

# RA- عضو ميقيقتل نمالا لوصول نيوكت ISE مادختساب VPNaS

## تايوتحمل

---

[قمدقمل](#)

[قيساسالابلطتمل](#)

[تابللطتمل](#)

[قمدختسملتانوكمل](#)

[قيساسا تامولعم](#)

[ككبللليطيطلتلا مسرلا](#)

[نيوكتلا](#)

[نمالا لوصول نيوكت](#)

[IP تاعمجت يلع RADIUS قعومجم نيوكت](#)

[ISE مادختسال VPN فيرعت فلم نيوكت](#)

[قماعل تادادعلا](#)

[قبساحمللاو ليوختلاو ققداصمل](#)

[بورمل ككرح هيچوت](#)

[Cisco نم نمل لي موع نيوكت](#)

[ISE تان نيوكت](#)

[ككبلللا قزجأ قميئاق نيوكت](#)

[قعومجم نيوكت](#)

[يلجم مدختسم نيوكت](#)

[چونلا قعومجم نيوكت](#)

[ضيوفتلا او جهنلا قعومجم ققداصم نيوكت](#)

[Active Directory يمدختسم وان نيولحمل RADIUS يمدختسم نيوكت](#)

[ISE قيعضون نيوكت](#)

[عضوللا طورش نيوكت](#)

[عضوللا تابللطتمل نيوكت](#)

[عضوللا جهن نيوكت](#)

[لي موعلا دادملا نيوكت](#)

[لي موعلا ريفوت جهن نيوكت](#)

[ليوختلا تافيصوت عاشنا](#)

[عضوللا جهن قعومجم نيوكت](#)

[قحصلا نم ققحتلا](#)

[عضوللا نم ققحتلا](#)

[زاوجللا يلع لياصتالا](#)

[ISE ي فالجسلا عيمجت قي فيك](#)

[اداي قنا](#)

[لاثت مللا مدع](#)

[ISE لماركتو نمالا لوصول عم يلاوالا تاوطللا](#)

[اهجالص او عاطخالا فاشكتسا](#)

[ISE قيعضو عاطخا جي حصت تالجس لي زنت قي فيك](#)

[نمالا دعبل لوصول تالجس نم ققحتلا قي فيك](#)

[نمالا لي موعلا يلع DART قمزح عاشنا](#)

## عم دق م ل ا

نع لوصول VPN ةكبش يم دخت سمل عضول م يقيقت نيوكت ةيفي ك دنت سمل اذه حضوي نم آل لوصول او (ISE) ةوه ل عم دخ كرحم مادخت س اب دع ب

## ةيساس آل ا تاب ل ط م ل ا

- [مدخت سمل ا ريفوت نيوكت](#)
- قف ن ل ا رب ع Cisco نم نم آل لوصول اب ةلصت م ISE

## تاب ل ط م ل ا

ةيلات ل ا عيضاوم ل ا ب ة فرعم كي دل نوكت ن اب Cisco ي صوت

- [ةوه ل ا عم دخ كرحم](#)
- [نم آل لوصول ا](#)
- [Cisco Secure Client](#)
- ISE Posture
- ةب س احم ل ا و لي وخت ل ا و ة ق داصم ل ا

## عم دخت سمل ا ت ا نو ك م ل ا

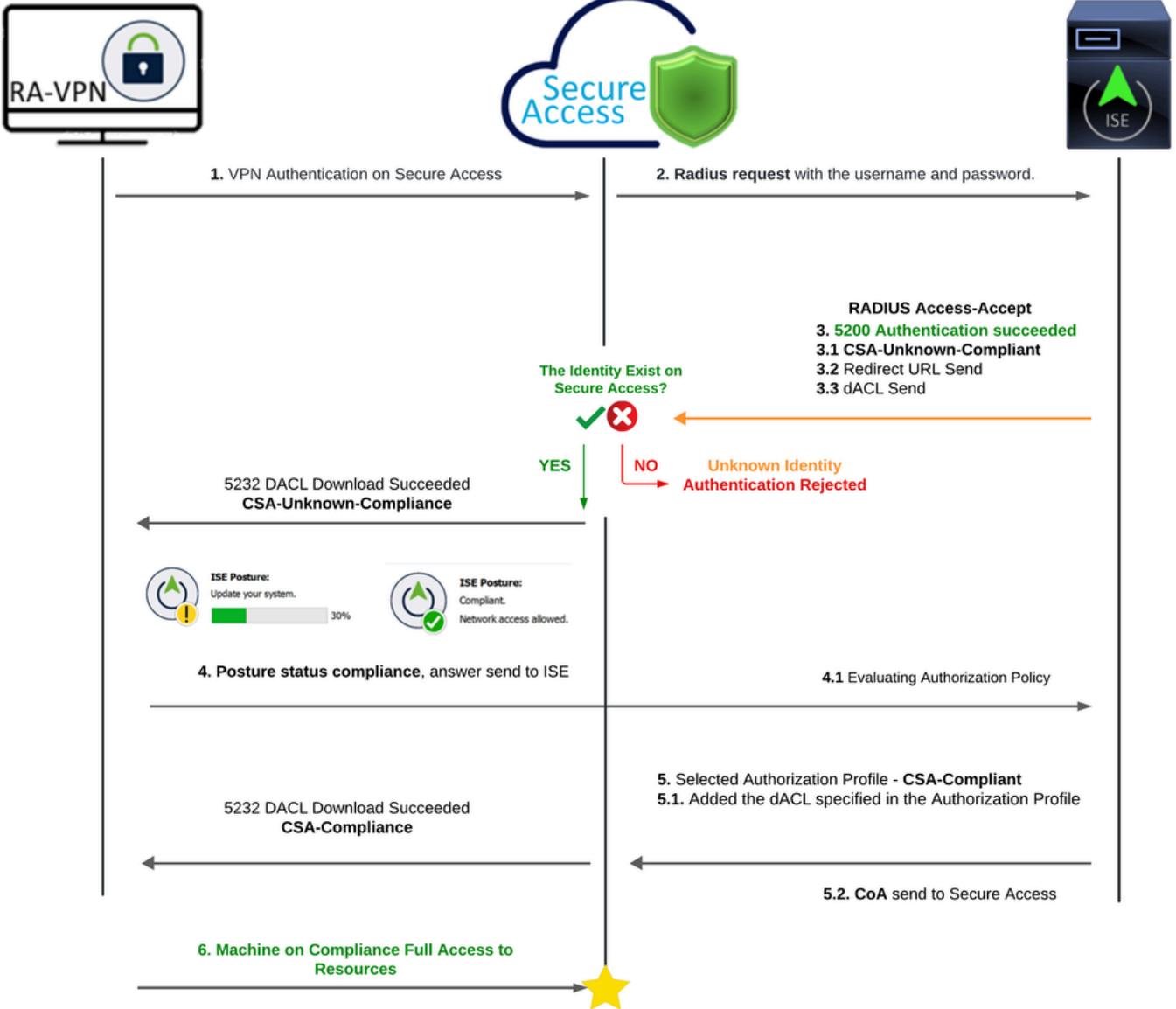
ي ل ا دنت سمل ا اذه ي ف ة دراو ل ا تامول عم ل ا دنت ست

- Identity Service Engine (ISE)، رادص ل ا 3.3 Patch 1
- نم آل لوصول ا
- Cisco Secure Client - AnyConnect VPN، رادص ل ا 5.1.2.42

ةصاخ ةي لم عم ةئي ب ي ف ة دوجوم ل ا ةزه ج آل ا نم دنت سمل ا اذه ي ف ة دراو ل ا تامول عم ل ا عاشن ا م ت ت ن ا ك ا ذ ا . (يضا رت ف ا) حوس مم نيوكت ب دنت سمل ا اذه ي ف عم دخت سمل ا ةزه ج آل ا عي م ج ت ا د ب رم ا ي آل ل م ت حم ل ا ري ث ا ت ل ل ك م ه ف نم د ك ا ت ف ، ل ي غ ش ت ل ا دي ق ك ت ك ب ش

## ةيساس ا تامول عم

vpnuser@ciscospt.es



ي طي تختال مسررل - ISE - ن م آل لوصول

يلع لمعي، الماش اينم اجهن (ISE) ةيوهلا تامدخ كرحم عم Cisco نم ن م آل لوصول اجمد رفوي ني مآتل، MS-CHAPv2 ك لذي ف امب، ةفل تخم ل ةقداصم لال و كوتورب نم ةدافت سالا لعل، ةمدقت م لال نام آل ةمدخ ةفاح ل م ادختس اب، Cisco Secure Access لمعي. تالاصتال ةكبش لال لثم تازيم رفوي امم، ةيزوتل ةديش تائيبل ربع ن م آل لاصلتال نيسحت ISE. تانك م ادختس اب اهتيامح نكمي يتل او، (VPNaaS) ةمدخك (VPNs) ةيرهاطلا ةصاخلا

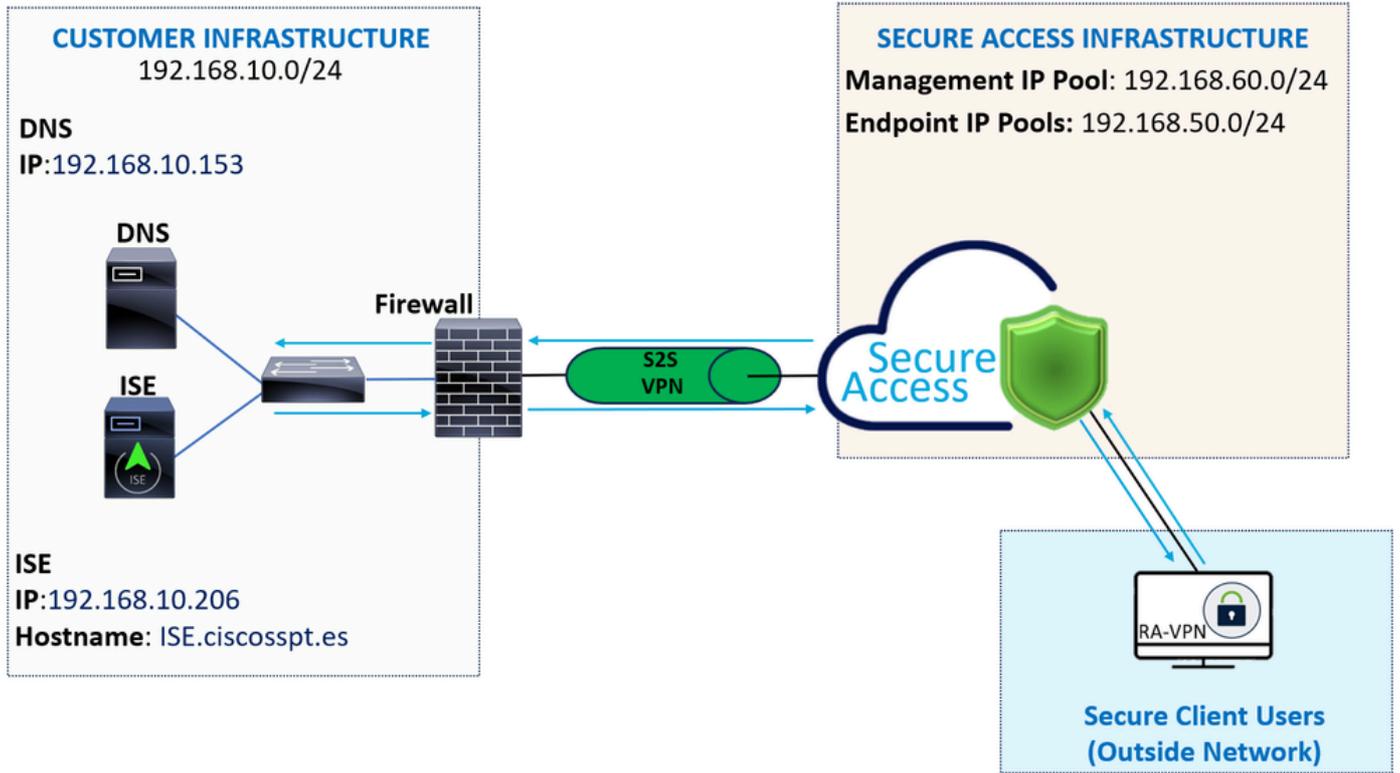
ةينك م ني م دختس م ل ل حيتي امم، نام آل او ةس ال سلاب مستت لوصول ةبرجت جم دلل اذه حيتي و نم ةمدقت م ل تازيم ل م ادختس ا ي دوي. نسحم نام او اءا عم نك م ا ي ف قي ب طت ا ب لاصلتال ةزهج ا قفاوت م ي ق ت ق ي رط نع اذه نام آل ا ج ذومن زي زعت ل ا، عضولا م ي ق ت لثم، Cisco ISE ةزهج آل ا ن م ضي اذهو. لوصول اب حامس لال لبق ةي ل خا دلل م دختس م ل تاس ايس عم رتوي ب م ك لال ةكبش لال دراوم ل ل لوصول اهنك م ي يتل ا يه طاقف ةسس ؤم لال نام ا تابل طتم ب ي فت يتل ا، ةين م آل تارغل لال رطاخم نم ل لقي امم.



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

---

ةكبشلل يطيختلا مسرلا



نيوكتلا

---

[مادختساب ىل وأل ات او طخ لآ](#) لامك إك ىل ع ب ج ي ، نيوكتلا ةي لم ع ادب لبق :ة طحال م [ISE](#) لم اك ت و "نم آل ا ل و ص و ل ا".

## نم آل ا ل و ص و ل ا نيوكت

IP تاع م ج ت ىل ع RADIUS ة و م ج م نيوكت

ة: ل ل ات ل ا ت او ط خ ل ا ل م ك أ ، RADIUS مادختساب VPN في ر ع ت ف ل م نيوكت ل

ك ب ة ص ا خ ل ا [نم آل ا ل و ص و ل ا ت ا م و ل ع م ة ح و ل](#) ىل ا ل ق ت ن ا

- **Connect > Enduser Connectivity > Virtual Private Network** قوف ر ق ن ا
- **Manage** قوف ر ق ن ا ، (Manage IP Pools) ع م ج ت ل ا نيوكت ت ح ت

## Manage IP Pools

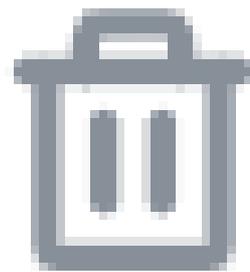
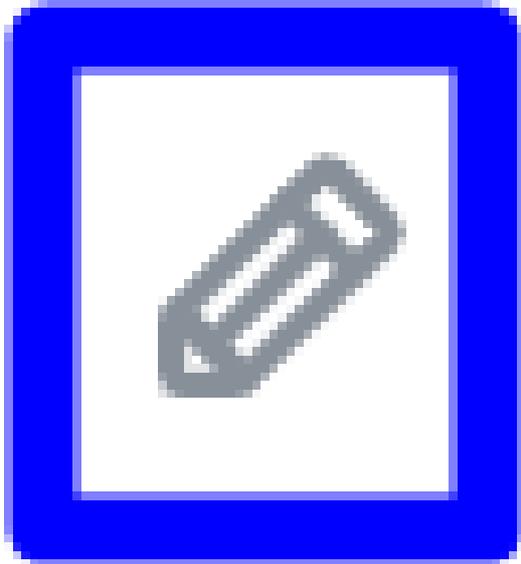
Manage

2 Regions mapped

- راديوس سرور لى تىلك شى 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 يىرتىل صاىر 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 ×



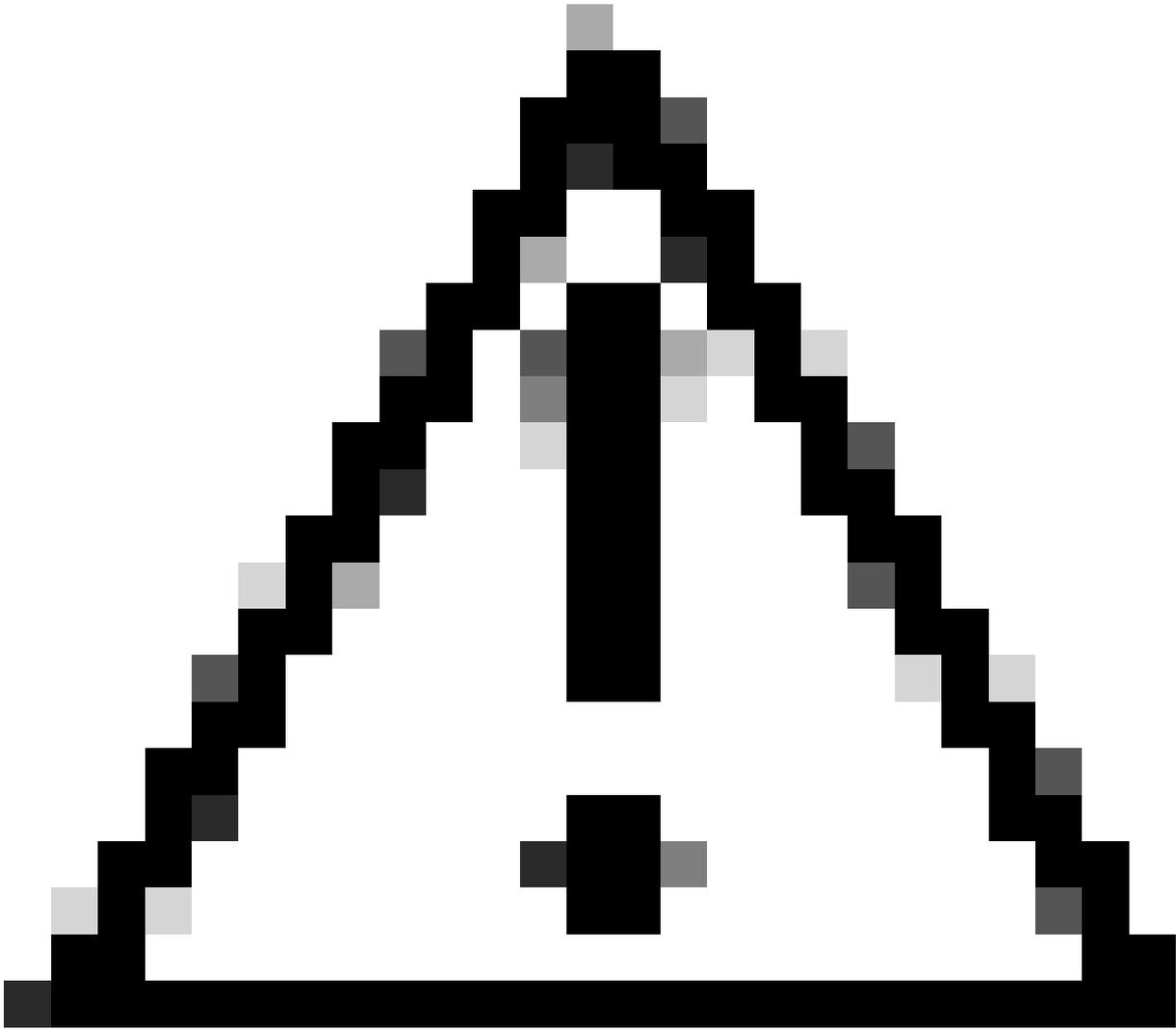
+ Add

#	Server Name	IP Address		
1	ISE_CSA	192.168.10.206		

## نمآلا لوصولا يف

### ◦ AAA method

- **Authentication:** وه، يضارتفا لكش ب، هدي دحتو **Authentication** ذفنم لل رايتخالالا ةناخ ىلع ةمالع عضو 1812
- ةقداصملا **Microsoft Challenge Handshake Authentication Protocol Version 2 (MCHAPv2)** بلطت ةلاحي يف رايتخالالا ةناخ ىلع ةمالع عضو
- **Authorization:** ذفنملا اذه ديدحتو ذفنملا ب **Authorization** ةصاخلا رايتخالالا ةناخ ىلع ةمالع عضو 1812 وه، يضارتفا لكش ب
- **Authorization mode Only Change of Authorization (CoA)** تاريغيغتو ةيعضوب حامسلاو **mode** ةناخ ىلع ةمالع عضو
- **Accounting:** 1813 وه، يضارتفا لكش ب، ذفنملا ديدحتو ليوختلل رايتخالالا ةناخ ىلع ةمالع عضو
- دحاو مداخ ىلا ةبساحملا تانايب لاسرا متي، درفملا عضو لا يف **Single or Simultaneous** رتخأ (ةومجمملا يف مداوخلال عيمجل 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 الـ **Authorization** نم لك مدختست Authentication نأ بجي : ريذحت

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

## RADIUS Servers

You can add up to 8 servers in each group

Assign servers

**+ Add**

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

- هتلا تارايل الل نيوكت ب مق ،كل ذ 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 مسانويكتب مق
- **IP Address:** نمال لوصول لالخنم هيل لوصول انكمي يذلا Cisco ISE زاهجل IP نويكت
- **Secret Key:** يرسل ال RADIUS حاتفم نويكت
- **Password:** كب ةصاخ ال RADIUS رورم ةملك نويكتب مق
- **كباب صاخ ال ISE مداخل ددحو رايل ال Assign Server نمض كباب 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 نويكتل ظفحل ىرخأ 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 ×

