

RA-عضو ميقيقتل نمالا لوصول نيوكت ISE مادختساب VPNaS

تايوتحمل

[قمدقمل](#)

[قيساسالاب لطلت مل](#)

[تابلطلت مل](#)

[قمدختس مل تانوك مل](#)

[قيساسا تامول عم](#)

[كيش ل ل يطيطختل مسرل](#)

[نيوكتل](#)

[نمالا لوصول نيوكت](#)

[IP تاعمجت يل ع RADIUS قعومجم نيوكت](#)

[ISE مادختسال VPN فيرعت فلم نيوكت](#)

[قماعل تادادع ال](#)

[قبساحمل او لي وختل او ققداص مل](#)

[بور مل كرح هيجوت](#)

[Cisco نم نمأ لي عم نيوكت](#)

[ISE تان نيوكت](#)

[كيش ل قزجأ قمي ا ق نيوكت](#)

[قعومجم نيوكت](#)

[يلجم مدختسم نيوكت](#)

[چونل قعومجم نيوكت](#)

[ضيوف تل او چهنل قعومجم ققداص مل نيوكت](#)

[Active Directory يمدختسم وأ ني يمل مل RADIUS يمدختسم نيوكت](#)

[ISE قيعضو نيوكت](#)

[عضول طورش نيوكت](#)

[عضول تابلطلت مل نيوكت](#)

[عضول چهن نيوكت](#)

[لي معل ا دامل نيوكت](#)

[لي معل ا ريفوت چهن نيوكت](#)

[لي وختل ا تافيصوت عاشن](#)

[عضول ا چهن قعومجم نيوكت](#)

[قحصل ا نم ققختل](#)

[عضول ا نم ققختل](#)

[زاهل ا يل عل لاصل ال](#)

[ISE ي فالچس ال ا عيمجت قيفي ك](#)

[اداي قنا](#)

[لاثت مل ا مدع](#)

[ISE لماركتو نمالا لوصول عم يل وال ا تاوطلل](#)

[اهجالصل او عاطخل ال افاشكتسا](#)

[ISE قيعضو عاطخل ا حي حصت فالچس لي زنت قيفي ك](#)

[نمالا دعب نعل لوصول ال فالچس نم ققختل قيفي ك](#)

[نمالا لي معل ا يل ع DART قمزح عاشن](#)

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 ةق داصم ل ا

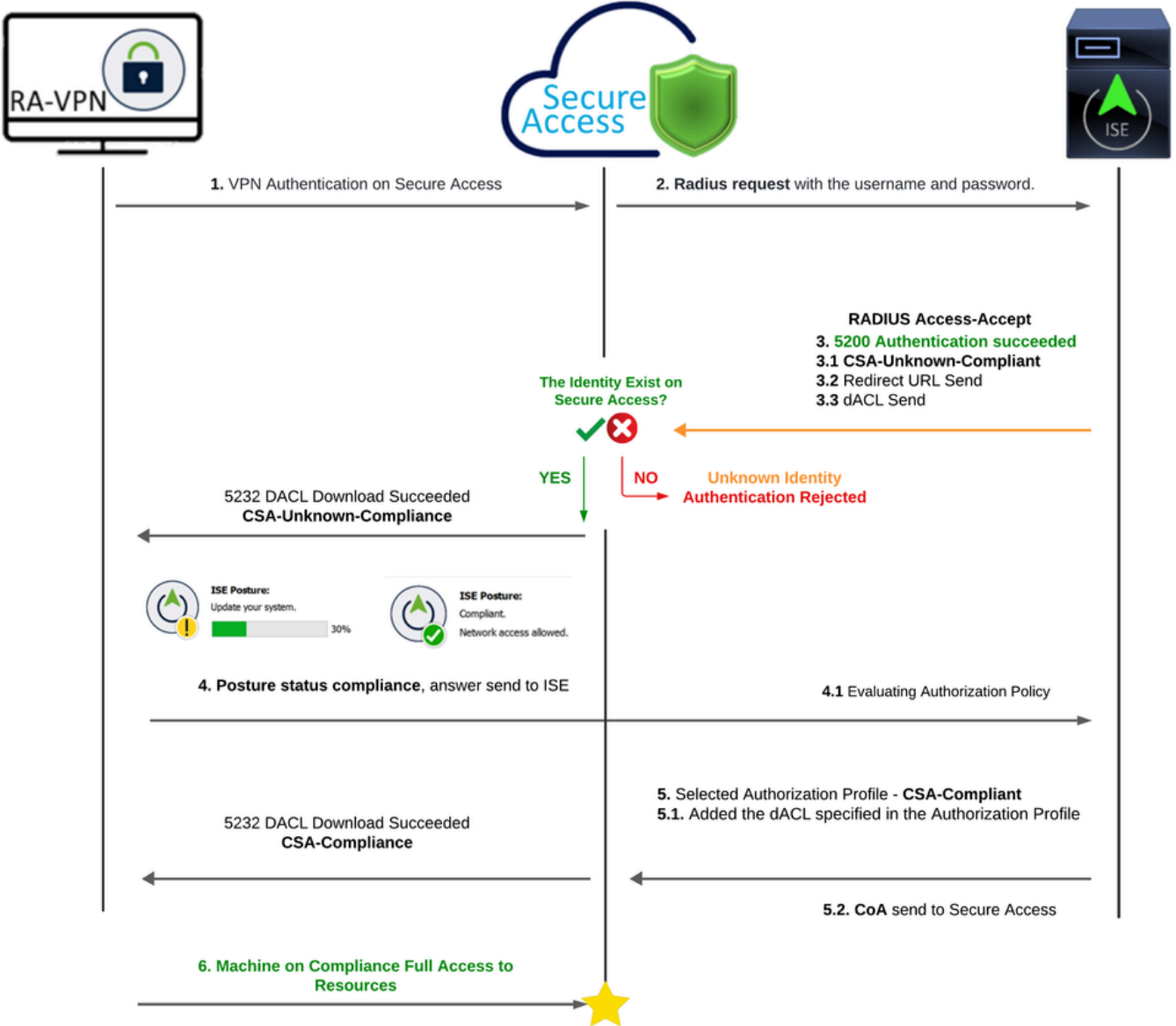
عم دخت سمل ا ت ا نو ك م ل ا

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 م م 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



ي طي تختال مسررل - ISE - ن م آل لوصول

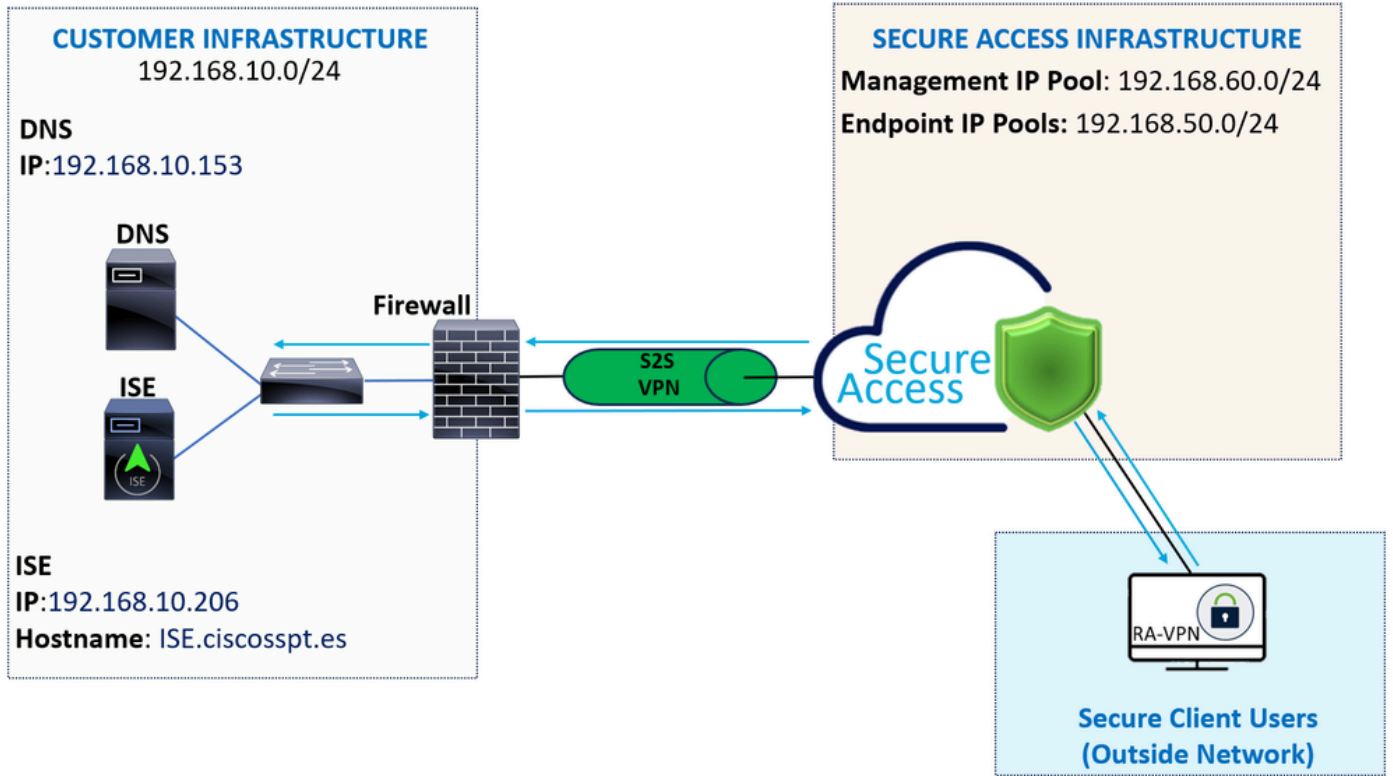
يلع لمعي، الماش اينم اجهن (ISE) ةيوهلا تامدخ كرحم عم Cisco نم ن م آل لوصول اجمد رفوي ني مآت ل MS-CHAPv2 ك لذي ف امب، ةفل تخم ل ةقداصم ل تالوكوتورب نم ةدافتسالا لعل، ةمدقتم ل نام آل ةمدخ ةفاح ل مادختساب Cisco Secure Access، تالاصتالا ةكبش ل لثم تازيم رفوي امم، ةيزوتل ةديش تائيبل ربع ن م آل لاصتالا نيسحت ISE تانك م مادختساب اهتيامح نكمي يتل او، (VPNAs) ةمدخك (VPNs) ةيرهاطلا ةصاخلا

ةينك م ني مدختسم ل لحي تي امم، نام آل او ةسال سلاب مستت لوصول ةبرجت جم دل اذه حي تي و نم ةمدقتم ل تازيم ل مادختس ا ي دوي. نسحم نام او اءا عم نك م ا ي ف قي ب ط ت ا ب لاصتالا ةزهج ا قفاوت مي ق ت قيرط نع اذه نام آل جذومن زيزعت ل ا، عضولا مي ق ت لثم، Cisco ISE ةزهج آل ا ن مضي اذهو. لوصولاب حامس ل لبق ةيلخا دل مدختسم ل تاسايس عم رتوي بمك ل ل، ةكبش ل دراوم ل لوصول اهنك م ي ت ل ا يه طاقف ةسسؤم ل نام ا تابل ط تم ب ي فت ي ت ل ا، ةين م آل تارغل ل 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 ، ني وكت لآ ة ىل مع ءد ب ل ب ق : ة ط ح ا ل م
[ISE ل م ا ك ت و "ن م آ ل ا ل و ص و ل ا"](#).

ن م آ ل ا ل و ص و ل ا ن ي و ك ت

IP تاع م ج ت ىل ع RADIUS ة و م ج م ن ي و ك ت

ة: ل ل ا ت ل ا ت او ط خ ل ا ل م ك أ ، RADIUS م ا د خ ت س ا ب VPN ف ي ر ع ت ف ل م ن ي و ك ت ل

ك ب ة ص ا خ ل ا [ن م آ ل 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** ق و ف ر ق ن ا
- **Manage** ق و ف ر ق ن ا ، (Manage IP Pools) ع م ج ت ل ا ن ي و ك ت ت ح ت

Manage IP Pools

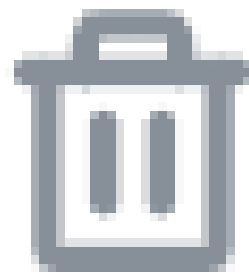
Manage

2 Regions mapped

- رادىوس سرڤر 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 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 ×



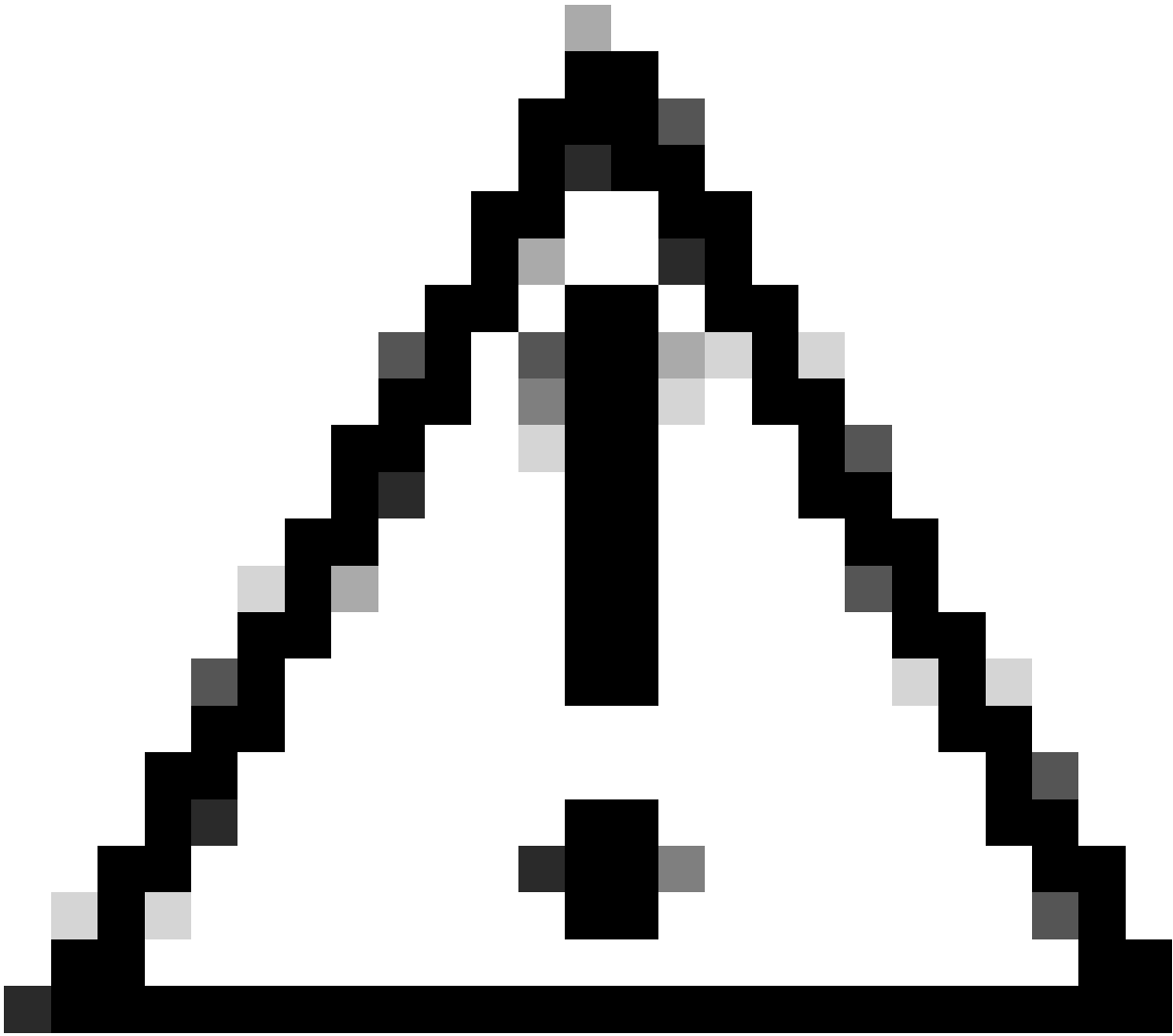
+ Add

#	Server Name	IP Address		
1	ISE_CSA	192.168.10.206		

نمآلا لوصولا يف

◦ AAA method

- **Authentication:** وه، يضارتفا لكش ب، هدي دحتو **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 ديدحتو ذفنم لاب **Authorization** ةصاخلا رايتخالالا ةناخ ىلع ةمالع عضو 1812 وه، يضارتفا لكش ب
- **Authorization mode Only Change of Authorization (CoA)** تاريغيغتو ةيعضوب حامسلاو **mode** رايتخالالا 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 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 بيلاسألأ Authorization نم لك مدختست Authentication أن بجي : ريذحت

-
- **RADIUS** مسقلا لىل AAA ربع قداصل ملل هم ادختسا متي يذلا **RADIUS Servers (ISE)** نيوكت لىل اجاتحت ، 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
---	-------------	------------

- هتلا تارايل الل نيوكت ب مق ،كذ 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 مسا نيوكتب مق
- IP Address: نمآلا لوصولالالغ نم هيلال لوصولال نكمي يذلا Cisco ISE زاوجل IP نيوكت
- Secret Key: ڤرسلال RADIUS حاتفم نيوكت
- Password: كب ةصاخال RADIUS رورم ةملك نيوكتب مق
- كب صاخال ISE مداخل ددحو رايلخال Assign Server نمض كب صاخال RADIUS مداخل ددحو Save رقنا

RADIUS Servers

You can add up to 8 servers in each group

Assign servers

^

ISE_CSA

[+ Add](#)

- مت يذلا نيوكتال طافحل 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 ×

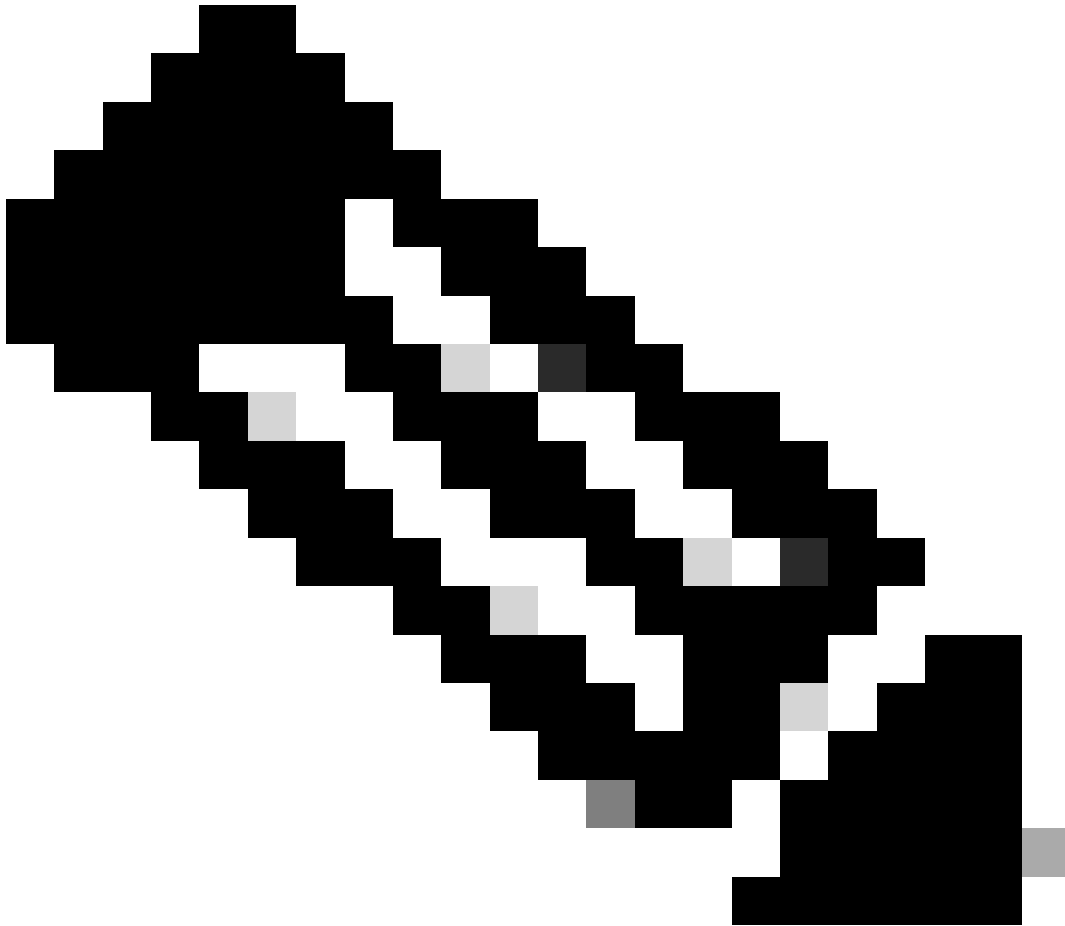
+ Add

#	Server Name	IP Address	
1	ISE_CSA	192.168.10.206	

◦ Protocols: رتخا Radius

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

• رقا Next



قطانم كيدل ناك اذا رطوق لافصن تااعومجم ديدحت و قطانم لار عيمجب ةصاخ لار رتخا لار ةناخ ديدحت كي ل ع بچي: ةظحالم اعونصم كب صاخ لار رزلا نو كي Next، كلذ اول عفت مل اذا. ةددعت م

