم امة مزح.
2. Compliance Module	Cisco ISE Compliance Module سي طمن لل اة ذولا
3. Agent Profile	دادع اة في رعت فلم في مكحت لل.
3. Agent Configuration	نم اهر في فوت م تي ية لل اة طمن لل اة ذولا دي دحت في رعت فلم ما دخت ساب ، دادم اة باوب دادع اة لل اة ذولا ليكول دراوم و ليكول.

### Step 1 اهلاي محت و ليكول دراوم لي زنت

- نأ بجي ؛ بيولا رشن امة مزح لي زنت م قو [Cisco Download Portal](#) لي زنت لخدم ية لل اة ذولا ، دي دج لي م ع دروم اة فاضال .pkg. قيسنت ب بيولا رشن فلم نوكي

Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg <a href="#">Advisories</a>	06-Feb-2024	58.06 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg <a href="#">Advisories</a>	06-Feb-2024	111.59 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>
Cisco Secure Client Headend Deployment Package (Mac OS) - Administrator rights or managed device required for install or upgrade. See Administrator Guide and Release Notes for details. cisco-secure-client-macos-5.1.2.42-webdeploy-k9.pkg <a href="#">Advisories</a>	06-Feb-2024	118.88 MB	<a href="#">↓</a> <a href="#">🛒</a> <a href="#">📄</a>

- مزح لة لي محت م قو Add > Agent resources from local disk + قوف رقنا



Step 2: إضافة قفاوت الة دحو ليزنت

- + Add > Agent resources from Cisco Site



Add



Duplicate



Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- Save قوف رقناو ةبولطم قفاوت ةدحول لكل رايتخالا ةناخ ىلع ةمالع عض

# Download Remote Resources

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3064.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleLinux64 4.3.3104.0	Cisco Secure Client Linux Compliance Module 4.
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3432.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleOSX 4.3.3472.6400	Cisco Secure Client OSX Compliance Module 4.3
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3940.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindows 4.3.3980.8192	Cisco Secure Client Windows Compliance Modul
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3940....	Cisco Secure Client WindowsARM64 Compliance
<input type="checkbox"/>	AnyConnectComplianceModuleWindowsARM64 4.3.3980....	Cisco Secure Client WindowsARM64 Compliance

For Agent software, please download from <http://cisco.com/go/ciscosecureclient>. Use the "Agent resource from local disk" add option, to import into ISE

Cancel

Save

ليكول فيرعت فلم نيوكت 3 Step

- قوف رقنا + Add > Agent Posture Profile

+ Add ^

☰ Duplicate

🗑️ Delete

Agent resources from Cisco site

Agent resources from local disk

Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile

- **Posture Profile** ل Name اءاشن

# Agent Posture Profile

Name \*



Description:

- كلذ دعب Save ةق طقو \* عض ،مداخل مسا دعاوق تحت

Posture Protocol		
Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay ⓘ	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit ⓘ	4	Number of retries allowed for a message.
Discovery host ⓘ		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List ⓘ	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules * ⓘ	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com*
Call Home List ⓘ		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer ⓘ	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

## Step 4 لېكول نېوك ت نېوك ت

- قوف رقا + Add > Agent Configuration



+ Add ^

📄 Duplicate

🗑 Delete

Agent resources from Cisco site

Agent resources from local disk


Native Supplicant Profile

Agent Configuration

Agent Posture Profile

AMP Enabler Profile


- في الخطوات التالية، نحتاج إلى إعداد ملف التكوين، لذلك دعنا:

\* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

\* Configuration Name:

Description:

### Description Value Notes

\* Compliance Module CiscoSecureClientComplianceModuleWi 

## Cisco Secure Client Module Selection

ISE Posture	<input checked="" type="checkbox"/>
VPN	<input type="checkbox"/>
Zero Trust Access	<input type="checkbox"/>
Network Access Manager	<input type="checkbox"/>
Secure Firewall Posture	<input type="checkbox"/>
Network Visibility	<input type="checkbox"/>
Umbrella	<input type="checkbox"/>
Start Before Logon	<input type="checkbox"/>
Diagnostic and Reporting Tool	<input type="checkbox"/>

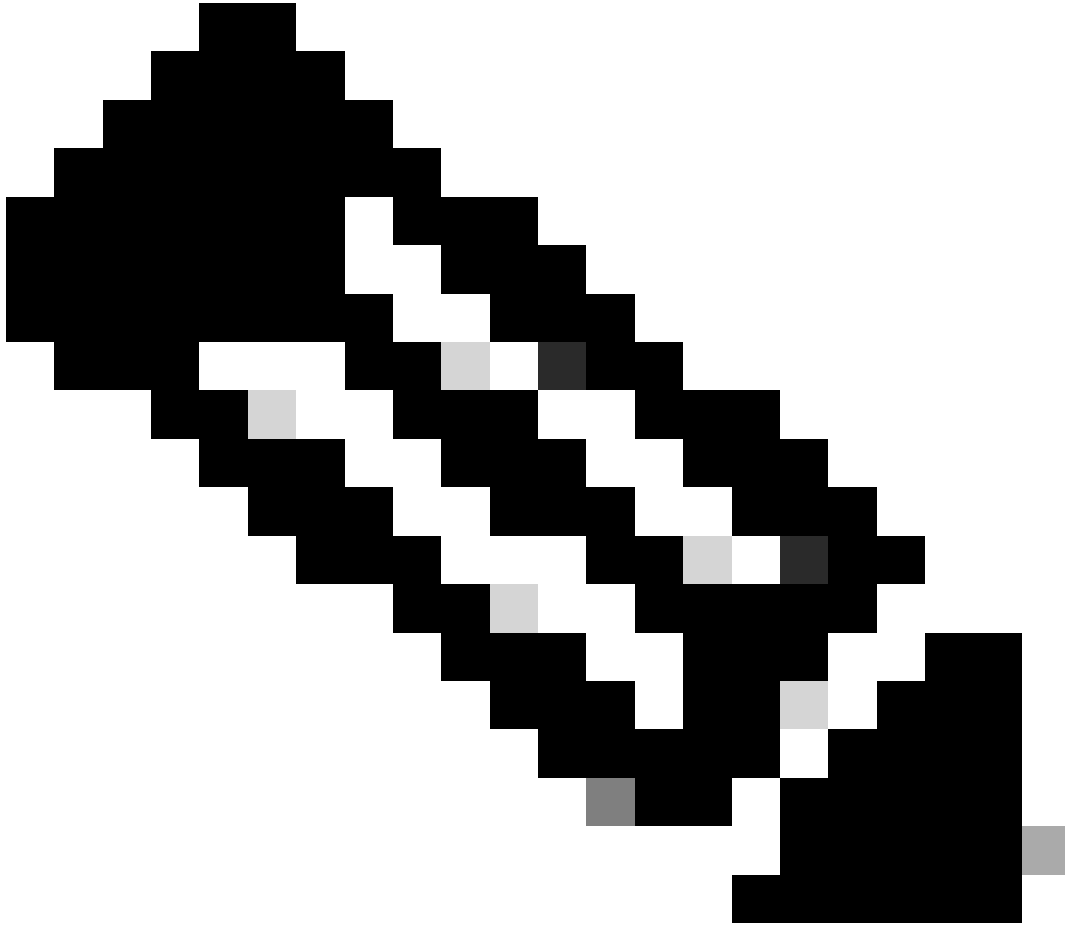
## Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- [اهلي محتول لي محتول لاي كود راوم لي زنت 1 ة و طخل لاي](#) يلع اهل لي محت مت ي تال ة م زحل رتخأ : Select Agent Package
- **Configuration Name:** يلع فر عت لل مسا را ي تخأ
- **Compliance Module:** [ق فاوت لاي ة د ح و ل ي زنت ب مق 2 ة و طخل لاي](#) يلع اهل ي زنت مت ي تال ق فاوت لاي ة د ح و رتخأ
- Cisco Secure Client Module Selection
  - **ISE Posture:** را ي تخال ة ناخ يلع ة مال ع عضو
- **Profile Selection**

• [ليكوليا فيرعت فلم نيوكت 3 قوطخللا](#) ىلع هنيوكت مت يذلا ISE فيرعت فلم رتخأ: ISE Posture

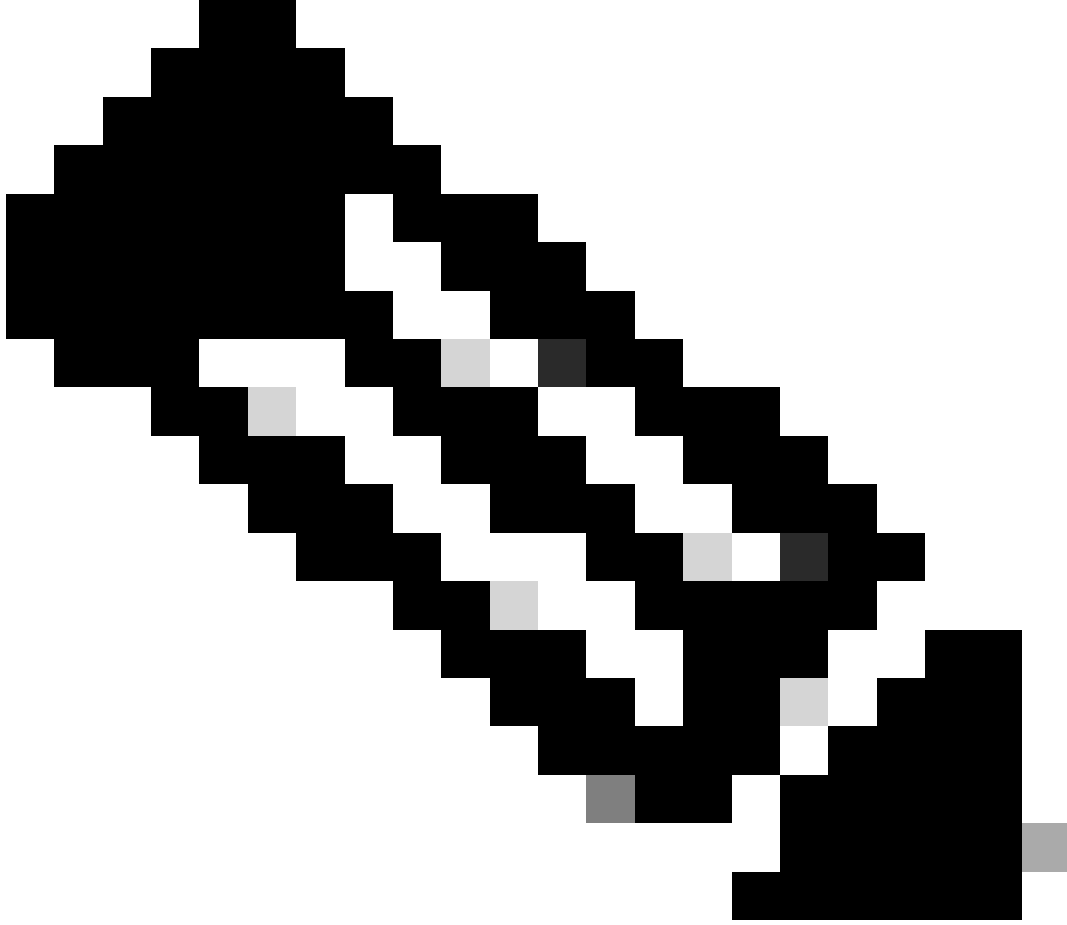
- Save رقنا



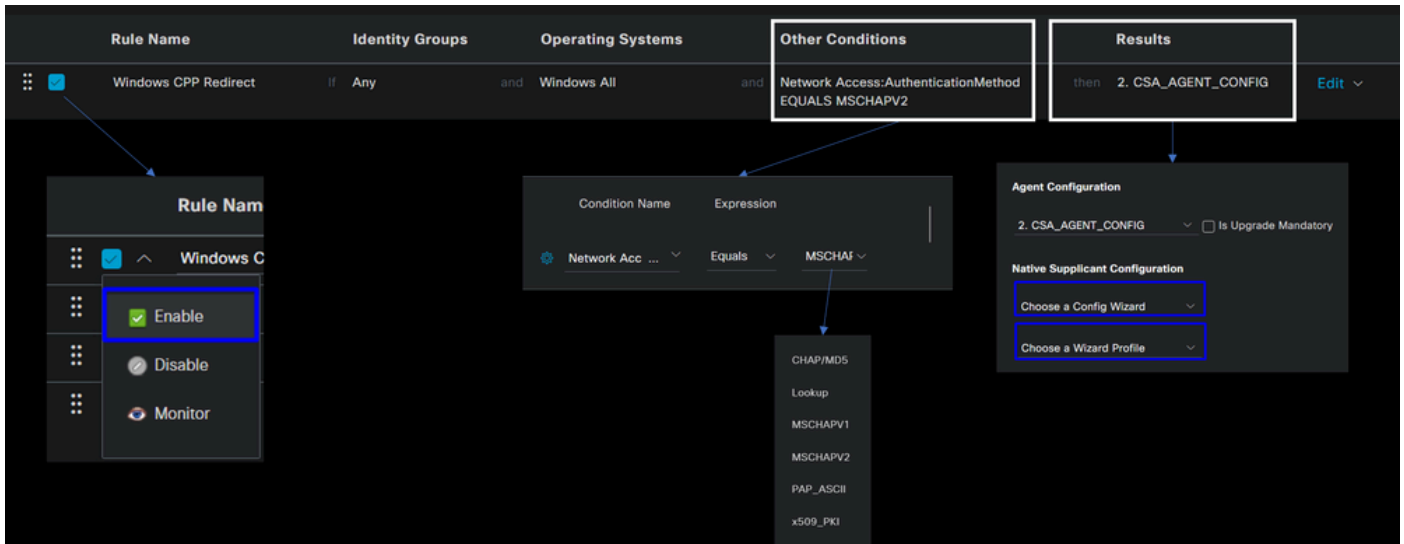
لقتسم دحاو ليمع نيوكت، Linux أو Mac OS أو Windows، ليغشت ماظن لكل نوكي ناب ىصوي: ةظحالم

نيوكت كمزلي، ةريخألا ةوطخالا في اهنيوكت مت يتلا ةيظمنلا تادحولاو (ISE) ةيوهلا تامدخ كرحم ةيعضو دادع| دادع| نيكمتل دادمإلا عاشنإل جهن.