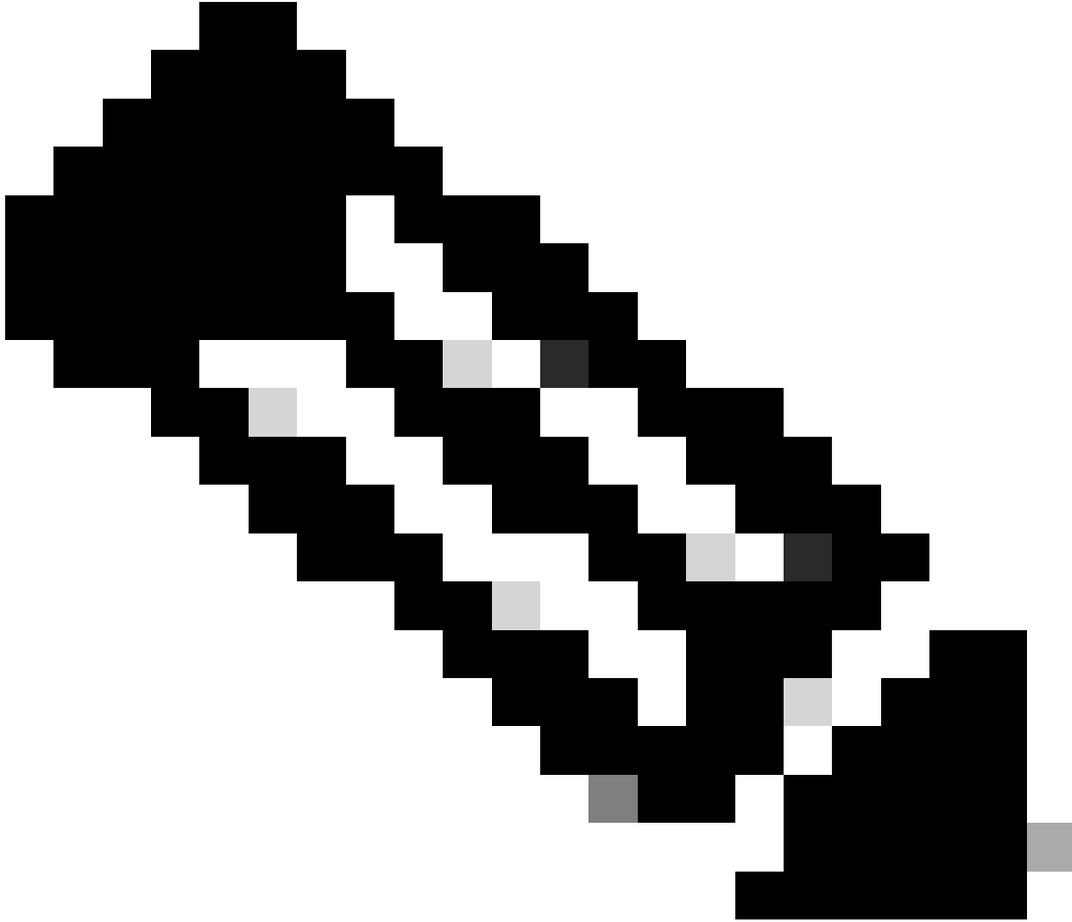
+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

◦ Protocols: رتخ Radius

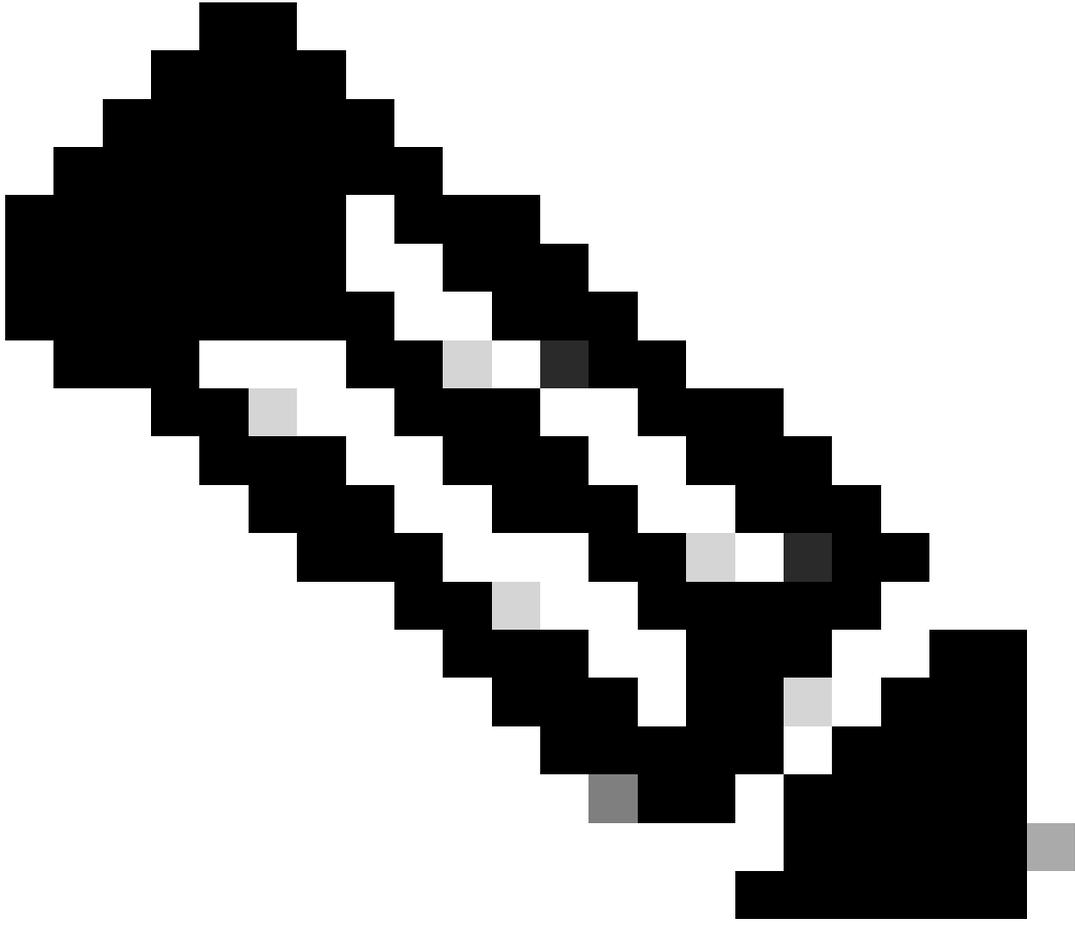
• Map authentication groups to regions: رتخ او قطانم لار رتخ Radius Groups

• رقا Next



قطانم كيدل ناك اذا رطوق لافصن تاعومجم ديدحت و قطانم لار عيمجب ةصاخ لار رتخ لال ةناخ ديدحت كي لع بچي: ةظحالم اعونصم كب صاخ لار رزلا نو كي Next، كلذ اول عفت مل اذا. ةددعت م





لمعت نلف ،ةفي طول Radio Authorization نيكمتب مقتم مل اذا :تظالم





- 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

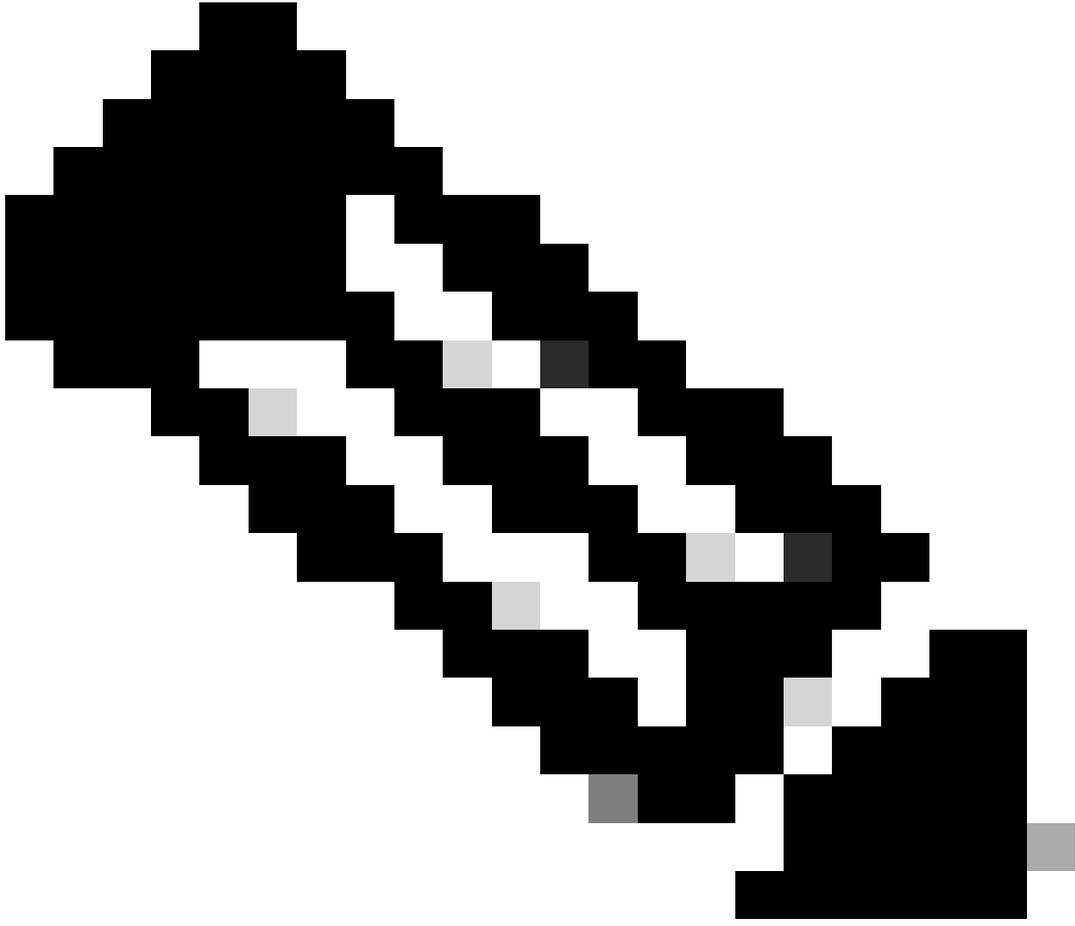


No matches found

[Cancel](#)

[Back](#)

[Next](#)



**Bypass Secure Access** كرايخ| دنع (ISE) ةيوهال تامدخ كرحم ةيعصو ISE Posture 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 مءث **Add**.

Cisco نم نم آل يممع 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**  
7 days

**Session Timeout Alert**  
30 minutes before

**Maximum Transmission Unit** ⓘ  
1240

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

ك ب صاخال نيوكتال صيصخت ديرت تنك اذا نكلو، Save رقنلواو يضارتفاك عيش لك ىلع ظافحلان كنكمي، ةوطخل هذه يف [Cisco](#) نم نم آلا لىمعل الوؤسم لىل نم ققحتال اعجالاف، رثكأ

ISE تانويكت

ةكبشلال ةزهجأةمئاق نيوكت

Cisco ISE ىلع تامالعتسا اعجالا هانكمي يتال اهب حومسمل ةزهجال نيوكت كمزلي، Cisco ISE لالخنم ةقداصمل نيوكتل كيدل:

- Administration > Network Devices ىل 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 كرتشملا رسلا سفن نيوكت، [يرسلاجاتفملا](#)
    - **CoA Port:** "نم آلا لوصول" ةزيم يف اضيأ 1700 زارطالا مادختسا متي شيح، ةيضارتفا ةميقك اهعد

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

ةومجم نيوكت

ةيلاتلا تاوطخال عبتا، نييلحملا نيمدختسملا 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' management interface. On the left, the 'Administration' menu is visible, with 'Identities' > 'Groups' selected. The main area shows the 'User Identity Groups' page with a 'New User Identity Group' form. The form includes a 'Name' field containing 'CSA-ISE' and a 'Description' field. Below the form is a 'Submit' button. On the right, a list of existing groups is shown, including 'ALL\_ACCOUNTS (default)', 'CSA-ISE' (marked as 'GROUP CREATED'), and 'Employee'. The 'Add' button in the top left of the form area is highlighted with a red box and the number 4. The 'Submit' button is highlighted with a red box and the number 6. The 'Groups' menu item is highlighted with a red box and the number 2. The 'User Identity Groups' folder in the breadcrumb is highlighted with a red box and the number 3.

يحلح م دختسم نيوكت

ك: صاخلا لم اكلال نم ققحتلل يحلح م دختسم نيوكتل

- Administration > Identities لى لقتنا
- Add + قوف رقنا

## Network Access User

\* Username

Status  Enabled ▼

Account Name Alias  ⓘ

Email

### Passwords

Password Type:  ▼

Password Lifetime:

With Expiration ⓘ

Never Expires ⓘ

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

## User Groups

CSA-ISE ▼

- **Username:** ةوطخلال ىل اذه دنن سسي Secure Access: يف فورعم UPN ريفوت مادختساب مدختسملا مسان نيوكت [ةيساسالاب لطلت مل او](#)
- **Status:** طشن
- **Password Lifetime:** كل اقفو، Never Expires، و With Expiration اهن نيوكت 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 ةقداصلما نييعت مت :نظالم

---

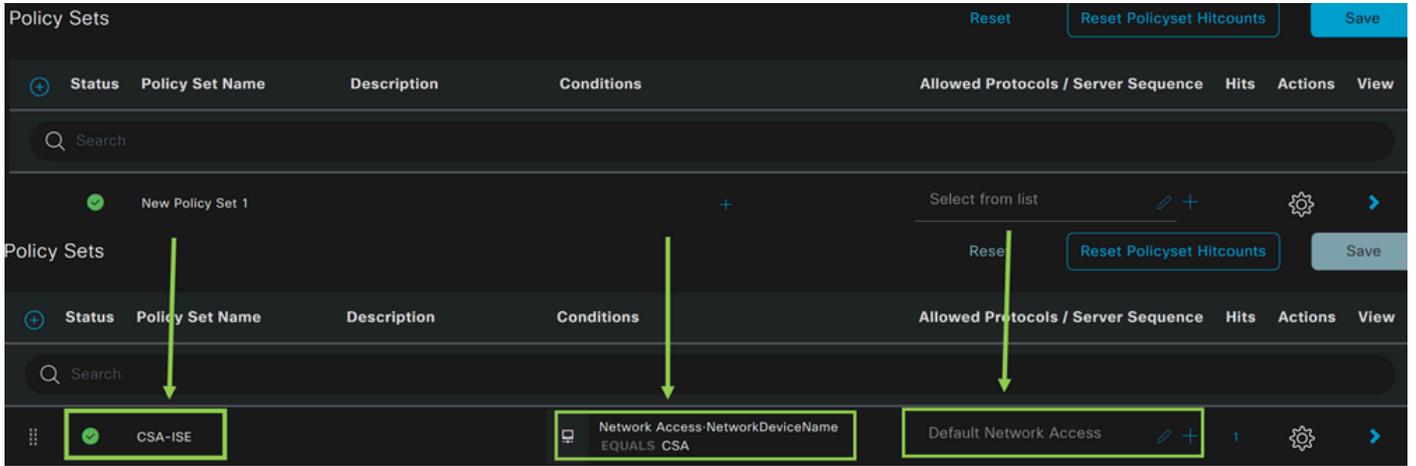
Configure Policy Set. ةوطخالاب ةعباتملاو نيوكتل Save كنكمي ،كلذ دعب

جهنلا ةعومجم نيوكت

ةلاح ويرانيسل اذه حضوي .ضيوفتل او ةقداصلما اناثا هذاختاب ISE موقوي يذلا ءارجال نيوكتب مق ،جهنلا ةعومجم راطا يف اذا امم ققحتي و RADIUS ةقداصلم 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 اذه نيوكتل

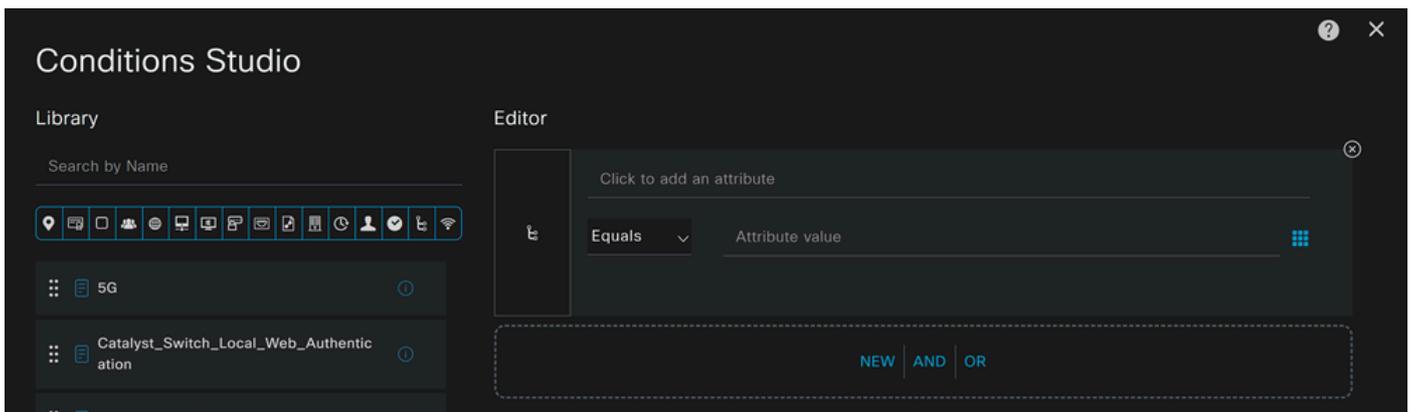
- Policy > Policy Sets قوف رقنا
- ةديج جهن ةعومجم ةفاضال + قوف رقنا



ةقداصملا نيوكتب مق ،كلذ دع .ةيضارتفالا ةعومجملا تحت لمعل نم ال دب ةديج جهن ةعومجم عاشناب مق ،ةالجال هذه يف ةوطخلال يف فرعمل ةكبشلا زاهج ىلا لوصولاب هنيوكت مت يذلا جهنل حمسي .هذه جهنل ةعومجم ىلا ادا نسا ضيوفتلاو ك جهنل يف لوخدلا مث CSA Network Device List نم يتأت ةقداصملا هذه نأ نم ققحتلل [ةكبشلا ةزهجأ ةمئلا نيوكت](#) **Default Network Access** لثم ،اهب حومسملا تالوكوتوربلا ،اريخأو **Conditions**.