دامت عال ة عباتم عاجرلا ، ة قداصملا عاجز أ عي مج نيوكت دع ب

دامت عال

- ✓ **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

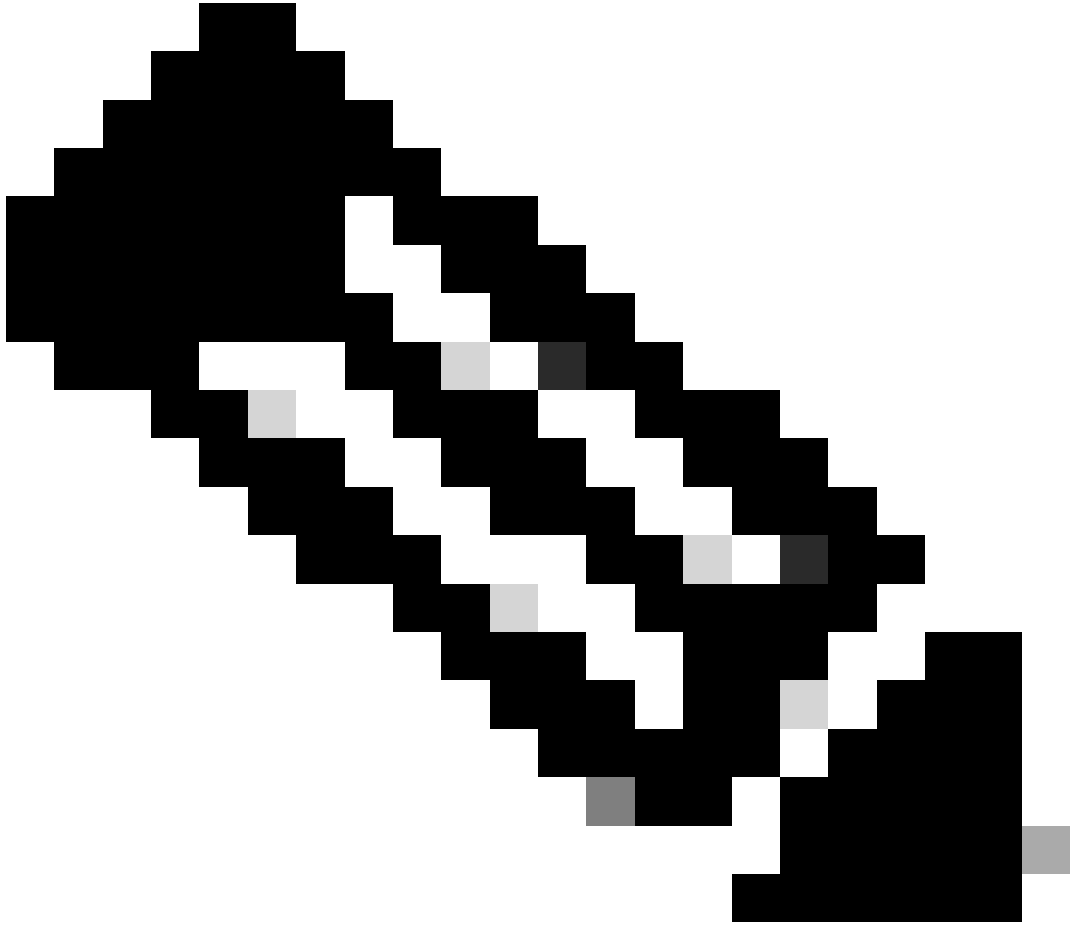
- **Authorization**

- **Enable Radius Authorization:** رADIUS ضيوفت نيكم تل رايتخال ة ناخ ة ل ع ة مال ع وضو

- نع لوصول تا عمت عي مجل ددحم دحاو RADIUS مداخ مادختسال رايتخال ة ناخ دح: قطنملا عي مجل ددحاو ة عومجم ددح لصفنم لكشب عمت لك ل اهفيعرتب مق وأ ، (RA-VPN) ة ره اظلال ة صخال ة كبشال - دع ب

- **Next** رقنا

Accounting مادختساب ة عباتملا عاجرلا ، عاجز ال **Authorization** لك نيوكت دع ب



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

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

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

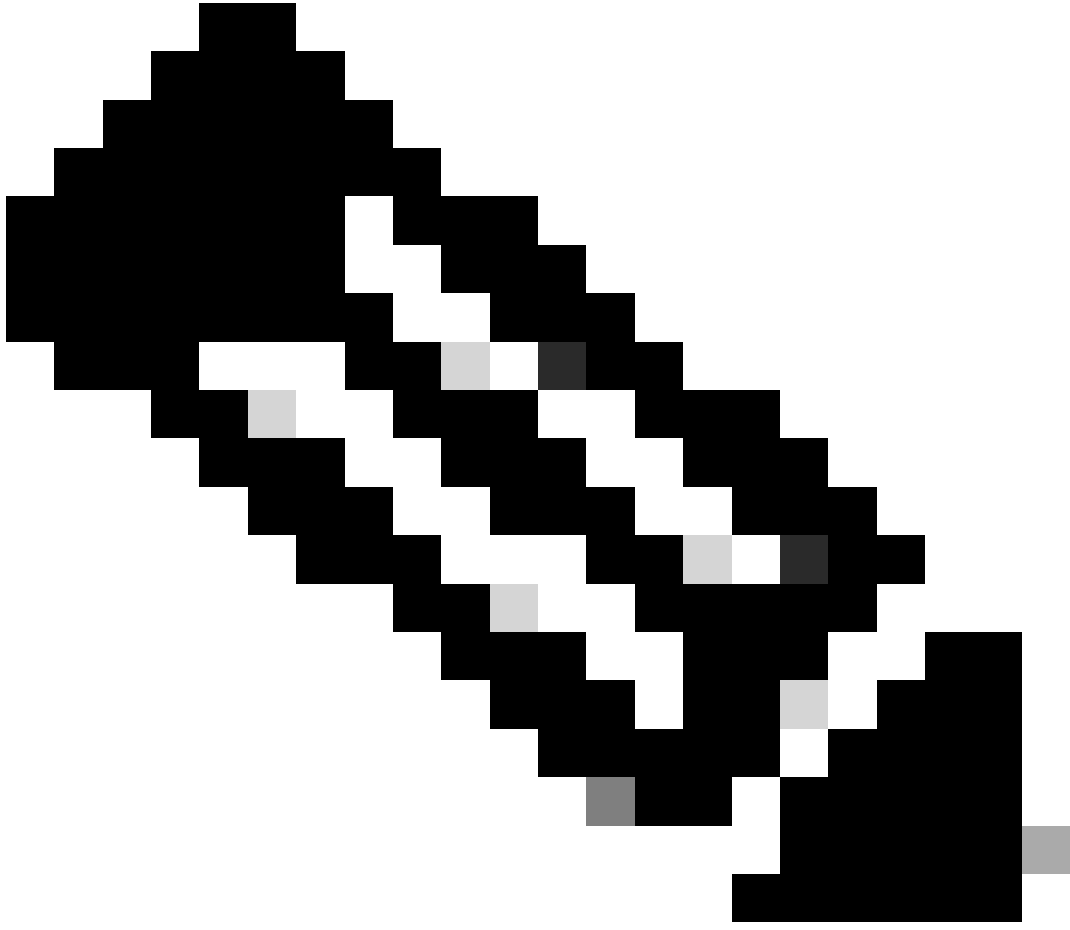


No matches found

Cancel

Back

Next



Bypass Secure Access كرايخ | دنع (ISE) ةيوهال تامدخ كرحم ةيعضو ISE Posture enroll.cisco.com 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 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
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 ظافحلح كنكمي، ةوطخل هذه يف [Cisco](#) نم نم آلا لىمعل الوؤسم لىل نم ققحتال اعجرفاف، رثكأ

ISE تانويكت

ةكبشلال ةزهجأةمئاق نيوكت


Cisco ISE ىلع تامالعستسا اعرج اهنكمي 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 ىلع هنيوكت مت يذلا كرتشملا رسلا سفن نيوكت، [يرسلاجاتفملا](#)
 - **CoA Port:** "نم آلا لوصول" ةزيم يف اضيأ 1700 زارطالا مادختسا متي شيح، ةيضارتفا ةميقك اهعد

لماكتلا نم ققحتلل يلحم مدختسم عاشنال ةعباتملا ب مق، حيحص لكشب لماكتلا لمع نم ققحتلل، **Save** رقنلا كلذ دعب

ةومجم نيوكت

ةيلاتلا تاوطخال عبتا، نييحلحملا ني مدختسملا عم مادختسالل ةومجم نيوكتل

- **Administration > Groups** يف رقنا
- **User Identity Groups** رقنا
- **Add** + رقنا
- **Submit** قوف رقناو ةومجم لملل Name ةومجم عاشنا ب مق

Administration

- System
- Deployment
- Licensing
- Certificates
- Logging
- Maintenance
- Upgrade

Network Resources

- Network Devices
- Network Device Groups
- Network Device Profiles
- External RADIUS Servers
- RADIUS Server Sequences
- NAC Managers

Identity Management

- Identities
- Groups**
- External Identity So
- Identity Source Seq
- Settings

Identity Groups

- Endpoint Identity Groups
- User Identity Groups**

User Identity Groups

User Identity Groups > New User Identity Group

Identity Group

Edit 4 + Add Delete Import

* Name 5 CSA-ISE

Description

Submit 6

User Identity Groups

Name

- ALL_ACCOUNTS (default)
- CSA-ISE → GROUP CREATED
- Employee

يحلح م دختسم نيوكت

ك: صاخلا لم اكتالا 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: 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 يوكا [ةيساسالاب لطلت مل او](#)
- **Status:** طشن
- **Password Lifetime:** كل اقفو، Never Expires، و With Expiration اهن يوكا كنكم مي
- **Login Password:** مدختسملل رورم ةملك عاشن |
- **User Groups:** ةوطخلال ىل ع اهواشن | مت يتللا ةومجملا رتخ [ةومجم نيوكا تب مق](#)

Secure Access نم ةمداقلا تارادصإلإ يف اهريريغتل UPN إلى ةدنتسمل ةقداصلما نييعت مت :نظالم

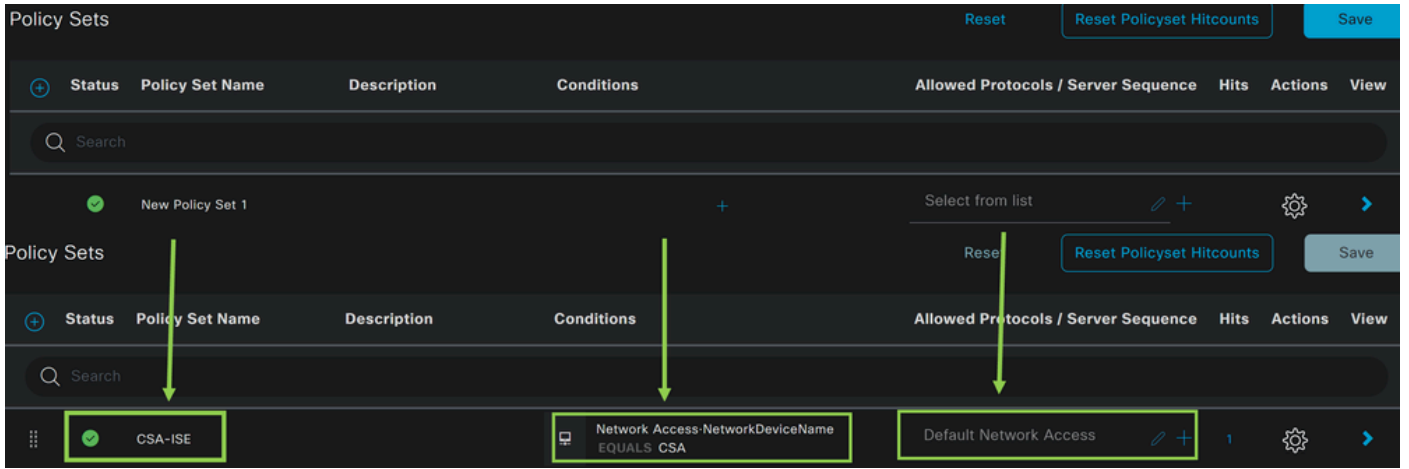
Configure Policy Set. ةوطخالاب ةعباتملاو نيوكتل Save كنكمي ،كلذ دعب

جهنلا ةعومجم نيوكت

ةلاح ويرانيسل اذ ءهضوي .ضيوفتل او ةقداصلما ءانثأ ءذاختاب ISE موقوي يذلا ءارجال نيوكتب مق ،جهنلا ةعومجم راطا يف اذا امم ققحتي و RADIUS ةقداصلم لصأ نم ISE ققحتي ،الوأ .مدختسمل لوصول ريفوتل ةطيسب ةسايس نيوكتل مادختسال لوصول ريفوتل ISE مدختسم تانايب ةدعاق يف ةدوجوم تايوهلا تناك

Cisco ISE تامولعم ءحول إلى لقتنا ،جهنلا اذ نيوكتل

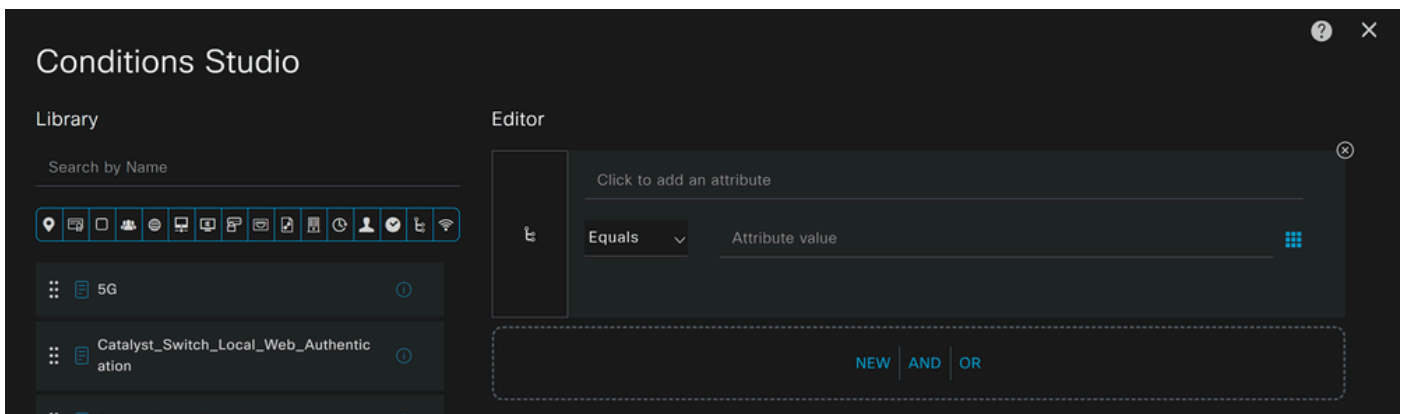
- Policy > Policy Sets قوف رقنا
- ةديج جهن ةعومجم ةفاضال + قوف رقنا



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 جهنلا حمسي .هذه جهنلا ةعومجم ىلا اذانتسا ضيوفتلاو ك جهنلا يف لوخدلا مث CSA Network Device List نم يتأت ةقداصملا هذه نأ نم ققحتلل [ةكبشلا ةزهجأ ةمئاق نيوكت](#) **Default Network Access** لثم ،اهب حومسملا تالوكوتوربلا ،اربخأو **Conditions**.

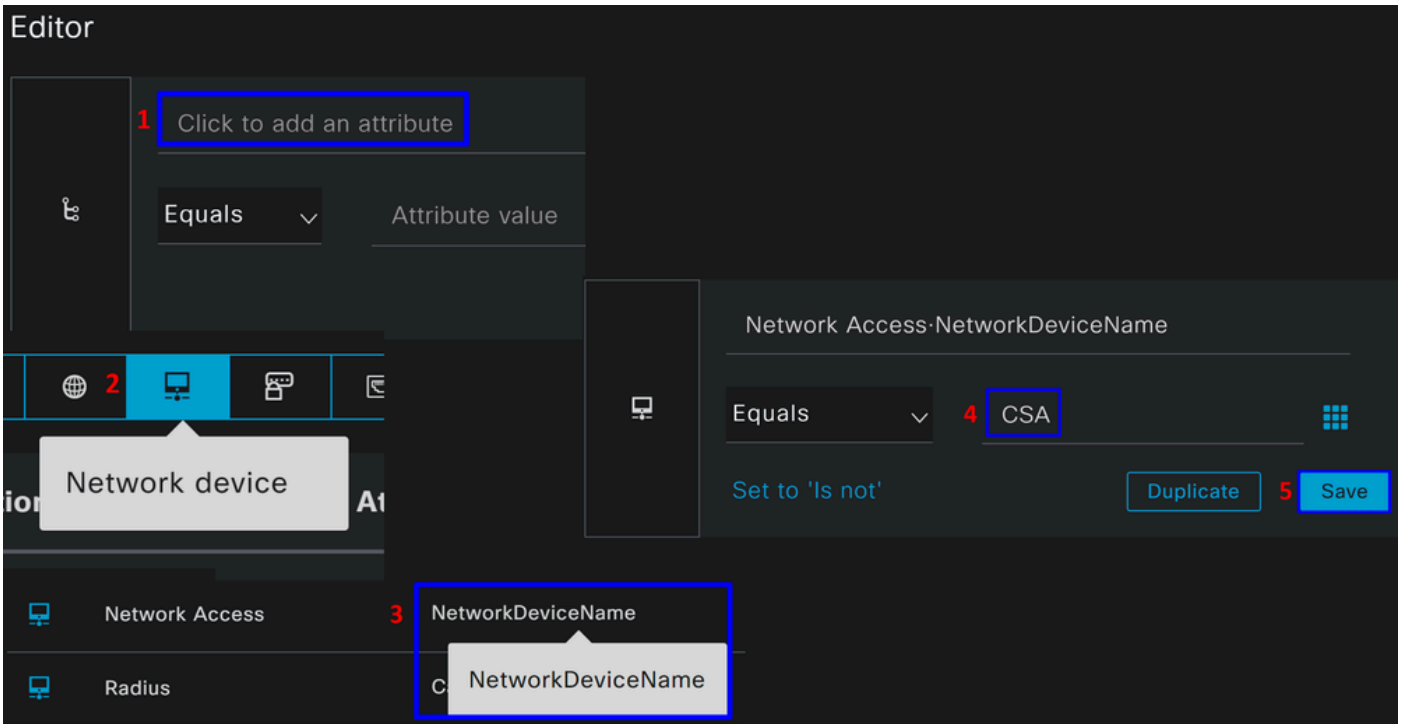
ةيالاتلا تاميلعلتلا مادختساب ةعباتملا ب مق ،جهنلا ةعومجم قباطت يتلا **condition** تاميلعلتلا عاشنال

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



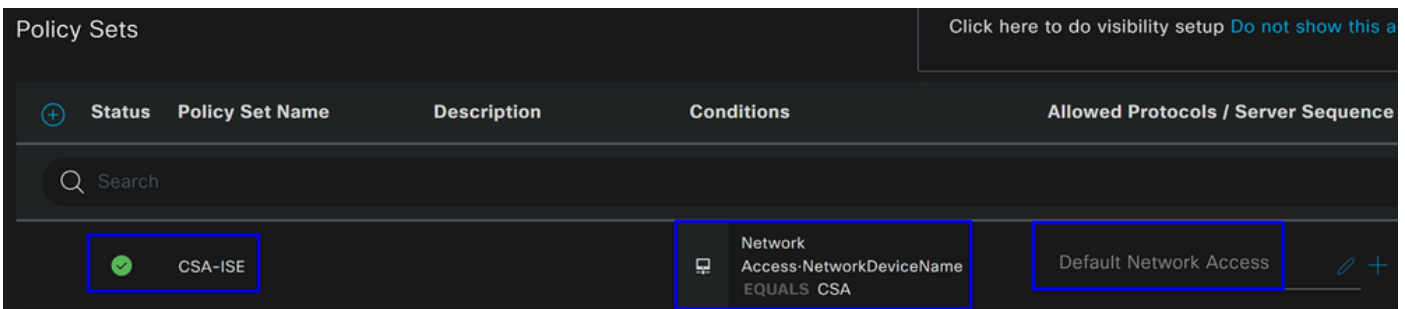
- Click to add an attribute قوف رقنا ،طورشلا عاشنال
- رزلا **Network Device** ىلع رقنا
- رايخ **Network Access - Network Device Name** قوف رقنا ،ةيفلخلال تارايخلال تحت

- [ههجا قوفاق نيوكت ب مق](#)، ةوطخلا تحت Network Device مسا بتكا، يواسي رايخ تحت
- Save رونا

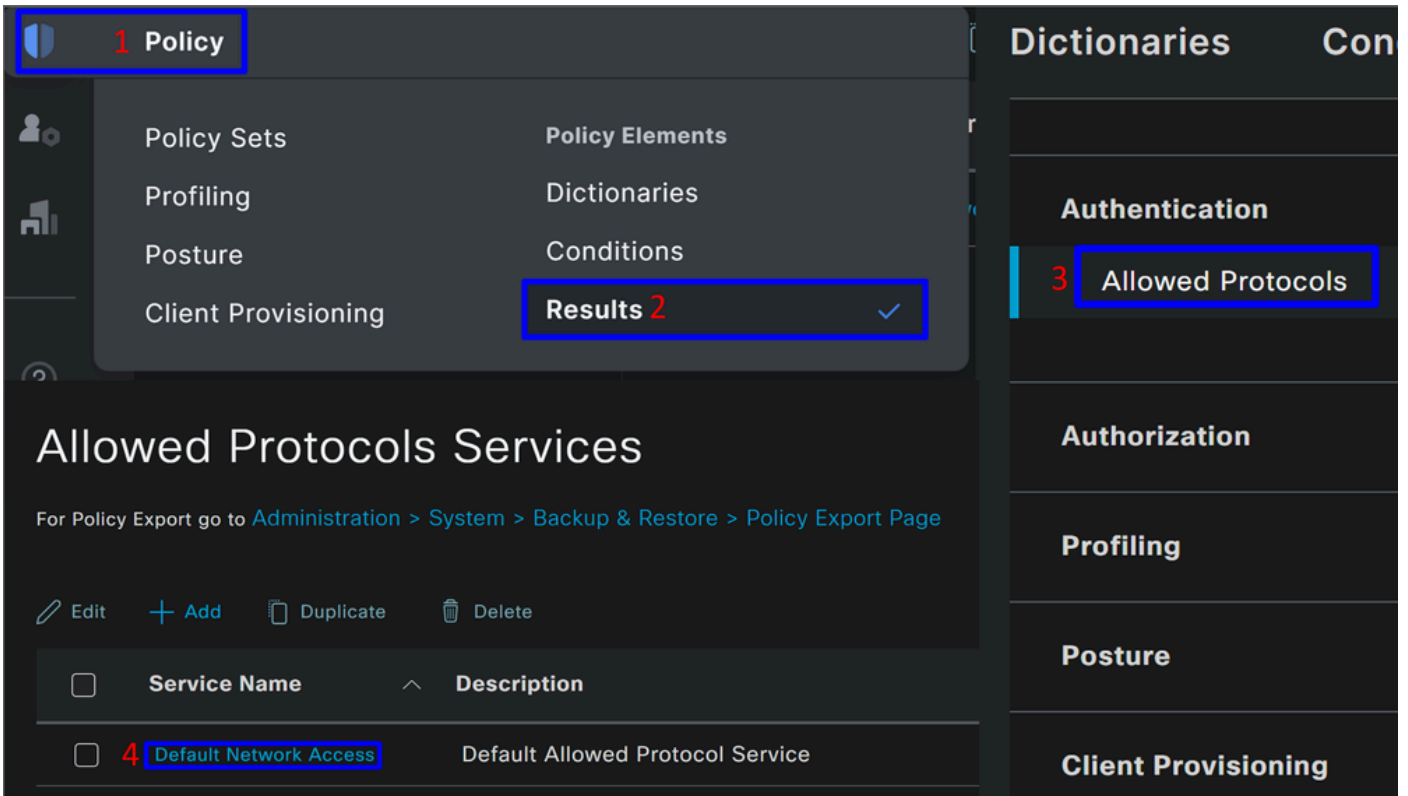


ةومجم نمض تانايب ال **Authorization** دادع او **Authentication** ةعبات مل CSA ردمصم نم دراووا بلطلا يلح ال جهنلا اذه قفاوي ال حومسم ال **Default Network Access** تالوك وتورب ال يل اذانتسا اهب حومسم ال تالوك وتورب ال نم ققحتي امك، **CSA-ISE** جهنلا اهب.