- ISE تامولعم ةحول ىلا لقتنا
- **Work Center > Client Provisioning** قوف رقنا



ةدحاو ليمع نيوكت ةسايس، Linux أو Mac OS أو Windows، ليغشت ماظن لكل نوكتي نأب ىصوي: ةظحالم



- **Rule Name:** هله سه قيرط لعل لوصحلل لوهاله عومجم ديدحت وزاهجلا عون لى ادا نسا ةسايسلا مسا نيوكت جهن لك فيرعتل
- **Identity Groups:** ةسايسلا لعل اهم يقيقت ديرت يتلا تايوهاله رتخأ
- **Operating Systems:** ةوطخلال في ةدحمالا ةلويكولا جم انربلا ةمزح لى ادا نسا ليغششلا ماظن رتخأ [قمح ددح](#)، ةوطخلال [جم انربلا](#)
- **Other Condition:** لعل انه نيوكت مت يتلا ةقيرطال **Authentication Method** EQUALS **Network Access** لى ادا نسا رتخأ، ةوطخلال اغراف رمأل كرت كنكمي وأ [RADIUS](#) [عومجم ةفاضلا](#)، ةوطخلال
- **Result:** [ليكولا نيوكت 4 ةوطخلال](#) في هنيوكت مت يذلا ليكولا نيوكت رايتخا
  - **Native Supplicant Configuration:** [Config Wizard](#) و [Wizard Profile](#) رايتخا
- رايتخالال ةناخ في نكممك هجاردا متي مل اذا جهنلا لعل "نكمم" ةمالع عضو

ليوختلا تافيصوت عاشنا

نم ققحتلا بجي. ةقداصلما ريرمت دعب ني مدختسما لى عضو لعل ءانب دراوملا لى لوصولا ليوختلا فيرعت فلم ددحي عضو لى ادا نسا اه لى لوصولا مدختسما لى نكمي يتلا دراوملا ديدحتل صيخرتلا

فيريقت فلم ليوختلا	فصولا
نعذم	عضولا نم ققحتلا مت - ليكولا تيبتت مت - مدختسما عم قفاوتم

فروع م ريغ قفاوتل	- ليلكولا تيبتتل هيچوتلا ةداغ - فروع مالا مدختسم لال عم قفاوتم ققحتلا دي ق عصولا
DenyAccess	لوصول اض فر - قفاوتم ريغ مدختسم

ISE تامولعم ةحول لال لقتنا، (DACL) ةيساسال ةينبال لوصولا يف مكحتلا ةمئاق نيوكتل

- Work Centers > Policy Elements > Downloadable ACLs قوف رقنا
- +Add قوف رقنا
- Compliant DACL ءاشن

\* Name **CSA-Compliant**

Description

IP version  IPv4  IPv6  Agnostic ⓘ

* DACL Content	Content
1234567	permit ip any any
8910111	
2131415	
1617181	
9202122	
2324252	
6272829	
3031323	
3343536	
3738394	
...	

- Name: DACL عم قفاوتل لال ريشي امسا فضا
- IP version: رتخا IPv4
- DACL Content: ةمئاق ءاشن لوصولا هيئت (DACL) ليزنلل ةلباق لوصولا يف مكحت ةمئاق ءاشن

<#root>

permit ip any any

فروع مالا ريغ قفاوتلاب ةصاخلا (DACL) لوصولاب مكحتلا ةمئاق ئشن أو Save رقنا

- قوف رقننا Work Centers > Policy Elements > Downloadable ACLs
- +Add قوف رقننا
- Unknown Compliant DACL ءاشننا

**\* Name** CSA\_Redirect\_To\_ISE

**Description**

**IP version**  IPv4  IPv6  Agnostic ⓘ

* DACL Content	
1234567	permit udp any any eq 67
8910111	permit udp any any eq 68
2131415	permit udp any any eq 53
1617181	permit tcp any host 192.168.10.206 eq 8443
9202122	permit tcp any any eq 80
2324252	
6272829	
3031323	
3343536	
3738394	

✓ Check DACL Syntax

- **Name:** فورعمل رېغ DACL عم قفاوتللا ىللا رېشې امسا فضا
- **IP version:** رتخا IPv4
- **DACL Content:** ادوحم الوصو يقطع يتلا (DACL) ةيساسألا ةينبلا ىللا لوصولو يف مكحت ةمئاق ءاشناب مق 8443 ذفنملا ربع دادملا لخدمو HTTP و DNS و DHCP و ةكبشلا ىللا

```

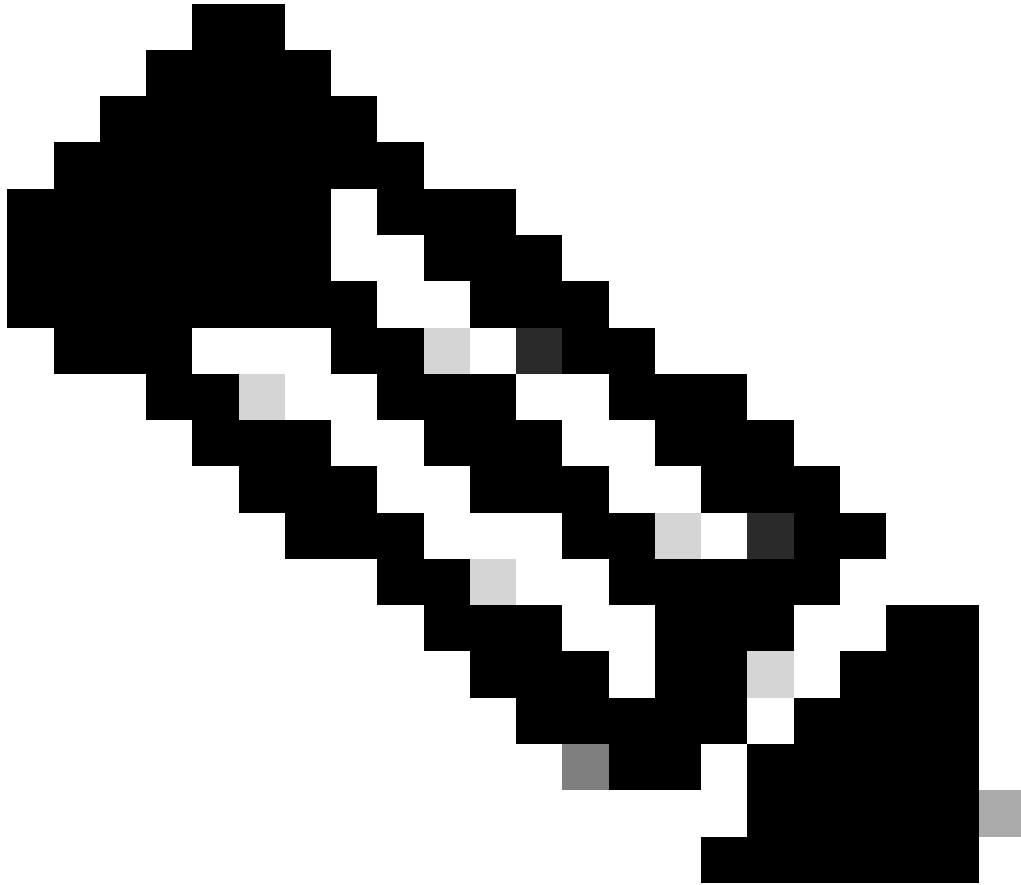
permit udp any any eq 67
permit udp any any eq 68
permit udp any any eq 53
permit tcp any any eq 80

```



```
permit tcp any host 192.168.10.206 eq 8443
```

---



م تي و Cisco، ن م (ISE) ة ي و ه ل ا ت ا م د خ ك ر ح م م د ا خ ع م 192.168.10.206 IP ن ا و ن ع ق ف ا و ت ي ، و ي ر ا ن ي س ل ا ا ذ ه ي ف : ة ظ ح ا ل م 8443 ذ ف ن م ل ا ر ب ع IP 192.168.10.206 ن ا و ن ع ي ل ا TCP ر و ر م ة ك ر ح ن ا ي ن ع ي ا ذ ه . د ا د م ا ل ا ل خ د م ل 8443 ذ ف ن م ل ا ص ي ص خ ت د ا د ع ا ل ا ل خ د م ي ل ا ل و و ص و ل ا ل ه س ي ا م م ، ا ه ب ح و م س م .

---

ل ي و خ ت ل ا ف ي ر ع ت ا ت ا ف ل م ء ا ش ن ا ل ة ب و ل ط م ل ا (DACL) ذ ف ن م ل ا ب ة ص ا خ ل ا ل و و ص و ل ا ي ف م ك ح ت ل ا ة م ئ ا ق ك ي د ل ، ة ط ق ن ل ا ه ذ ه د ن ع ل ISE ت ا م و ل ع م ة ح و ل ي ل ا ل ق ت ن ا ، ل ي و خ ت ل ا ف ي ر ع ت ا ت ا ف ل م ن ي و ك ت ل

• [Work Centers](#) > [Policy Elements](#) > [Authorization Profiles](#)

• [+Add](#) قوف رقنا

• [Compliant Authorization Profile](#) ءاشن

## Authorization Profile

\* Name

CSA-Compliant

Description

\* Access Type

ACCESS\_ACCEPT

Network Device Profile



Cisco



Service Template

Track Movement



Agentless Posture



Passive Identity Tracking



## Common Tasks

DACL Name

CSA-Compliant

IPv6 DACL Name

ACL

ACL ID (Filter ID)

- **Name:** قفاوتم لايوختلا فيرعت فلم ىل ريشي مسا عاشن |
- Access Type: ACCESS\_ACCEPT رتخ |

- **Common Tasks**





- **DACL NAME:** في مكحتلا عمئاق رايتخ | طئاسولل لوصوللا في مكحتلا عمئاق رايتخ | [عمئاق قفاوتم لايوختلا \(DACL\)](#) طئاسولل لوصوللا

Unknown Authorization Profile ئشن أو Save رقنا

- Work Centers > Policy Elements > Authorization Profiles قوف رقنا
-

+Add قوف رقنا

- Uknown Compliant Authorization Profile ءاشننا

* Name	CSA-Unknown-Compliant
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	 Cisco
Service Template	<input type="checkbox"/>
Track Movement	<input type="checkbox"/> 
Agentless Posture	<input type="checkbox"/> 
Passive Identity Tracking	<input type="checkbox"/> 

Common Tasks

<input checked="" type="checkbox"/> DACL Name	CSA_Redirect_To_ISE
---	---------------------



**redirect** وه رشننل تاي لمع عي مجل Secure Access يلع هي جوتللا ةداعل لوصولا يف مكحتللا ةمئاق مسا :ةظحالم

Attributes Details تحت لثامم عيش كي دل نوكي نأ بجي ،ميقلا هذه لك فيرعتب موقت نأ دعب

```
Attributes Details
Access Type = ACCESS_ACCEPT
DAACL = CSA_Redirect_To_ISE
cisco-av-pair = url-redirect-acl=redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=
&action=cpp
```

ةةلالتل ةوطخلل ةعباتم ونيوكتللا ءاهنل Save رقنا

عضولآ جهن ةعوم جم نيوكت

ال كنأل و DenyAccess: اهن نيوكتب تمق يتلآ ليوختلآ فيرعت تافللم لآ اءاشن اب موقت يتلآ ةثالثلآ جهنلآ هذه دن تست ىرأ ةدحاو ءاشن آل آاتحت

ليوختلآ - جهنلآ ةعوم جم	ليوختلآ فيرعت فللم
نعذم	<a href="#">قفاوتم - ليوختلآ فيرعت فللم</a>
قفاوتملآ فسورعم ريغ	<a href="#">عم قفاوتم - ضيوفتلآ فيرعت فللم</a> <a href="#">UNKNOWN</a>
قفاوتم ريغ	<a href="#">DenyAccess</a>