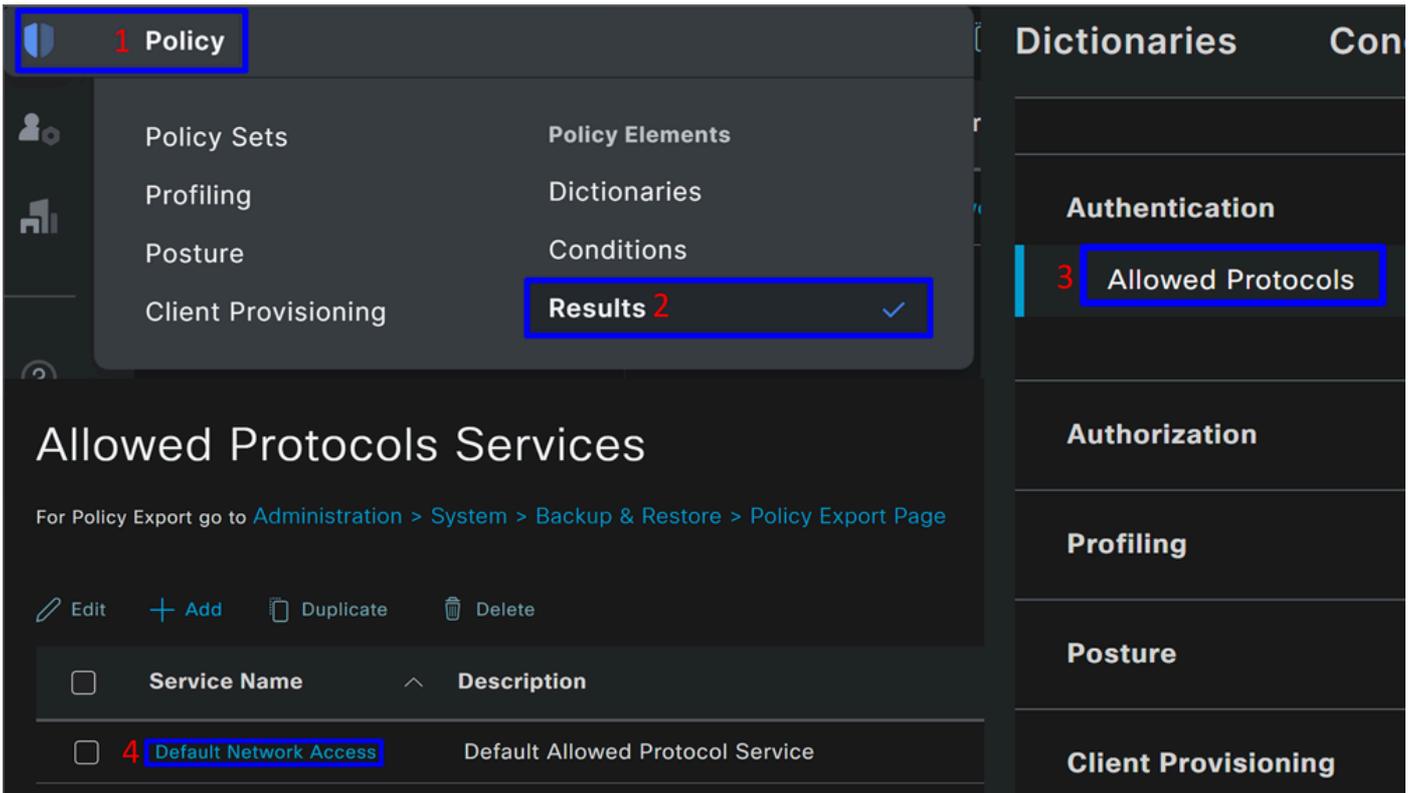
ةيالاتلا تاميلعلا مادختساب ةعباتملا مق ،جهنل ةعومجم قباطت يتلا **condition** تاميلعلا عاشنال

- + قوف رقنا
- يلي ام هاندا **Condition Studio** ةحاتملا تامولعمل نمضتو



- 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



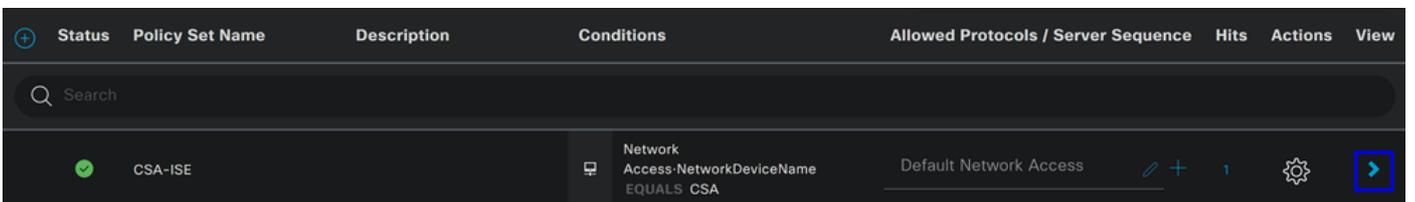


- **Default Network Access** يلى ع اهب حوم سمل تالوكوتورب لاي عي مج يلى ع اطلال انك مي، كذا دع ب

ضيوف تالوا جه نال اة وم جم اة قدا صم نيوك ت

ة: لال تالوا طخال اب رم ت سا، **Policy Set** نمض جه نال **Authorization** و **Authentication** عاش نال

- > قوف رقنا



- ة: ضرع مل **Authorization** تاسا ي س ل **Authentication** يرت، كذا دع ب

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
🟢	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access
<a href="#">&gt; Authentication Policy(2)</a>				
<a href="#">&gt; Authorization Policy - Local Exceptions</a>				
<a href="#">&gt; Authorization Policy - Global Exceptions</a>				
<a href="#">&gt; Authorization Policy(2)</a>				

### قواعد العمل جهن

تزوجاً قمي؛ اق نيوكت ةوطخالل يف ددحملل زاهلل ةسايس ىرت، ةالجال هذه يف قرط ةدعب نيوكتلل كنكمي، ةقداصلمل جهنل ةددحملل ريعام ىلعل ءانب ةقداصلمل نم ققحتتو، ةكبشلا

- ةضوفرمل وأ ةحجان ةقداصلمل مهيدل **Network Device CSA** ةقداصلمل لالخل نم مهتقداصلمل تمت نيذلل نومدختسملل

Status	Rule Name	Conditions	Use
🟢	Authentication Secure Access	Network Access:NetworkDeviceName EQUALS CSA	Internal Users
<a href="#">Options</a>			

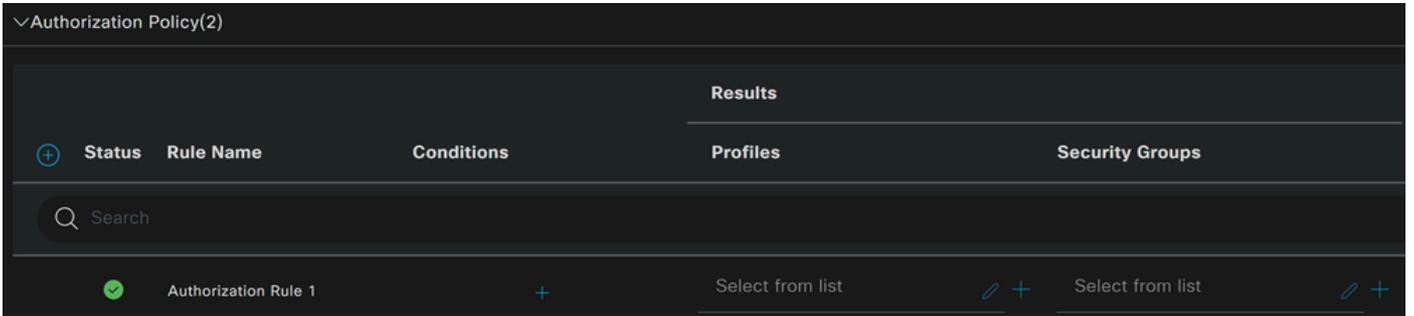
ةوطخالل نيوكت جهن ةعومحمل نمض ددحملل سفن وه جهنل

### ليوختل ةسايس

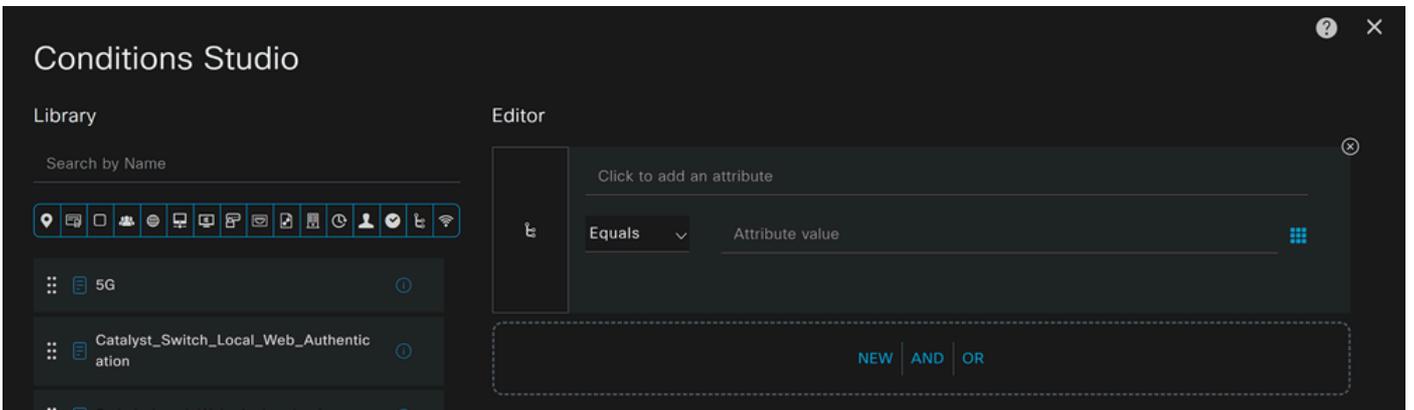
نيوكت ةوطخالل يف ةددحملل ةعومحملل يف نيومدختسملل ليوختب مق، ةالجال هذه يف قرط ةدعب ليوختل جهن نيوكتلل كنكمي كبا صاخلل ليوختل جهن نيوكتلل لئاللل لائلل ءجار. ةعومحمل

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

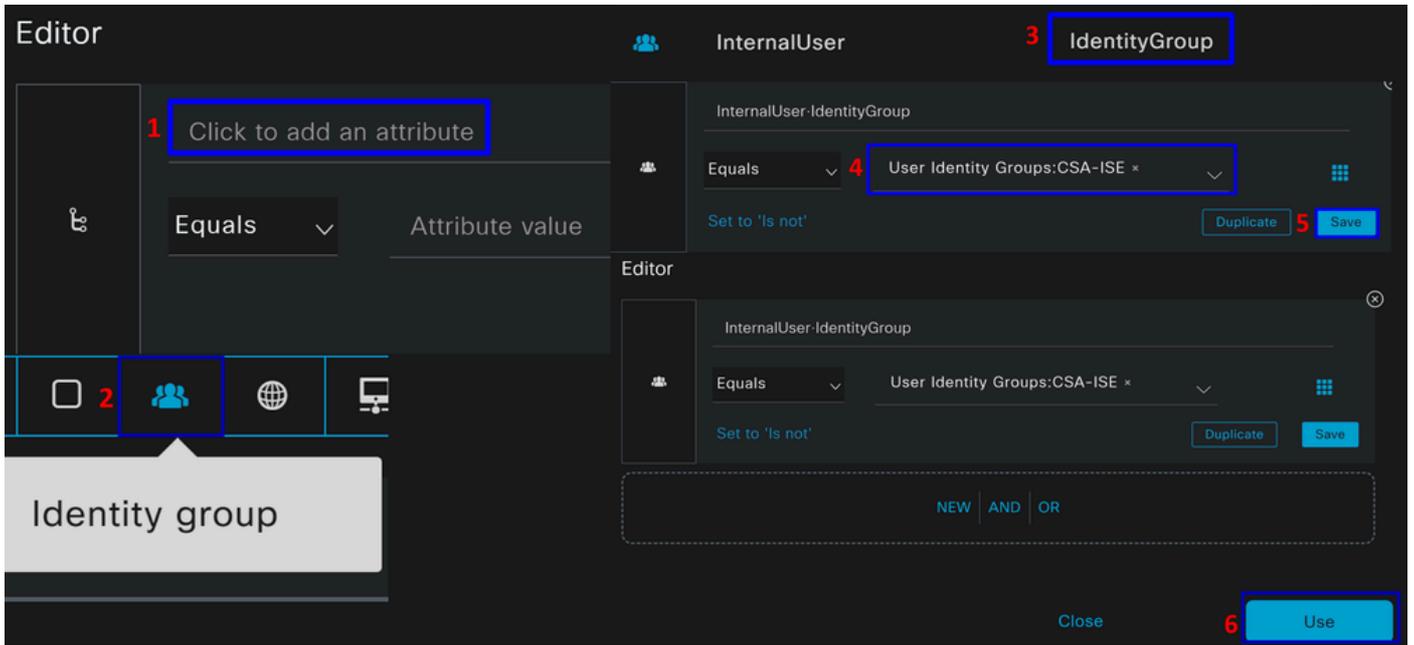
- **Authorization Policy** قوف رقنا
- لثم لي وختلا جهن دي دحتل + قوف رقنا:



- Rule Name، Conditions و Profiles ري غتب مق، ةلالتا ةوطخلل
- ةلوه سب لي وختلا جهن دي دحتل مسا ني وكت Name ني عت دن
- + قوف رقنا، مكحتلا رصن Condition ني وكتل
- تام ول عمل دجت **Condition Studio**، اه تحت

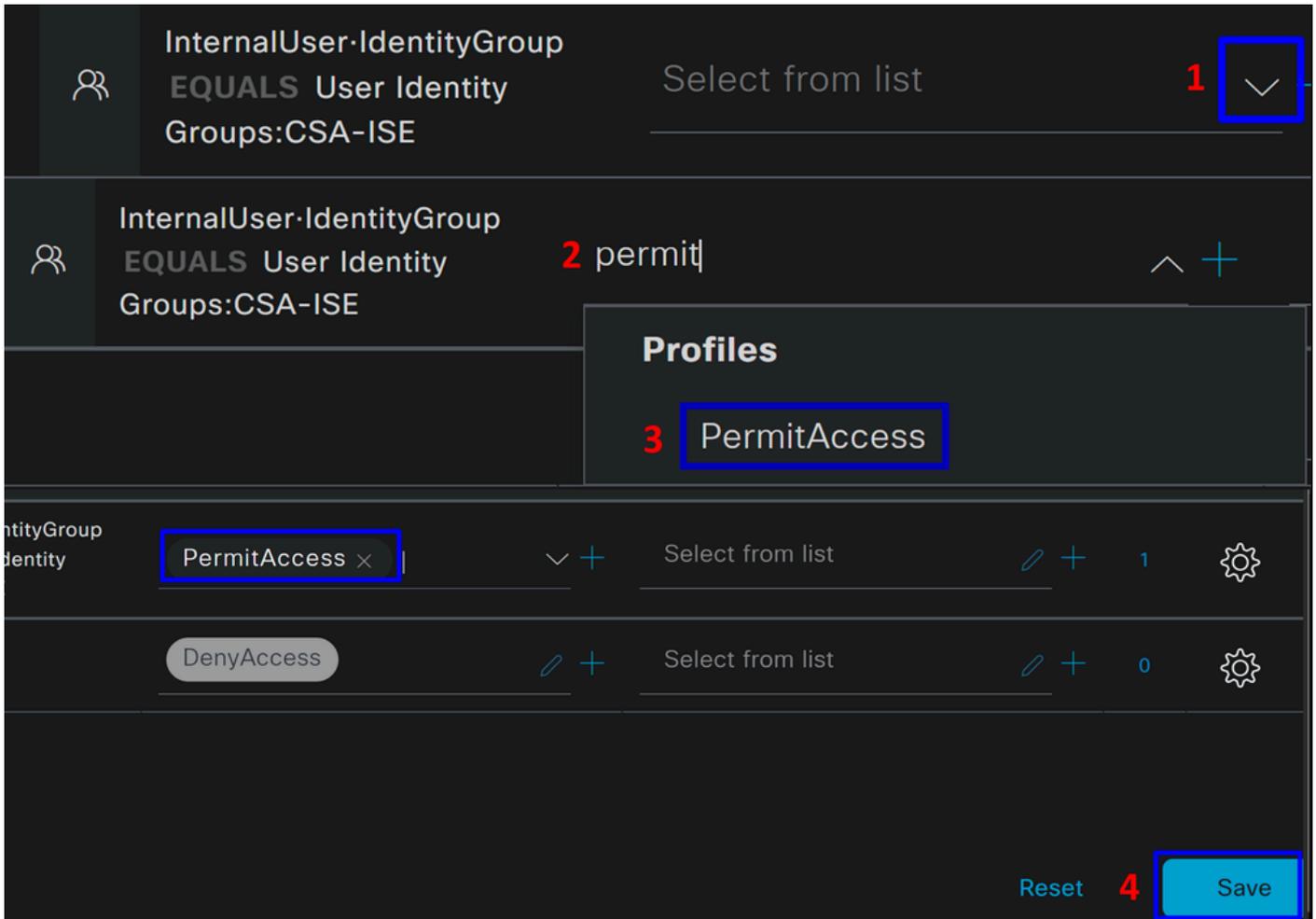


- Click to add an attribute قوف رقنا، طورشلا ءاشنال
- رزل **Identity Group** ل ع رقنا
- رايخ **IdentityGroup** - لي خاد مدختسم قوف رقنا، هاندأ تارايل تحت
- [ني وكتب مق](#)، ةوطخلال ي ةقداصل لل دمت عمل **Group** ل ع روثل لل ةلدسنم ل ةمئاقلا مدختسأ، رايخال **Equals** تحت [ةعومجم](#)
- Save رقنا
- Use رقنا



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 نع شحبالا
- PermitAccess دي دحت
- Save رونا



نود لصتې مدختسملناك اذام ققحتلل ةقداصللاب مق .كتسايسو Authentication Authorization فيرعتب تمق ،كلذ دعب ISE و Secure Access ىلع تالجسلا ةيؤركنكمي ناك اذامو ةلكشم ثودح

لاصتال او Secure Access ىلع هؤاشنم ت يذلا فيرعتلا فلم مادختسا كنكمي ،(VPN) ةيره اظلا ةصاخلا ةكبشلاب لاصتال ل ISE فيرعت فلم مادختساب Secure Client لالخنم

- ةقداصللاب ىلع ةقفاوملا دنع Secure Access في لجسلا ضرع متي فيكي

- [نمألا لوصول تامولعم ةحول](#) ىل لقتنا

- **Monitor > Remote Access Log** قوف رقنا

## 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 لجلسلا ضرع متي فيك

◦ ىلا لقتنا Cisco ISE Dashboard

- ىلا لقتنا Operations > Live Logs قوف رونا

Status	Details	Identity	Authentication Policy	Authorization Policy
×	∨	Identity	Authentication Policy	Authorization Policy
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access
		vpnuser@...	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> Authorization Secure Access

Active Directory ىم دختسم وأ ىن ىل حملا RADIUS ىم دختسم نيوكت

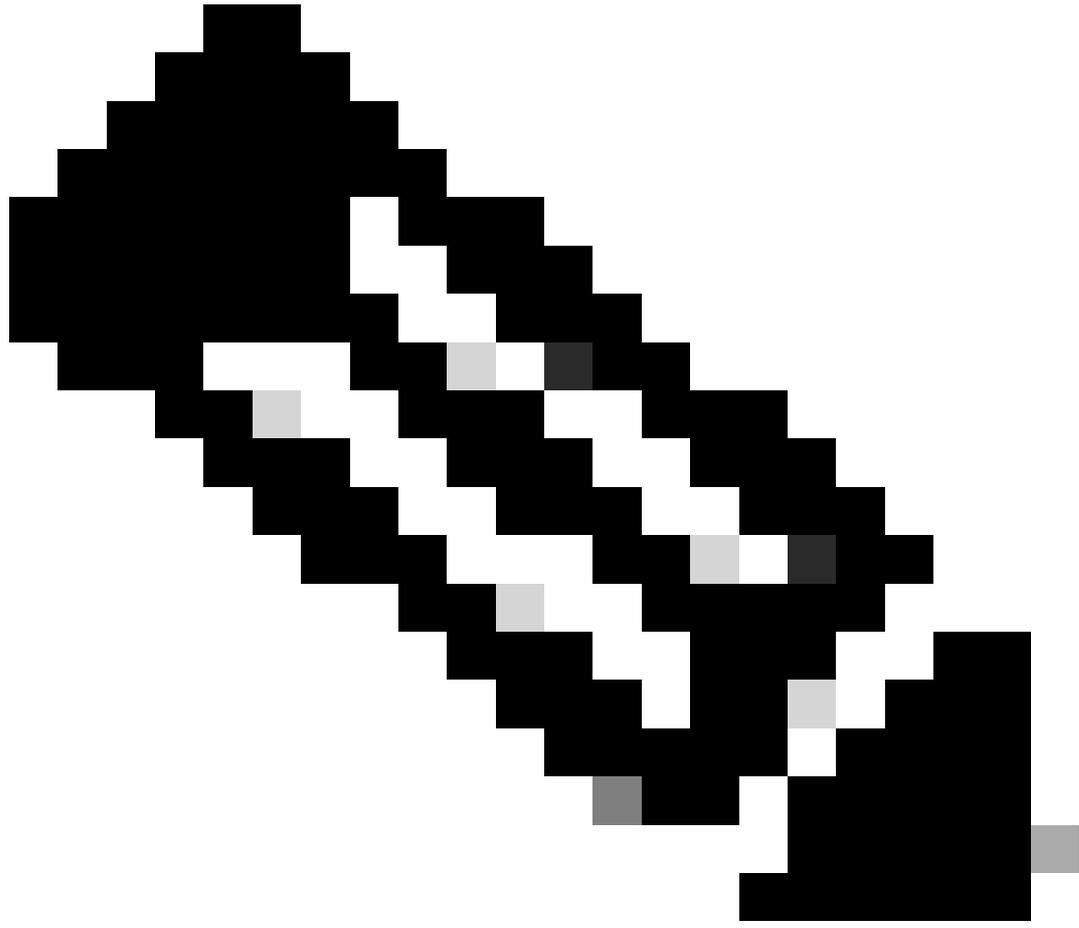
ISE ةىعضو نيوكت

وأ ةىلخادلا دراوملا ىلا لوصولا حنم لبق ةىاهنلا ةطقن قفاوت نم ققحتلل نيوكتلا ءاشناب مق ،ويران ىسلا اذه فى هضفر.