يه ددحم ال جهنلا ةجيتن نوكت نأ بجي:



- ةيلاتا تاداشرال عبتا، حومسم ال **Default Network Access Protocols** نم ققحتلل
 - Policy > Results قوف رونا
 - Allowed Protocols قوف رونا
 - Default Network Access قوف رونا

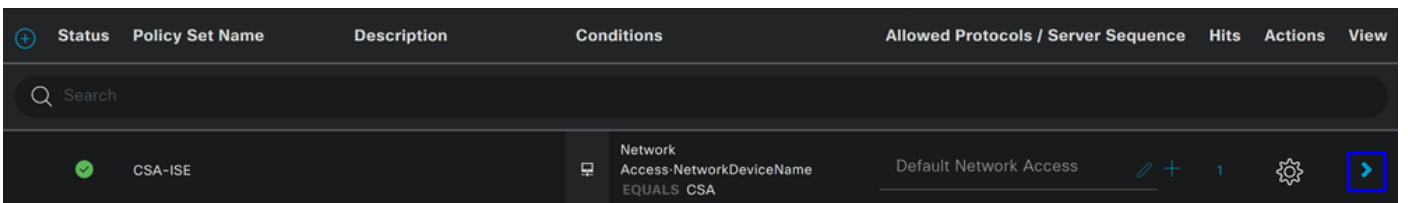


- **Default Network Access** يلى ع اهب حومس الم تالوكوتورب لاي عي م ج يلى ع ا لاطالال كن كن مي ، ك ل ذ دعب

ضيوف تال او جه نال اة و م ج م ة ق د اص م ني و ك ت

ة: ل ل ال ت او ط خ ل ا ب ر م ت س ا ، **Policy Set** ن م ض ج ه ن ل ا **Authorization** و **Authentication** اء ا ش ن ل ا

- > ق و ف ر ق ن ا



- ة: و ر ع م ل ا **Authorization** ت ا س ا ي س ل ا **Authentication** ي ر ت ، ك ل ذ دعب

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
🟢	CSA-ISE		Network Access:NetworkDeviceName EQUALS CSA	Default Network Access
> Authentication Policy(2)				
> Authorization Policy - Local Exceptions				
> Authorization Policy - Global Exceptions				
> Authorization Policy(2)				

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
> Options			

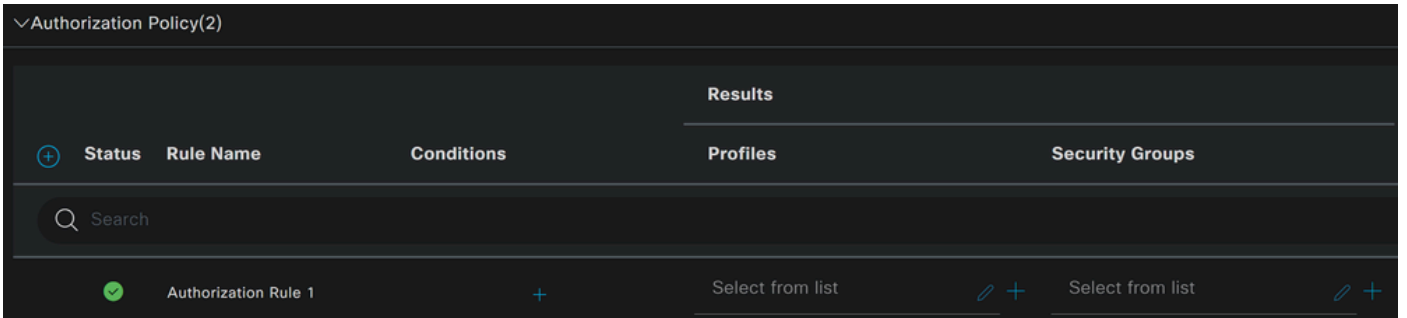
ةوطخالل نيوكت جهن ةعومحمل نمض ددحملل سفن وه جهنل.

ليوختل ةسايس

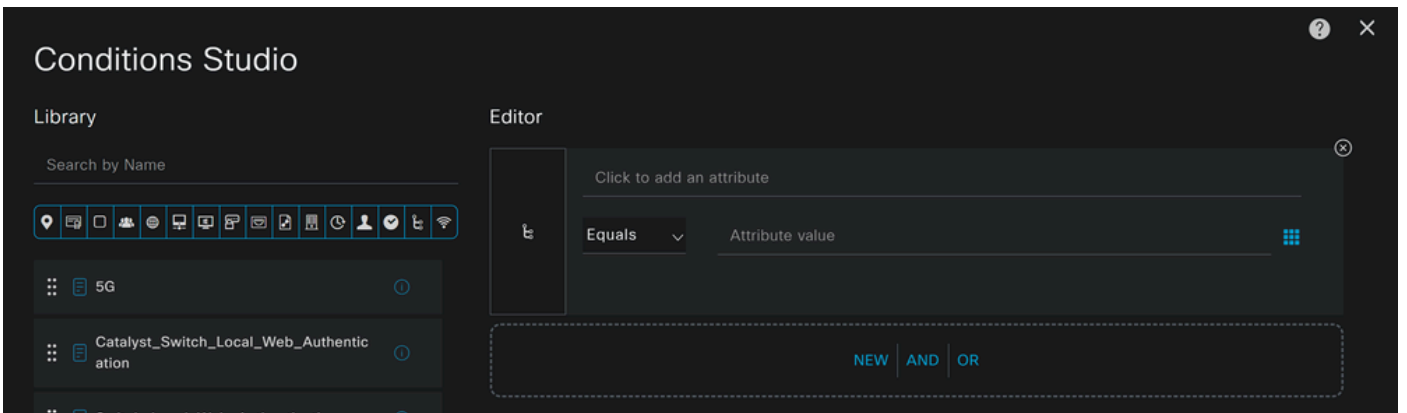
نيوكت ةوطخالل يف ةددحملل ةعومحملل يف نيومدختسملل ليوختب مق، ةالجال هذه يف. قرط ةدعب ليوختل جهن نيوكتلل كنكمي كب صاخلل ليوختل جهن نيوكتلل لاللل لاثملل عجار. ةعومحمل

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

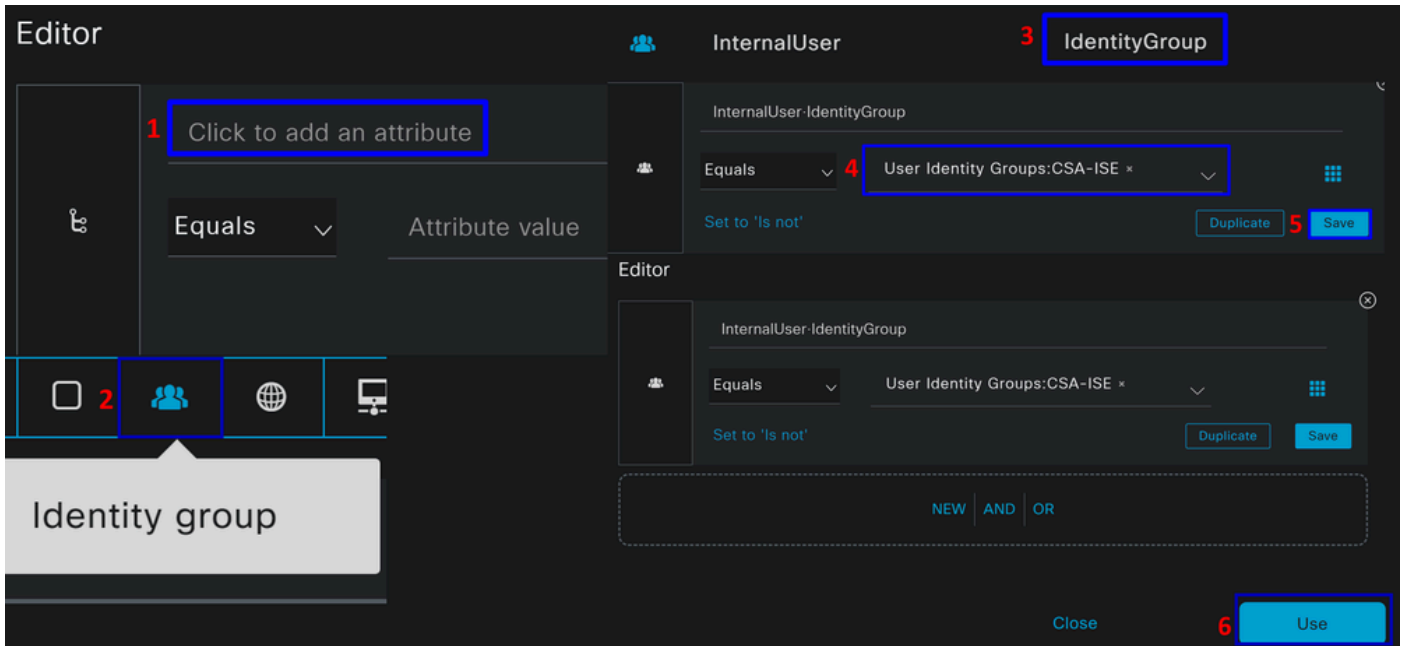
- **Authorization Policy** قوف رقنا
- لثم لي وختلا جهن دي دحتل + قوف رقنا:



- Rule Name، Conditions و Profiles ري غتب مق، ةلالتا ووطخلل
- 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، اهتحت

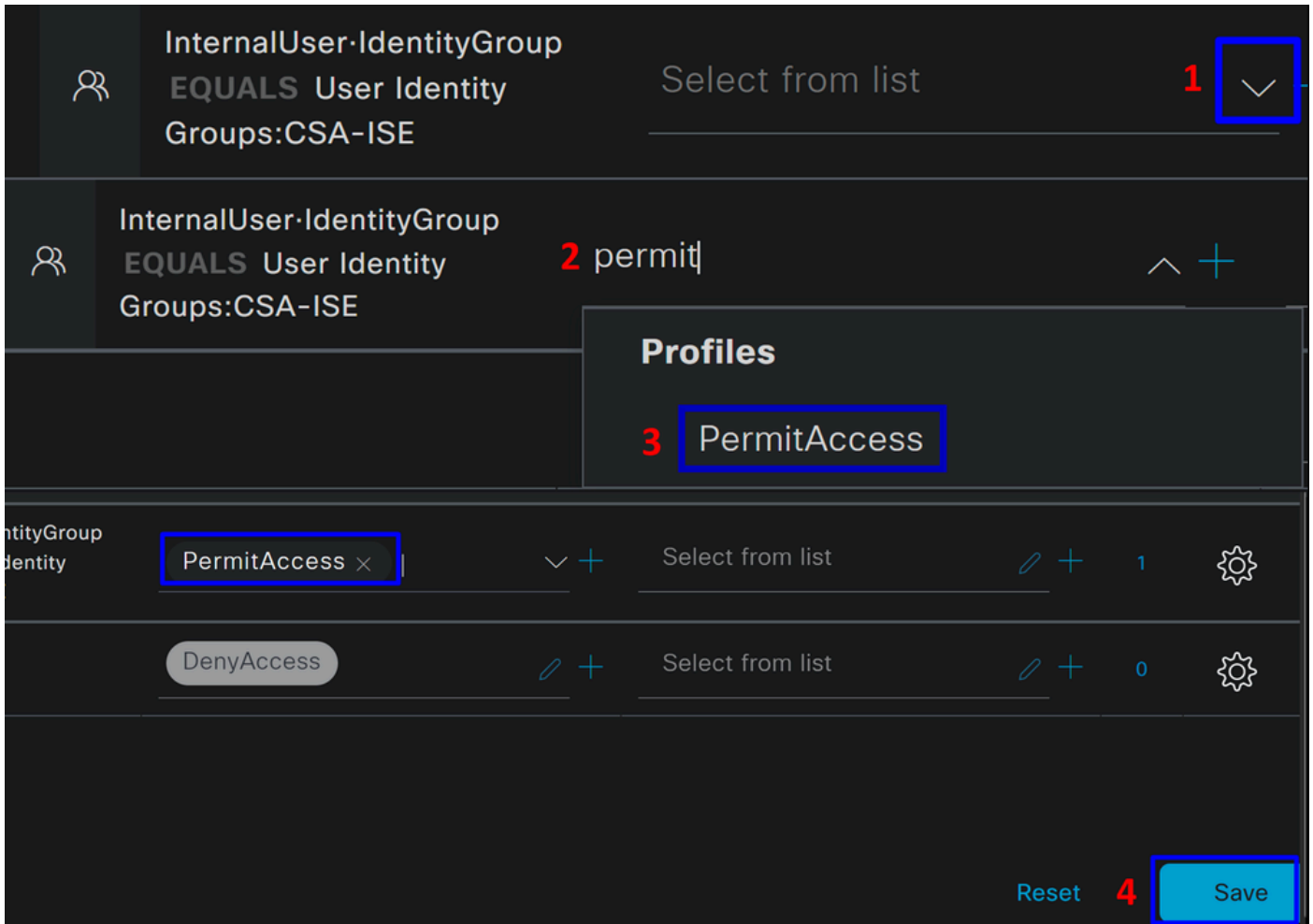


- Click to add an attribute قوف رقنا، طورشلا عاشنال
- رزل Identity Group لى ع رقنا
- راىخ IdentityGroup - لي خاد مدختسم قوف رقنا، هاندأ تاراىخلا تحت
- [ني وكتب مق](#)، ةوطخلال يفة قداصل لل دمتعمل Group لى ع روثلل ةلدسنم لةمئاقلا مدختسأ، راىخلا Equals تحت [ةعومجم](#)
- Save رقنا
- Use رقنا



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 اذا ام ققحتلل ةقداصلاب مق .كتسايسو Authentication Authorization فيرعتب تمق ،كلذ دعب ISE و Secure Access ىلع تالچسلا ةيؤر كنكمي ناك اذا امو ةلكشم ثودح



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

- ةقداصلاب ىلع ةقفاوملا دنع Secure Access يفلچسلا 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 لجسلا ضرع متي فيك

◦ ىلا لقتنا Cisco ISE Dashboard

- ىلا لقتنا Operations > Live Logs قوف رقنا

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

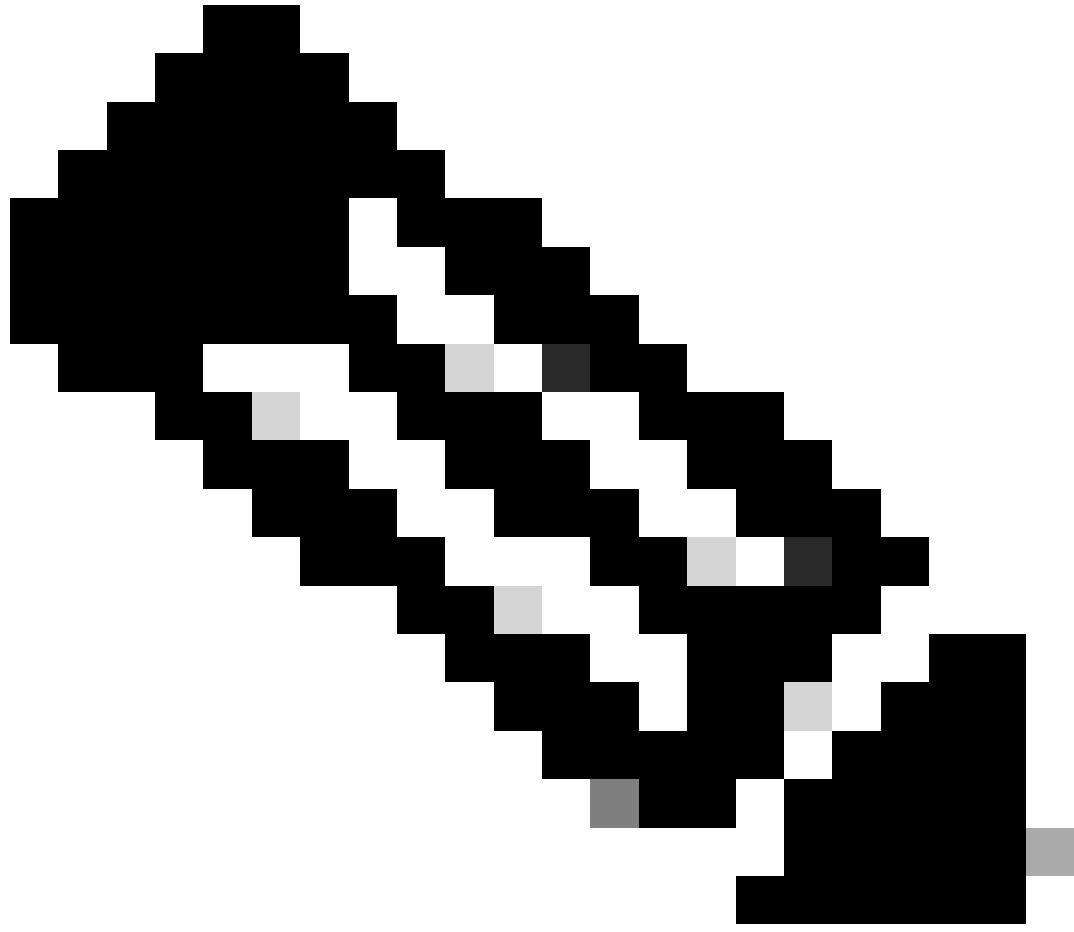
ISE ةىعضو نيوكت

وأ ةىلخادلا دراوملا ىلا لوصولا حنم لبق ةىهاللا ةطقن قفاوت نم ققحتلل نيوكتلا عاشناب 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 رقنا
- Anti-Malware قوف رقنا



تاسايسلا ىلع ءانب حىحصلا مئيقىتلا ءارج او كتزءء ءعضو نم ققحتلل تارايءلا نم ديدءال دءت ،كانه :ءظءالم
كء ءصاءلا ءىءءءلا