ISE تامولعم ةحول لآ لقتنا

- Work Center > Policy Sets قوف رقنا
- هئاشناب تمق يذلا جهنلا ىلا لوصولل > قوف رقنا

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Search						
✓	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370	⚙️	➔

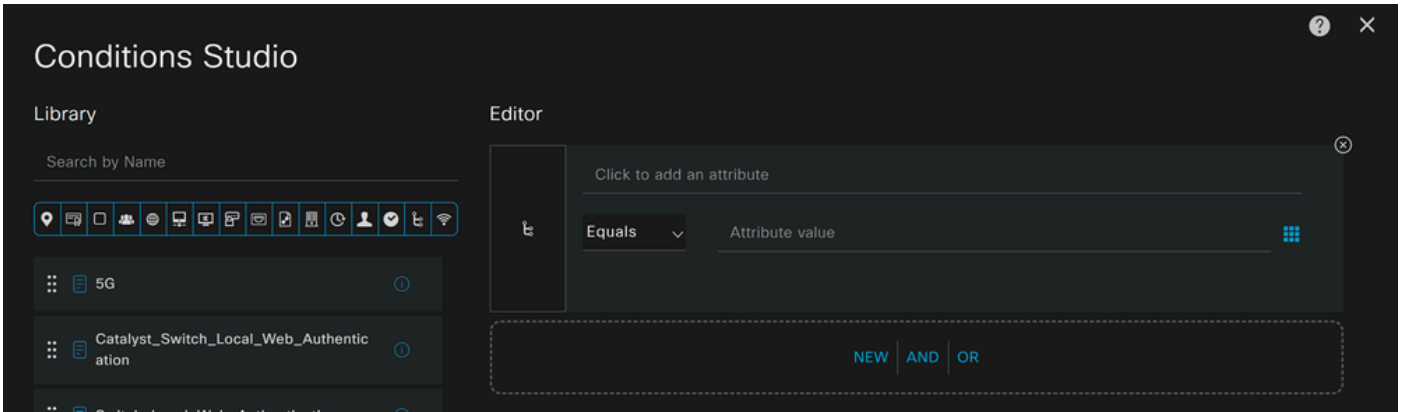
- Authorization Policy قوف رقنا

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
+	Search				
✓	CSA-ISE		Network Access-NetworkDeviceName EQUALS CSA	Default Network Access	370
> Authentication Policy(2)					
> Authorization Policy - Local Exceptions					
> Authorization Policy - Global Exceptions					
> Authorization Policy(4)					

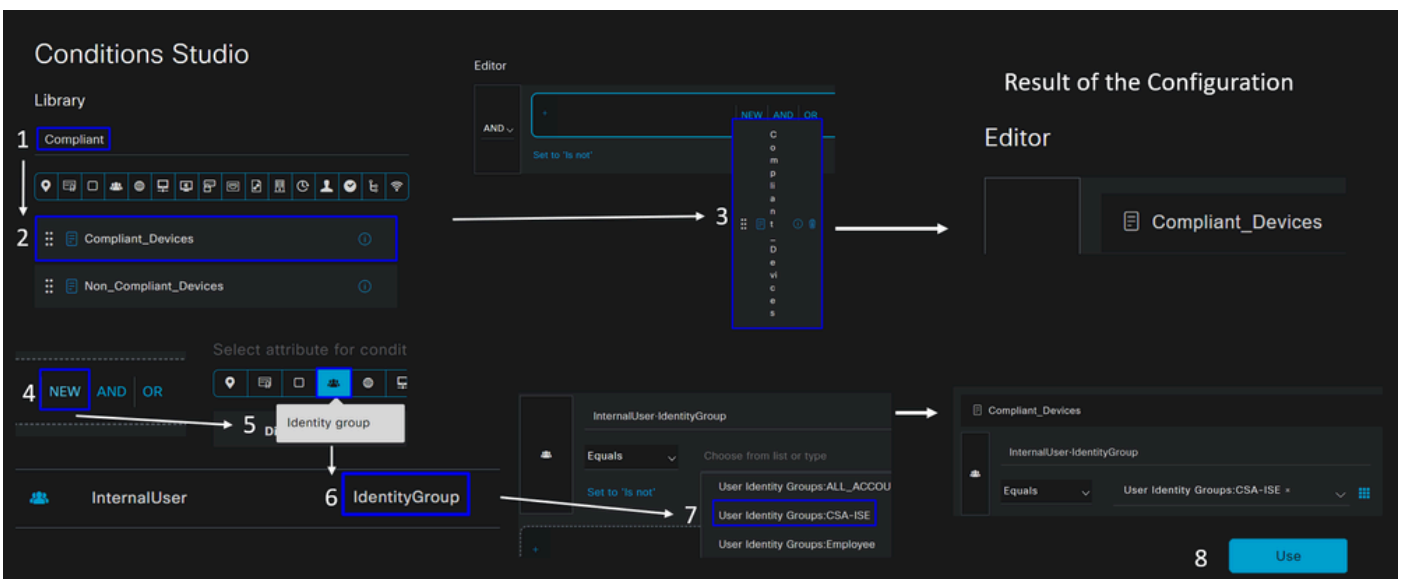
- هئاشناب تمق يذلا جهنلا ىلا لوصولل > قوف رقنا







- **compliant** نع شحبا، طارشلا عاشنإل
- **Compliant\_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **New** لوخدل Editor لفسأ رقنا
- **Identity Group** ىلع رقنا
- **Internal User Identity Group** رتخا
- **Equals** تحت هتقباطم ديرت يذلا **User Identity Group** رتخا
- **Use** رقنا



- ةيلالات ةروصل لكيدل ، ةجيتنك

The screenshot shows a configuration rule with a green checkmark on the left. The rule name is 'SAML-Compliant'. The operator is 'AND'. There are two conditions: 'Compliant\_Devices' (with a list icon) and 'InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE' (with a user icon).

- [في رعت فلم](#) ، ةوطخلال يلع نوكملا يوكشلا ليوخت في رعت فلم رتخاو لدس نم لارزلا تحت رقنا **Profile** تحت [قفاوتم ليوخت](#)

This screenshot is identical to the previous one, but it includes a grey button labeled 'CSA-Compliant' on the right side of the rule configuration area.

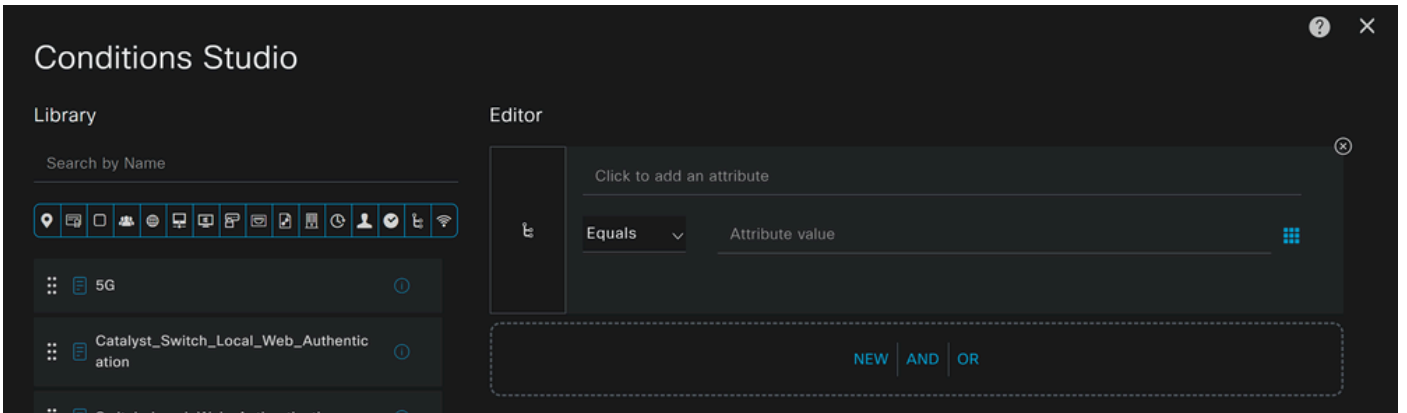
دقلا **Compliance Policy Set** نيوكتب نألا تمق دقلا

- : ةسايسلا **CSA-Unknown-Compliance** ديحتل + رقنا

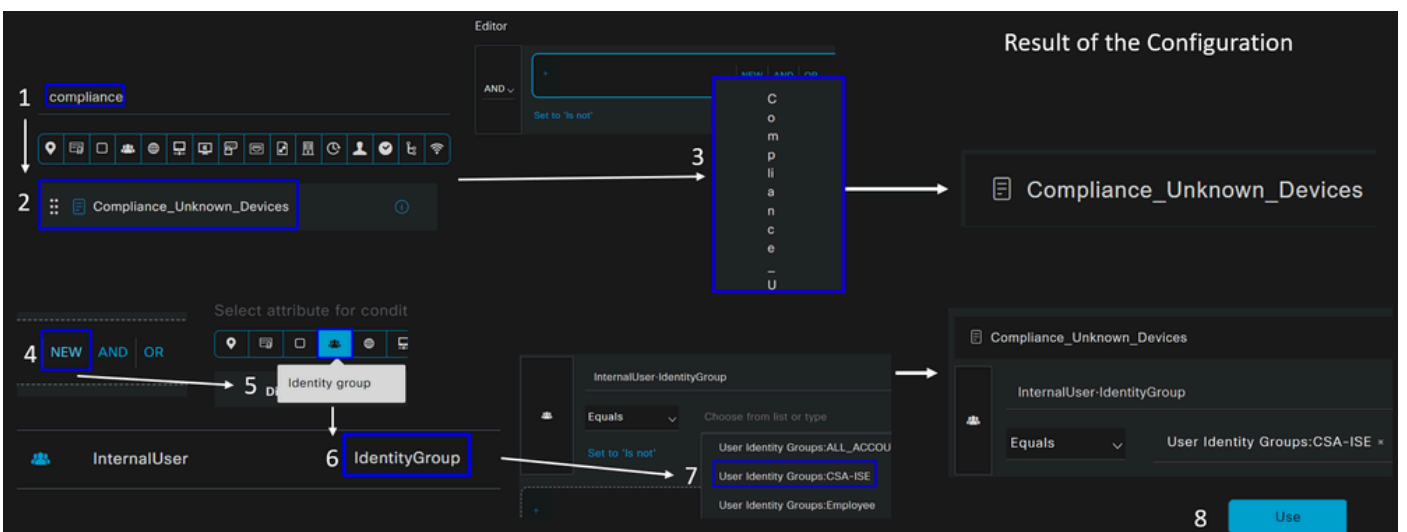
The screenshot shows a table with the following columns: Status, Rule Name, Conditions, Profiles, and Security Groups. The first row has a green checkmark in the Status column, 'Authorization Rule 1' in the Rule Name column, a plus sign in the Conditions column, 'Select from list' in the Profiles column, and 'Select from list' in the Security Groups column. There is also a search bar at the top left of the table.

- Profiles و ةوطخلل Rule Name، Conditions و ريوختب مق ، ةيلالات ةوطخلل

- CSA-Unknown-Compliance إلى نيوكتال Name مس ا ن ي ي ع ت د ن ع
- + قوف ر ق ن ا ، م ك ح ت ل ا ر ص ن ع Condition ن ي و ك ت ل
- ت ا م و ل و ع م ل ا د ج ت Condition Studio ، ا ه ت ح ت :



- compliance ن ع ش ح ب ا ، ط ر ش ل ا ع ا ش ن ا ل
- Compliant\_Unknown\_Devices ت ض ر ع د ق ن و ك ت ن ا ب ج ي
- Editor ت ح ت ت ا ل ف ا ل ا و ب ح س ل ا
- New ل و خ د ل Editor ل ف س ا ر ق ن ا
- Identity Group ي ل ع ر ق ن ا
- Internal User Identity Group ر ت خ ا
- ه ت ق ب ا ط م د ي ر ت ي ذ ل ا User Identity Group ر ت خ ا ، Equals ت ح ت
- Use ر ق ن ا