ةىلاتلا تاوطخلا ىلا لقتنا ،هنيوكتل

عضولا طورش نيوكت

- ISE تامولعم ةحول ىلا لقتنا
- Work Center > Policy Elements > Conditions قوف رونا
- Anti-Malware قوف رونا



تاسايسلا ىلع ءانب حىحصلا مئيقىتلا ءارجاؤ كتزءجأ ءضونم ققحتلل تاراىءلا نم دىءءال دءت ،كانه :ءظءالم  
كء ءصاوءلا ءىءءءلا

## Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource

File

Firewall

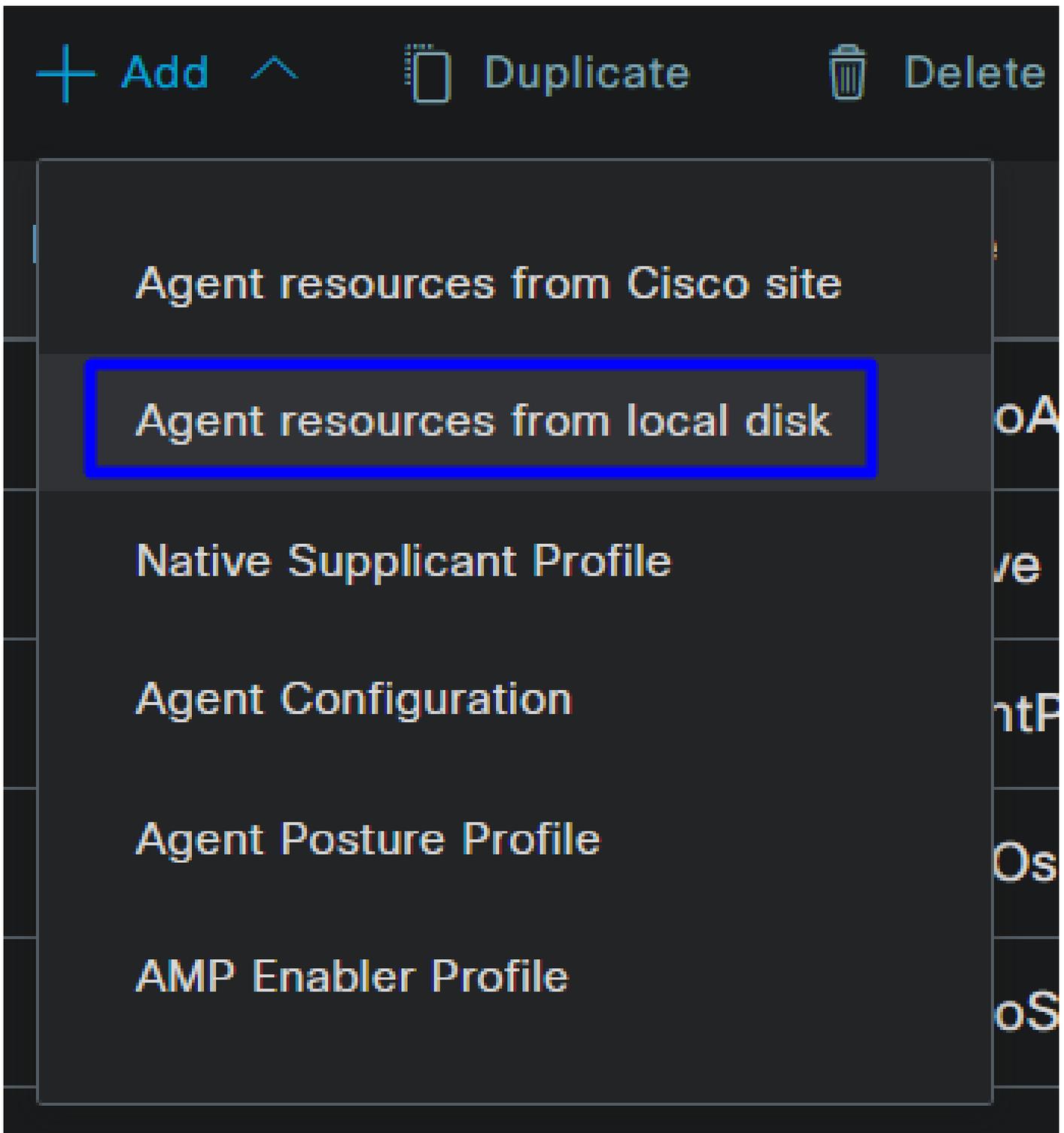
1. Agent Resources	للمعلم لى ةنم آل بيول دا دم ا ةم زح .
2. Compliance Module	Cisco ISE Compliance Module ةي طمن ل ا ة د ح و ل ا
3. Agent Profile	دادع ا ل ا في ر ع ت ف ل م ي ف م ك ح ت ل ا
3. Agent Configuration	ن م ا ه ر ي ف و ت م ت ي ي ت ل ا ة ي ط م ن ل ا ت ا د ح و ل ا د ي د ح ت ف ي ر ع ت ف ل م م ا د خ ت س ا ب ، دادم ا ل ا ة ب ا و ب دادع ا ل ا ل خ ل ل . ل ي ك و ل ا د ر ا و م و ل ل ي ك و ل ا

### Step 1 اه ل ا ي م ح ت و ل ل ي ك و ل ا د ر ا و م ل ي ز ن ت

- ن ا ب ح ي ؛ ب ي و ل ا ر ش ن ة م ز ح ل ي ز ن ت ب م ق و [Cisco Download Portal](#) ل ي ز ن ت ل ل خ د م ي ل ا ل ق ت ن ا ، د ي د ج ل ي م ع د ر و م ة ف ا ض ا ل .pkg . ق ي س ن ت ب ب ي و ل ا ر ش ن ف ل م ن و ك ي

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	  
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	  
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	  

- م ز ح ل ا ل ي م ح ت ب م ق و Agent resources from local disk + ق و ف ر ق ن ا >



Step 2: إضافة قوائم الاختلافات ودعم تنزيل Step 2

- + 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 ةدحوللكل رايتخالال ةناخ يلع 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

- **Name ل Posture Profile** 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 ليكول نيوك ت نيوك 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، نضيف ملف التكوين، كما يلي:

\* Select Agent Package: CiscoSecureClientDesktopWindows 5.1 

\* Configuration Name:

Description:

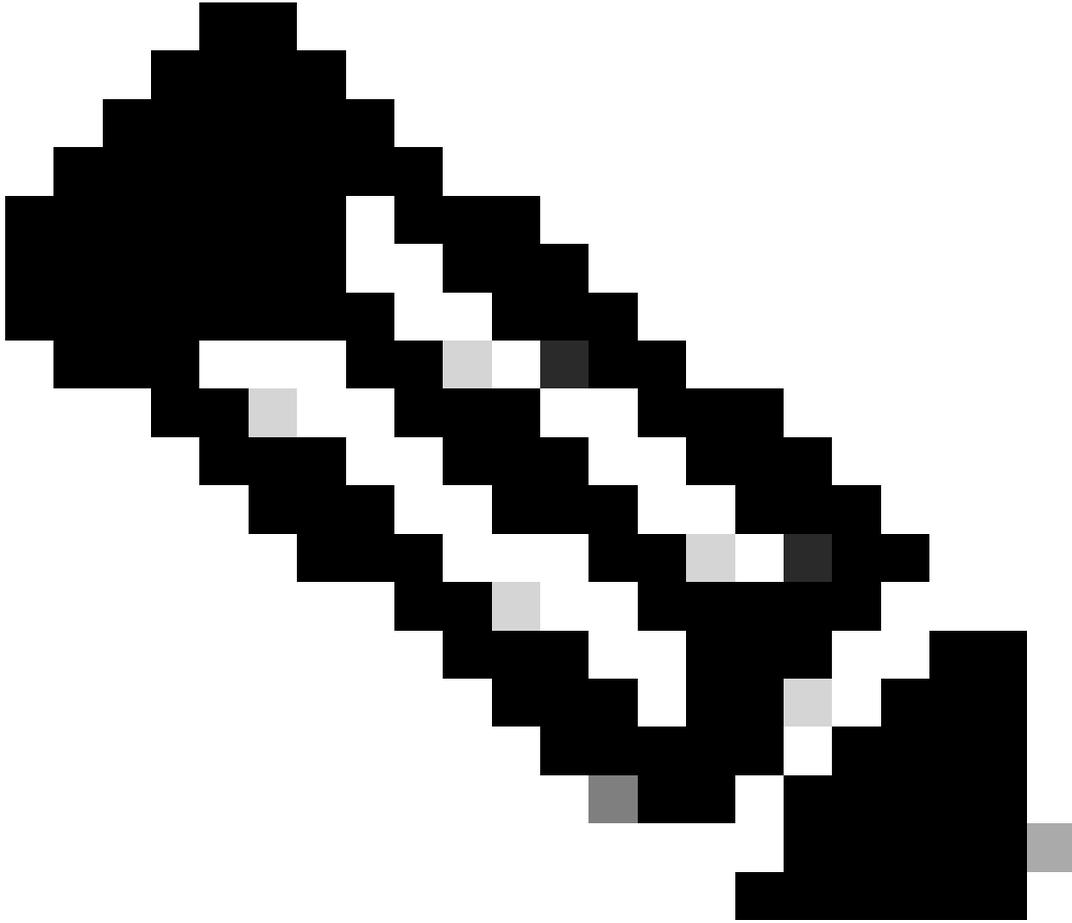
### Description Value Notes

\* Compliance Module CiscoSecureClientComplianceModuleWi 



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

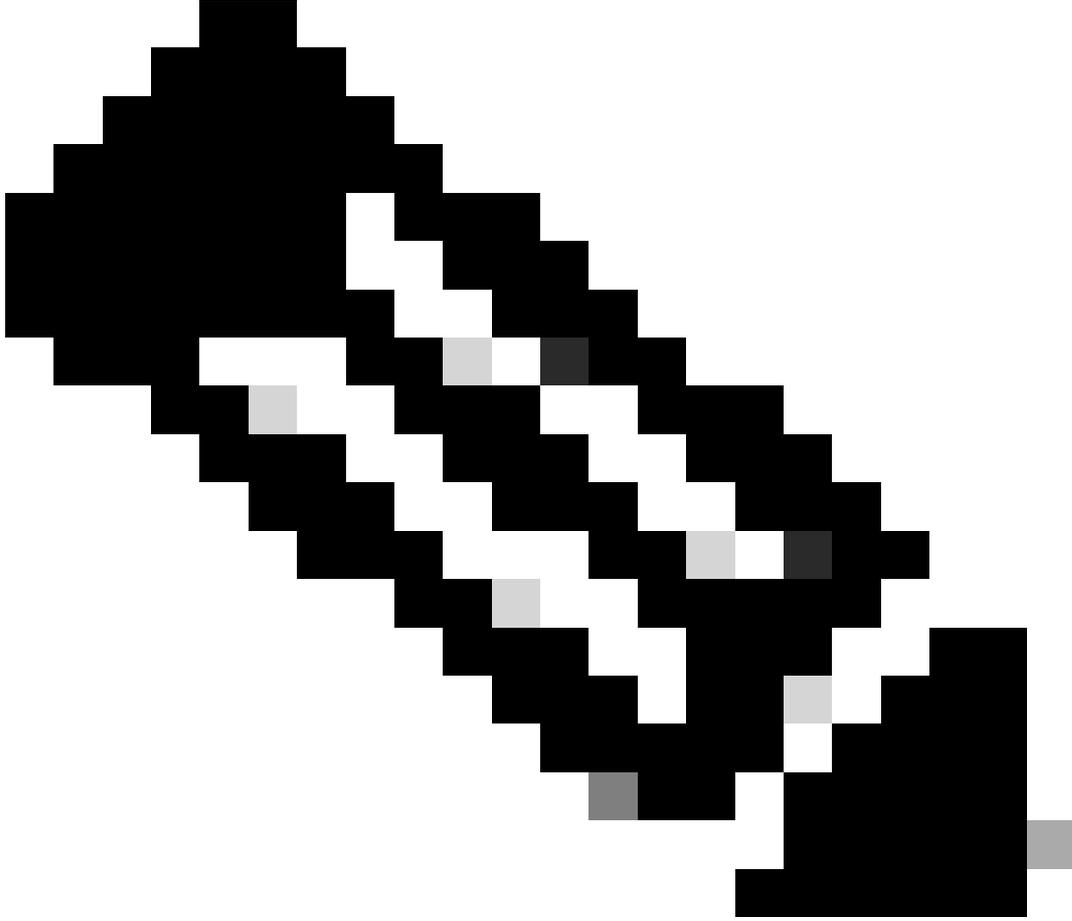
- Save رقنا



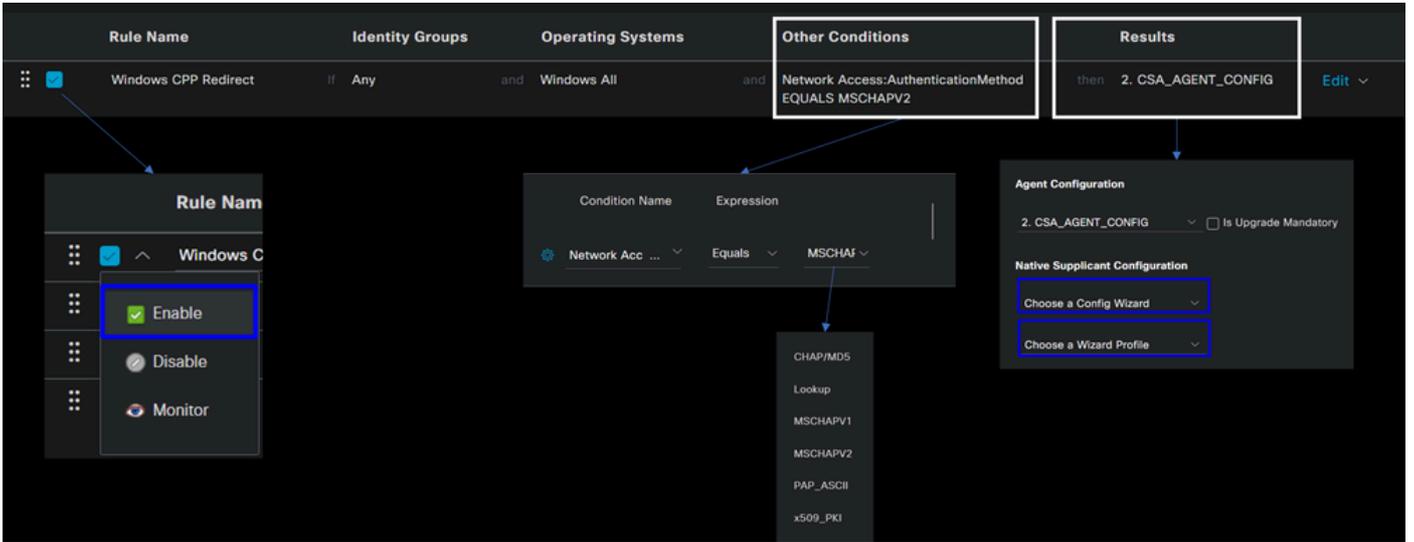
لقتسم دحاو ليمع نيوكت، Linux أو Mac OS أو Windows، ليغشت ماظن لكل نوكي نأب ىصوي: ةظحالم

نيوكت كمزلي، ةريخألا ةوطخالا في اهنيوكت مت يتلا ةيظمنلا تادحولاو (ISE) ةيوهلا تامدخ كرحم ةيعضو دادع| دادع| نيكم تل 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 ةللي كولا جم انربلا ةمزح لى ادا نسا ليغششلا ماظن رتخأ [قمزح 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:** [Wizard](#) و [Config Wizard](#) 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 ةعضو 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	- ليلكول تيبتتل هيجوتلا ةداعإ - فروع م لا مدختسم لا عم قفاوتم قحاتل دي ق عضولا
DenyAccess	لوصول ص فر - قفاوتم ريغ مدختسم

ISE تامولعم ةحول ليل لقتنا ، (DACL) ةيساسألا ةينبالا لوصولا يف مكحتلا ةمئاق نيوكتل

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

The screenshot shows the configuration page for a DACL named 'CSA-Compliant'. The 'Name' field is filled with 'CSA-Compliant'. The 'Description' field is empty. Under 'IP version', the 'IPv4' radio button is selected. The 'Content' field contains a list of IP addresses followed by the command 'permit ip any any'.

* Name	CSA-Compliant	
Description		
IP version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Agnostic <span style="float: right;">?</span>	
* DACL Content	1234567 8910111 2131415 1617181 9202122 2324252 6272829 3031323 3343536 3738394 2111010	permit ip any any