Conditions



Anti-Malware

Anti-Spyware

Anti-Virus

Application

Compound

Dictionary Compound

Dictionary Simple

Disk Encryption

External DataSource

File

Firewall

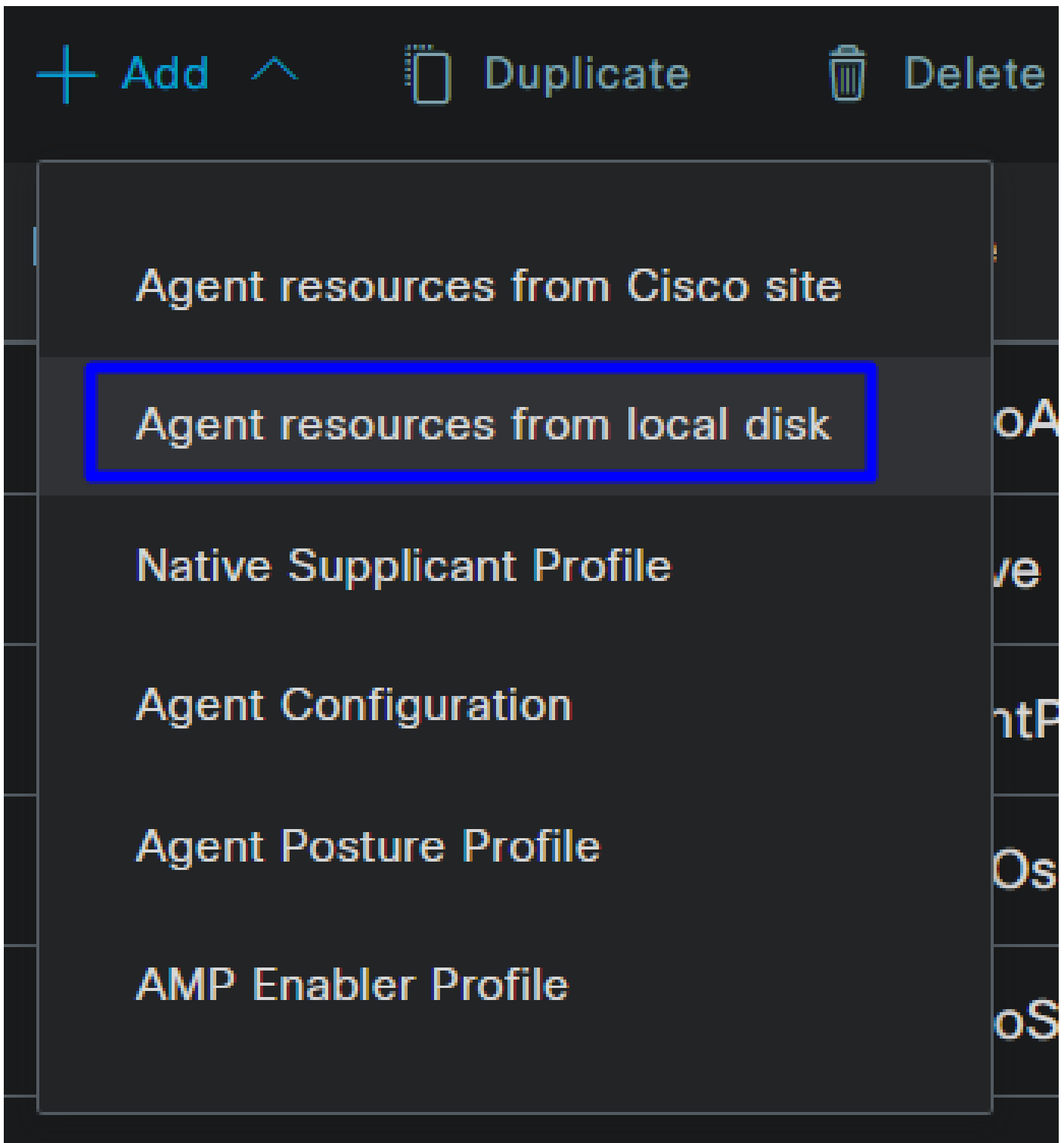
1. Agent Resources	لېمعلل ټول ډاډم اړخونه.
2. Compliance Module	Cisco ISE Compliance Module ټول ډاډم اړخونه
3. Agent Profile	ډاډم اړخونه ډاډم اړخونه.
3. Agent Configuration	نوموړې ډاډم اړخونه ډاډم اړخونه، ډاډم اړخونه ډاډم اړخونه لېمعلل ټول ډاډم اړخونه.

Step 1 اول ډاډم اړخونه لېمعلل ټول ډاډم اړخونه

- نوموړې ډاډم اړخونه لېمعلل ټول ډاډم اړخونه [Cisco Download Portal](#) لېمعلل ټول ډاډم اړخونه، ډاډم اړخونه ډاډم اړخونه ډاډم اړخونه .pkg.

Cisco Secure Client Headend Deployment Package (Linux 64-bit) cisco-secure-client-linux64-5.1.2.42-webdeploy-k9.pkg Advisories	06-Feb-2024	58.06 MB	↓ 🛒 📄
Cisco Secure Client Headend Deployment Package (Windows) cisco-secure-client-win-5.1.2.42-webdeploy-k9.pkg Advisories	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 Advisories	06-Feb-2024	118.88 MB	↓ 🛒 📄

- مزل لېمعلل ټول ډاډم اړخونه مزل لېمعلل ټول ډاډم اړخونه + Add > Agent resources from local disk



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 ةدحولكل رايتخالاةناخ 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 نيوكت3 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

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 لئكول نئوك ت نئوك ت

- قوف رقنا + 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"/>

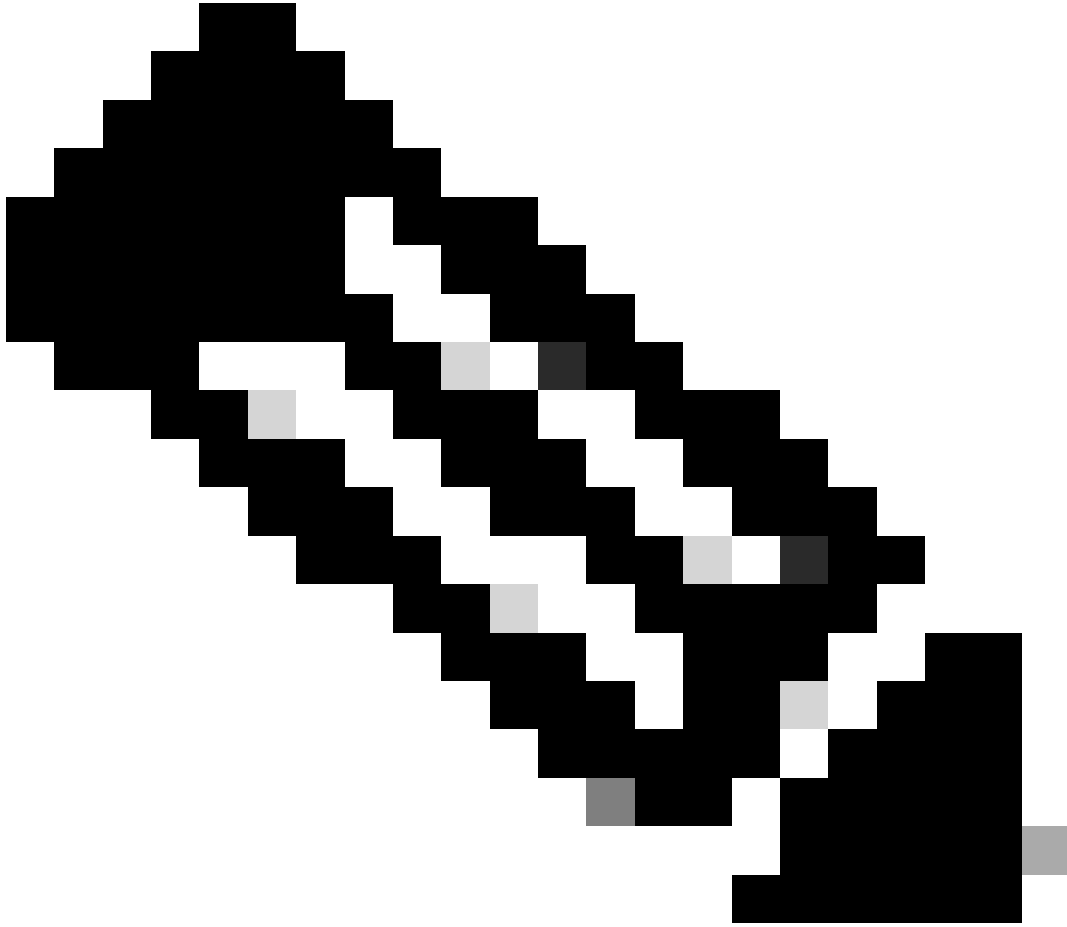
Profile Selection

* ISE Posture	1.CSA_PROFILE	▼
VPN		▼

- [اهلي محتوولي محتلا ليلي كودراوم ليليننت 1 ةوطخللا](#) ىلع اهلي محت مت يتلا ةمزلال رتخأ : Select Agent Package
- **Configuration Name:** ىلع فرعتلل مسا رايتخأ **Agent Configuration**
- **Compliance Module:** [قفاوتلا ةدحوليليننتب مق 2 ةوطخللا](#) ىلع اهلي زنت مت يتلا قفاوتلا ةدحور تخأ
- Cisco Secure Client Module Selection
 - **ISE Posture:** رايتخال ةناخ ىلع ةمالع عضو
- **Profile Selection**

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

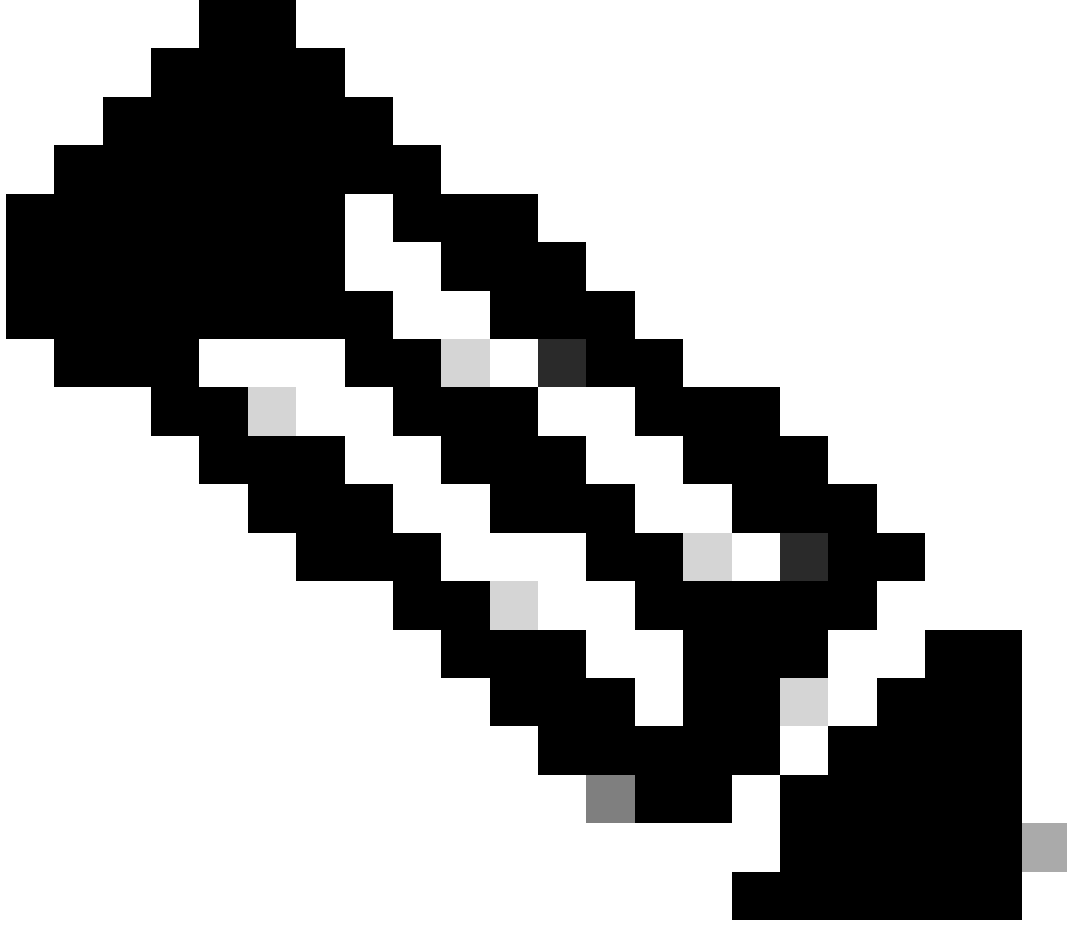
- Save رقنا



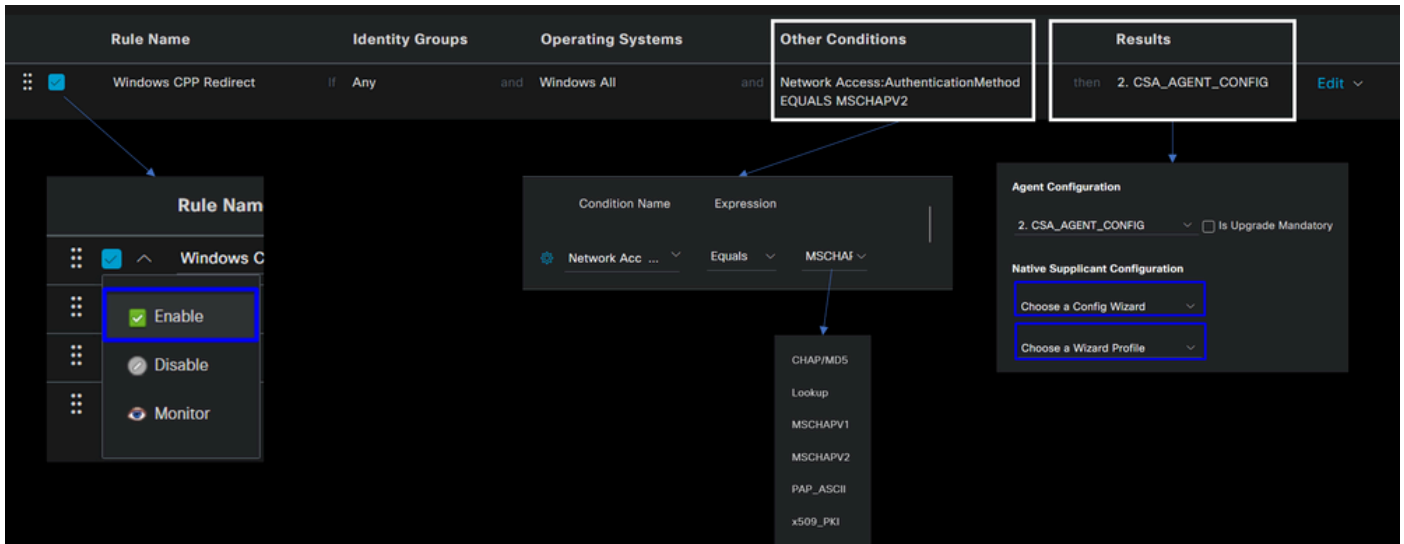
لقتسم دحاو لي مع نيوكت، Linux أو Mac OS أو Windows، ليغشت ماظن لكل نوكي نأب ىصوي: ةظحالم

نيوكت كمزلي، ةريخألا ةوطخالا في اهنيوكت مت يتلا ةيظمنلا تادحولاو (ISE) ةيوهلا تامدخ كرحم ةيعضو دادع| دادع| 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 ةلبيكولا 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:** [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 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