- ةيلات ال ةرول ال كيدل ،ةجيتنك

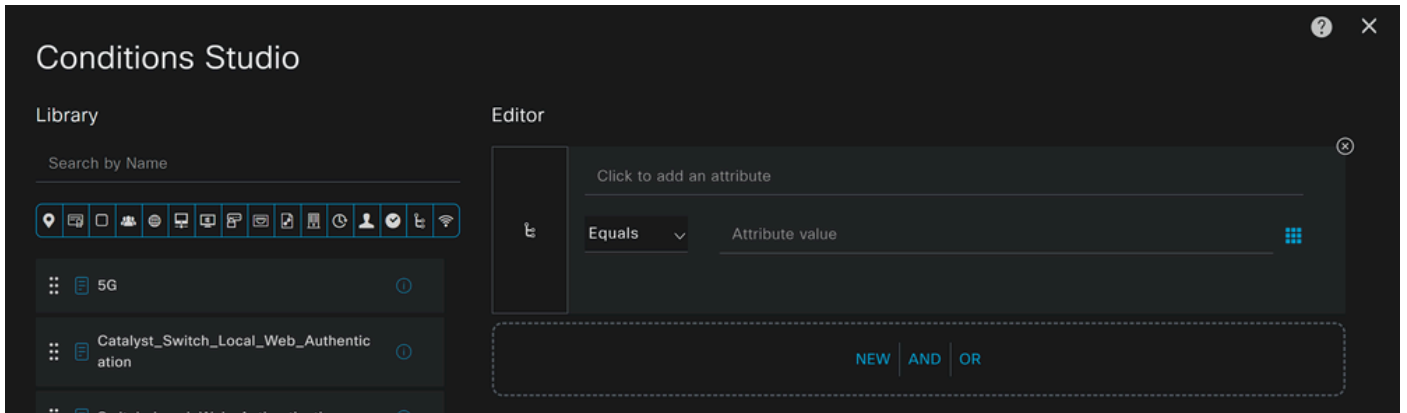
- [فيريعة فليم](#) ،ةوطخال ال يلع نوكم ال يوكشال ليوخت فيرعة فلم رتخاو لدس نمل رزلا تحت رقن ال Profile تحت [قفاوتم فوعم ريغ ليوخت](#)

Unknown Compliance Policy Set. نيوكت ب نالآ تمق دقل

- ةسايس ال CSA- Non-Compliant ديحتل + قوف رقنا

- ةيلات ال ةوطخلل Rule Name، Conditions و Profiles ريغيغت ب مق ،ةيلات ال ةوطخلل

- **CSA-Non-Compliance** إلى نيوكتال Name مسان يي عت دن ع
- + قوف رونا، مكحتال رصن **Condition** نيوكتال
- تامولعمل دجت **Condition Studio**، اهتحت



- **non** ن ع شحبا، طارشال عاشنال
- **Non\_Compliant\_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **New** لوخدال Editor لفسأ رونا
- ةنوقيال **Identity Group** ل ع رونا
- **Internal User Identity Group** رتخا
- هتقباطم ديرت يذال **User Identity Group** رتخا، **Equals** تحت
- **Use** رونا

Library

1 non

2 Non-Compliant\_Devices

Editor

3 AND

4 NEW AND OR

5 Identity group

6 IdentityGroup

7 Equals

8 Use

Result of the Configuration

Non-Compliant\_Devices

Non-Compliant\_Devices

InternalUser-IdentityGroup

InternalUser-IdentityGroup

Equals

User Identity Groups:ALL\_ACCOU

User Identity Groups:CSA-ISE

User Identity Groups:Employee

- ةيلات ةروصل ال كيدل ، ةجيتنك

✓ SAML-Non-Compliant

AND

Non-Compliant\_Devices

InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE

- DenyAccess يوكشال ليوخت فيرعت فلم رتخاو لدسنم الزلا تحت رونا Profile تحت

✓ SAML-Non-Compliant

AND

Non-Compliant\_Devices

InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE

DenyAccess

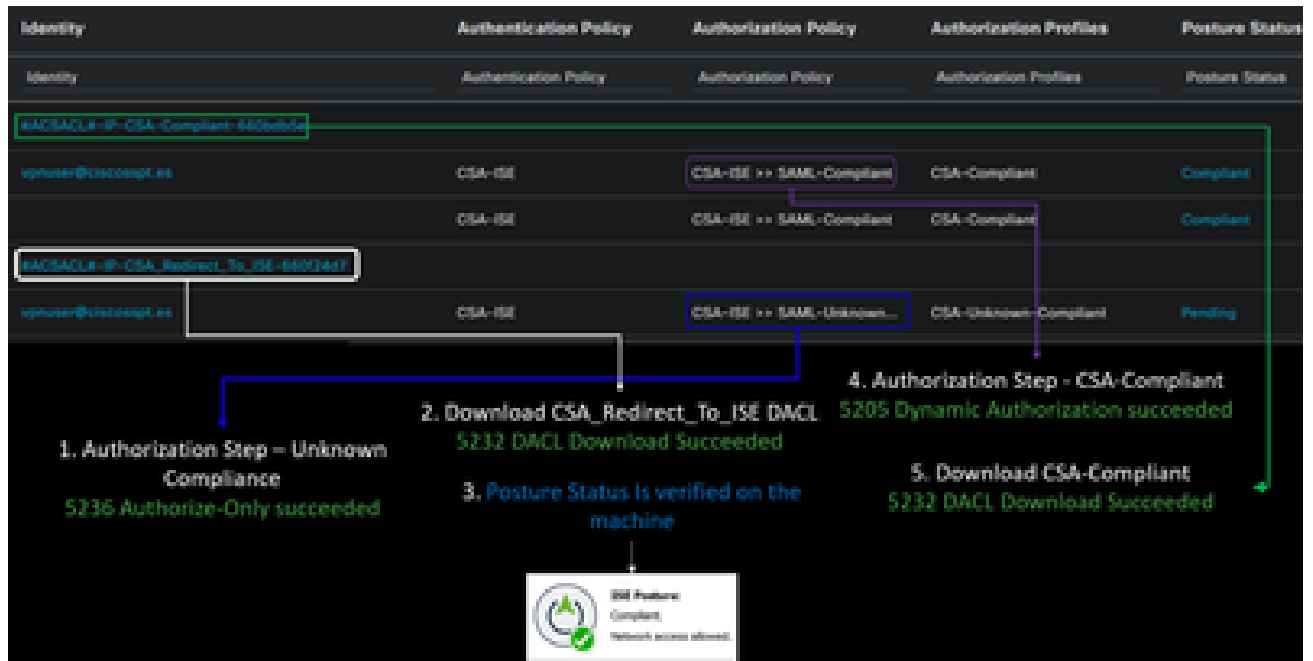
عضولوا عم لمكثال رابتخال ازهاج حبصت ، ةثالثل تافيصوتال نيوكت ةاهان | درجب

ةحصلا نم ققحتلا

عضولا نم ققحتلا

زاهجلا لعل لاصتالا

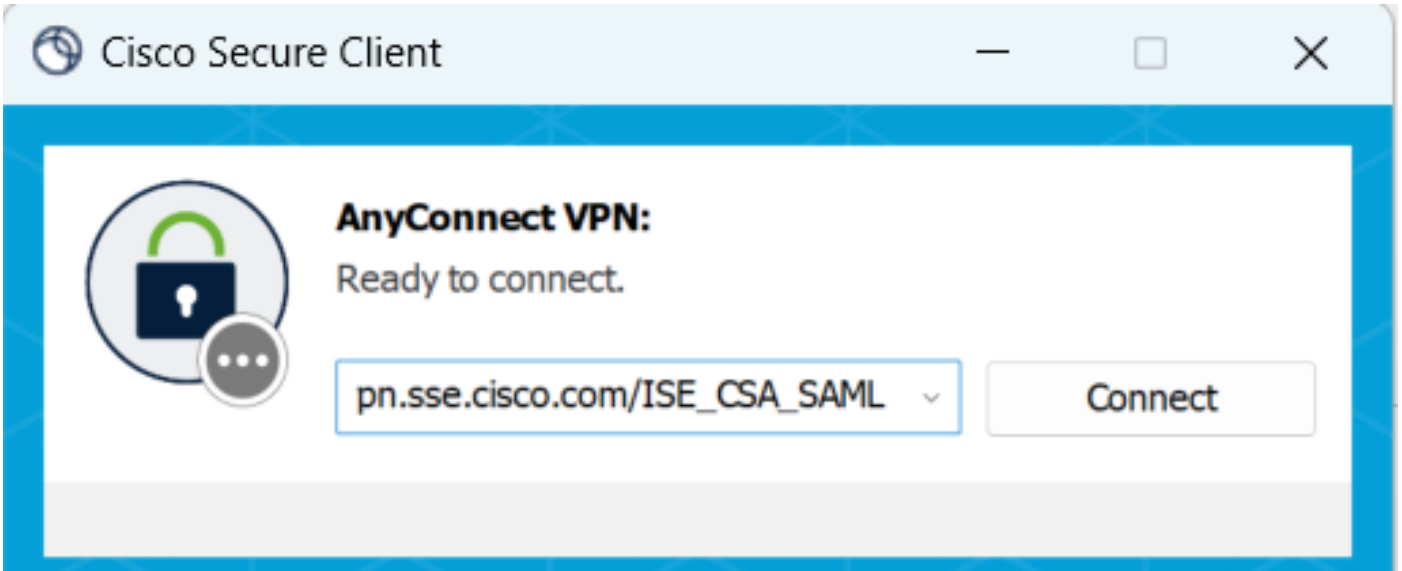
Secure Client ربع نم آلا لوصوللا لعل دوزملاو كبا صاخلا RA-VPN لاجمب لاصتالا



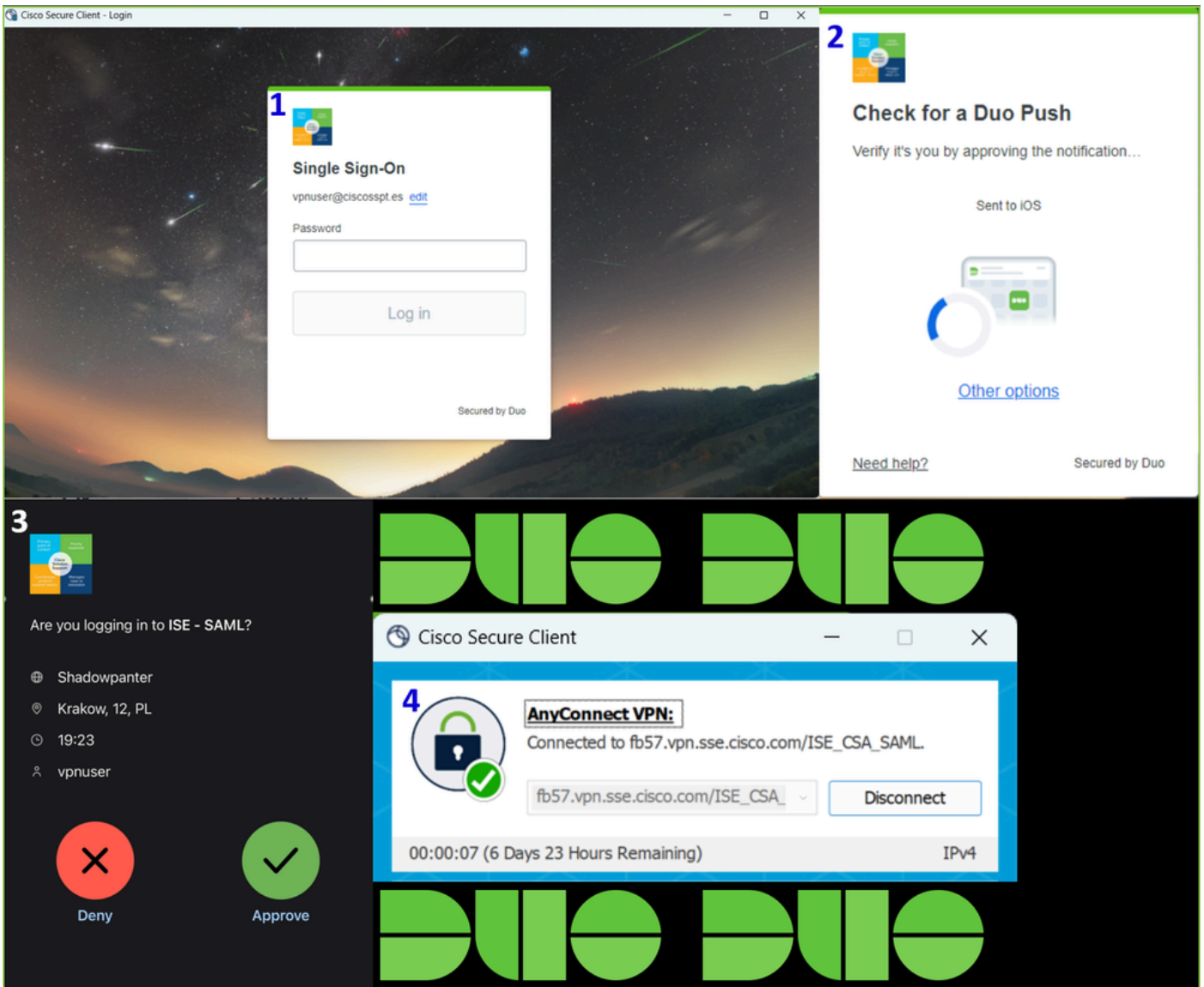
ةوطخلا هذهل ةيظم نلا ISE ةدحو تيبثت مدع بجي: ةظحالم

1. Secure Client مادختساب لاصتالا.





2. Duo ربيع ةقداصل لل دامت عال تانايب ريفوت .



3. رمأل نكي مل اذاو ISE: لى كهيحوت ةداع| متت ام ابلاغو (VPN) ةيرهاطلا ةصاخلا ةكبشلاب كلصوت متي ، ةطقنلا هذه دنع .  
لكذك http:1.1.1.1 لى لىقننتلا ةلواحم كنكمي ،