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

<#root>

permit ip any any

فروع م 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	
0111010	

✓ Check DACL Syntax

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

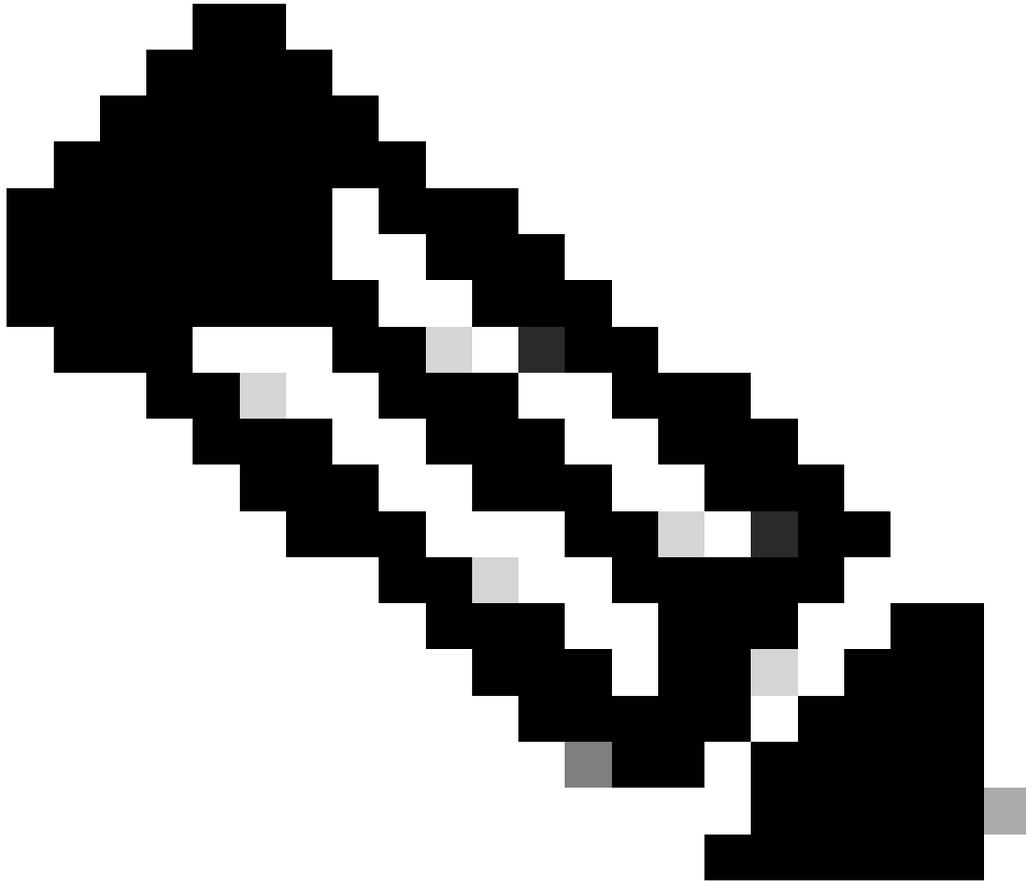
```

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 IP 192.168.10.206 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: رتخ | ACCESS\_ACCEPT

- **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 :ةظالم

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 تم ق يتلآ ليوختلآ فيرعت تافل م ىلإ اهئاشن اب موقت يتلآ ةثالثلآ جهنلآ هذه دن تست ىرخأ ةدحاو ءاشن آل جاتحت

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

ISE تامولعم ةحول ىلإ 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)					

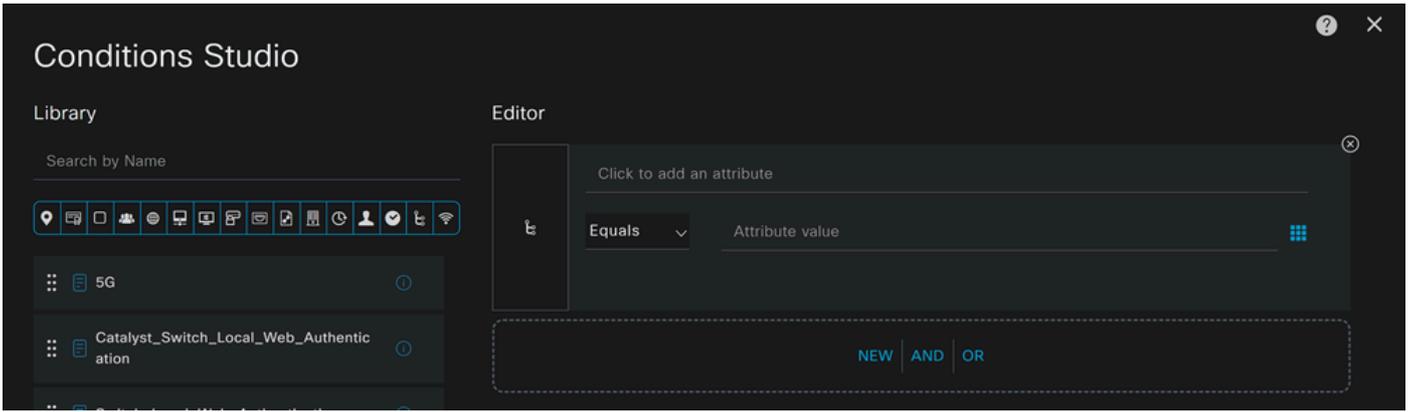
- يلاتلا بېترتلاب ةيلاتلا ةثاللا تاسايسلا ءاشناب تمق:

✓	CSA-Compliant	AND	<ul style="list-style-type: none"> <li>Compliant_Devices</li> <li>Network_Access_Authentication_Passed</li> <li>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</li> </ul>	CSA-Post-Compliant
✓	CSA-Unknown-Compliant	AND	<ul style="list-style-type: none"> <li>Network_Access_Authentication_Passed</li> <li>Compliance_Unknown_Devices</li> <li>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</li> </ul>	CSA-Unknown-Compliant
✓	CSA-Non-Compliant	AND	<ul style="list-style-type: none"> <li>Non_Compliant_Devices</li> <li>Network_Access_Authentication_Passed</li> <li>InternalUser-IdentityGroup EQUALS User Identity Groups:CSA-ISE</li> </ul>	DenyAccess

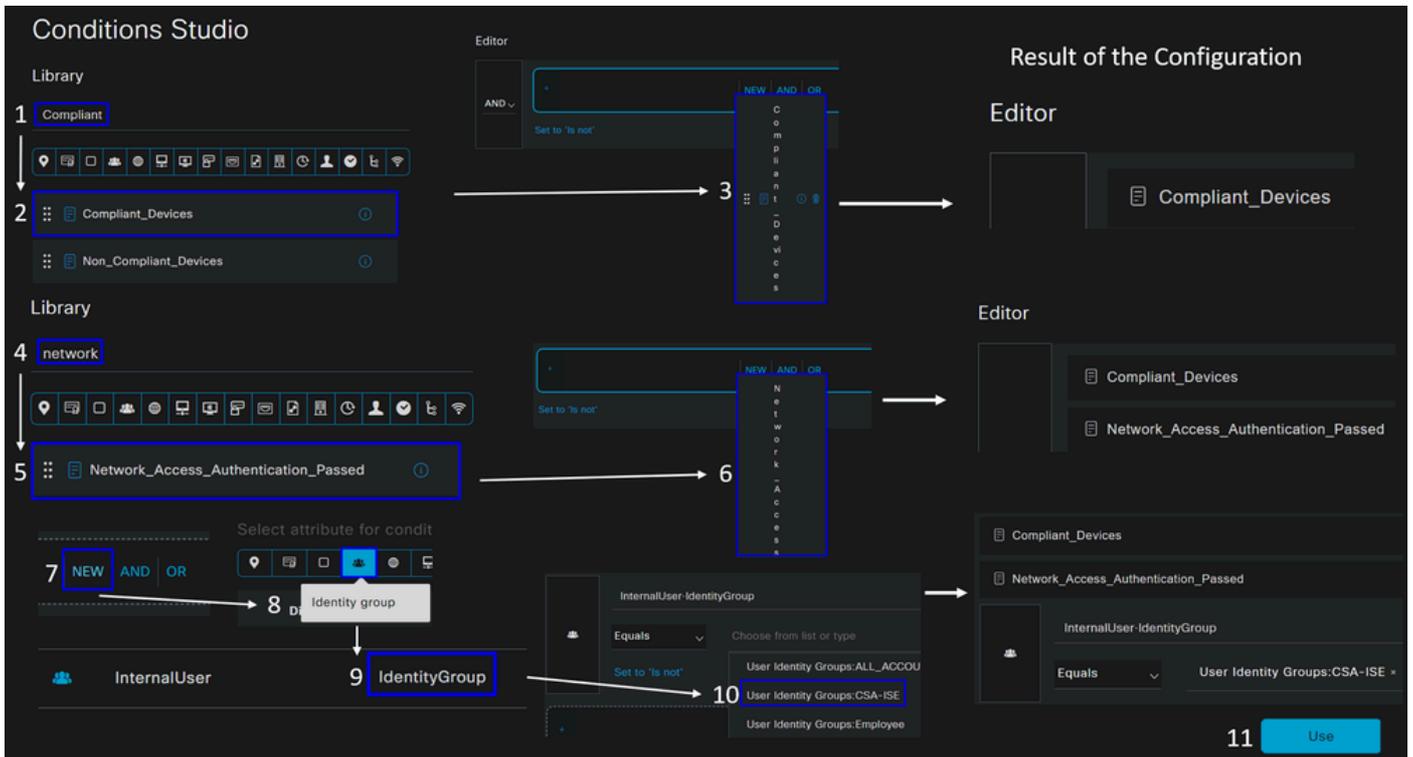
- ةساي سلا CSA-Compliance دي دحتل + رقنا :

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

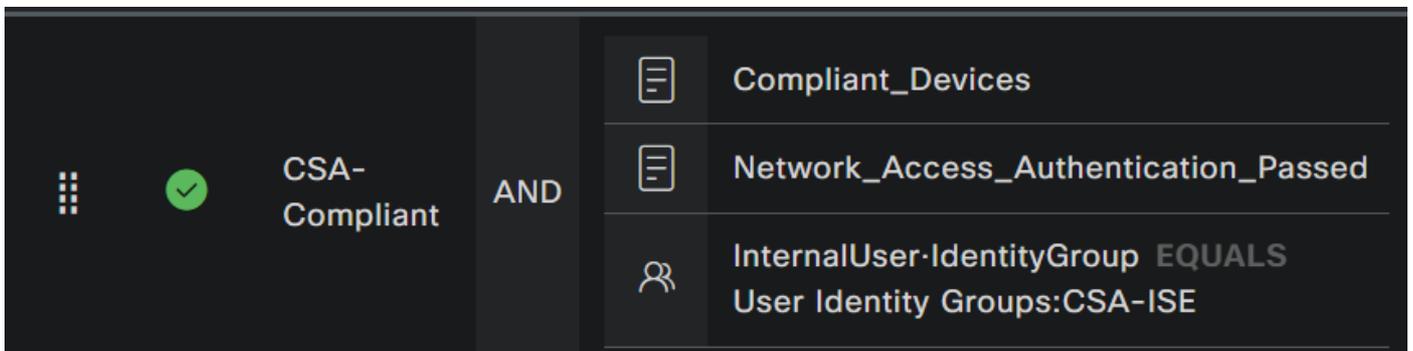
- Rule Name، Conditions و Profiles ري يغب مق ،ةلالتا ةوطلل
- CSA-Compliance لى نيوكالتا Name مسا نييعت دنع
- + قوف رقنا ،مكحتلا رصنع Condition نيوكتلا
- تامولعمل دجت Condition Studio ،اهتحت



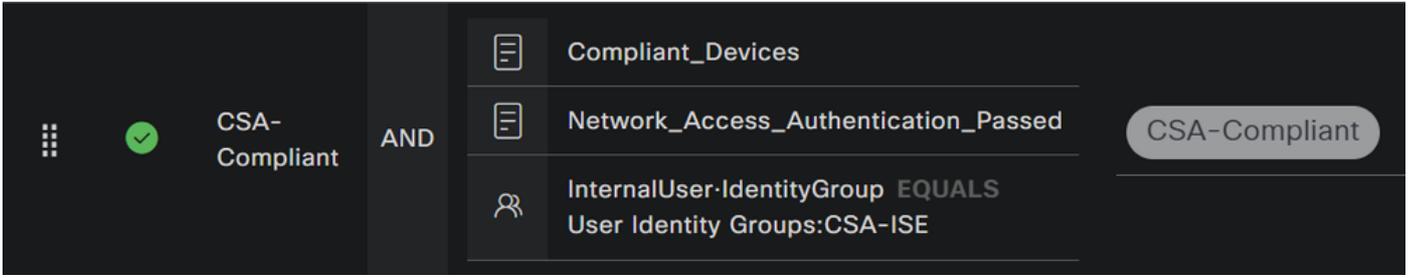
- **compliant** ن ع شحبا ، طرشللا ءاشنال
- **Compliant\_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **network** ن ع شحبا ، يناللا طرشللا ءاشنال
- **Network\_Access\_Authentication\_Passed** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **New** لوخدل Editor لفسأ رقنا
- **Identity Group** لىل ع رقنا
- **Internal User Identity Group** رتخا
- **User Identity Group** رتخا ، **Equals** تحت
- **Use** رقنا



- ةيلات الة روصال كيدل ،ةجيتنك

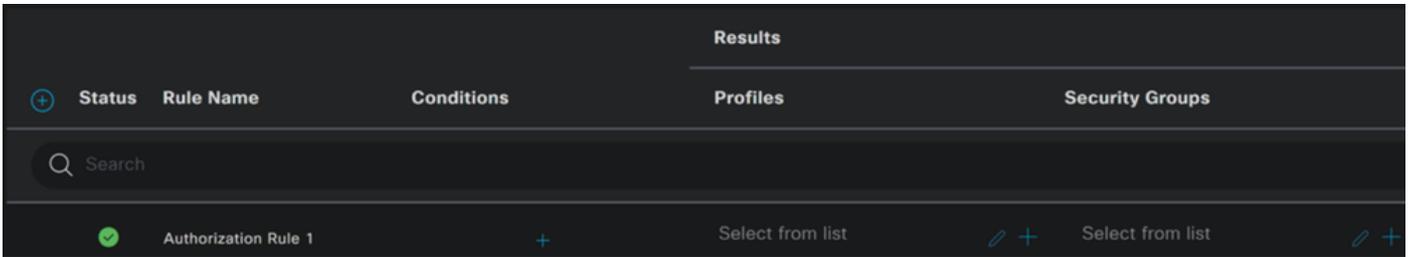


- [فیرعت فایلم](#) ،ةوطخال الة نوكم الة یوكش الة لیوخت فیرعت فلم رتخاو لدسنم الة رزلا تحت رقنا **Profile** تحت [قفاوتم لیوخت](#)

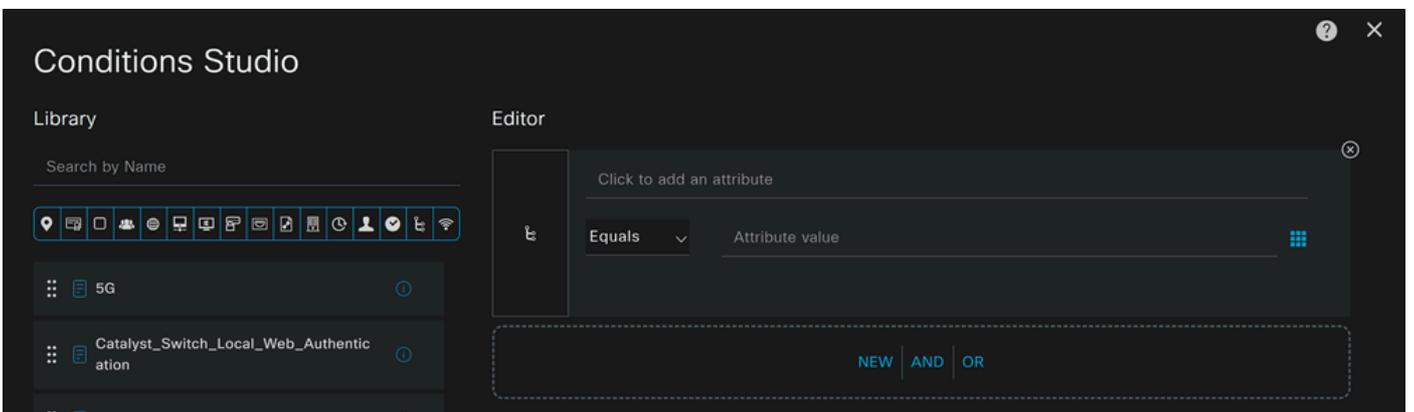


Compliance Policy Set. نيوكتب نآلا تمق دقل