- 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

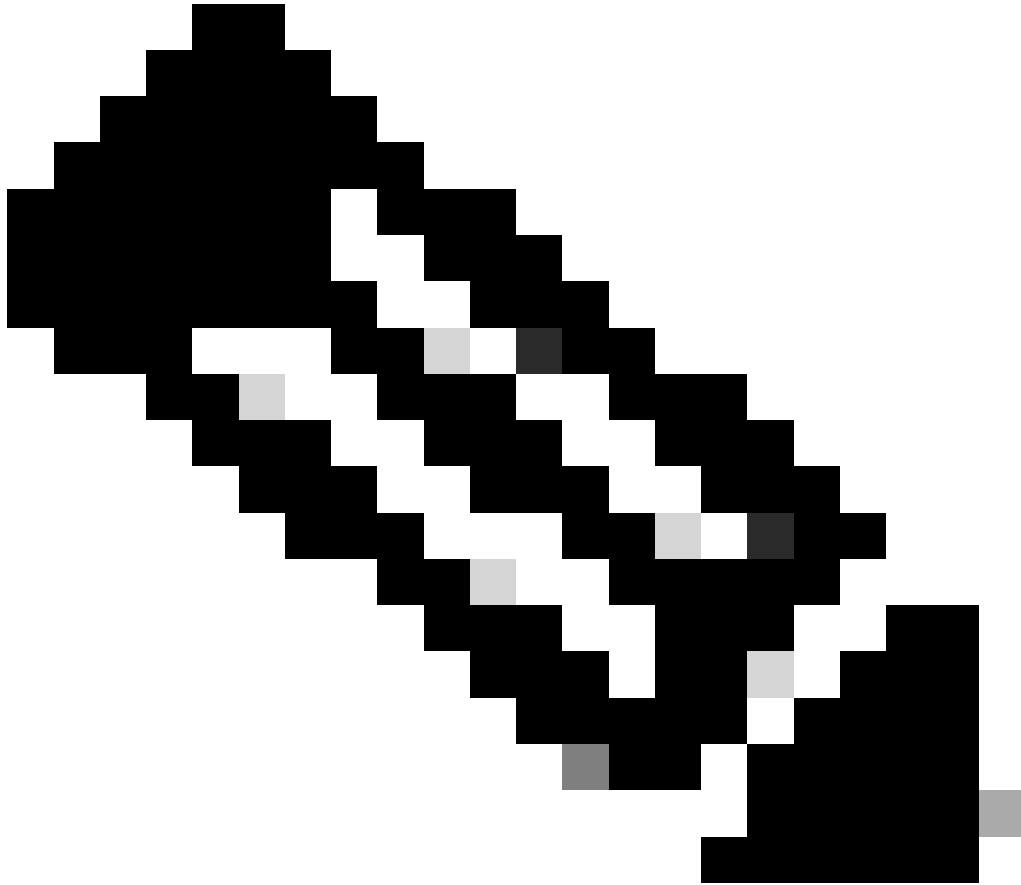
- **Name:** فورعمل رېغ DACL عم قفاوتللا ىللا رېشې امسا فضا
- **IP version:** رتخا IPv4
- **DACL Content:** ادوحم الوصو يقطع يتللا (DACL) ةيساسالا ةينبلا ىللا لوصولو يف مكحت ةمئاق ءاشناب مق 8443 ذفنملا ربع دادملا لخدمو HTTP و DNS و DHCP و ةكبشلا ىللا

```

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 وه ل ا تام د خ ك ر ح م م دا 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 ف ل م ء ا ش ن ا ل ة ب و ل ط م ل ا (DAACL) 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 ف ل م ن ي و ك ت ل

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

• [+Add](#) قوف رونا

• [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 :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

لويوختلآ - جهنلآ ةعوم جم	لويوختلآ فيرعت فللم
نعذم	قفاوتم - ليوختلآ فيرعت فللم
قفاوتملآ فسورعم ريغ	عم قفاوتم - ضيوفتلآ فيرعت فللم UNKNOWN
قفاوتم ريغ	DenyAccess

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
<ul style="list-style-type: none"> > Authentication Policy(2) > Authorization Policy - Local Exceptions > Authorization Policy - Global Exceptions > Authorization Policy(4) 					

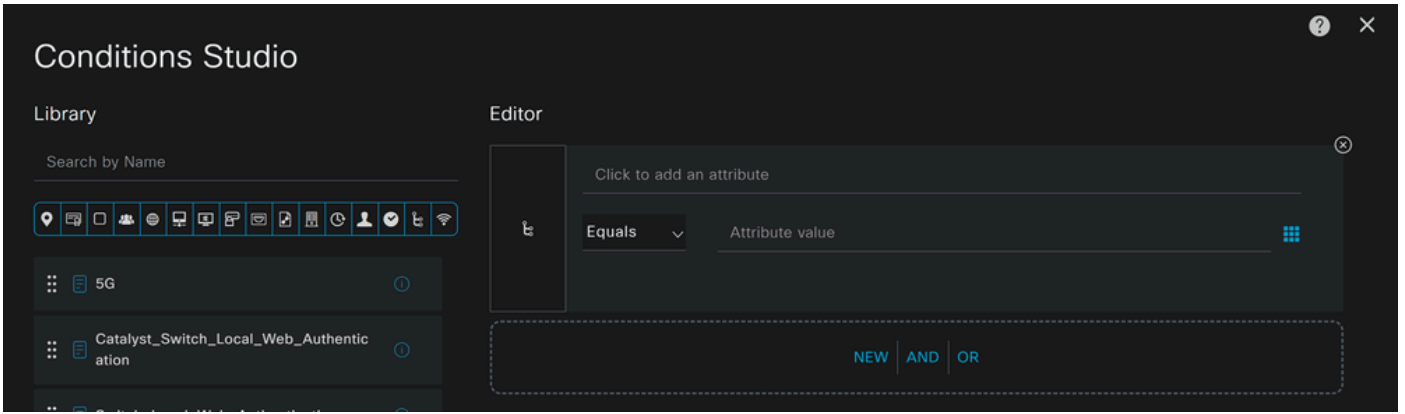
- هئاشناب تمق يذلا جهنلا ىلا لوصولل > قوف رقنا

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

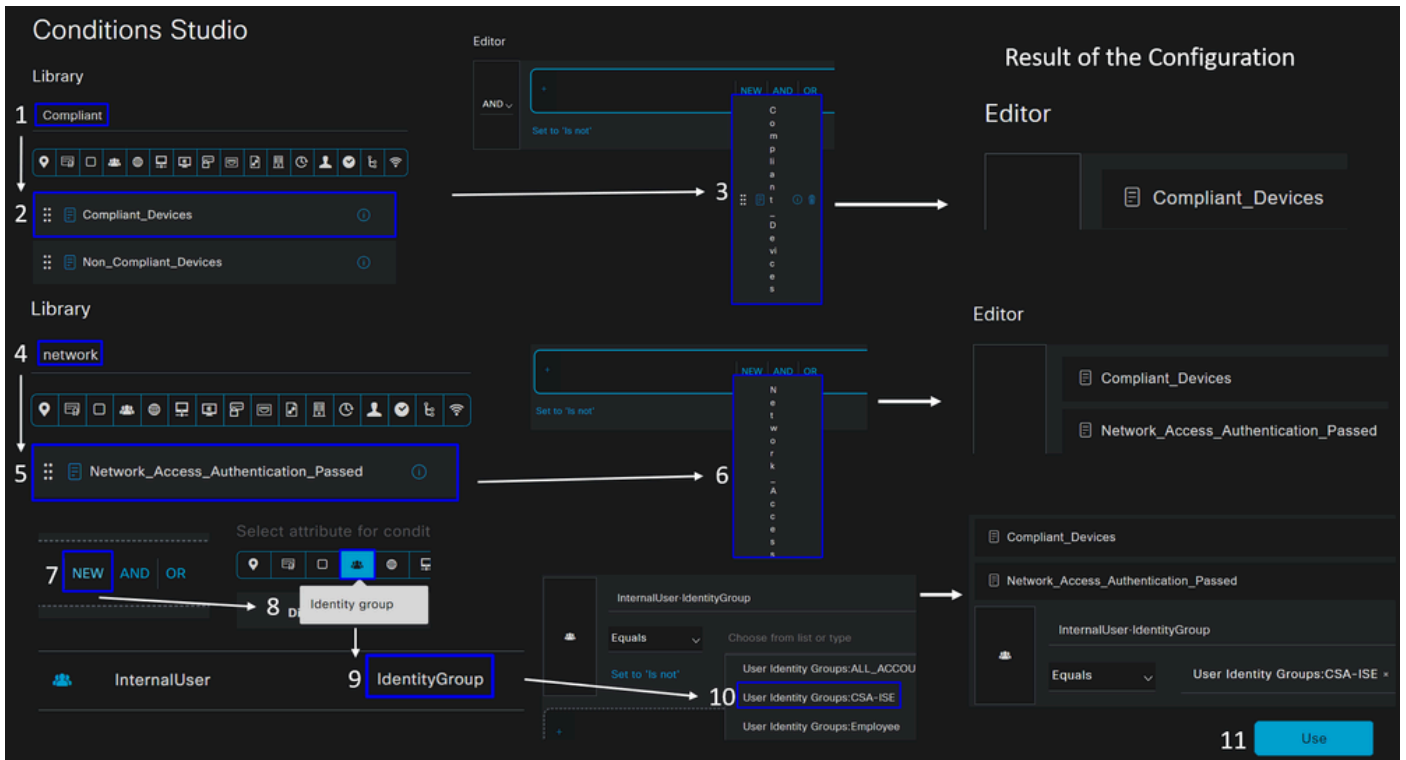
- ةساي سلا CSA-Compliance دي دحتل + رقنا :

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

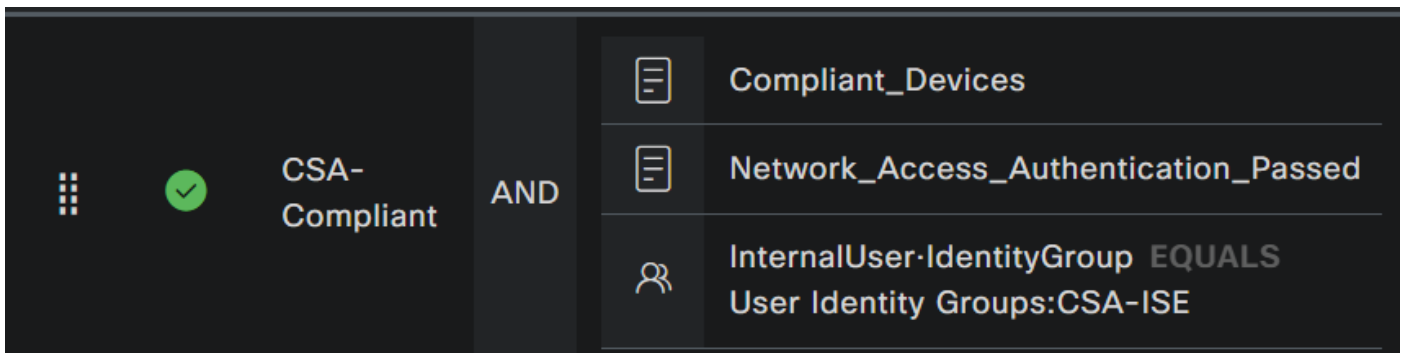
- Rule Name، Conditions و Profiles ري يغتب مق، ةيلاتلا ةوطخلل
- CSA-Compliance لى نيوكتلا Name مسا نييعت دنع
- + قوف رقنا، مكحتلا رصنع Condition نيوكتلا
- تامولعمل دجت Condition Studio، اهتحت



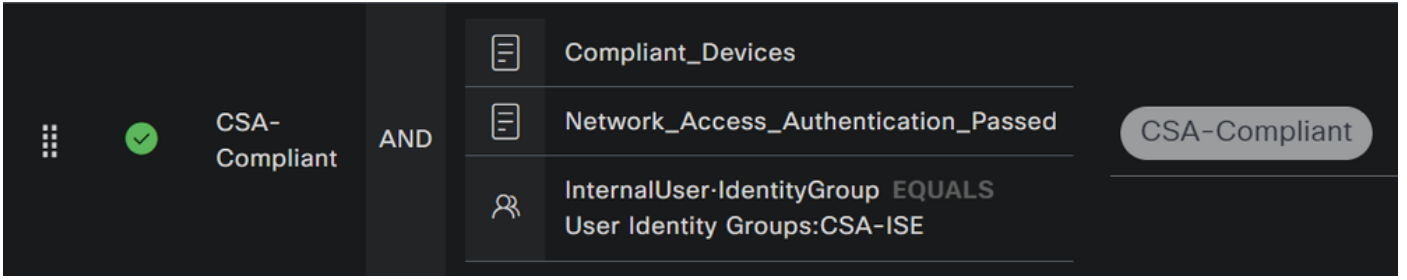
- **compliant** ن ع شحبا ، طرشللا ءاشنال
- **Compliant_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **network** ن ع شحبا ، يناللا طرشللا ءاشنال
- **Network_Access_Authentication_Passed** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **New** لوخدل Editor لفسأ رقنا
- **Identity Group** لىل ع رقنا
- **Internal User Identity Group** رتخا
- هتقباطم ديرت يذلا **User Identity Group** رتخا ، **Equals** تحت
- **Use** رقنا



- ةيلات الة روص الة كيدل، ةجيتنك

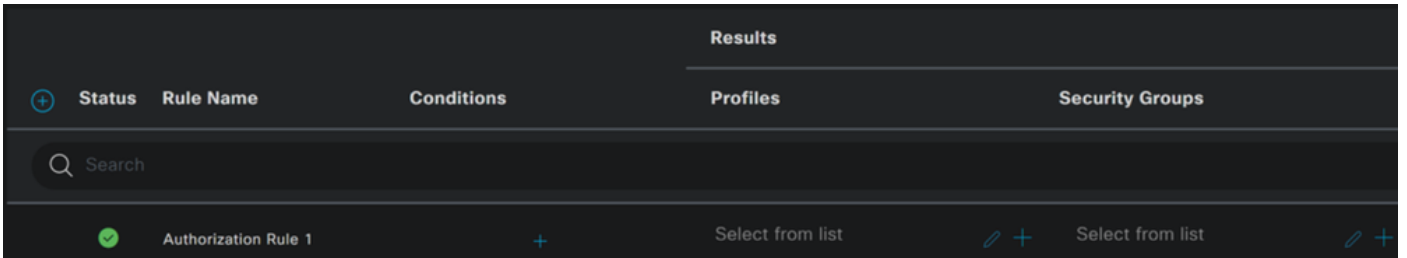


- [فیرعت فایلم](#)، ةوطخال الة نوكم الة یوكش الة لیوخت فیرعت فلم رتخاو لدسنم الة رزلا تحت رقنا Profile تحت قفاوتم لیوخت

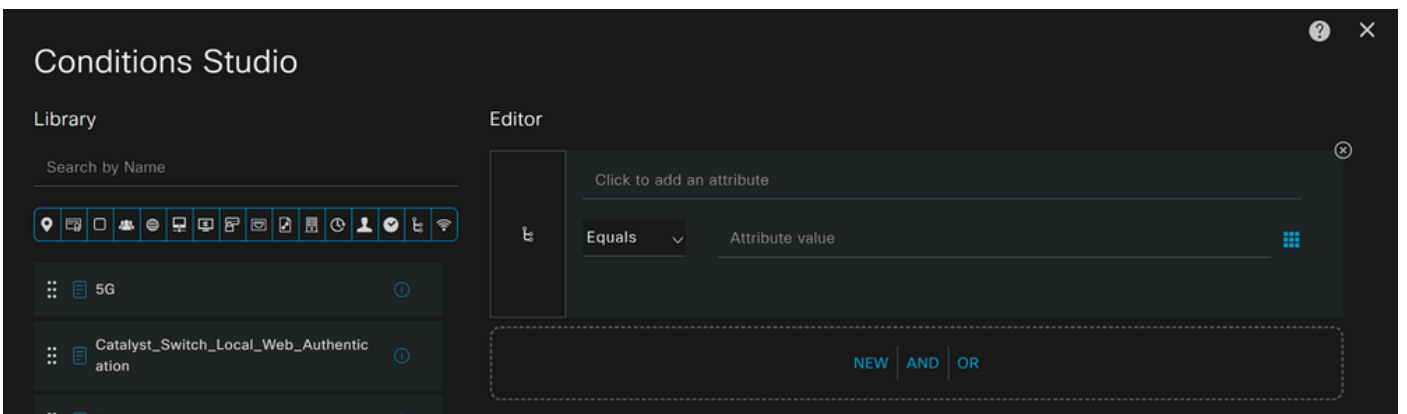


Compliance Policy Set. نيوكتب نآلا تمق دقل

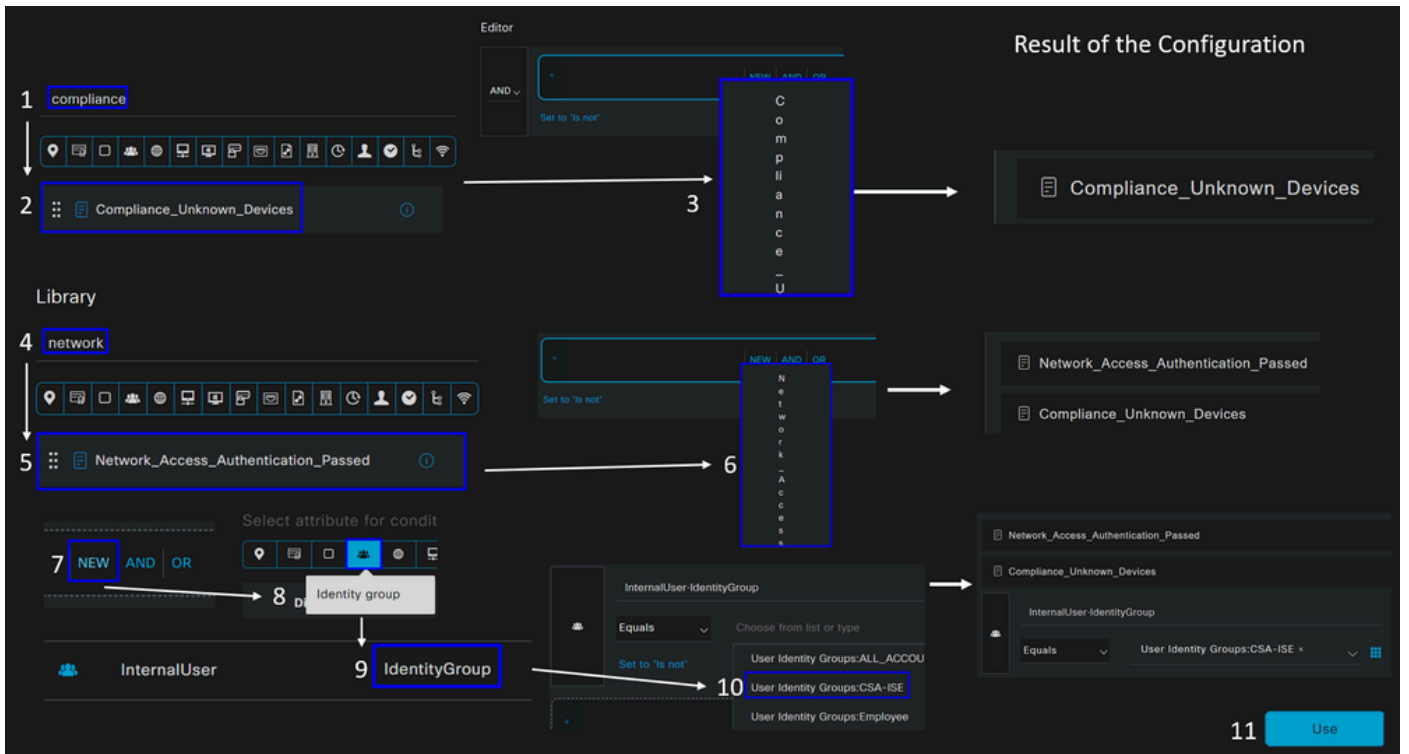
- ةسايسال CSA-Unknown-Compliance ديحتل + رقن :



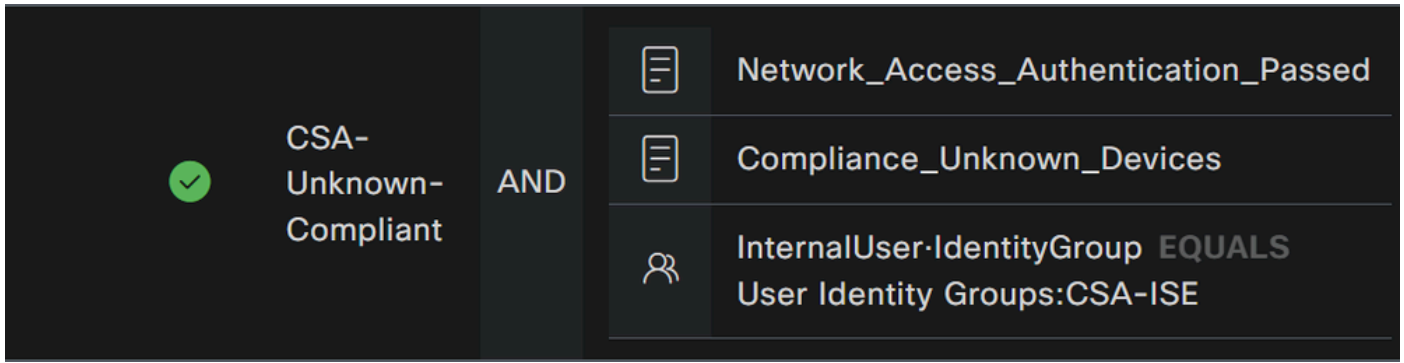
- Rule Name، Conditions و Profiles ريغيغت ب مق، ةيلاتال ةوطخلل
- CSA-Unknown-Compliance لى نيوكتال Name مسا نييعت دنع