Cisco Secure Client



AnyConnect VPN

Connected: ISE\_CSA - IKEv2 - Auto Select  
Nearest Location

InPrivate

Device Security Check



Not secure

https://ise.ciscospt.es:8443/portal/PortalSetup.action?portal=d9276eb2-c440-42d6-8055-3c72ed4

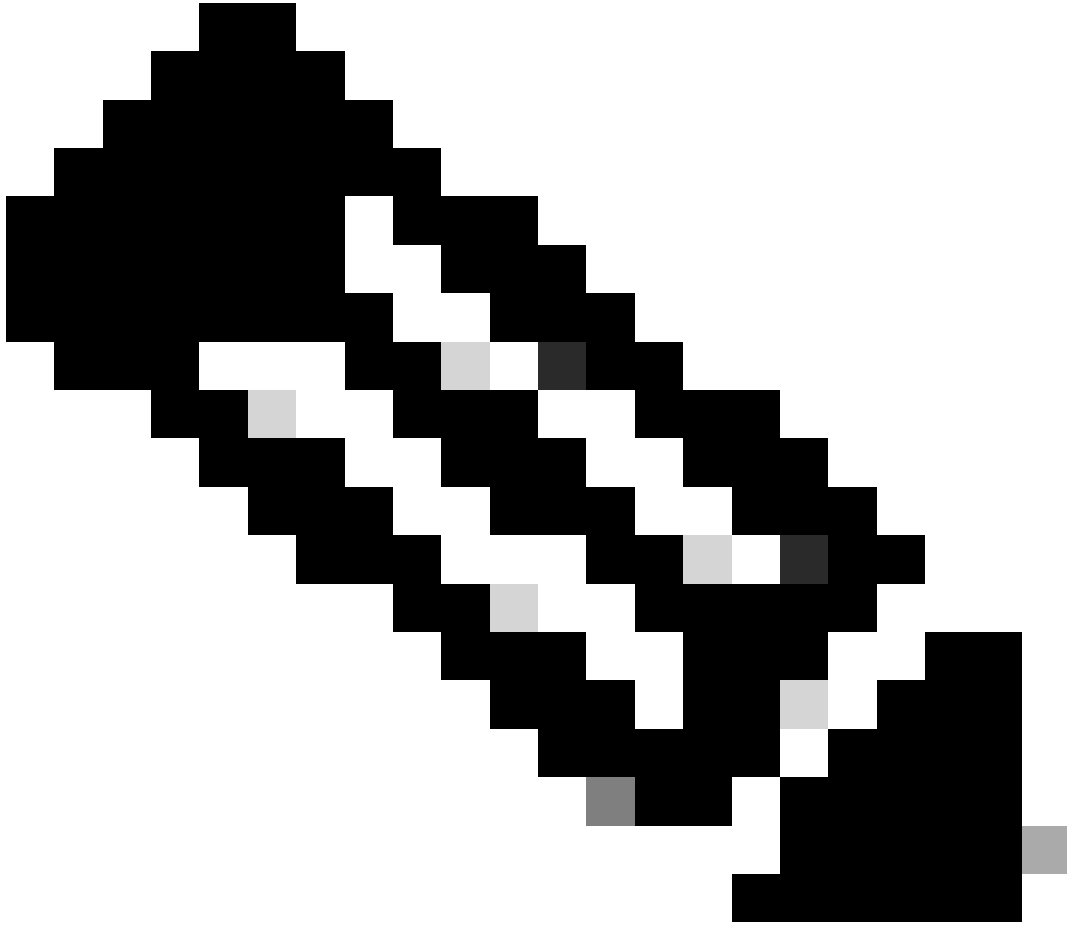


Client Provisioning Portal

**Device Security Check**

Your computer requires security software to be installed before you can connect to the network.

[Start](#)



لماع تي بثت مدعل ارطن [CSA-Unknown-compliance](#) تاسايسال ةومجم - ليوختال نمض عقت ةطقنللا هذو دنع :ةظالم  
للكولا تي بثتل ISE دادم ةباوب لى لكهيجوت ةداع متتو ،زاهال لىل ع ISE Posture Agent

4. لىللكولا ريفوت ةبامل "ءب" قوف رقنا .

#### Device Security Check

Your computer requires security software to be installed before you can connect to the network.

9 Detecting if Agent is installed and running...

5. قوف رقنا + **This is my first time here.**

## Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent



+ This is my first time here



+ Remind me what to do next

6. قوف رقنا Click here to download and install agent



### + This is my first time here

1. You must install Agent to check your device before accessing the network. [Click here to download and install Agent](#)
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.



You have 4 minutes to install and for the compliance check to complete

7. لي عمل تي ب ث ت

# Downloads



cisco-secure-client-ise...aBf8STpS5Nr1nzotleQ.exe

[Open file](#)

[See more](#)

Network Setup Assistant



## Network Setup Assistant



Installation is completed.

Quit

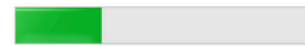
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. مدع ةلاح يف ةيلاحلا ةزهجألا ةلاح نم ققحتلا يف (ISE) ةيوهلا تامدخ كرحم ةيعضو ISE Posture أدبي ،ليكولا تيبتت دعب . قفاوتلا وحن كدشري اقتب نم نأ رهظي ،ةسايسلا تابلطتم ةيبلت



# ISE Posture

1 Update(s) Required



30%

Time Remaining:

**3 Minutes**



## Action Required to Enable Access

**Updates are needed on your device before you can join the network.**

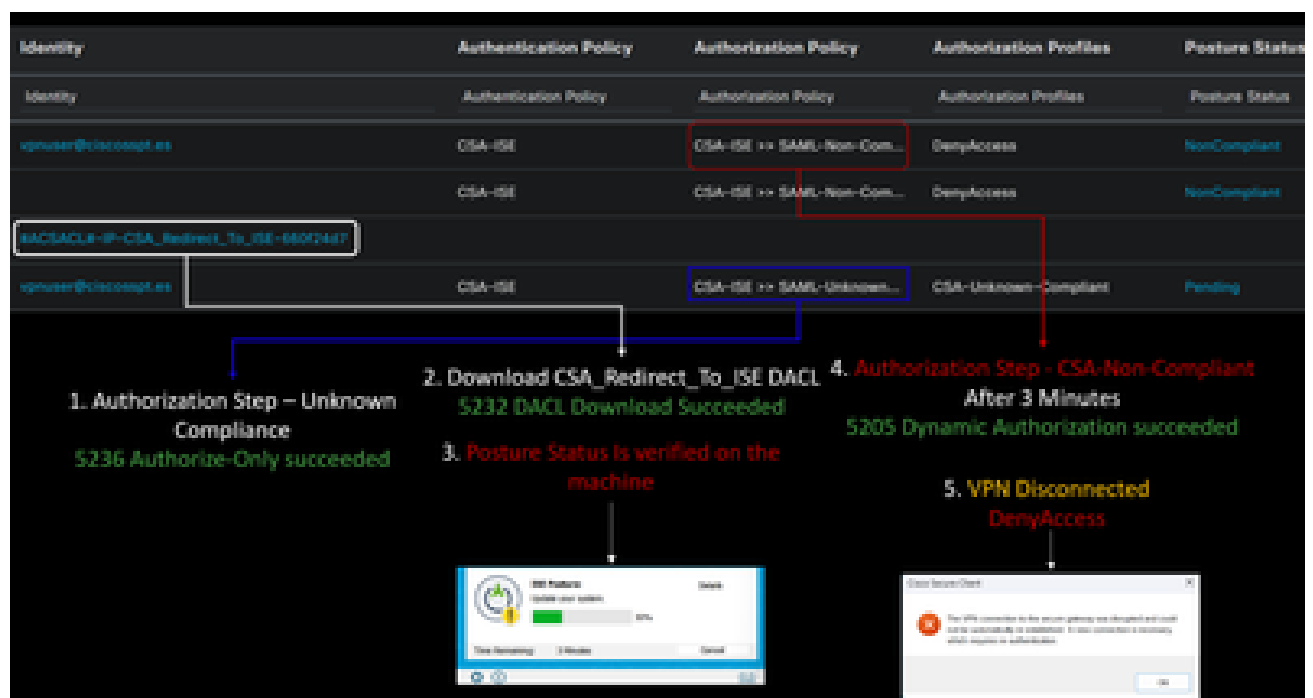
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details



Cancel



ليوختل جهن ةومجم نمض لخدتو ، قفاوتم ريغ ايئاقلت حبصت ، ةيقتبتم ال Cancel ةلهملا ةاها نأ ةلاحي في : قظالم [CSA-Non-Compliance](#) ، VPN ةكبش نع اروف لصفنو .

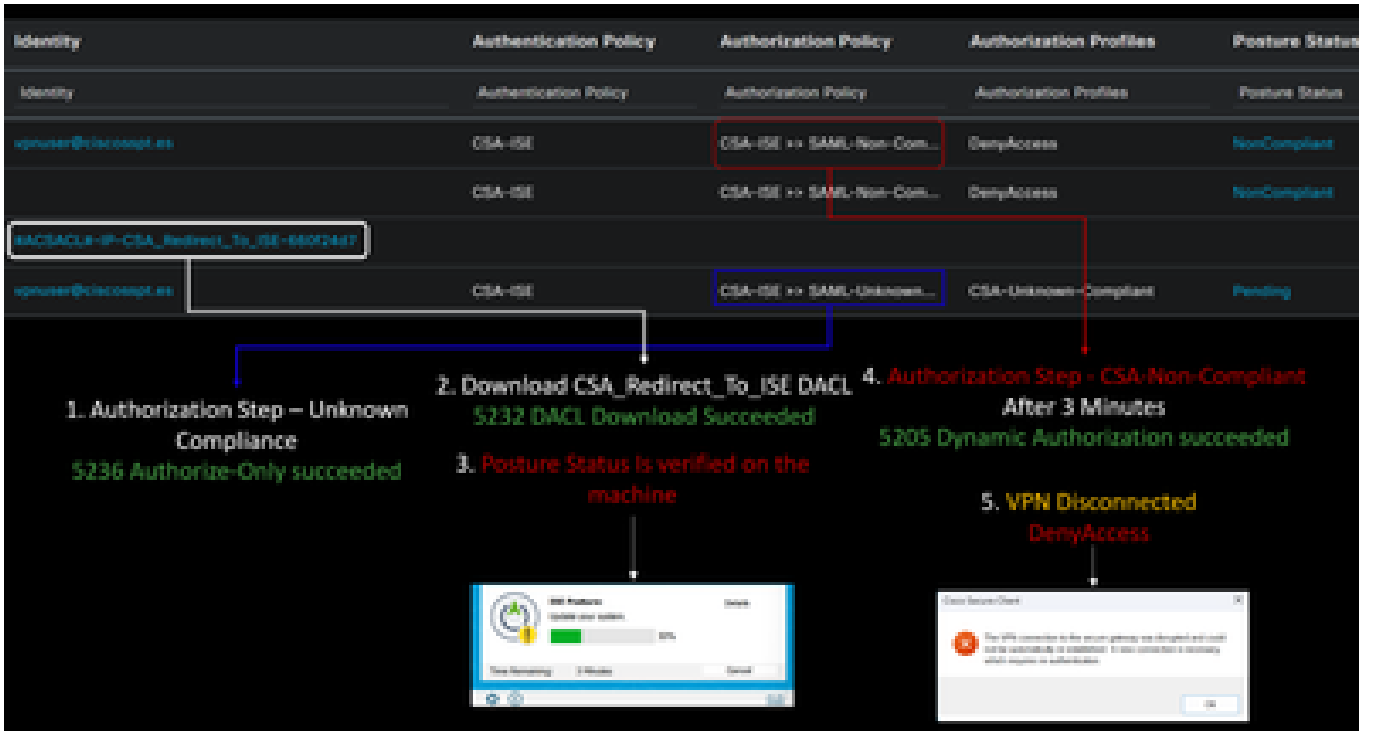
9. (VPN) ةيره اظلال ةصاخلا ةكبش لابل رخأ ةرم لصتاو "نم آلا ةياهنلا ةطقن لماع" تيبثت مق 9.

**Secure Endpoint Installed**      **Agent Scanning**      **ISE Posture Successful validated**

**Scan Summary - Compliance**

Required	Status
1	Done

10. لىلا لوصول قح حنميو ويوكش ةلاحي في نوكت يكل كعضو ريغت ، قفاوت ةلاحي في زاهجلا نأ نم لىمعل ققحتي نأ دعب 10. ةكبش لىل ةدوجوملا دراوملا عيجم .



لوصولك نك ميو، [CSA عم ق ف اوت م ل ا](#) لي و خ ت ل ا ت ا س ا ي س ة و م ج م ل ا ع ض ا خ ح ب ص ت ، ا ق ف ا و ت م ح ب ص ت ن ا د ع ب : ن ظ ح ا ل م ة . ك ب ش ل ا د ر ا و م ع ي م ج ي ل ا ا ر و ف .