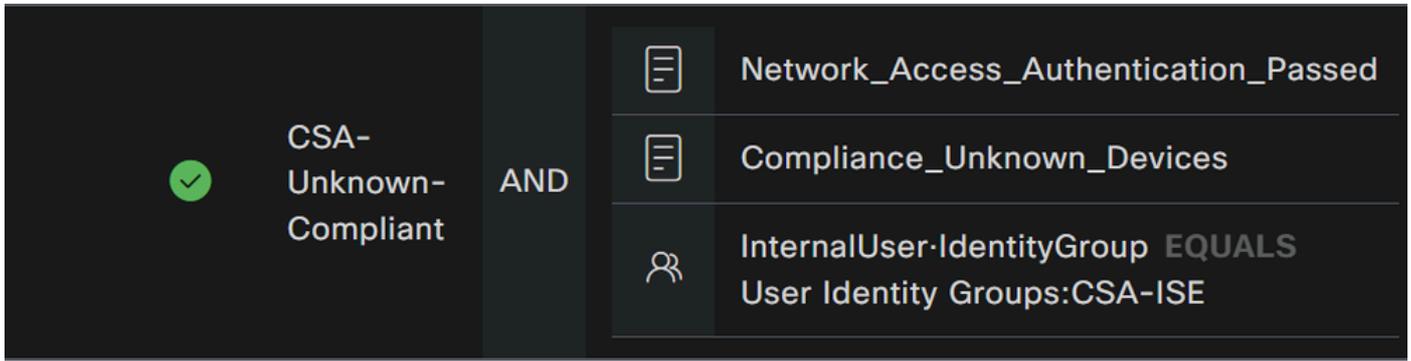
- ةسايسال CSA-Unknown-Compliance ديحتل + رقن :



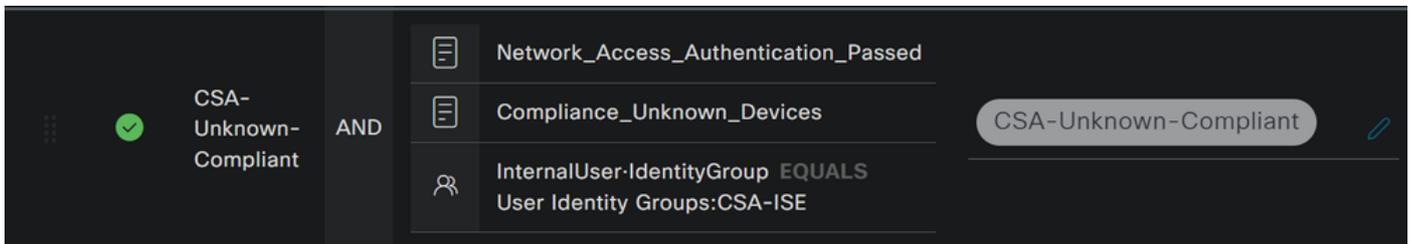
- Rule Name، Conditions و Profiles ريغت ب مق، ةيلاتال ةوطخلل
- CSA-Unknown-Compliance لىل نيوكتال Name مسا نييعت دنع
- + قوف رقن، مكحتال رصنع Condition نيوكتل
- تامولعمل دجت Condition Studio، اهتحت





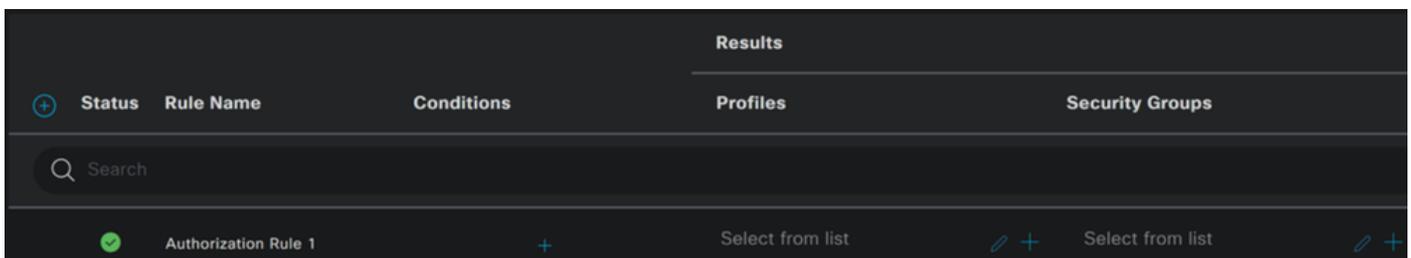


- [في برع ت فلم](#)، ةوطخلال ىلع نوكملا ىوكشلال لىوخت في برع ت فلم رتخا و لدس نمل رزلا تحت رقنلا **Profile** تحت [قفاوتم فورعم ريغ لىوخت](#)



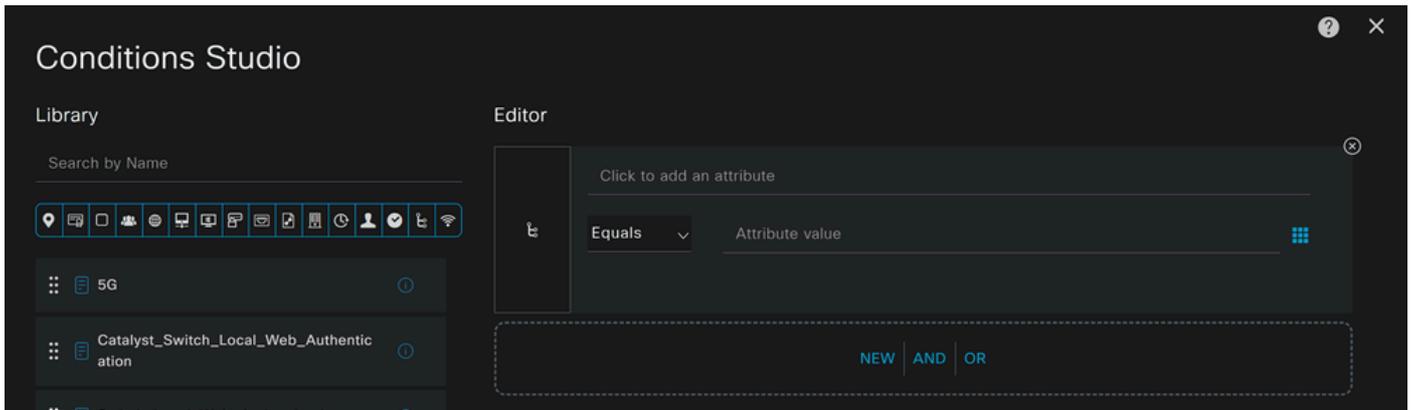
Unknown Compliance Policy Set. نيوك ت ب نآلا تمق دقل

- ةسايسال **CSA- Non-Compliant** دي دحتل + قوف رقنا

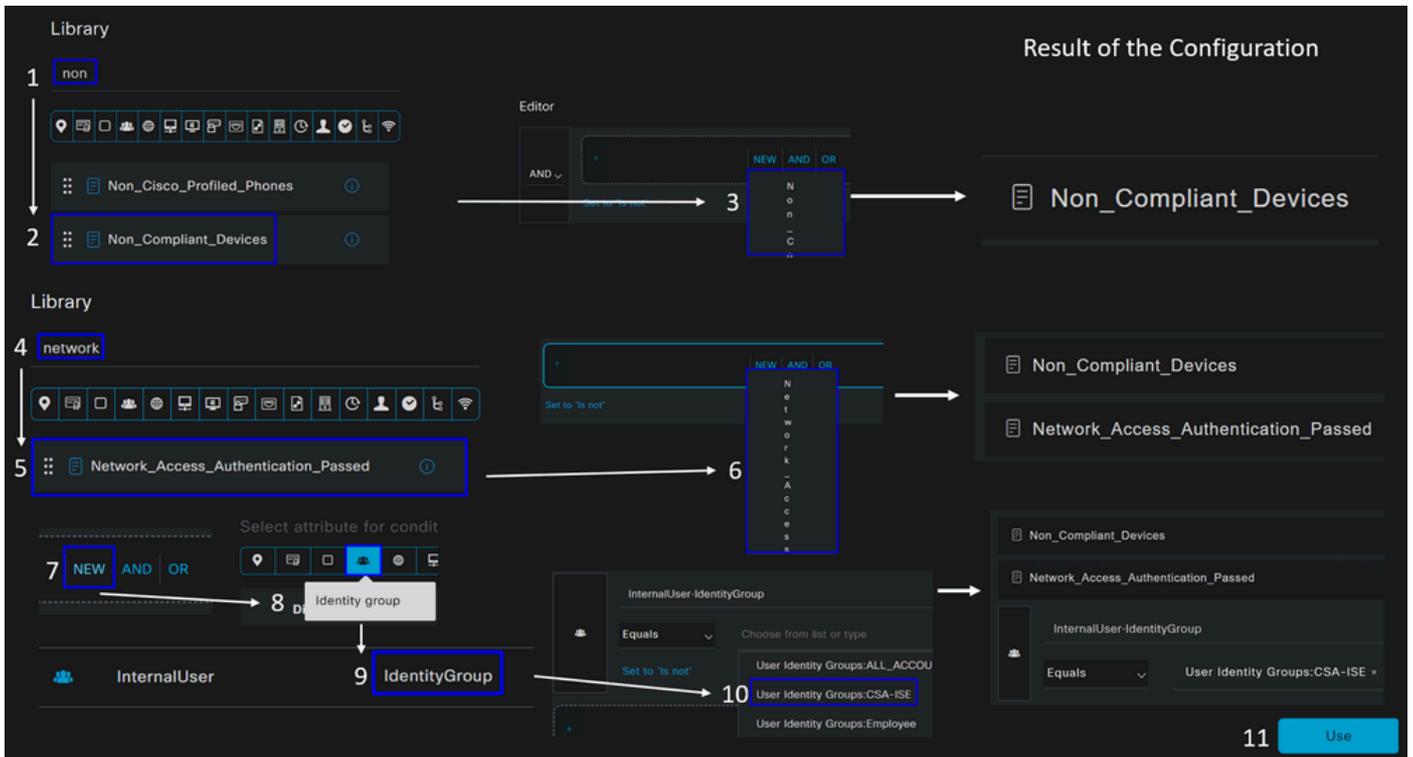


- Profiles و Conditions، Rule Name، ةيغ ت ب مق، ةيلاللا ةوطخلل
- **CSA-Non-Compliance** لىل نيوك تال **Name** مس نييعت دنع
- + قوف رقنا، مكحتال رصنع **Condition** نيوك تال

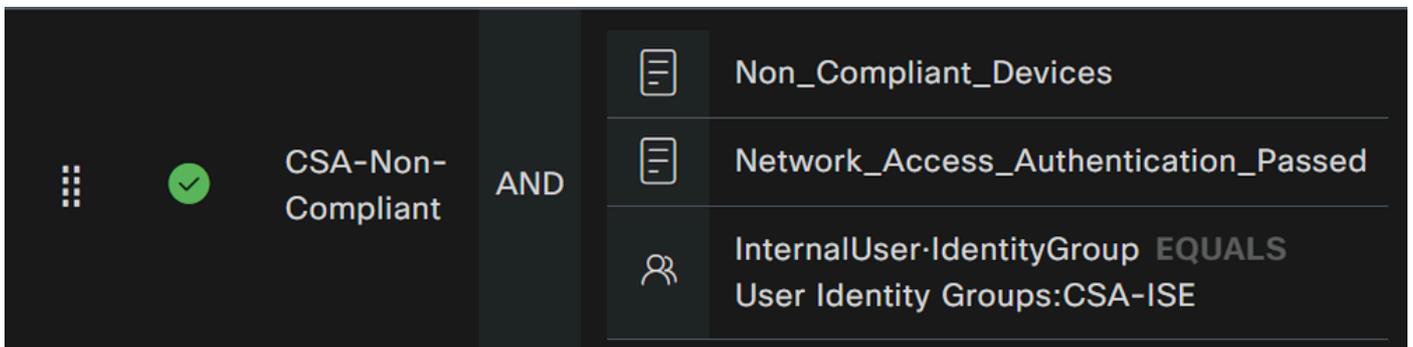
- تامولعمل دجت **Condition Studio**، اهتحت



- **non** نع شحبا، طارشلا عاشنال
- **Non\_Compliant\_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **network** نع شحبا، يئناثلا طارشلا عاشنال
- **Network\_Access\_Authentication\_Passed** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **New** لوخدل Editor لفسأ رقنا
- ةنوقيال **Identity Group** لىع رقنا
- **Internal User Identity Group** رتخا
- هتقباطم ديرت يذلا **User Identity Group** رتخا، **Equals** تحت
- **Use** رقنا

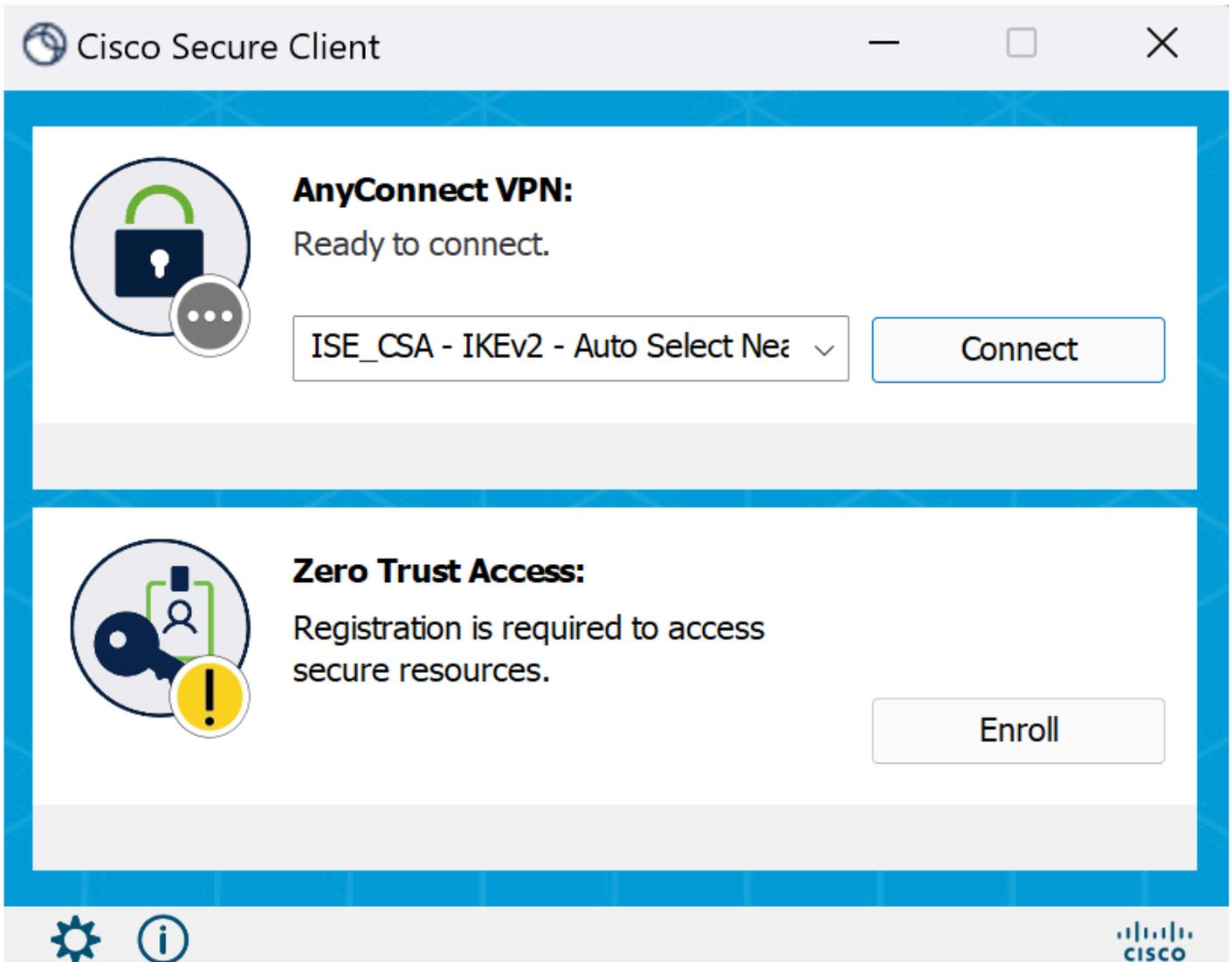


- قیالات لارو وصل كېدل، ډېجېټنك

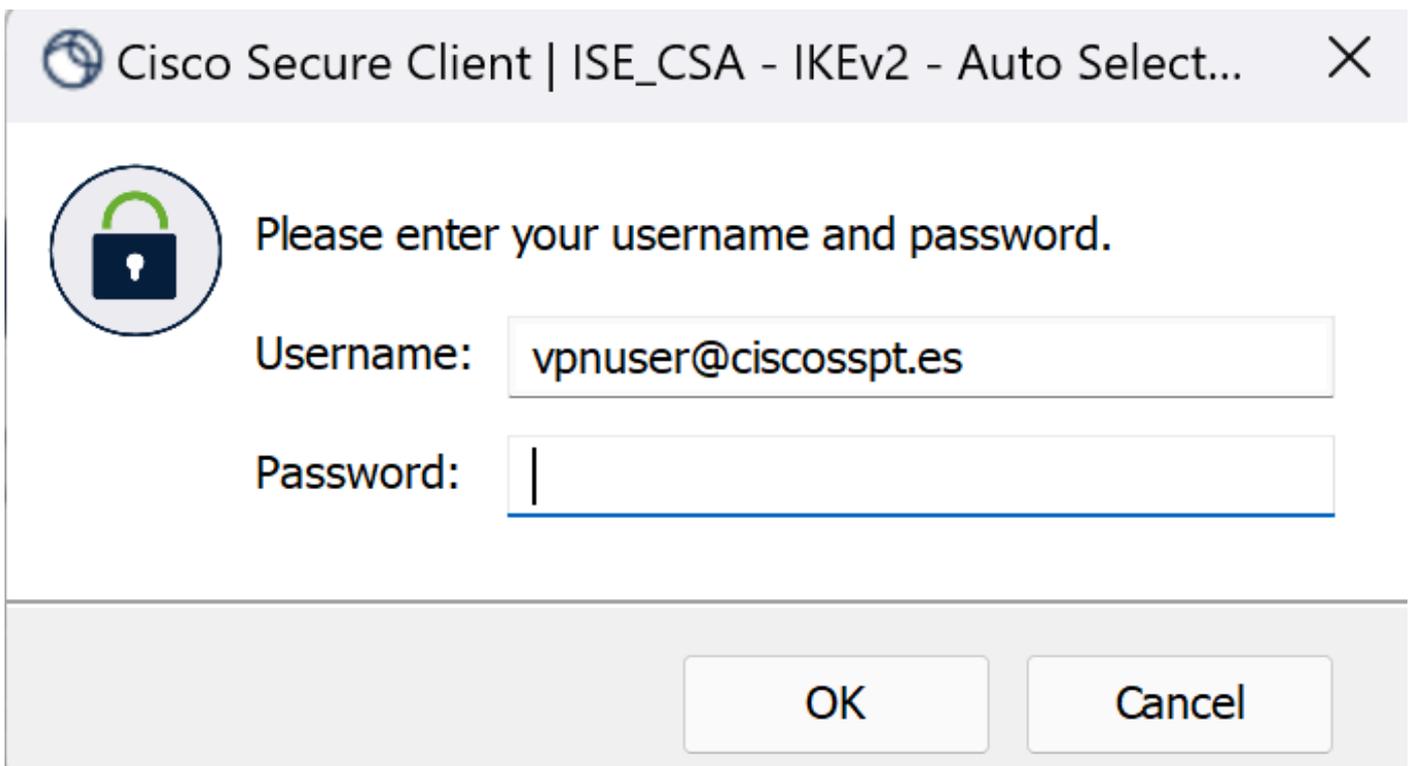


- **DenyAccess** ډوكشال لېوخت فيرعت فلم رتخاو لډس نمل رزلا تحت رونا **Profile** تحت

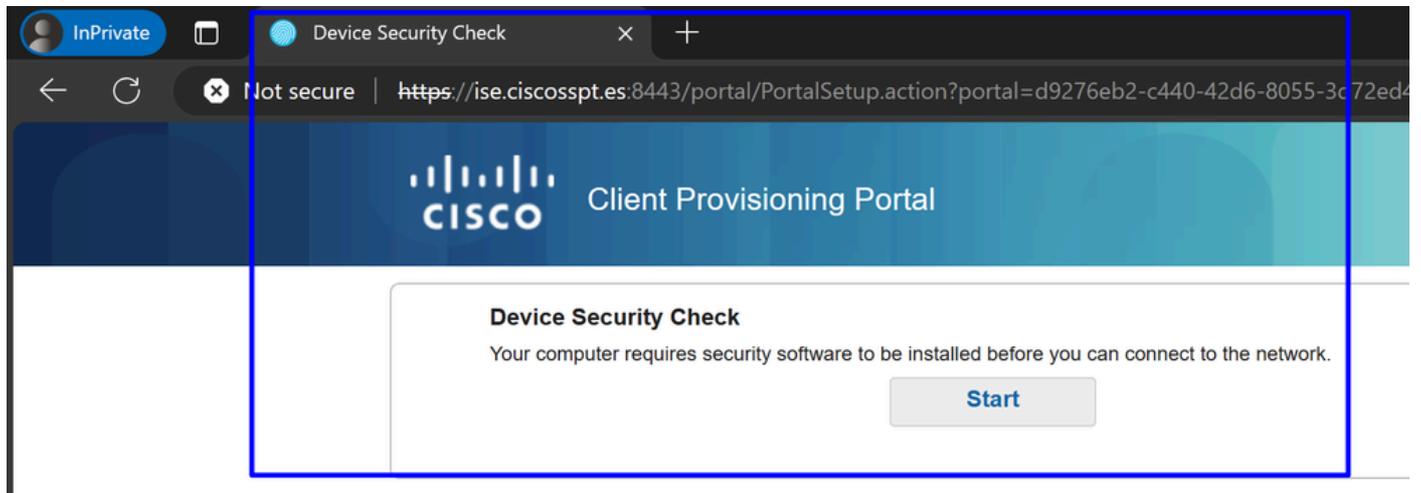
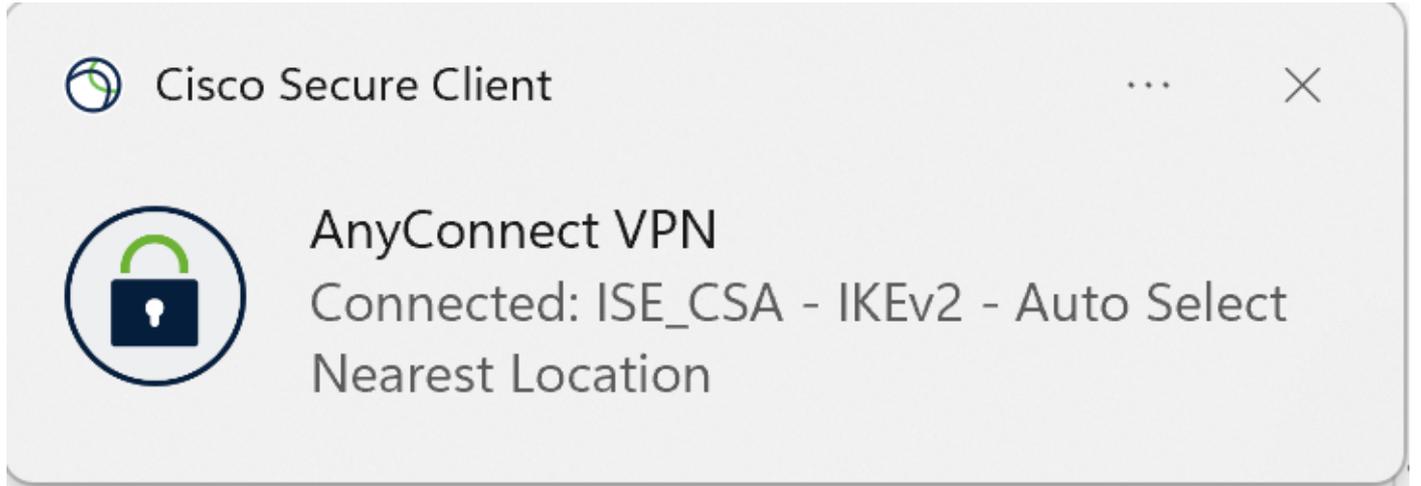


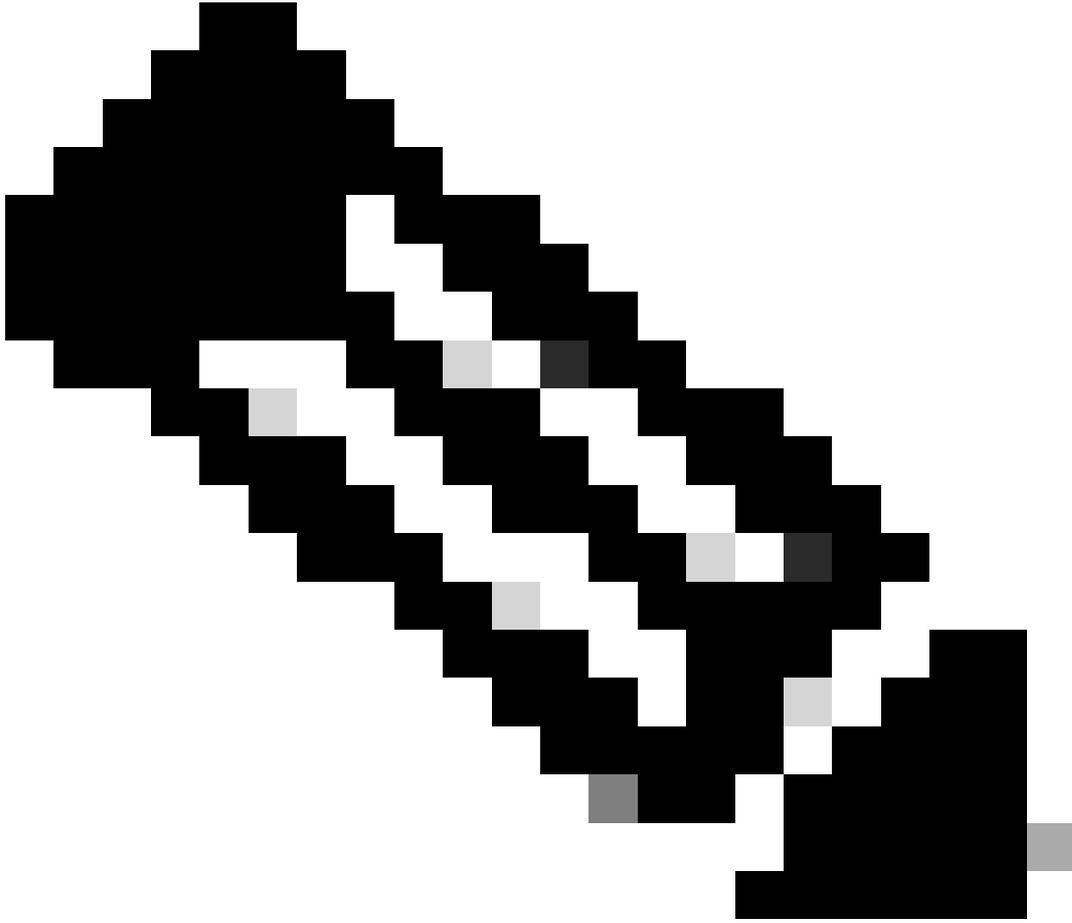


2. ةقداصم لل دامت عال اتا نايب ريفوت .



3. رمألا نكي مل اذوا ISE؛ كهي جوت ةءاعإ متت ام ابلاغو (VPN) ةيره اظلال ةصاخلا ةكبشلاب كل صوت متي، ةطقنلا هذه دنع 3. كذلك http:1.1.1.1 إلى لقتنلا ةلواجم كنكمي، كذلك





لماع تيپثت مدعل ارطان [CSA-Unknown-compliance](#) تاسايسال ةومجم - ليوختال نمض عقت ةطقنللا هذه دنع :ةظالم  
للكوللا تيپثتل ISE دادم ةباوب لى لكهيجوت ةداع متتو ،زاهال لىل ع ISE Posture Agent

4. لىللكوللا ريفوت ةعباتمل "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

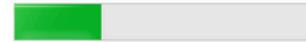
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

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.**

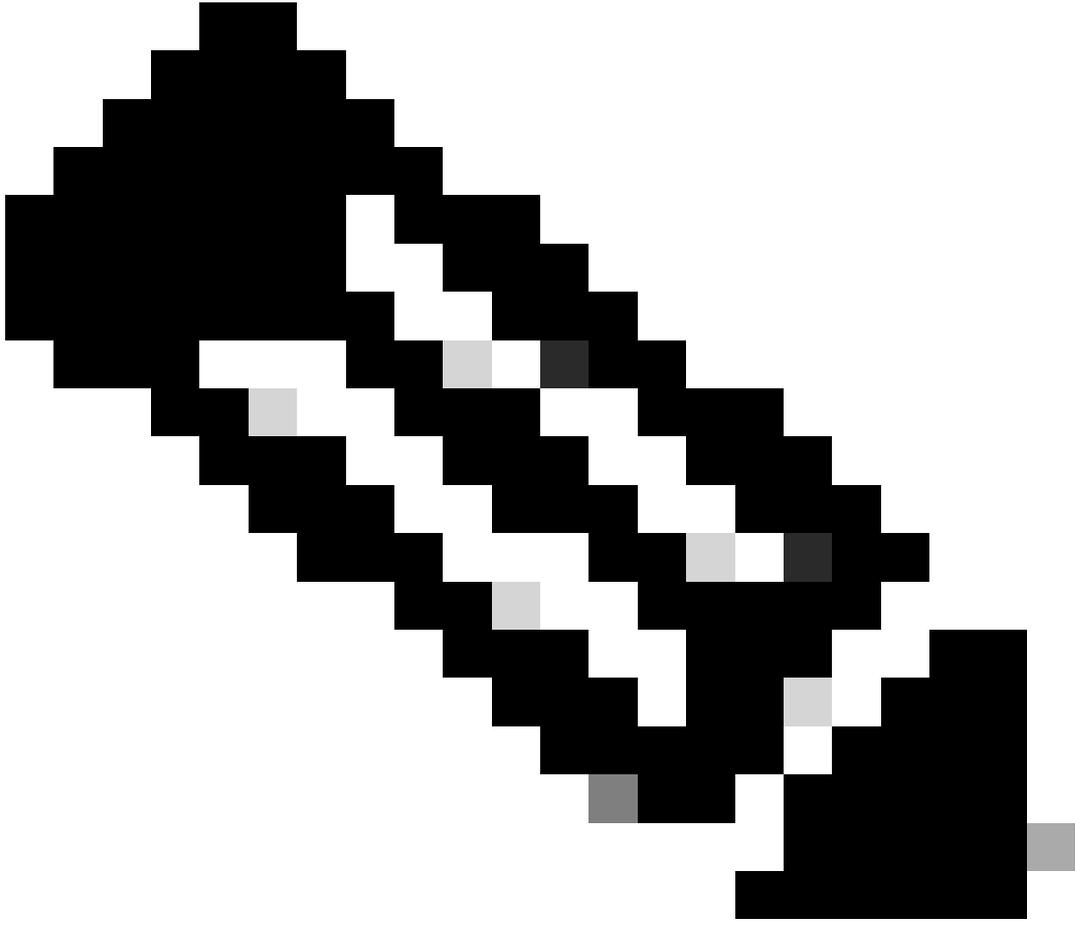
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details



Cancel

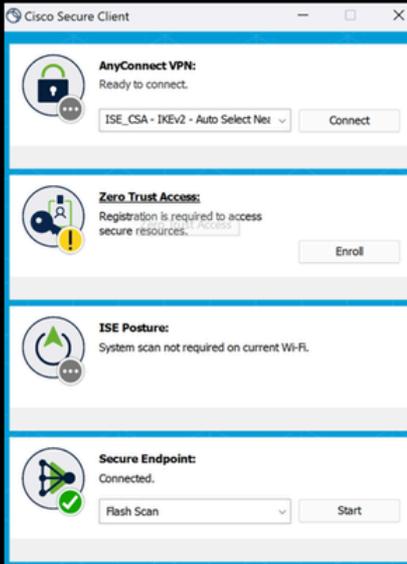


ليوختال جهن ةعومجم نمض لخدتو، قفاوتم ريغ ايئاقولت حبصت، ةيقيبتمال Cancel ةلهملا ءاهتنا ةلاحي في: ةظالم  
VPN ةكبش نع اروف لصفتو، [CSA-Non-Compliance](#).