- + قوف رقن، مكحتال رصنع Condition نيوكتل
- تامولعمل دجت Condition Studio، اهتحت



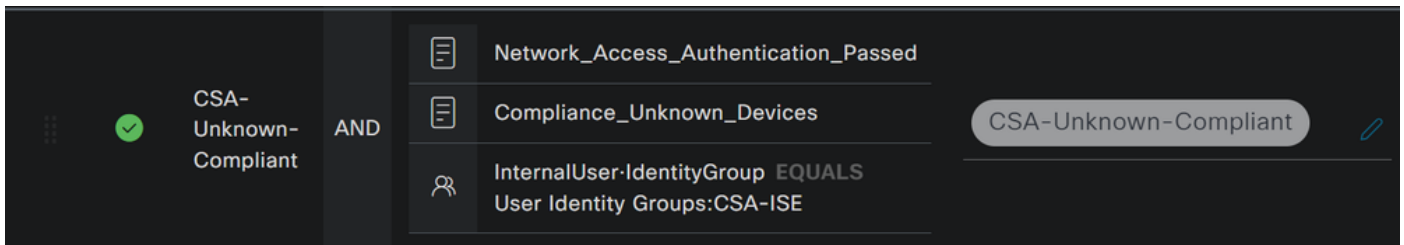
- **compliance** ن ع شحبا ، طرشلل ءاشنال
- **Compliant_Unknown_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تال فال او بحسلا
- **network** ن ع شحبا ، ينائل طرشلل ءاشنال
- **Network_Access_Authentication_Passed** تضرع دق نوكت نأ بجي
- **Editor** تحت تال فال او بحسلا
- **New** لوخل دل Editor لفسأ رقنا
- ةنوق يأل **Identity Group** ل ع رقنا
- **Internal User Identity Group** رتخا
- هتق باطم ديرت يذل **User Identity Group** رتخا ، **Equals** تحت
- **Use** رقنا



- ةيلال ةروصلل كيدل ، ةجيتنك

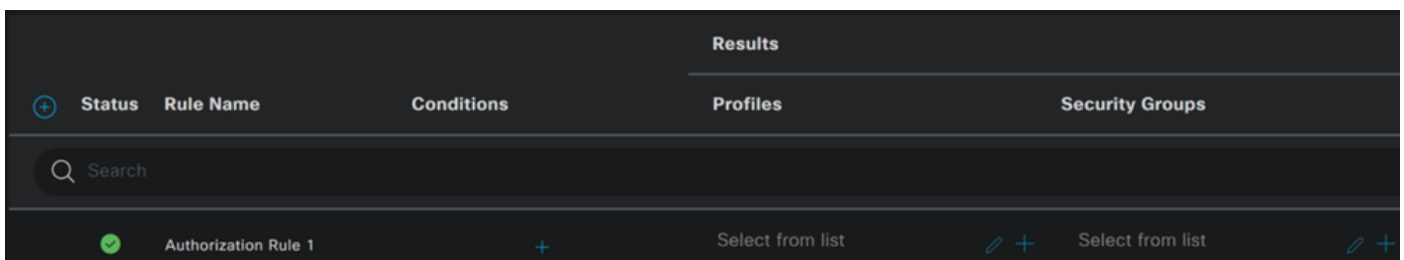


- [في برع ت فلم](#)، ةوطخلال ىلع نوكملا ىوكشلال لىوخت في برع ت فلم رتخا و لدس نمل رزلا تحت رقنلا **Profile** تحت [قفاوتم فورعم ريغ لىوخت](#)



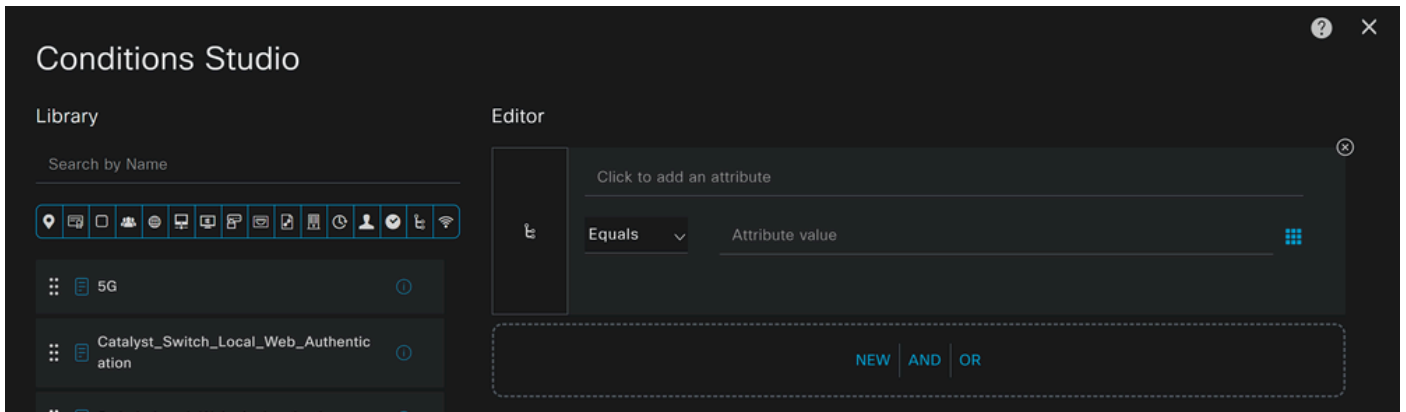
Unknown Compliance Policy Set. نيوك ت ب نآلا تمق دقل

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

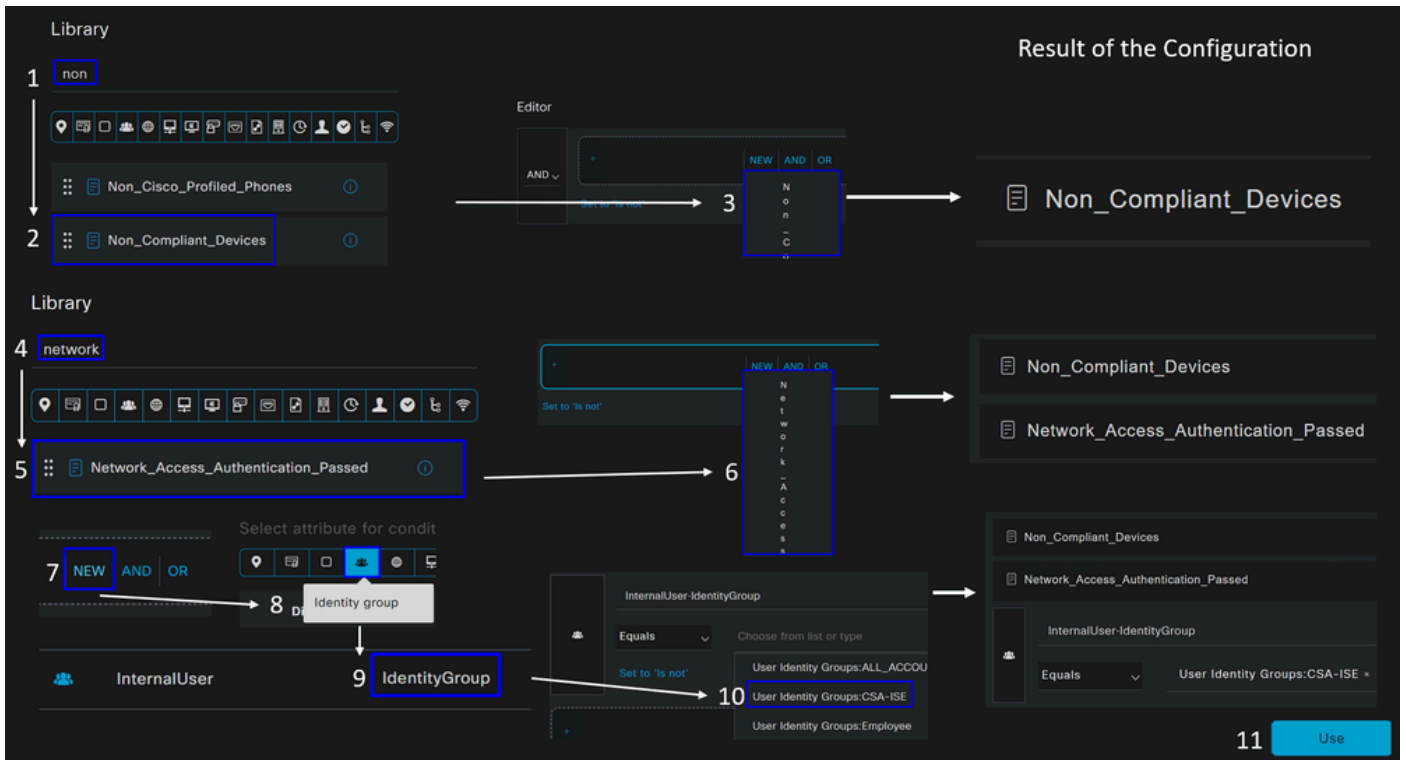


- **Rule Name**، **Conditions** و **Profiles** ريغ ت ب مق، ةيلال ةوطخلل
- **CSA-Non-Compliance** لىل نيوك تال **Name** مس نييعت دنع
- + قوف رقنا، مكحتال رصنع **Condition** نيوك تال

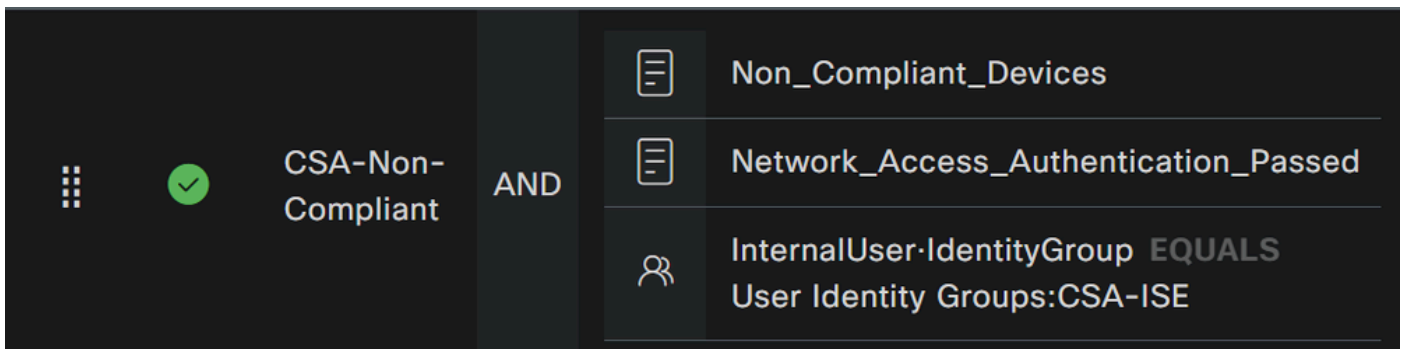
- تامولعمل دجت **Condition Studio**، اهتحت



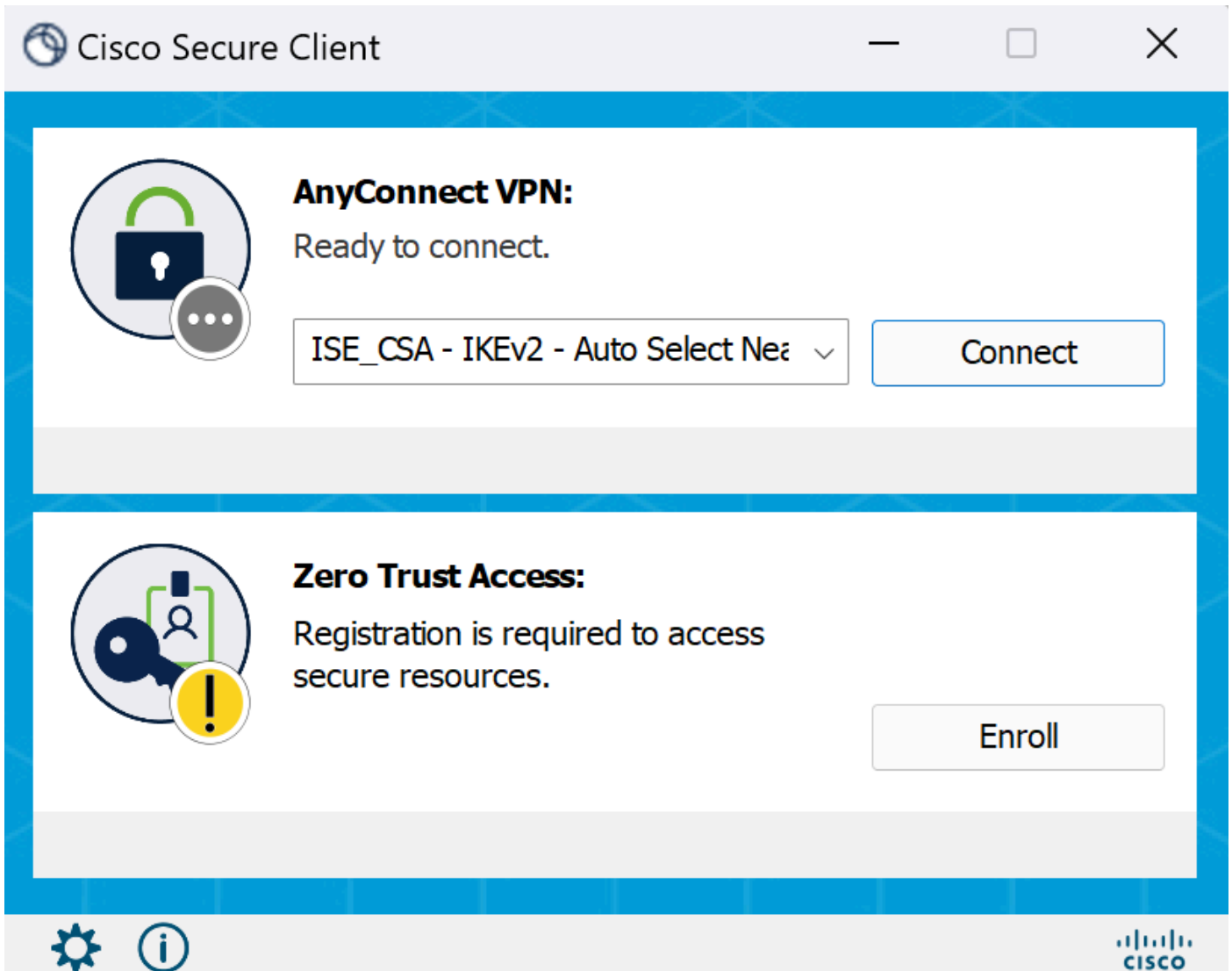
- **non** نع شحبا، طارشلا عاشنال
- **Non_Compliant_Devices** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **network** نع شحبا، يئناثلا طارشلا عاشنال
- **Network_Access_Authentication_Passed** تضرع دق نوكت نأ بجي
- **Editor** تحت تالفال او بحسلا
- **New** لوخدل Editor لفسأ رقنا
- **Identity Group** ىلع رقنا
- **Internal User Identity Group** رتخا
- هتقباطم ديرت يذلا **User Identity Group** رتخا، **Equals** تحت
- **Use** رقنا



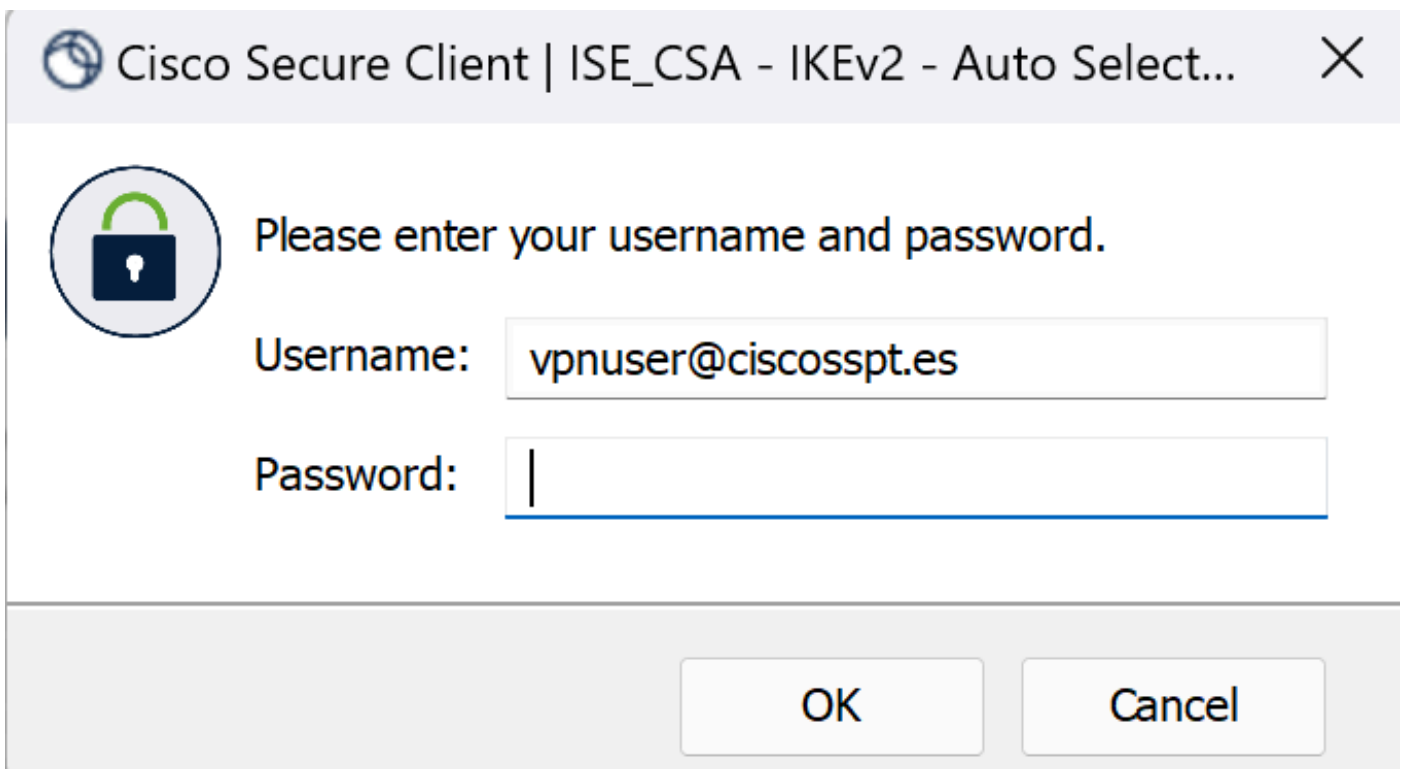
- قیالات لارو وصل كېدل، ډېجېټنك



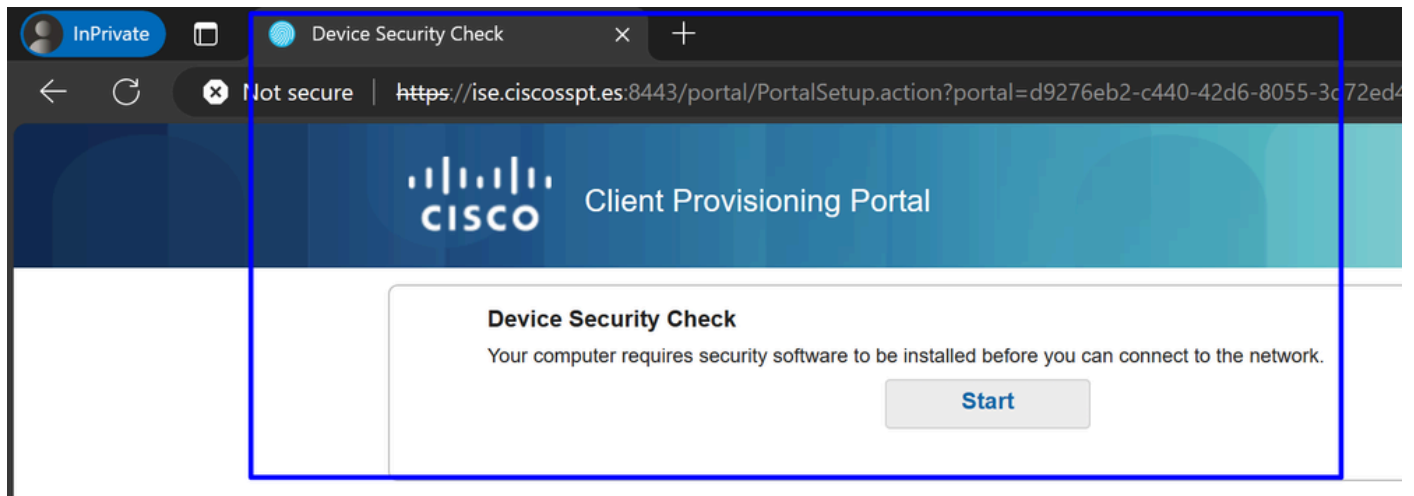
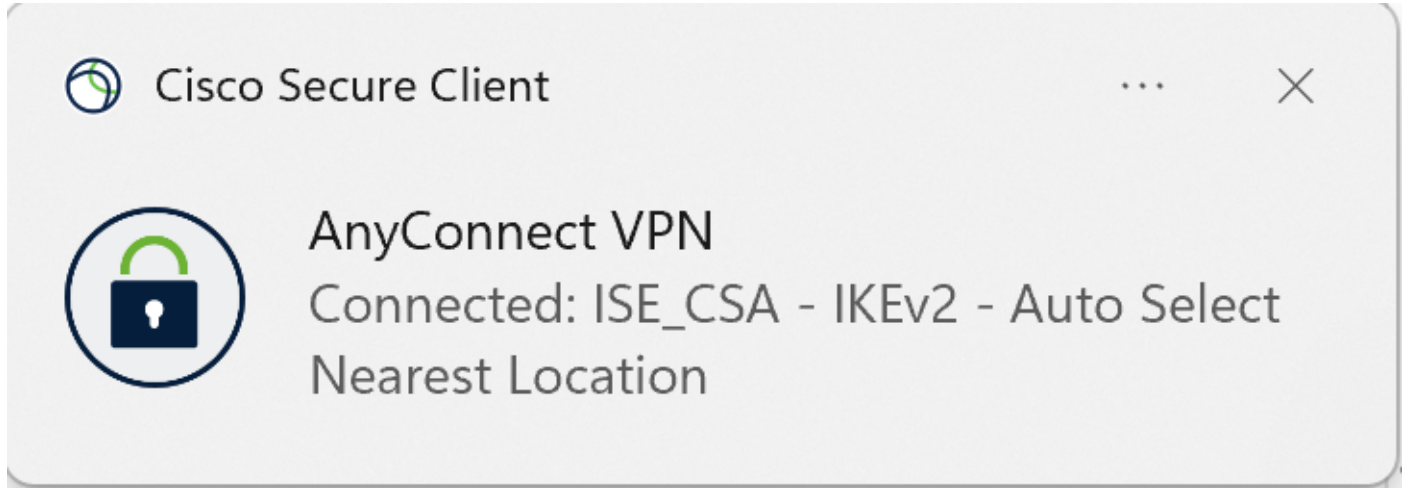
- **DenyAccess** یو كشل لېوخت فيرعت فلم رتخاو ل دس نمل رزلا تحت رونا **Profile** تحت

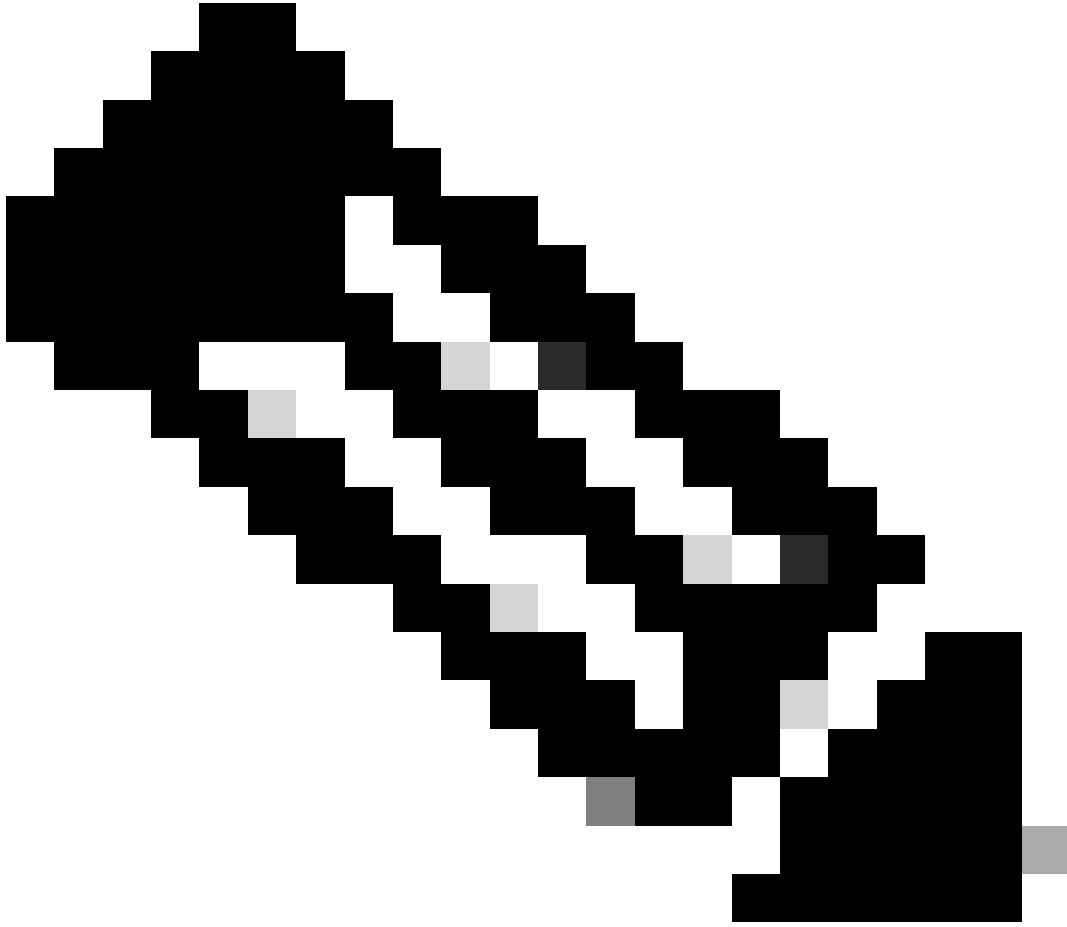


2. ةقداصم لل دامتعالا تانايب ريفوت.



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





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

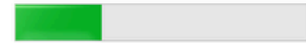
(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

8. مدع ةلاح يف ةيلاحلا ةزهجألا ةلاح نم ققحتلا يف (ISE) ةيوهلا تامدخ كرحم ةيعضو ISE Posture أدبي، ليكولا تيبتت دعب. قفاوتلا وحن كدشري اقتبم 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.

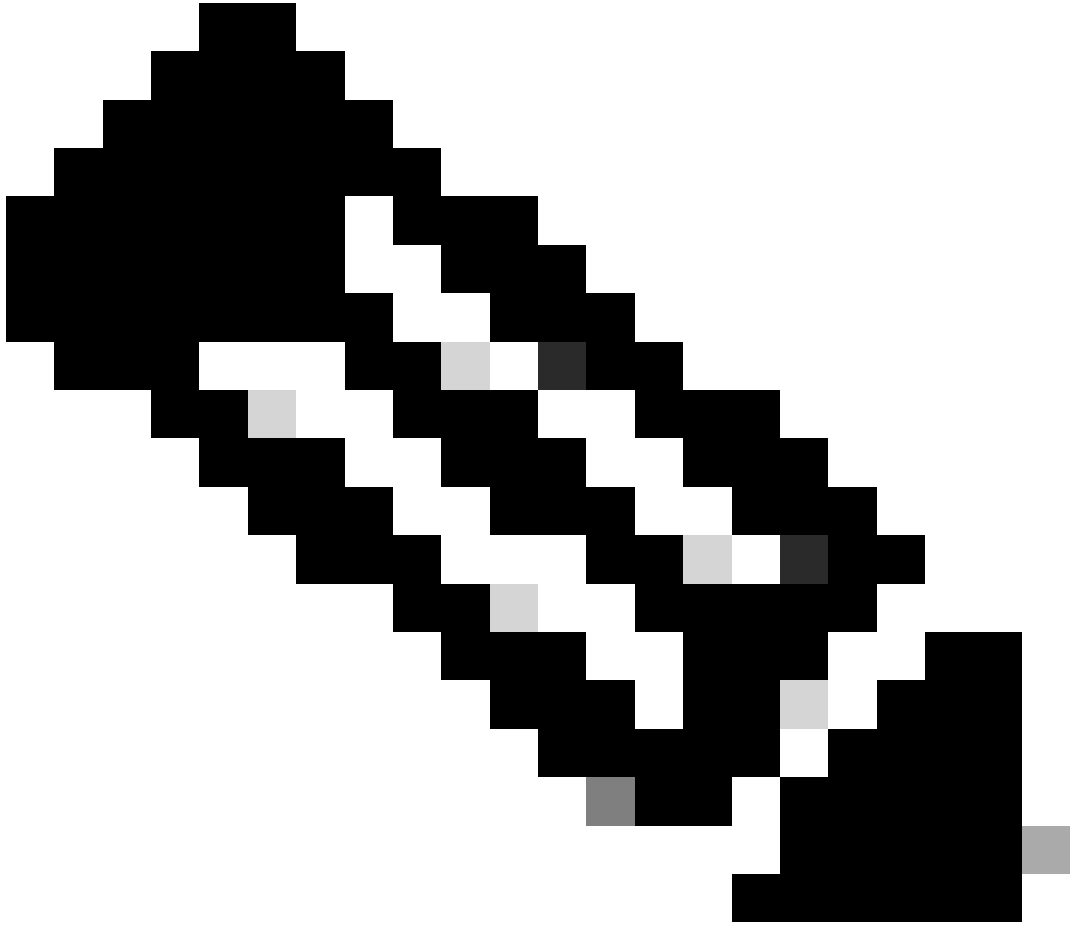
This endpoint has failed to check. Please ask your network administrator to install a Secure Endpoint.

Start

More Details



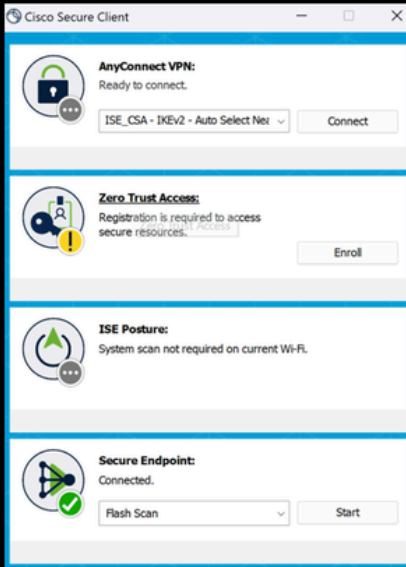
Cancel



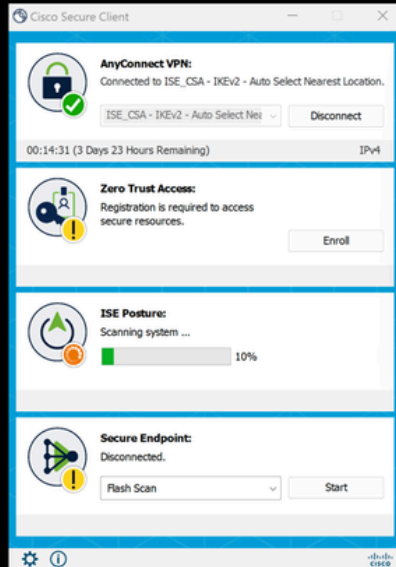