ISE في ت ا ل ج س ل ا ن م ق ق ح ت ل ا ا ي ف ي ك

ة، و ه ل ا ت ا م د خ م س ق ي ف ا ه ت ع ج ا ر م ل . ل ا ث م ا ل ا م د ع و ق ف ا و ت ل ا ي ل ع ن ا ل ا ث م ك ي د ل ، م د خ ت س م ل ل ة ق د ا ص م ل ا ة ج ي ت ن ن م ق ق ح ت ل ل ة : ي ل ا ت ل ا ت ا د ا ش ر ا ل ا ع ب ت ا :

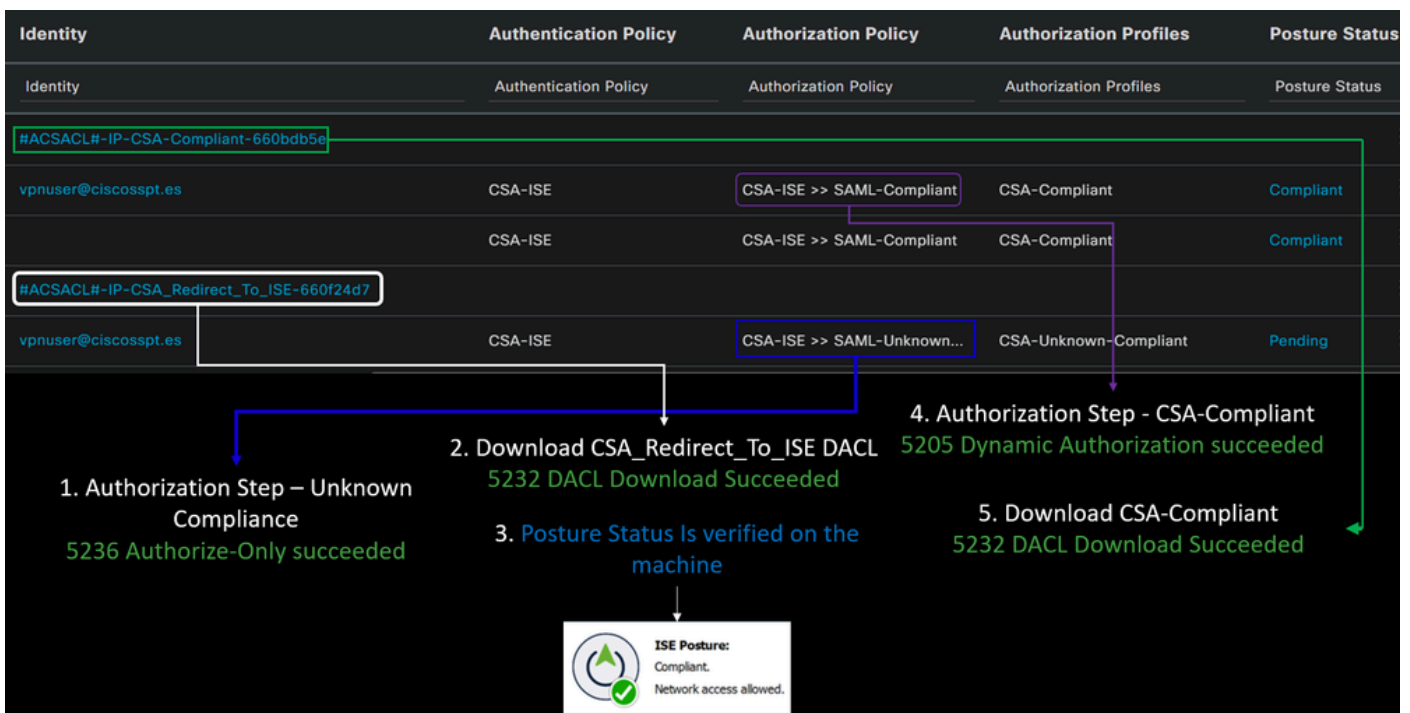
- ISE ت ا م و ل ع م ة ح و ل ي ل ا ل ق ت ن ا
- Operations > Live Logs ق و ف ر ق ن ا



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter		
0	0	0	0	0		
Refresh: Never   Show: Latest 50 records   Within: Last 60 minutes						
Reset Repeat Counts   Export To   Filter   Settings						
Status	Details	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
		Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture
🔵	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCom
✅	📄	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending
✅	📄	#ACSACL#-IP-CSA-Compliant-660bdb5e				
✅	📄	vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Compliant	CSA-Compliant	Complia
✅	📄	#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				

Live Logs: رابط يفتح جداول الأحداث والمدعوق فواتير الأحداث عرضة في كلياتها ويرانيسلها حوضي

ادايقنا

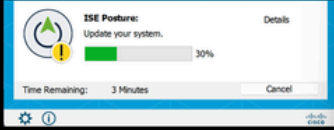



لأحداث المدعوق

Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Posture Status
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Non-Com...	DenyAccess	NonCompliant
#ACSACL#-IP-CSA_Redirect_To_ISE-660f24d7				
vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> SAML-Unknown...	CSA-Unknown-Compliant	Pending

1. Authorization Step – Unknown Compliance  
5236 Authorize-Only succeeded
2. Download CSA\_Redirect\_To\_ISE DACL  
5232 DACL Download Succeeded
3. Posture Status Is verified on the machine
4. Authorization Step - CSA-Non-Compliant After 3 Minutes  
5205 Dynamic Authorization succeeded
5. VPN Disconnected DenyAccess

ISE لم اكنت و نم آلا لوصول عم يلوال تاوخلال

لالخ نم اهلا لوصول نكمي يتلا تاكبشلا نيوكت ةفاضا مزلي، 192.168.10.0/24 ةكبشلا نمض، يتلا لاثملا يف قفنلا نيوكت تحت قفنلا

Step 1: قفنلا نيوكت نم ققحتلا:

نم آلا لوصول تامول عم ةحول لى لاقنتال اعرجلا، كلذ نم ققحتلل

- قوف رقنا Connect > Network Connections
- قفنلا Network Tunnel Groups > قوف رقنا

HomeFTD	Connected	Europe (Germany)	sse-euc-1-1-0	1	sse-euc-1-1-1
---------	-----------	------------------	---------------	---	---------------

- كبا صاخال Cisco ISE نوكي شيح ناوئعلا ةحاسمل قفنلا نيوكت نم ققحت، صخلم تحت

## Summary

✔ Connected

Region Europe (Germany)

Device Type FTD

Routing Type Static Routing

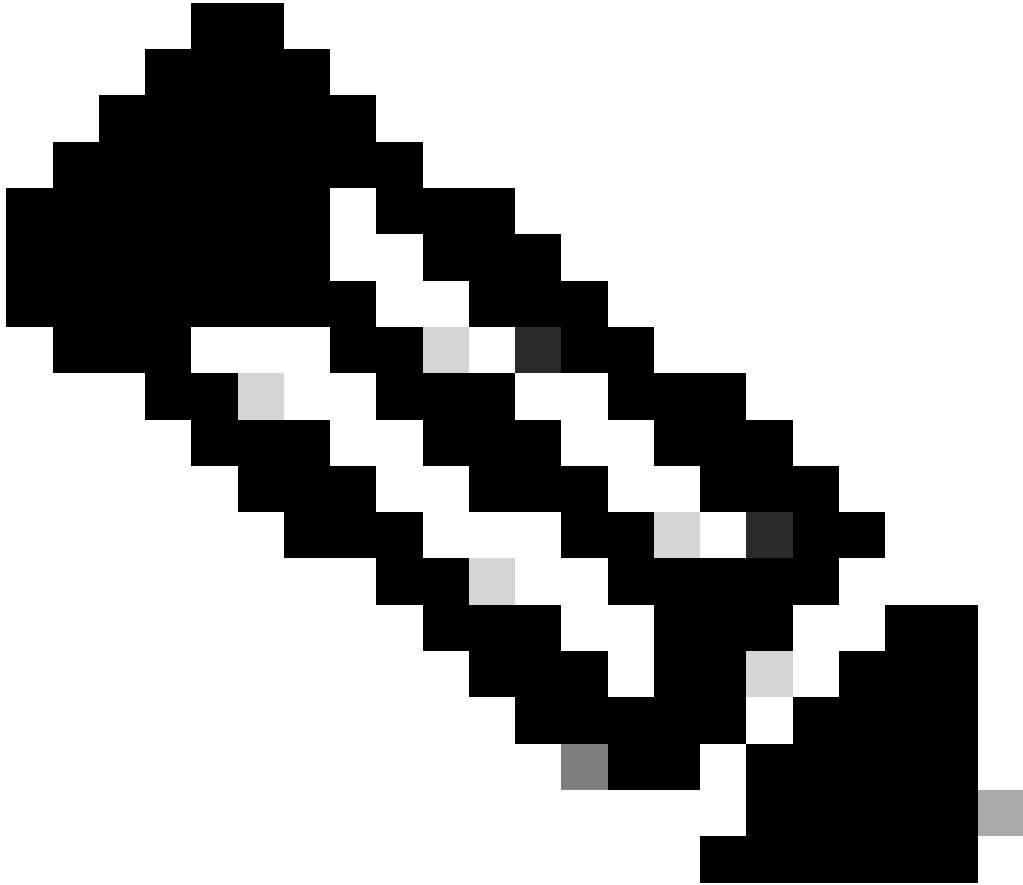
IP Address Range 192.168.10.0/24

Last Status Update Mar 19, 2024 11:13 AM

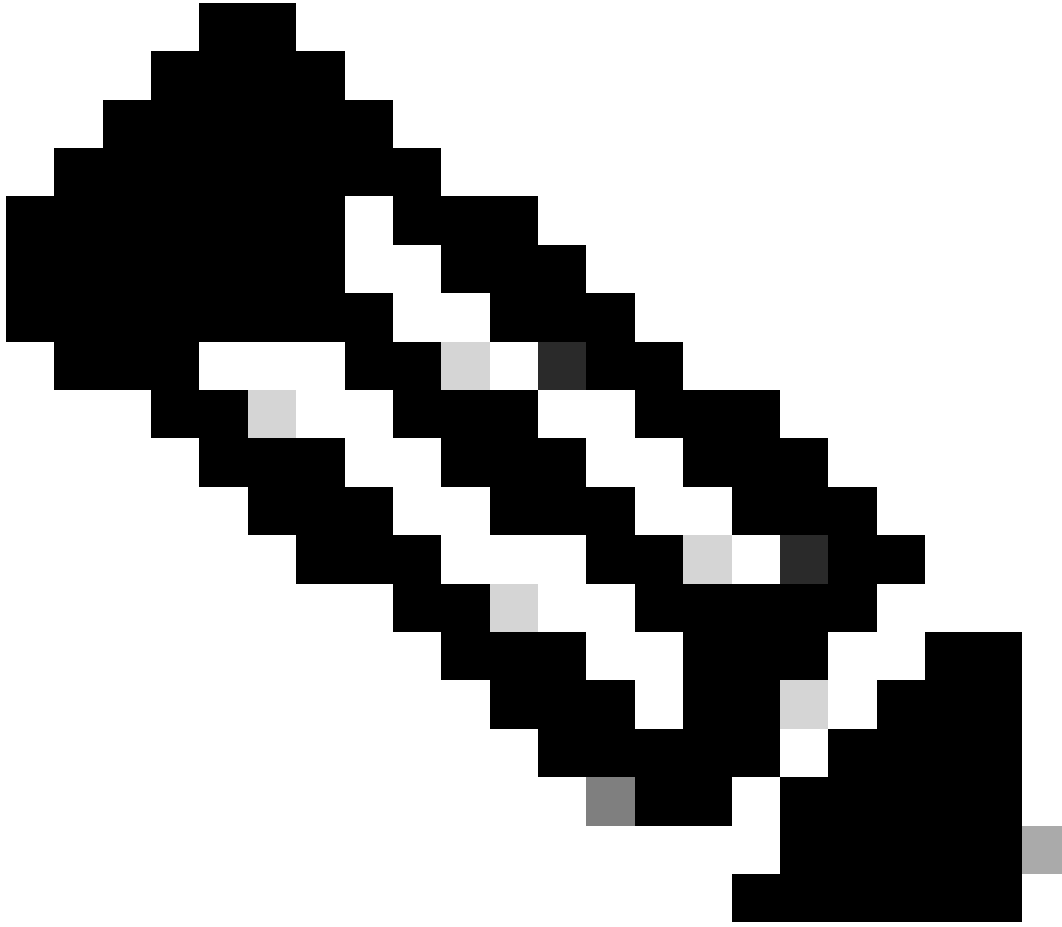
Step 2: إعداد الراوتر لإرسال الطلبات إلى الخادم.

لتكتميل العملية، يجب إعداد الخادم لإرسال الطلبات إلى الراوتر. في هذا المثال، سنستخدم خادم RADIUS لإرسال الطلبات إلى الراوتر. يجب إعداد الخادم لإرسال الطلبات إلى الراوتر. يجب إعداد الخادم لإرسال الطلبات إلى الراوتر.