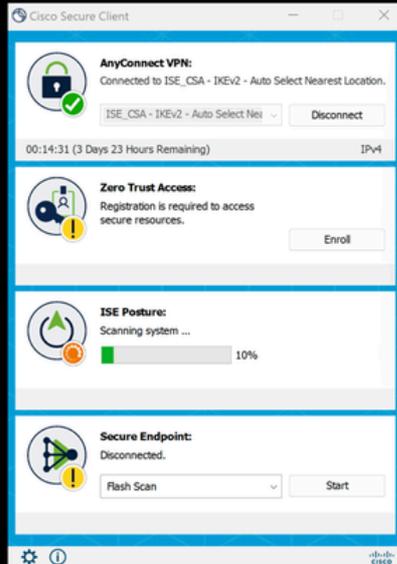
---

9. (VPN) ةيرهاظلا ةصاخلا ةكبشلاب ىرخأ ةرم لصفتاو "ةنمآلا ةياهنلا ةطقن لماع" تيثبثب مق.

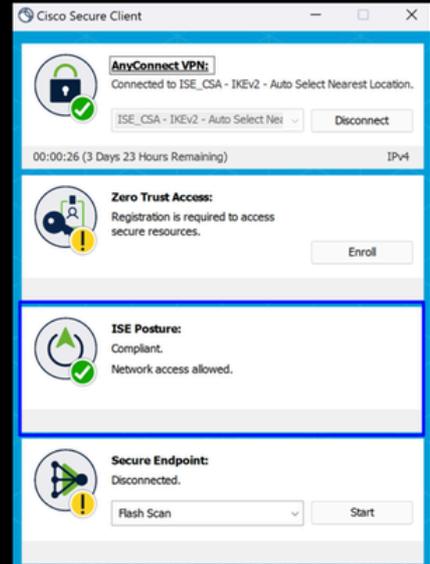
## Secure Endpoint Installed



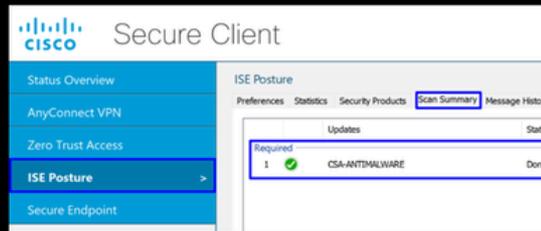
## Agent Scanning



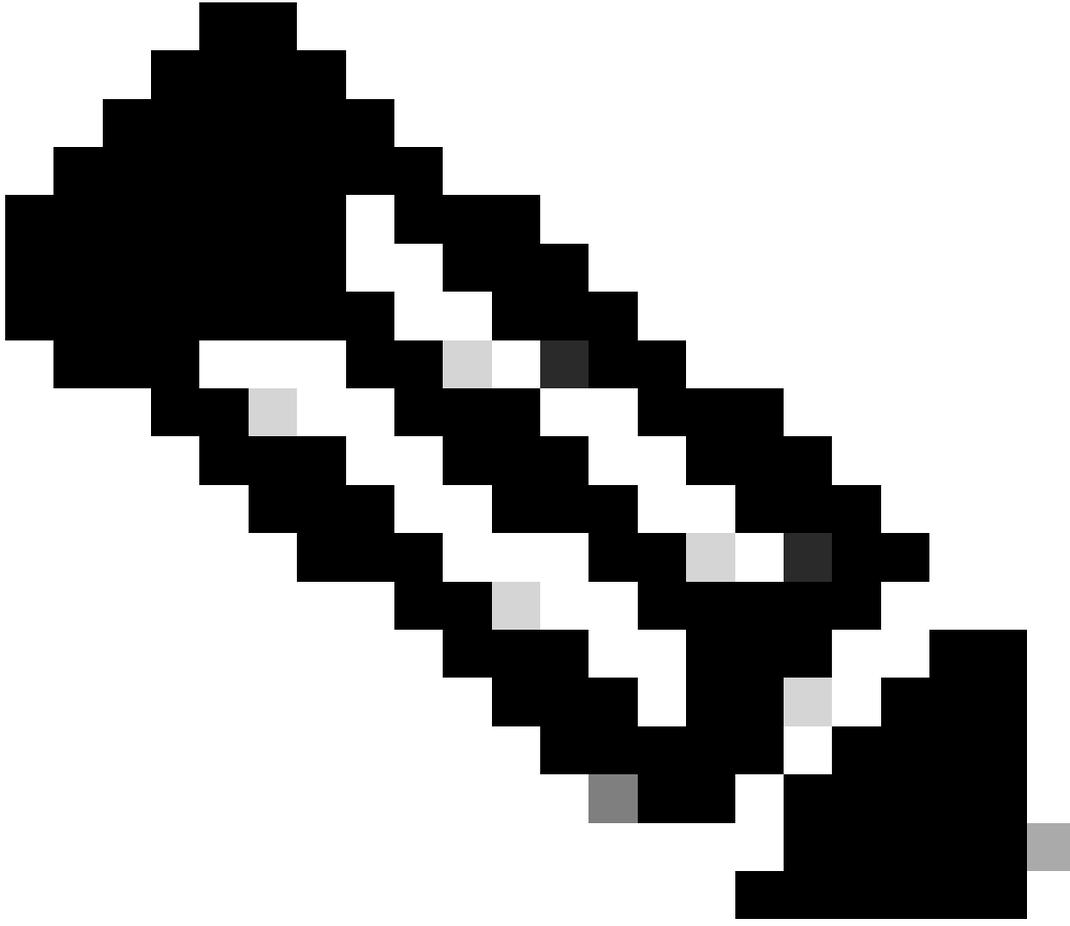
## ISE Posture Successful validated



## Scan Summary - Compliance



إلى لوصول قح حنميو وكش ةلاح في نوكت يكل كعضو ريغتي، قفاوت ةلاح في زاهال نأ نم ليمعلا ققحتي نأ دعب 10. ةكبشال لىل ةدوجومال دراومال اعيج



لوصولك نك ميو، [CSA عم قفاوت ملنا](#) لي وختالتا تاسايس ة وومجمل اعضاخ حبصت، اقفاوت م حبصت نأ دعب: **تظالم**  
ة. ك بشل دراوم عي مج ىلا اروف.

---

ISE في تال جسال عي مجت ة في فيك

ة، وهلا تامدخ مسق في اهت عجارمل. لاثتمالا مدعو قفاوتلا ىلع نالاثم كيدل، مدخت سملل ة قداصلما ة جيتن نم ققحتلل  
ة: لالتا تاداش رالا عبتا

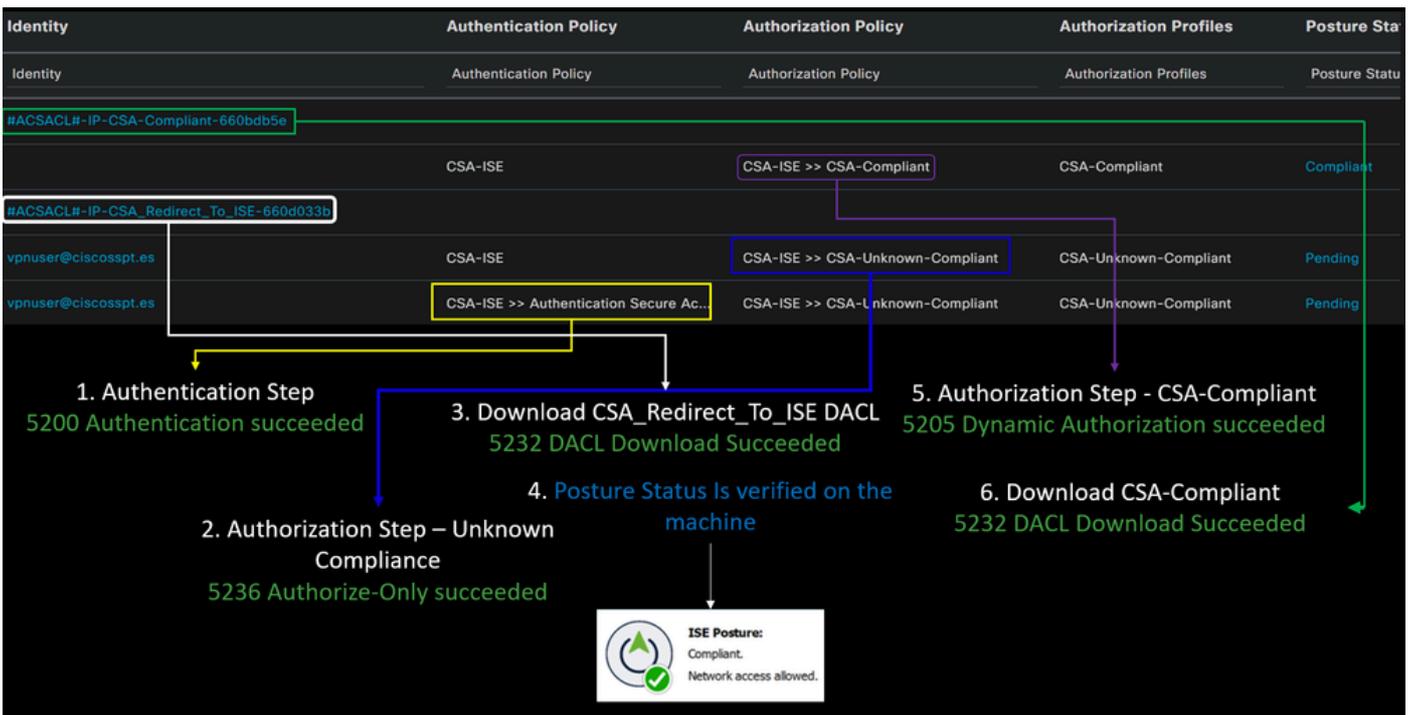
- ISE تامول عم ة حول ىلا لقتنا

- [Operations > Live Logs](#) قوف رقنا

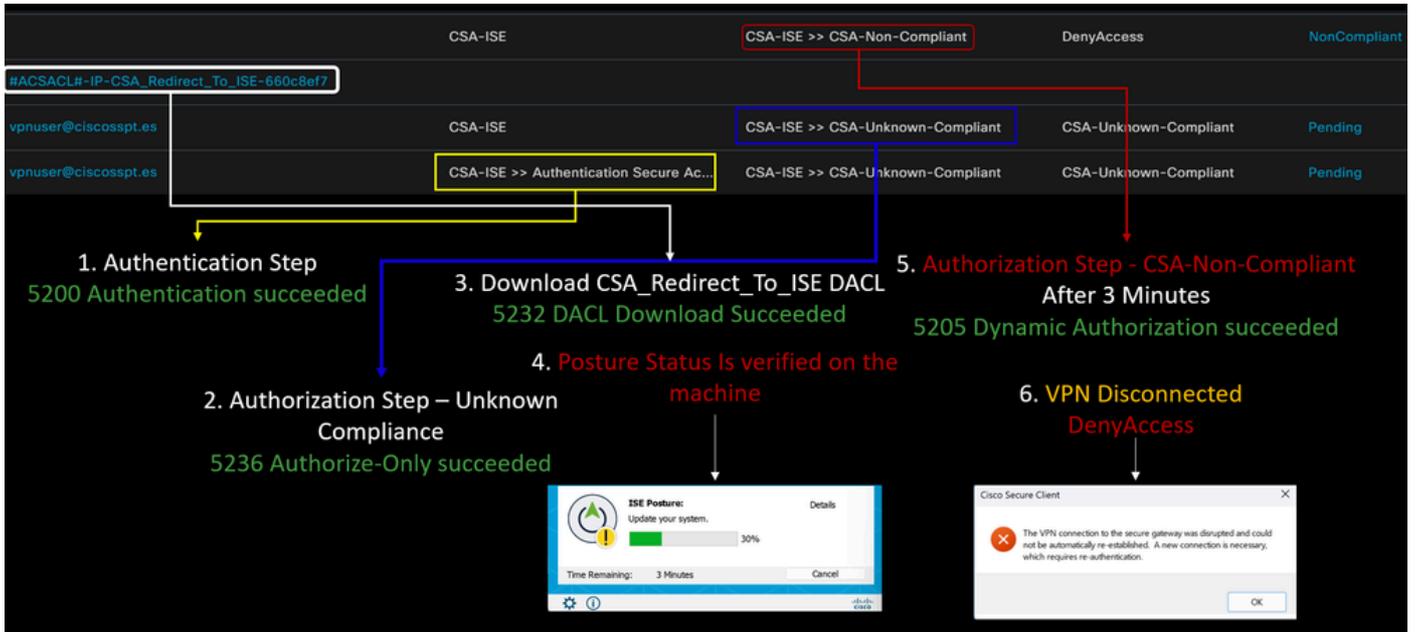
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter	
0	0	0	0	0	
Refresh Never		Show Latest 50 records		Within Last 24 hours	
Reset Repeat Counts		Export To		Filter	
Time	Status	Details	Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 07:00:27.7...	✓		Identity	Authentication Policy	Authorization Policy
Apr 03, 2024 06:56:15.4...	✓		#ACSACL#-IP-CSA_Redirect_To_ISE-660d033b	CSA-ISE	CSA-ISE >> CSA-Non-Compla
Apr 03, 2024 06:56:15.3...	✓		vpnuser@ciscospt.es	CSA-ISE	CSA-ISE >> CSA-Unknown-Co
Apr 03, 2024 06:56:15.2...	✓		vpnuser@ciscospt.es	CSA-ISE >> Authentication Secure Ac...	CSA-ISE >> CSA-Unknown-Co

Live Logs رابط في ةحجانال لاثتمالال مدعو قفاوتال شادحاً ضرع ةيفيك يلاتال ويرانيسال حضوي

ادايقنا



لاثتمالال مدعو



ISE لم اکت ونم آلا لوصول عم یل وائل تاوطلال

لالخ نم اهل لوصول نکم ی تال تاکبشلل نیوکت ةفاضل مزلی، 192.168.10.0/24 ةکبشلل نمض، یل لال لاثم ال ی قفنل نیوکت تحت قفنل

Step 1: ققنل نیوکت نم ققحتل:

نم آلا لوصول تامول عم ةحول یل لاقنن الاءجرلا، کلذ نم ققحتلل

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

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

- کب صال Cisco ISE نوکی شیح ناوئعل ةحاسمل قفنل نیوکت نم ققحت، صللم تحت

## Summary

✓ Connected

Region Europe (Germany)

Device Type FTD

Routing Type Static Routing

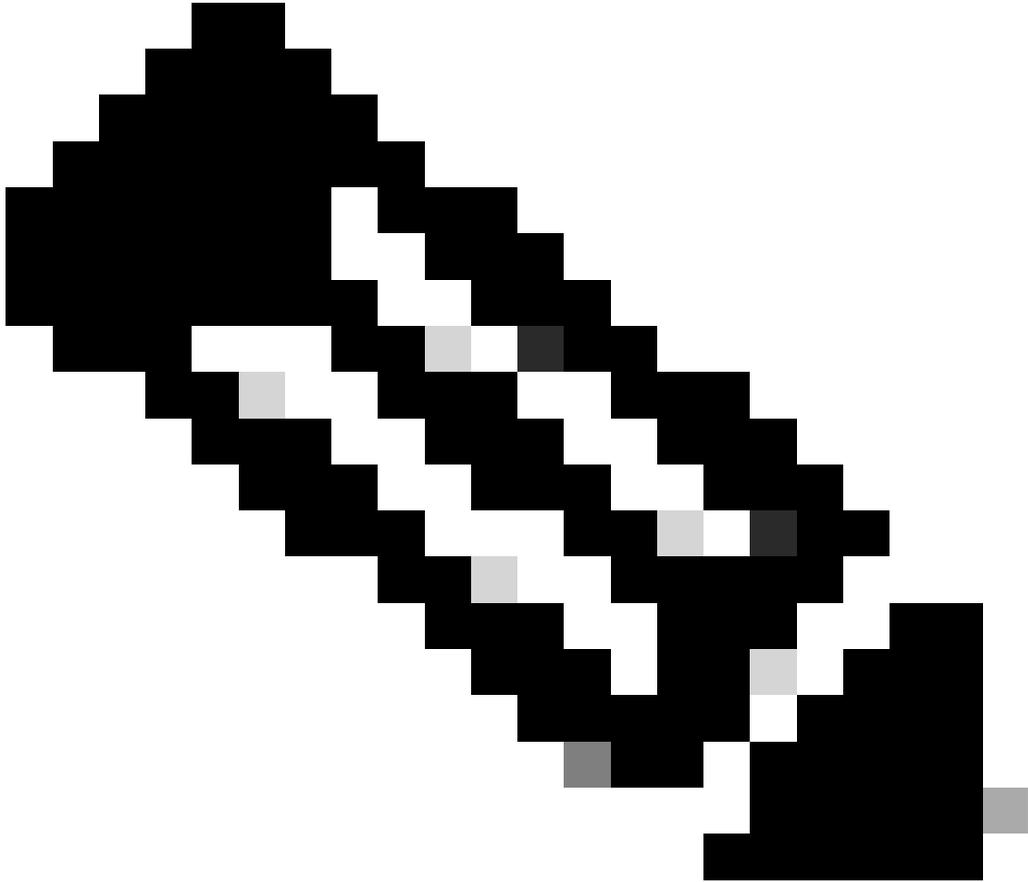
IP Address Range 192.168.10.0/24

Last Status Update Mar 19, 2024 11:13 AM

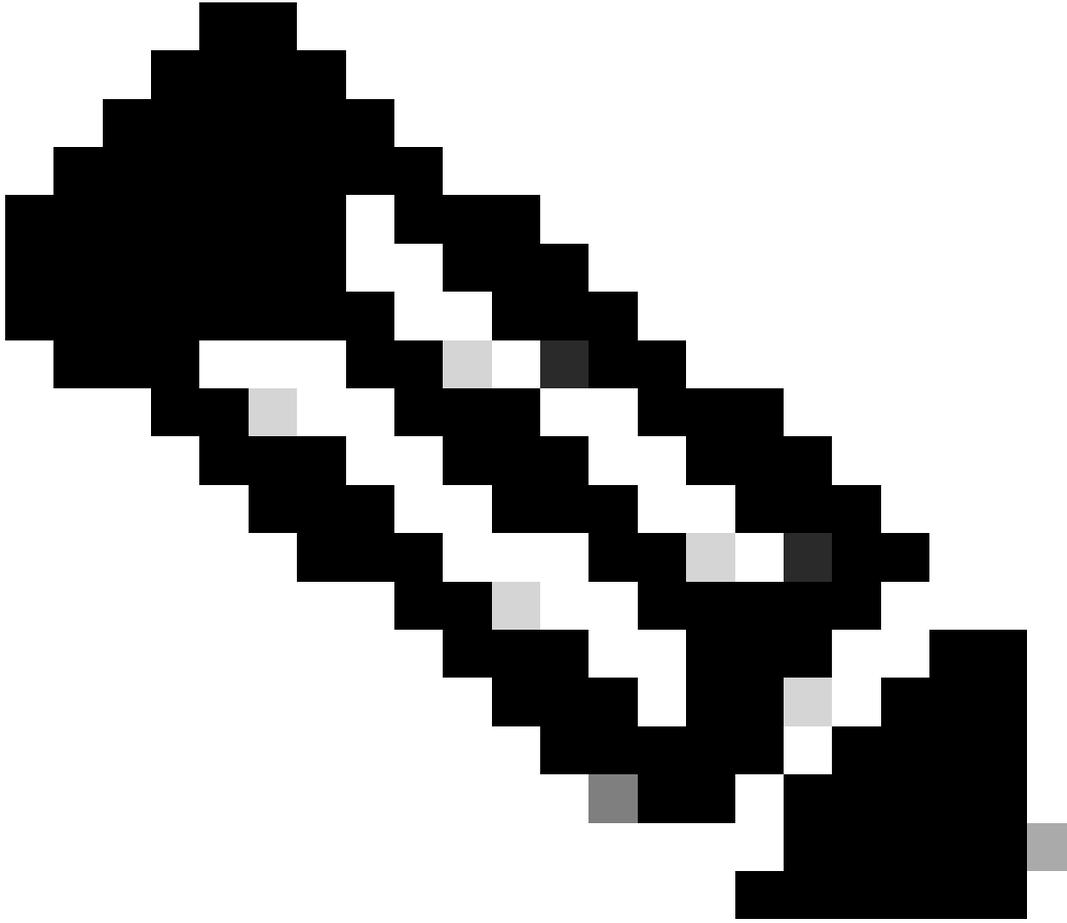
Step 2: إعداد الراجل رورملا ةكرحب حامسلا.

كتكبش ىلا نمآلا لوصولو نم ةدعاق نيوكت كمزلي. RADIUS ةقداصلم ل ISE زاغ مادختسال نمآلا لوصولاب حامسلا  
ةبولطملا RADIUS ذفانم مادختساب

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 ققداصلما (يضا رتفالا ذفنملا) UDP 1812 قبساحم (يضا رتفالا ذفنملا) UDP 1813
ISE ىلا نمآلا لوصولا ةطقنل IP عمجت	ةطقنل IP عمجت ةياهنلا	ISE_Server	ريفوتل 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 ةدعاق دوجو مزلي :ةظالم

---

ةيفرطلا ةطقنلل IP عمجتو ةرادال عمجت

كب ةصاځال [نمآلا لوصولا تامولعم ةحول](#) ىلا لقتنا ،ةيفرطلا ةطقنلاو ةرادال IP عمجت نم ققحتلل

- **Connect > End User Connectivity** قوف رقنا
- Virtual Private Network 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) ةيرهاطلال 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 لوصولا تامولعم ةحول](#) ىلى لقتنا ،جحص 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="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px; display: inline-block;">CSA (ciscospt.es\CSA) ✕</div>	<div style="background-color: #f0f0f0; border: 1px solid #ccc; padding: 2px; display: inline-block;">CiscoISE ✕</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:

VPN 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:

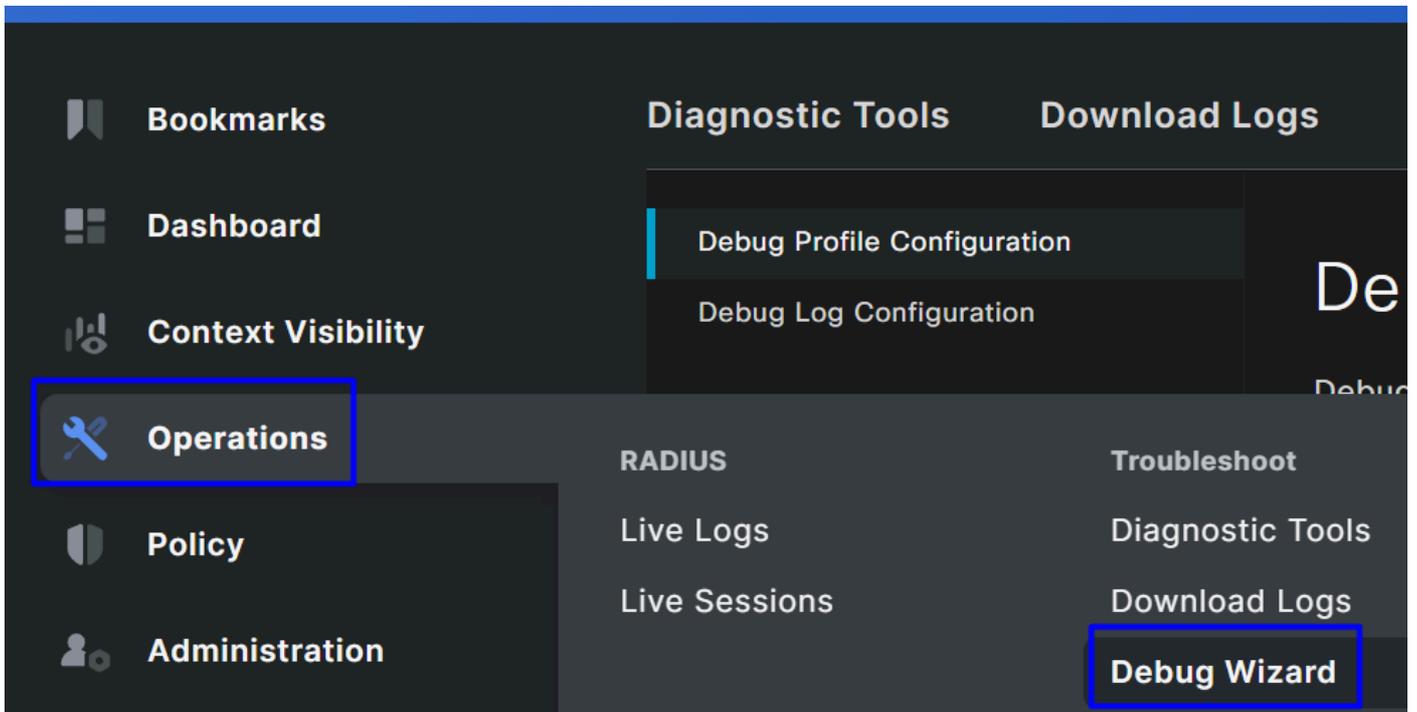
Branch Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

اهحالص او اءاطخ ال فاشك سا

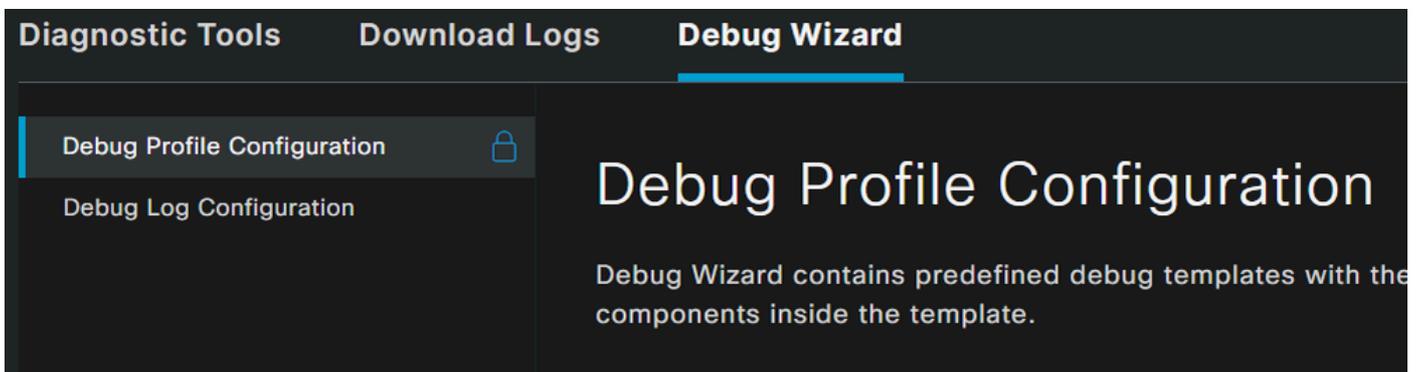
ISE ةي عضو اءاطخ اءي حصت تال جس لي زنت ةي فيك

ةي ل ال تاو طخ ال 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

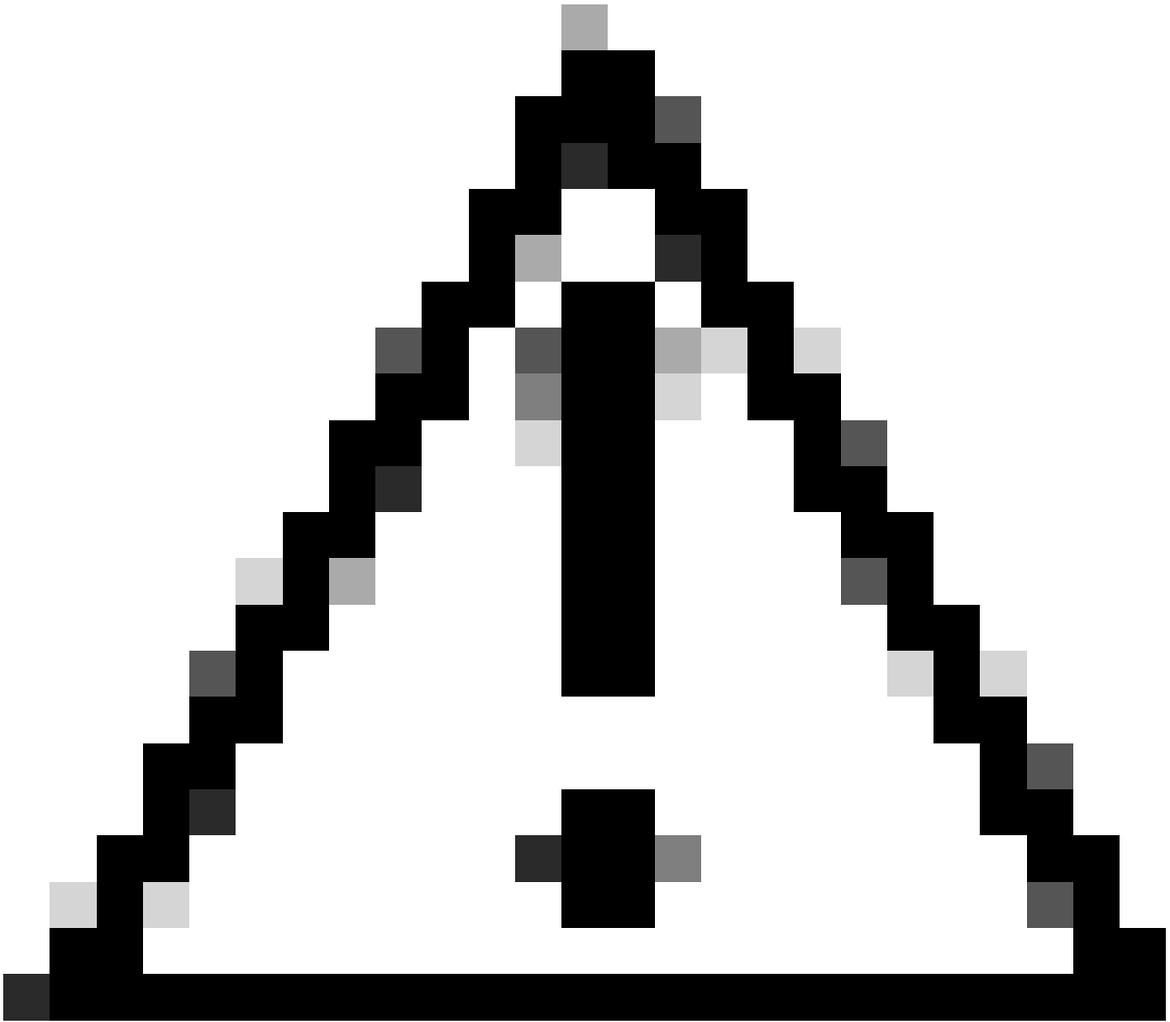
Choose on which ISE nodes you want to enable this profile.

 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 عبال ؁ ةلكشمللا ءسن مءل نأ ءعب

- قوف رقنلا Operations > Download Logs
- اهنم ءالءسللا ذءأ ءلرءل ءللا ةءقءللا رءءأ

## Appliance node list

ISE

- ءةللللا ءاراءللا 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

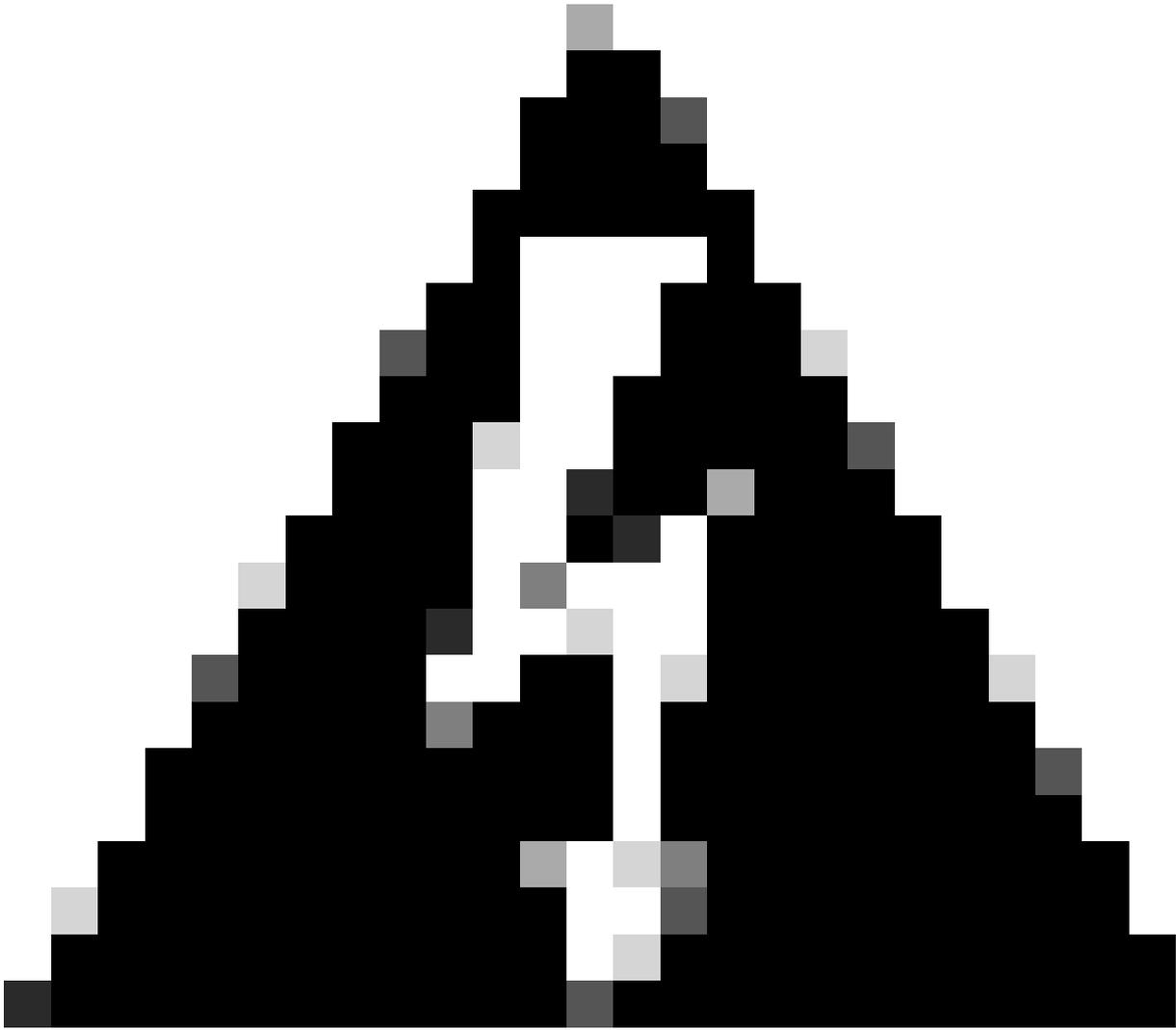
File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

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

Size(KB): 52165.0

[Download](#)

[Delete](#)



[ءاطخألا حيصت في رعت فلم نيوكت](#)، ةوطخالا لىع هن يكمت مت يذلا ءاطخألا حيصت عضو لىطعت: ريذحت

---

نمألا دعب نع لوصولتالجس نم ققحتلالا ةيفيك

كبة صاخلا نمألا لوصولت امولعم ةحول لىلا لقتنا

- Monitor > Remote Access Logs قوف رقنا

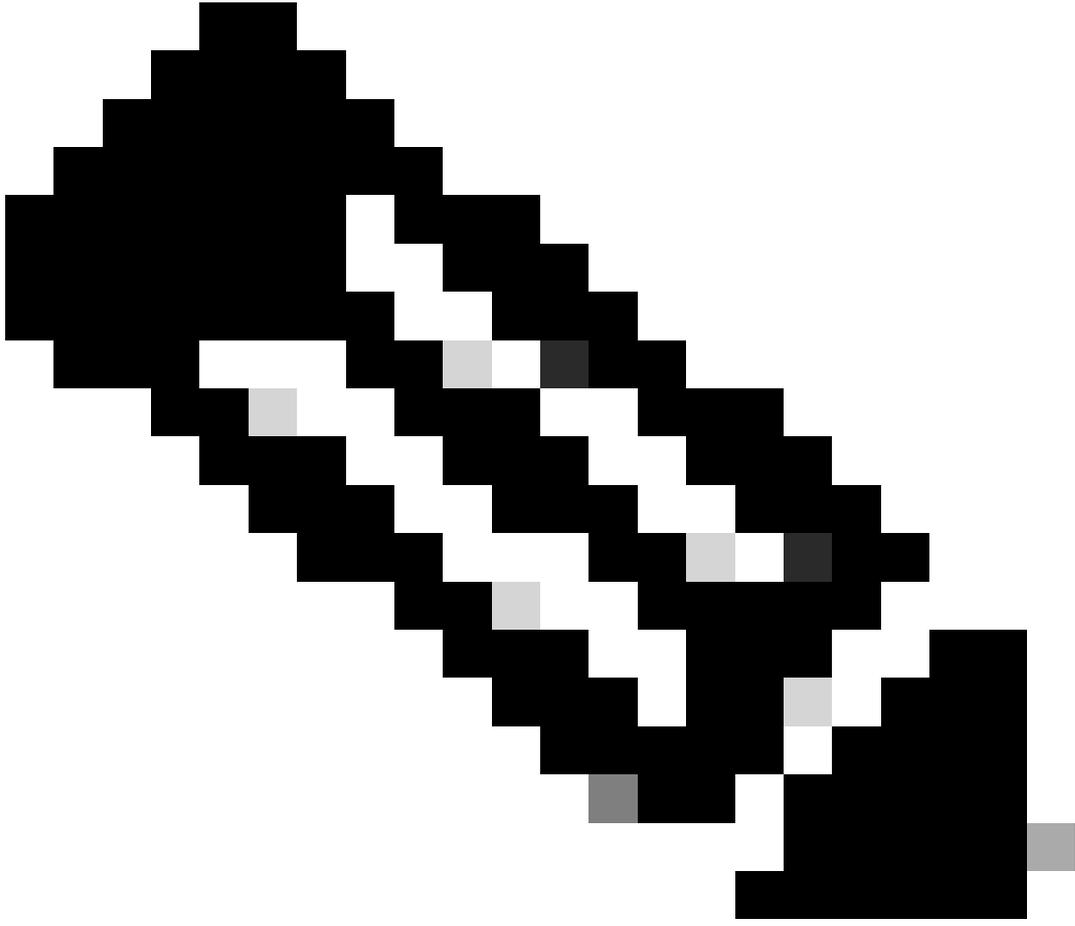
## 100 Events

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 ةمزح عاشنا

ةليلال ةلاقمل نم ققحت ،كزاهج لىل ع DART ةمزح عاشنال

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



عمالة حتف ىجري، اءالص او اءاخأل فاشككسأ مسق ىف اءلءا راءمءا ءالءسءا عىمءء ءرءمء: ءظءالم  
ءامولءمءا لىلءء ىف ءءبءءمءا TAC.

---

ءلص ءاءءامولءمء

- [Cisco نمءال ىزنءءل او ىنءلءمءل](#)
- [ءءءسءمءل لىلءءو نمءال لوءولء قىءءءو](#)

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

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءء ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنلءل دن تسمل