ليوختال جهن ةعومجم نمض لخدتو، قفاوتم ريغ ائاقولت حبصت، ةيقبتم ال Cancel ةلهملاءهت نالاج يف: ةظالم
VPN ةكبش نع اروف لصفتو، [CSA-Non-Compliance](#).

9. (VPN) ةرهاظلا ةصاخلا ةكبشلاب ىرخأ ةرم لصفتاو "ةنمآلا ةياهنلا ةطقن لماع" تيبثت ب مق.

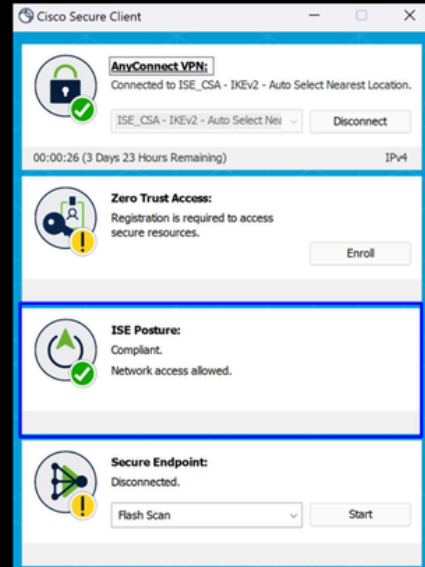
Secure Endpoint Installed



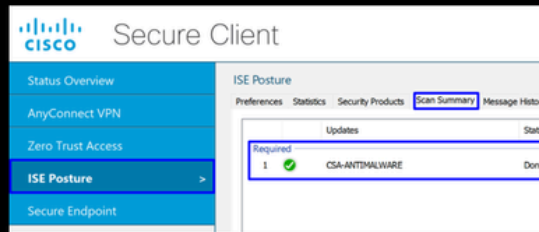
Agent Scanning



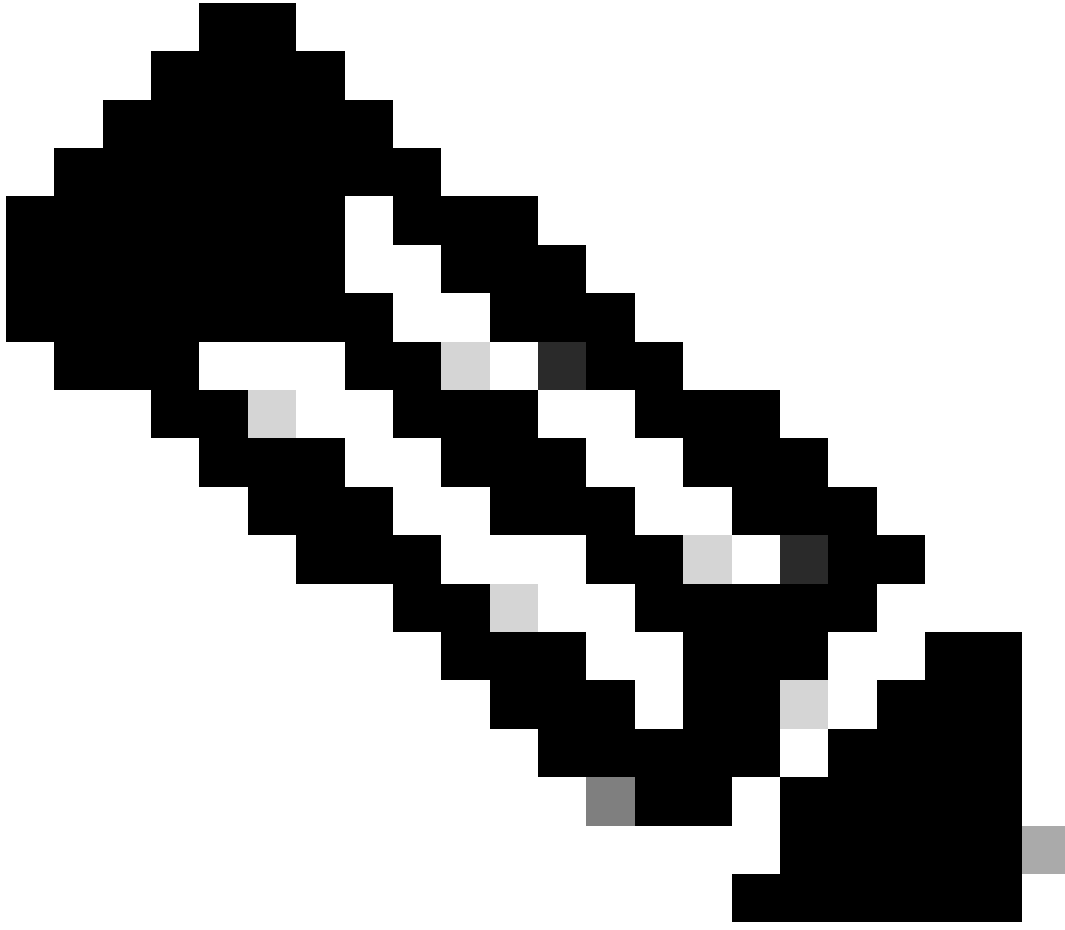
ISE Posture Successful validated



Scan Summary - Compliance



10. إلى لوصولها قرح حنمي وىوكش ةلاح في نوكت يكل كل عرض وريغتي، قفاوت ةلاح في زاهال أن نم ليمعلا ققحتي أن دعب 10. ةكبشال إلى لعدوجومال دراومال اعيجم.



لوصولك نك ميو، [CSA عم قفاوت ملنا](#) لي وختالتا تاسايس ة و م ح مل اع ضا خ ح ب ص ت ، اق ف ا و ت م ح ب ص ت نأ د ع ب : ة ظ ح الم ة . ك ب ش ل ا د ر ا و م ع ي م ج ي ل ا ا ر و ف .

ISE في تال ج س ل ا ع ي م ح ت ة ي ف ي ك

، ة ي 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 ت 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 : ة ي ل ا ت ل ا ت ا د ا ش ر ا ل ا ع ب ت ا

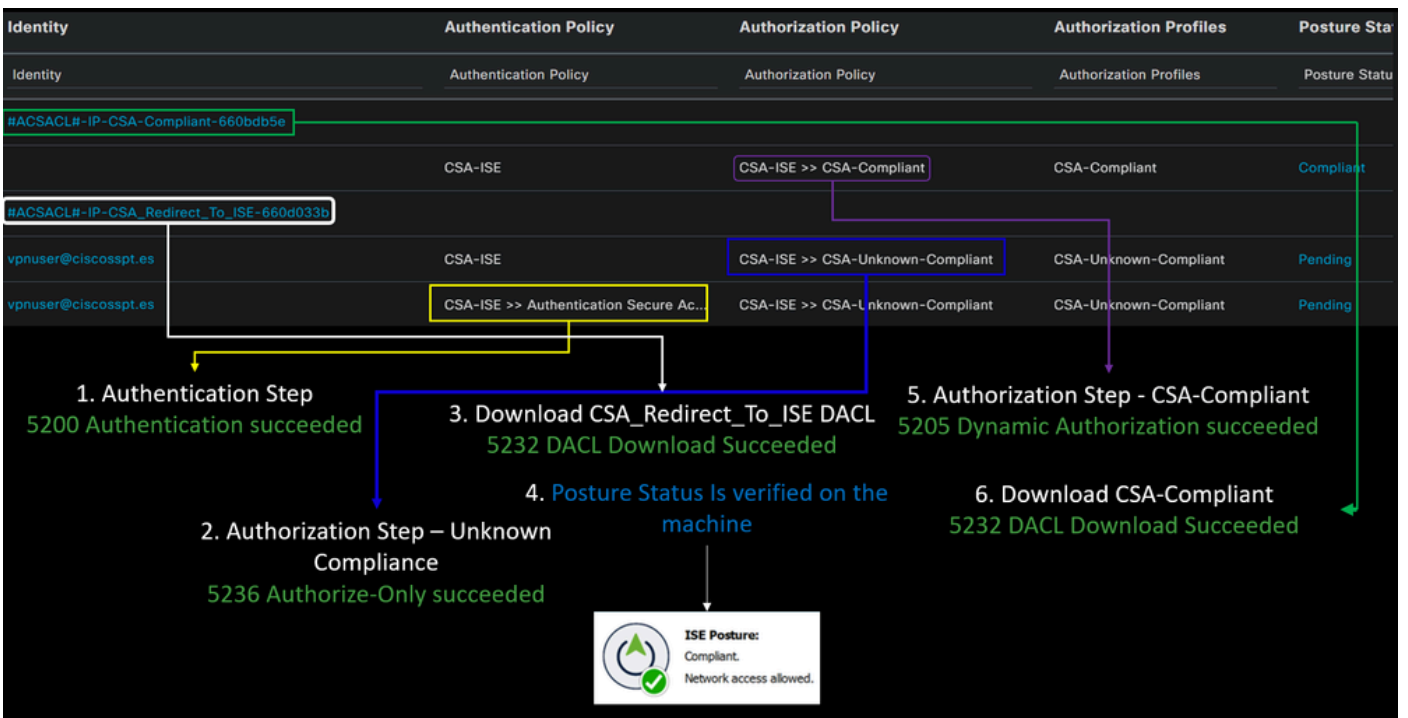
- ISE تاملول عم ة حول يلا لقتنا

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

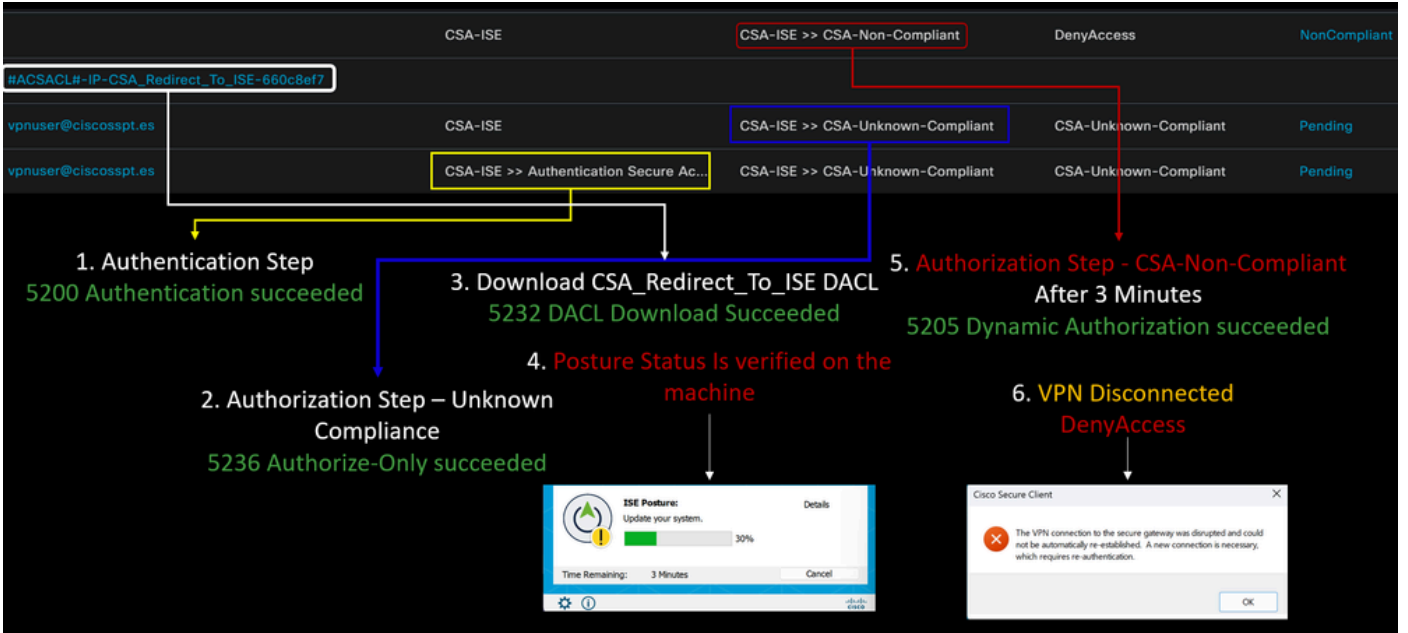
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter	
0	0	0	0	0	
Refresh Never		Show Latest 50 records		Within Last 24 hours	
Reset Repeat Counts		Export To		Filter	
Time	Status	Details	Identity	Authentication Policy	Authorization Policy
Apr 03, 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 ةيفي ك يلاتال ويرانيسال حضوي

ادايقنا



لاثتمالال مدعو



ISE لم اکت ونم آلا لوصول عم یل وائل تاوطلال

لالخ نم اهل لوصول نكم یل تاك بشل ل نیوكت ةفاضل مزلی، 192.168.10.0/24 ةكب بشل نمض، یل لال لاثم ال ی قف نل نیوكت تحت قف نل.

Step 1: قف نل نیوكت نم ققحت ال:

نم آلا لوصول تامول عم ةحول یل لاق نال اءارل، كلذ نم ققحت لل

- قوف رقنا Connect > Network Connections
- قف نل Network Tunnel Groups > قوف رقنا

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

- ك ب صال ال Cisco ISE نوک ی شیح ناو نال ةحاسمل قف نل نیوكت نم ققحت، صل لم تحت

Summary



Connected

Region Europe (Germany)

Device Type FTD

Routing Type Static Routing

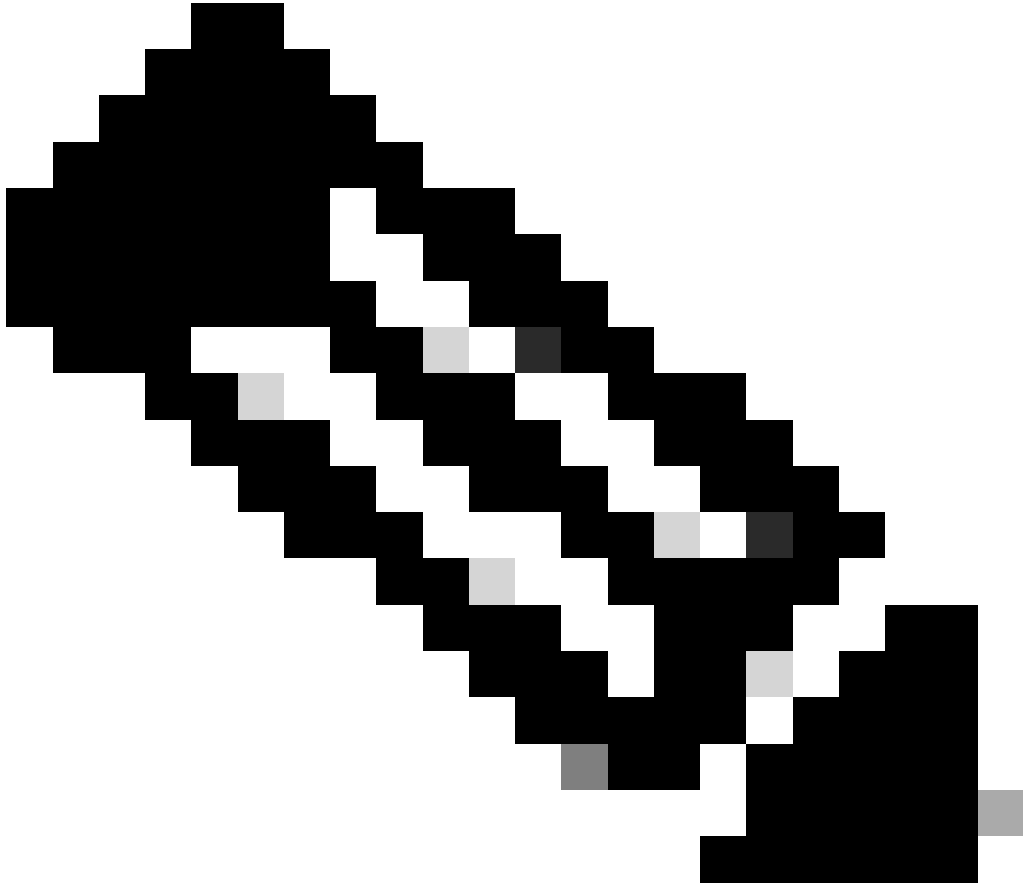
IP Address Range 192.168.10.0/24

Last Status Update Mar 19, 2024 11:13 AM

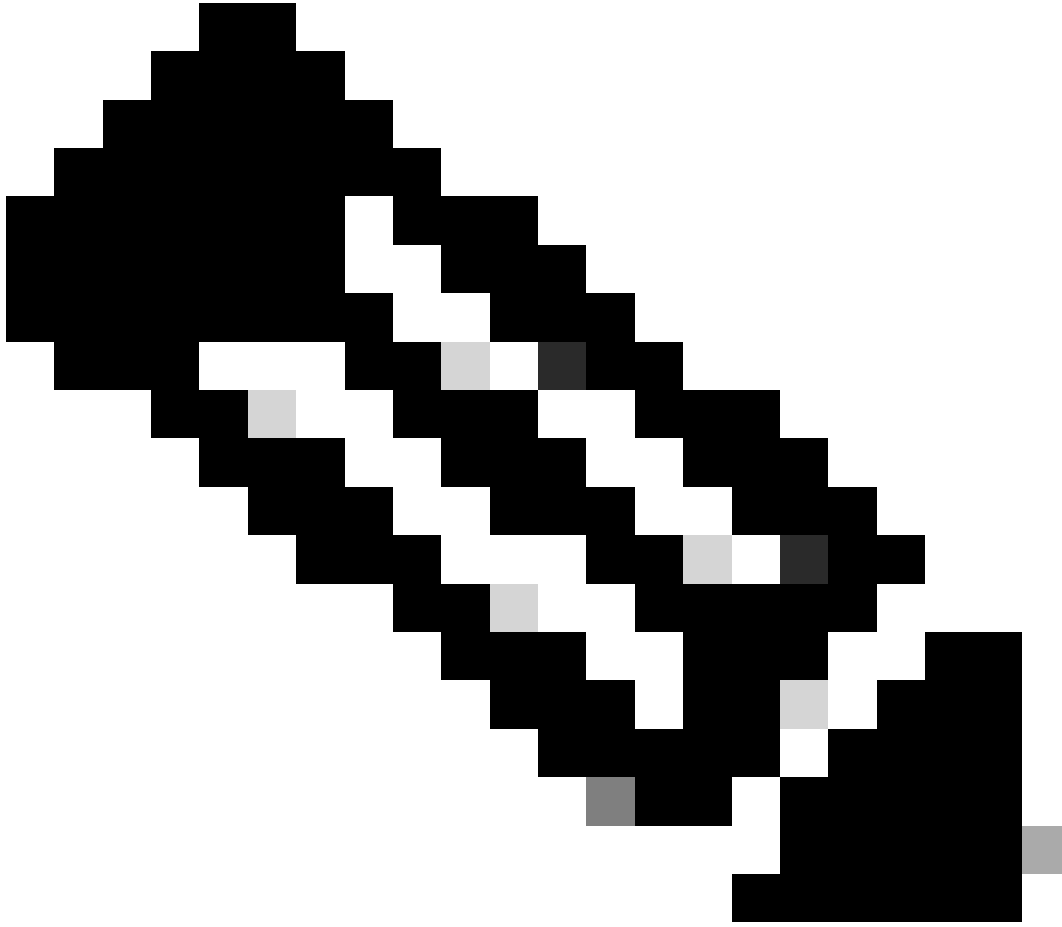
Step 2: إعداد رادج إيلع رورملا ةكرحب حامسلا.

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

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



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



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

ءي فرطلا ءطقنلل IP عمءت و ءراءالا عمءت

:كب ءصاځال [نم آالا لوصولا تامولعم ءءول](#) ىلا لقتنا ،ءي فرطلا ءطقنلا و 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 ب صاخلا ISE نيوكت نم دكأت: **3** ةوطخلا