تدعاق	ردصملا	ةهوجلوا	عانيم ةياغ
نمآلا لوصولل ISE ةرادإلا عمجت	ISE_Server	ةرادإلل IP عمجت (RA-VPN)	واكاك (يضا رتفالا ذفنملا) UDP 1700
ISE ىلا نمآلا لوصولا ةرادإل IP عمجت	ةرادإلل IP عمجت	ISE_Server	ليوختل او ققداصملا (يضا رتفالا ذفنملا) UDP 1812 قبساحم (يضا رتفالا ذفنملا) UDP 1813
ISE ىلا نمآلا لوصولا ةطقنل IP عمجت	ةطقنل IP عمجت ةياهنلا	ISE_Server	ريفوتلا لخدم ذفنملا (TCP 8443 لوكوتورب (يضا رتفالا ذفنملا)
مداخ ىلا نمآلا لوصولا ةطقنل IP عمجت DNS	ةطقنل IP عمجت ةياهنلا	DNS مداخ	DNS



[ذفنملا عجرم - مدختس ملال لیلد](#) نم ققحتف، ISE بة قلعتملا ذفانملا نم ديزملا ةفرعم ديرت تنك اذا: ةظحالم



ise.ciscospt.es لثم ،مسا لالځ نم فاشتكال كب صاځال ISE نيوكتب تمق اذا DNS ءءاق ءوځو مزلي :ءظالم

---

ءي فرطلا ءطقنلل IP عمءتو ءراءالا عمءت

:كب ءصاځال [نم آالا لوصولا تامولعم ءءول](#) ىلا لقتنا ،ءي فرطلا ءطقنلاو ءراءال IP عمءت نم ققءتلل

- **Connect > End User Connectivity** قوف رقنا
- Virtual Private Network قوف رقنا

- Manage IP Pools تحت
- Manage قوف رقنا

EUROPE						1	^
Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers	RADIUS Groups		
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House	ISE_CSA		

ةصاخلا دراوملا نمض ك بصاخلا ISE نيوكت نم دكأت: 3 ةوطخلا

كمزلي، ISE Provisioning Portal يلى لقتنلاب (VPN) ةيره اظلال ةصاخلا ةكبشلا ربع نيلصت مل ني مدختست ملل حامس لل ISE يئاقلتلا دادم الاب حامس لل هم ادختسا متي يذلاو، لوصولا ريفوتل صاخ درومك ك بصاخلا زاهجل نيوكت نم دكأتلا Posture Module ةصاخلا ةكبشلا (VPN).

ك: ةصاخلا [نمآلا لوصولا تامولعم ةحول](#) يلى لقتنا، جيحص لكشب ISE نيوكت نم ققحتلل

- Resources > Private Resources قوف رقنا
- ISE دروم قوف رقنا

**Private Resource Name**

CiscoISE

**Description** (optional)

## Communication with Secure Access Cloud

Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address.

[Help](#)**Internally reachable address**

(FQDN, Wildcard FQDN, IP Address, CIDR)

**Protocol****Port / Ranges**

192.168.10.206

TCP - (HTTP/HTTPS)

Any

[+ Protocol & Port](#)[+ IP Address or FQDN](#) **VPN connections**

Allow endpoints to connect to this resource when connected to the network using VPN.

(8443) دادعإلا لخدم ذفنمب ةدعاقلا ديقت كنكمي، رمألا مزلا اذا



---

VPN تالاصتال رايتخالالا ةناخ ىلع ةمالع عضو نم دكأت :ةظحالم

---

لوصول ةسايس بجومب ISE لوصولب حامسلا :4 ةوظخال

كمزلي **ISE Provisioning Portal** ىلى لقتنلاب (VPN) ةيره اطلالا ةصخاللا ةكبشلا ربع نيلصتملا نيمدختسملل حامسلا لىلى لوصولاب ةدعاقلا هذه بجومب مهنيوكت مت نيذلا نيمدختسملل حامسلا لىلى **Access Policy** دحأ نيوكتب تمق كنأ نم دكأتلا لىلى Step3. في هنيوكت مت يذلا صخاللا دروملا


كب ةصخاللا [نمآلا لوصولاب تامولعم ةحول](#) ىلى لقتنا ،حيحص لكشب ISE نيوكت نم ققحتلل


- قوف رقنا Secure > Access Policy
- ISE | VPN ةكبش يم دختسم ىلا لوصولاب خامس لل اهن وكت مت يتلا ةدع اقل قوف رقنا

## 1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

### Action


 **Allow**  
Allow specified traffic if security requirements are met.

 **Block**  
Block specified traffic.

From	To
Specify one or more <b>sources</b> .	Specify one or more <b>destinations</b> .
<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> <span style="background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;">CSA (ciscospt.es\CSA)</span> <span style="margin-left: 10px;">✕</span> </div>	<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> <span style="background-color: #f0f0f0; border-radius: 3px; padding: 2px 5px;">CiscoISE</span> <span style="margin-left: 10px;">✕</span> </div>
Information about sources, including selecting multiple sources. <a href="#">Help</a>	Information about destinations, including selecting multiple destinations. <a href="#">Help</a>


### Endpoint Requirements

For VPN connections:

 End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ

Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#)

For Branch connections:

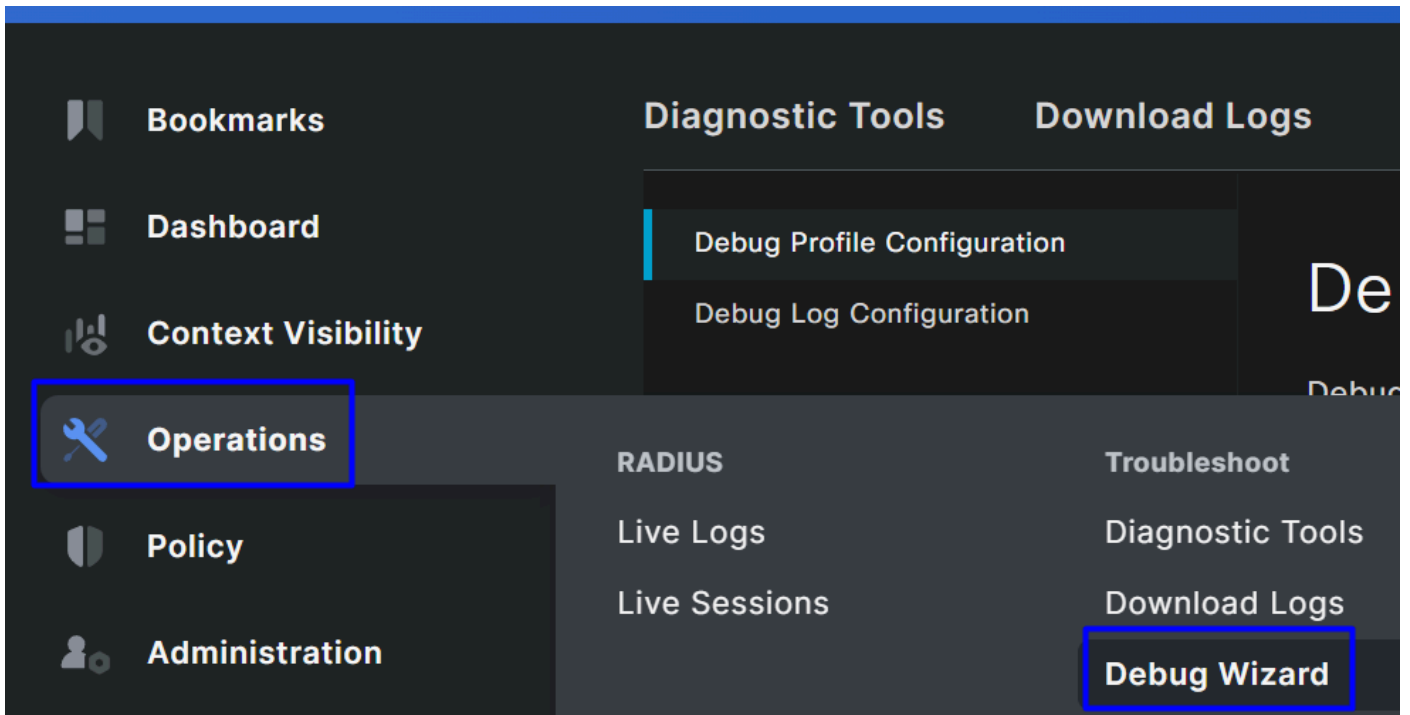
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

اهحالص او اءاطخ ال فاشك سا

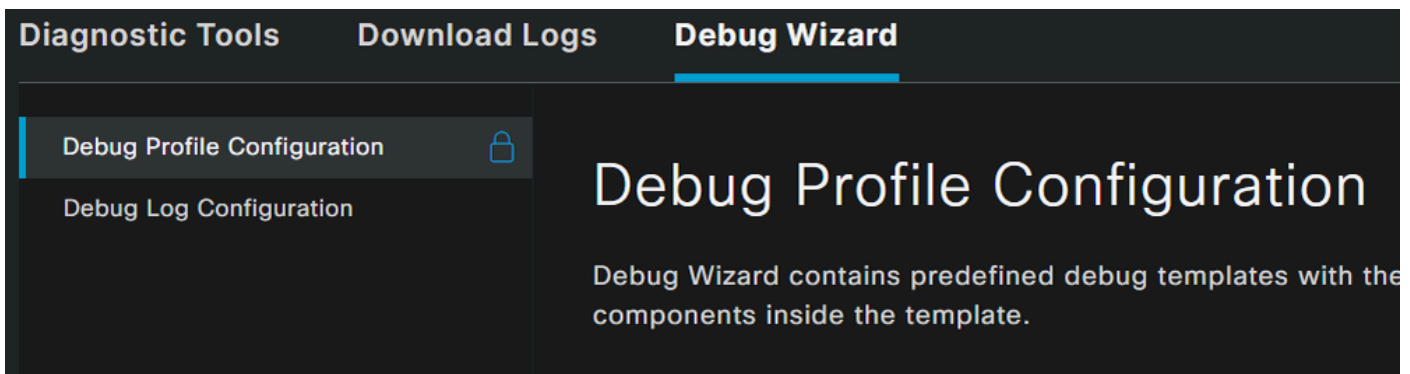
ISE ةي عضو اءاطخ اءي حصت تال جس لي زنت ةي فيك

:ةي ل ال تاو طخال ةعباتم اءرلا ،عضولاب قلعتت ةلكشم دوجو نم ققحت لل ISE تال جس لي زنتل

- ISE تامول عم ةحول ىلا لقتنا
- Operations > Troubleshoot > Debug Wizard قوف رقنا



- [Debug Profile Configuration](#) قوف رقتنا



- [Posture > Debug Nodes](#) ل رايته خالاه قناخ ديدحت



Add



Edit



Remove 2



Debug Nodes



Name

Des



802.1X/MAB

802



Active Directory

Acti



Application Server Issues

App



BYOD portal/Onboarding

BYO



Context Visibility

Con



Guest portal

Gue



Licensing

Lice



MnT

MnT

1



Posture

Pos

- فاشك تسال اه لعل اعاطخ ال اع حصت عضو نيك م ت ب موقت س ي ت ل ا ISE د ق ل راي ت خ ال ا ن ا خ ل ع م ال ع ع ض ا ه ا ح ال ص ا و ك ت ل ك ش م

Warning

Enabling the node will override its debug log configuration

OK

<input checked="" type="checkbox"/>	Host Name	Persona
<input checked="" type="checkbox"/>	ISE.ciscosspt.es	Administration, Monitoring, Policy Serv

- Save ر ق ن ا

# Debug Nodes

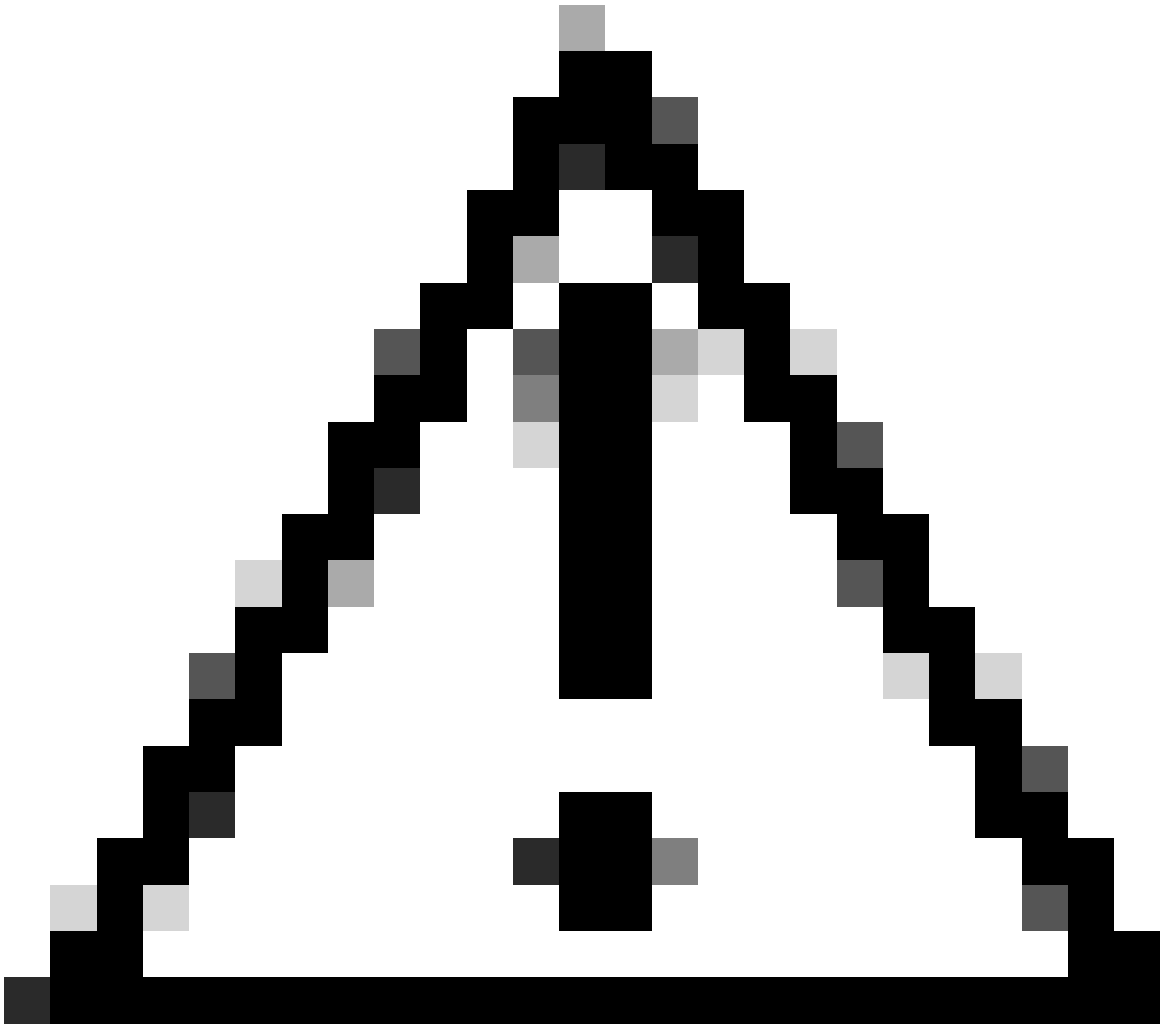
Selected profile Posture

Choose on which ISE nodes you want to enable this profile.

 Filter  

<input checked="" type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> ISE.ciscosppt.es	Administration, Monitoring, Policy Service	STANDALONE

[Cancel](#) [Save](#)



---

the debug logs can affect the performance of your device. كاتل شمش جاتنإ ةءاع| ف أدبت نأ بءي ، ةطقنللا هءه ءعب :رئذء

---

ءةللللا ءاوطءللللا عءاء ، ةلشمللا ءسن مءئ نأ ءعب

- قوف رقنا Operations > Download Logs
- اهنم ءالءسللا ذءأ ءئرت ءئلا ةءقءللا رءءأ

## Appliance node list

ISE

- ءةللللا ءاراءءللللا رءءأ Support Bundle ءءء :

## Support Bundle

## Debug Logs

- Include full configuration database ⓘ
- Include debug logs ⓘ
- Include local logs ⓘ
- Include core files ⓘ
- Include monitoring and reporting logs ⓘ
- Include system logs ⓘ
- Include policy configuration ⓘ
- Include policy cache ⓘ

From Date

(mm/dd/yyyy)

To Date

(mm/dd/yyyy)

\* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

### Support Bundle - Encryption

- Public Key Encryption ⓘ
- Shared Key Encryption ⓘ

\* Encryption key ..... ⓘ

\* Re-Enter Encryption key .....

Create Support Bundle

- Include debug logs
- **Support Bundle Encryption**
  - **Shared Key Encryption**
    - Encryption key و Re-Enter Encryption key



- [رقننا Create Support Bundle](#)
- [رقننا Download](#)

## ✓ Support Bundle - Last Generated

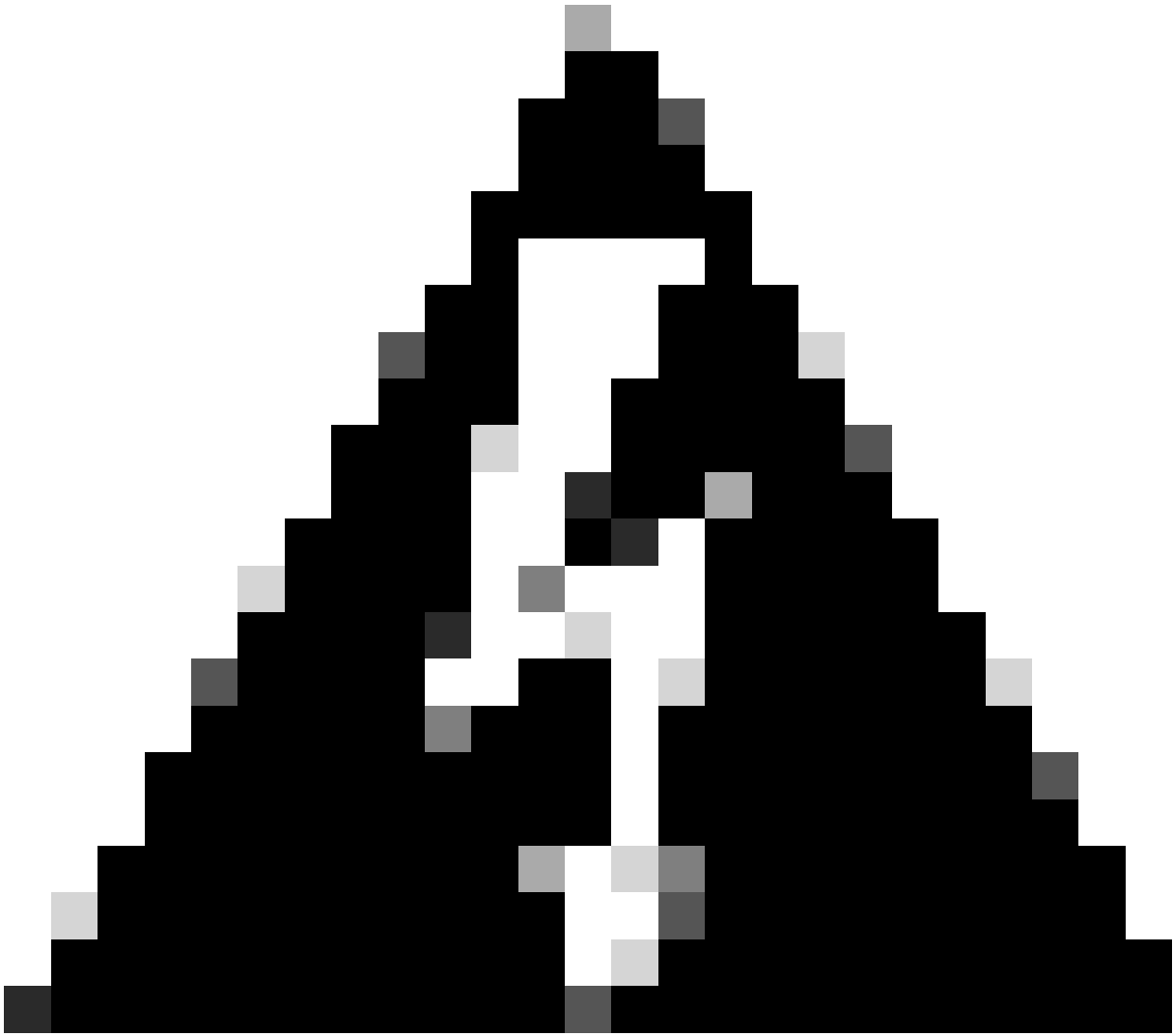
File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

Time: Thu, 04 Apr 2024 14:35:35 UTC

Size(KB): 52165.0

[Download](#)

[Delete](#)



[ءاطخألا اءي ءصت في رعت فلم نيوكت](#)، ةوطخالا لىع هنيكمت مت يذلا ءاطخألا اءي ءصت ءضو لىطعت :ريذءت
















---

نمألا دءب نع لوصولءا ءالءس نم ققءءءالا ةي فيك

كء ءصءءالا نمألا لوصولءا ءامولءم ءءول لىل لءقءنا

- Monitor > Remote Access Logs قوف رءنا

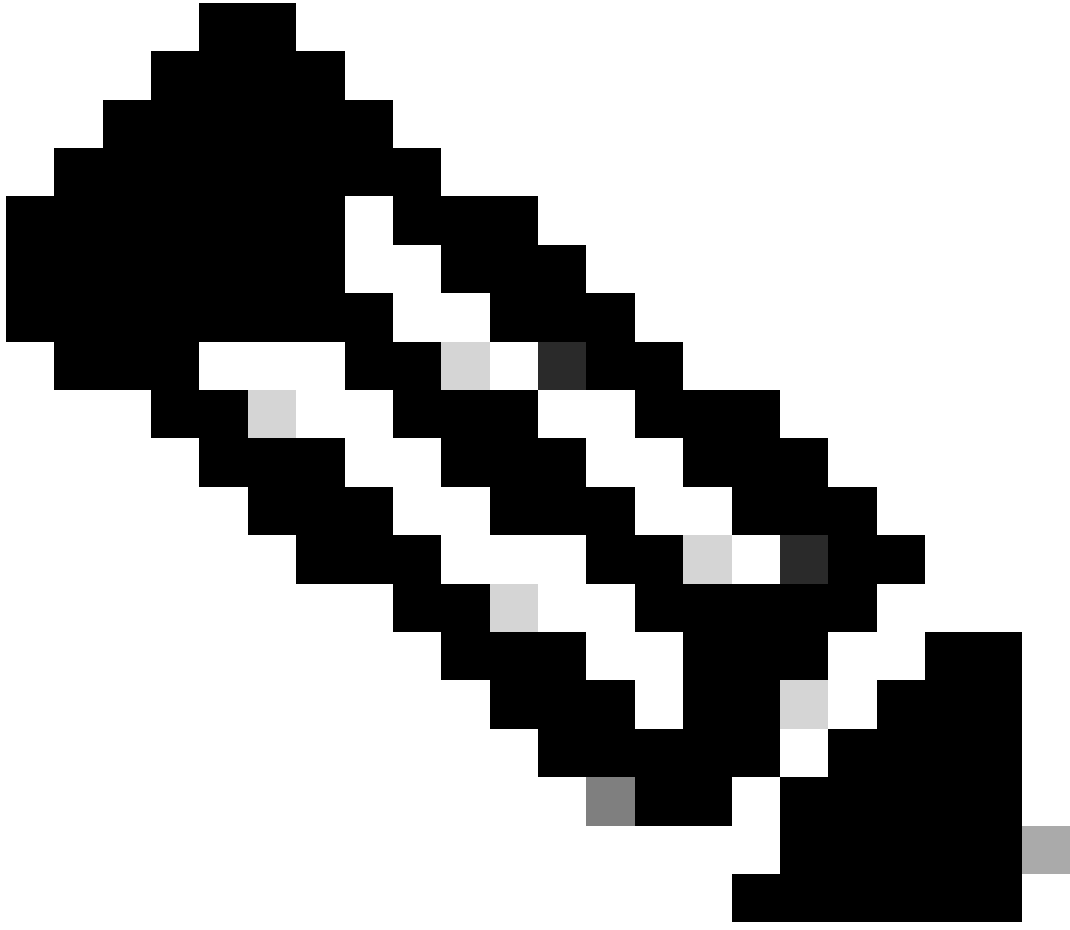
## 100 Events

User	Connection Event	Event Details	Internal IP Address
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.130
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.129
 vpn user (vpnuser@ciscospt.es)	 Disconnected	User Requested	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Disconnected	Unknown	192.168.50.1
 vpn user (vpnuser@ciscospt.es)	 Connected		192.168.50.1
<i>Unknown Identity</i>	 Failed	AUTHORIZATION-CHECK	

نم آلا ليمعلا لىل ع DART ةمزع عاشنا

ةللاتلا ةلاقملا نم ققحت ،كزاهج لىل ع DART ةمزع عاشنال

[ألا Cisco Secure Client Diagnostic and Reporting Tool \(DART\)](#)



عمالة حتف ىجري، اءالص او اءطء الء فاشكك ساء مسق ىف اءىءا راءمءا ءالءسءا عىمءء ءرءمء: ءظءالم  
ءامولءمءا لىءءء ىف ءءبءءمءا TAC.

---

ءلص ءاءءامولءمء

- [Cisco نمءال ىزنءءل او ىنءلءمءءل](#)
- [ءءءسءمءل لىءءءو نمءال لوءولء قىءاءءو](#)

- [Cisco Secure Client](#) جمان رپ لی زنت
- [3.3 رادصالا Cisco](#) نم ؤی وهلا تامدخ لکرحم لوؤسم لیلد

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نء مء دختسمل معد وء مء مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظءالم ءرء. ةصاءل مء ءبل ب  
Cisco ءلءت. فرءم مچرت مءم دقء ءلءل ةء فارءءال ةمچرتل عم لءل او  
ءل ءمءءاد ءوچرلاب ءصوء وء ءامچرتل هذه ةقء نء اهءل وءس م  
Systems (رفوءم طبارل) ءلصل ءل ءلءل ءلءل دن تسمل