كمزلي، **ISE Provisioning Portal** لى لقتنلاب (VPN) ةيره اظلا ةصاخلا ةكبشلا ربع نيصلصتملا نيمدختستم لىل حامس لىل ISE يئاقلتلا دادم لىل حامس لىل همادختسا متي يذلاو، لوصولا ريفوتل صاخ درومك ك ب صاخلا زاهجلا نيوكت نم دكأتلا Posture Module ةكبش لىل (VPN).

ك: ةصاخلا [نم آلا لوصولا تامولعم ةحول](#) لى لقتنا، جيحص لكش ب ISE نيوكت نم ققحتل

- **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 ةوطخال

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 sources .	Specify one or more destinations .
<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> CSA (ciscospt.es\CSA) ✕ </div>	<div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center;"> CiscoISE ✕ </div>
Information about sources, including selecting multiple sources. Help	Information about destinations, including selecting multiple destinations. Help


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:

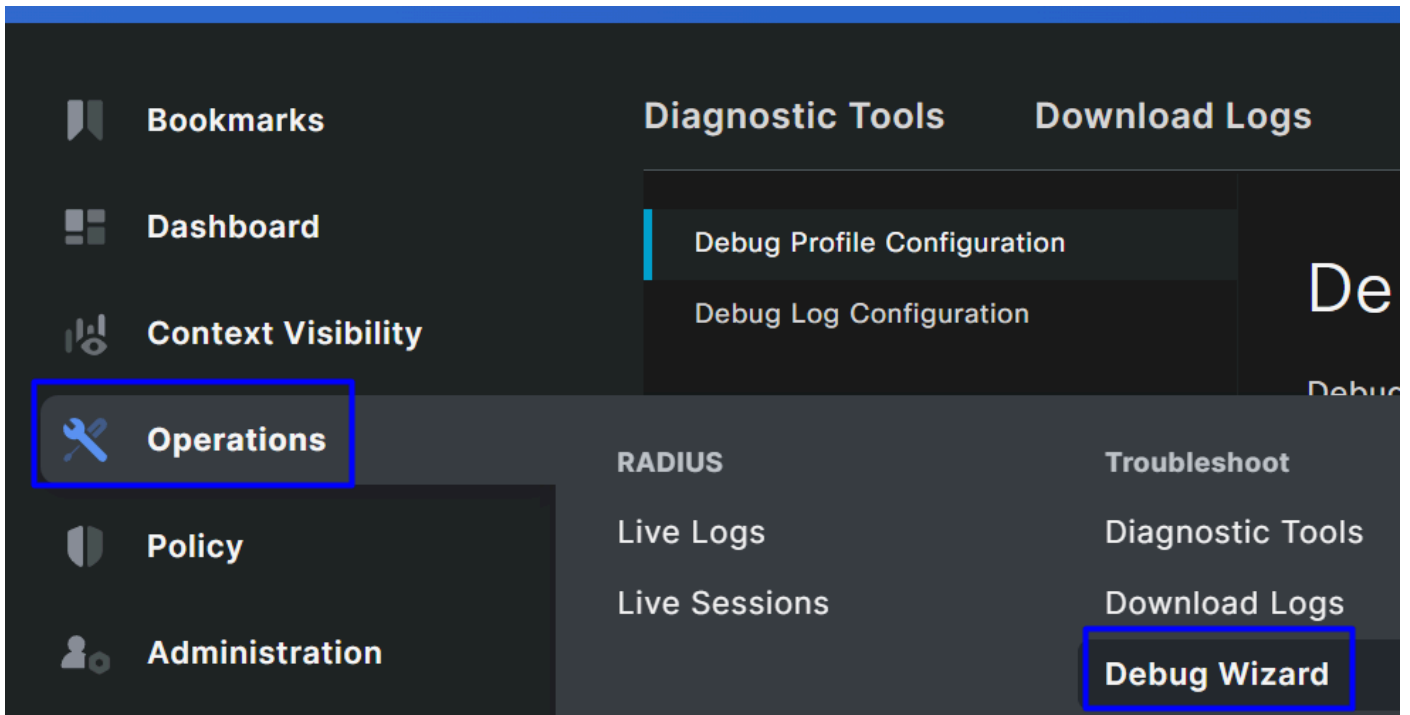
 Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

اهحالص او اءاطخ ال فاشك سا

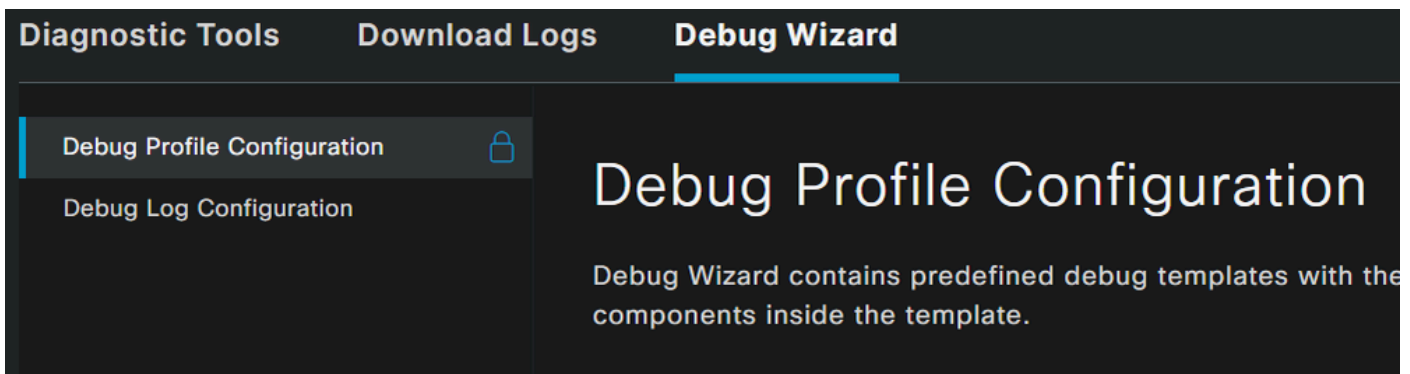
ISE ةي عضو اءاطخ اءي حصت تال جس لي زنت ةي فيك

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

- 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 ة ن ا خ ل ع ة 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

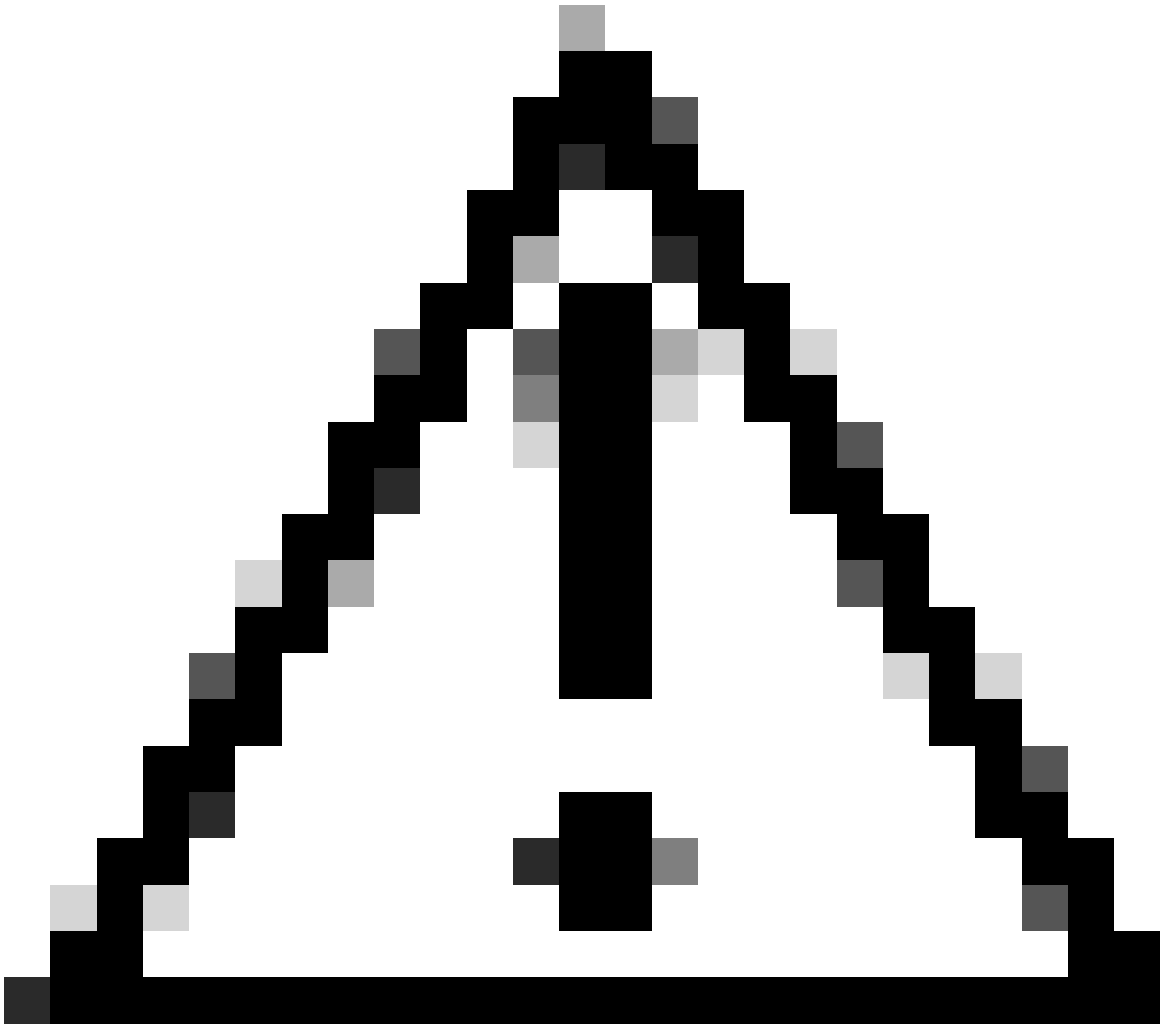
Choose on which ISE nodes you want to enable this profile.

 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 رقنللا Operations > Download Logs
- اهنم ءالءسللا ذءل ءئءئ ءللا ةءقءللا رءءل

Appliance node list

ISE

- ءةللللا ءاراءءللللا رءءل 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

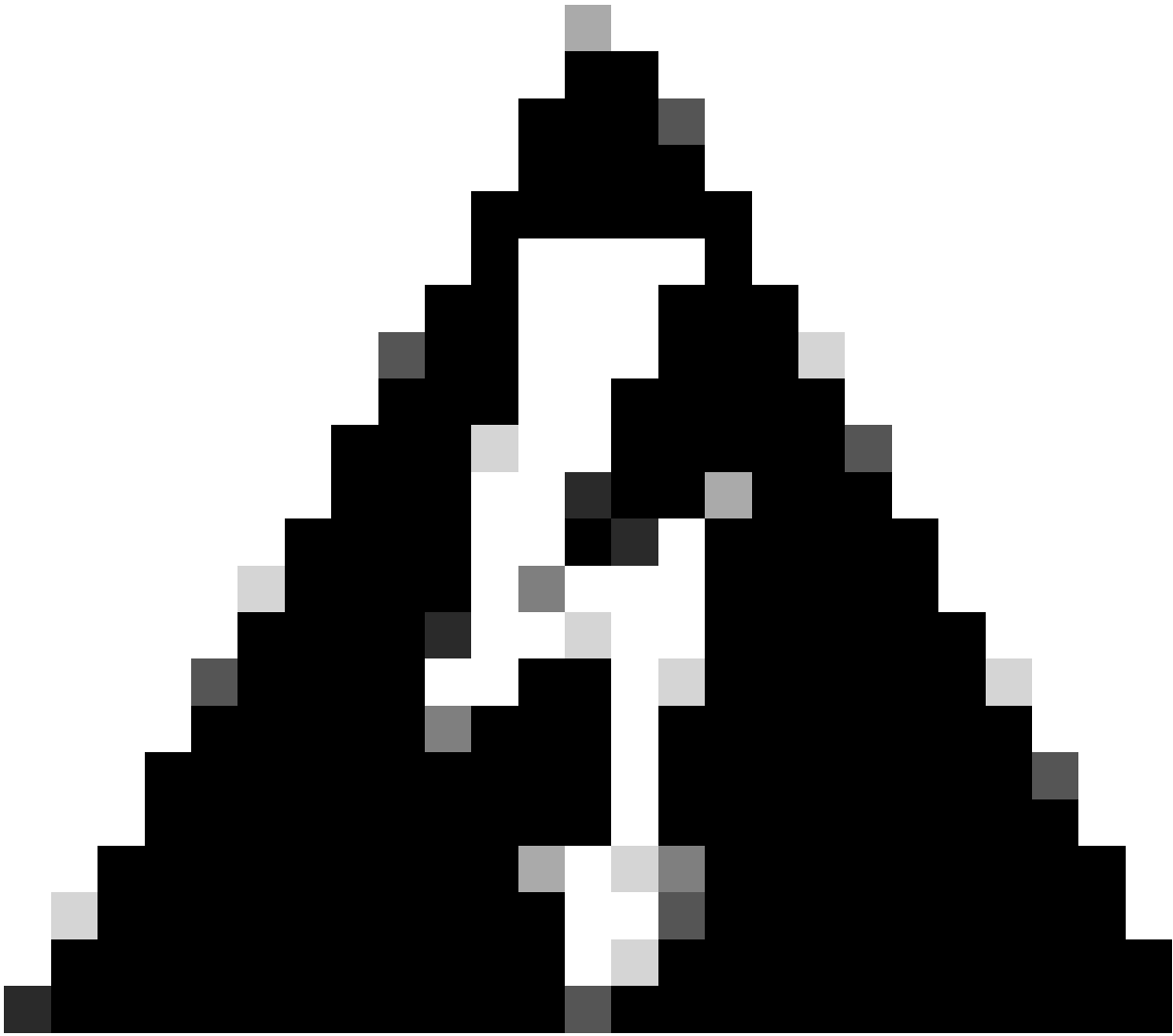
File Name: ise-support-bundle-ISE-admin-04-04-2024-14-27.tar.gpg

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

Size(KB): 52165.0

[Download](#)

[Delete](#)


















[ءاطخألا حيصت فيرعت فلم نيوكت](#)، ةوطخالا لىع هنكمت مت يذلا ءاطخألا حيصت عضو لىطعت :ريذحت

نمآلا دعب نع لوصولتالجس نم ققحتلالا ةيفيك

كبة صاخلا نمآلا لوصولت امولعم ةحول لىلا لقتنا

- Monitor > Remote Access Logs قوف رقنا

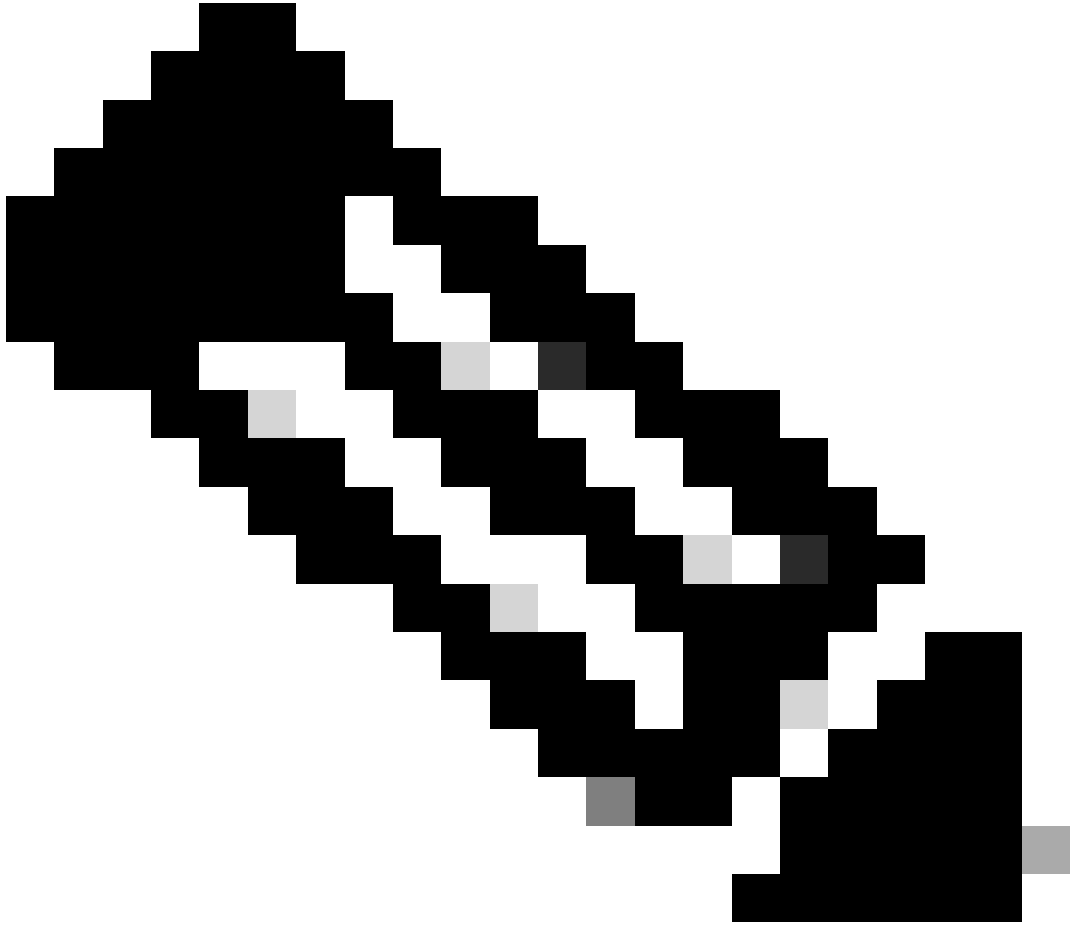
100 Events

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 ىلع DART ةمزح عاشنا

ةليلاتلا ةلاقملا نم ققحت ،كزاهج ىلع DART ةمزح عاشنال

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



عمالة حتف ىجري، اءالص او اءاخأل ا فاشككسأ مسق ى ف اءل ا راءم ال الءس ال ا عىمء ءرءم ب: ءظء الم
ءامول عم ال لىلء ف ءع بءم ال TAC.

ءلص ءا ءامول عم

- [Cisco نم ءال ىزنءل او ىنفل ا معءل](#)
- [ءءءسءم ال لىلءو نم ال لوصول ا ءىءو](#)

- [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 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 تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل