

AnyConnect Secure Access SSO SAML Duo عم م ادختساب ISE Posture

تايوتحمل

[عمدقمل](#)

[قيساس الابلطتمل](#)

[تابلطتمل](#)

[عمدختسمل تانوكمل](#)

[نيوكتل](#)

[كيشلل ليطيطختل مسرل](#)

[رورمل كرح قفدت](#)

[تانوكتل](#)

[Duo لوؤسم لخدم نيوكتل -](#)

[\(DAG\) يئانثلا لوصولا قرابع نيوكتل -](#)

[ASA نيوكتل -](#)

[ISE نيوكتل -](#)

[قحصل نم ققحتل](#)

[مدختسمل اقبحت](#)

[اهجالص او اعاطخال فاشكتسا](#)

[قلص تاذتامولعم](#)

عمدقمل

فيكتلل لباقل نامال زاخ عم Duo SAML SSO حمل نيوكتل الالام دنتمسمل اذه فصمي مبيقت ارجال Cisco ISE لغتسي يذلا Cisco AnyConnect Secure Mobility Client Access (ASA) (DAG) ةيئانثلا لوصولا قرابع م ادختساب Duo SAML SSO ذي فننت متي. عضولل لصفم يئانثلا نامال لصلتت م م دختسمل لةلوالا ةقداصل ل Active Directory ب لصلتت يتلا ريفوتل ضيوفت م داخك Cisco ISE م ادختسا متي. لم اوعل اددعتم ةقداصل ملل (ةباحسل) عضول مبيقت م ادختساب ةياهنلا ةطقن نم ققحتل

Cisco HTTPS س دنهم، انيسكاس تيكلوب و ليجدوم شينيد اهي ف مهاس

قيساس الابلطتمل

تابلطتمل

Cisco Adaptive Security Device Manager (ASDM) ل حامسلل هنيوكتل متو لم الكلا ليغشتلا ديقي ASA نأ دنتمسمل اذه ضررت في نيوكتلل تاريغت ارجاب (CLI) رماوالا رطس ةهجاو و (ASDM) Security Device Manager

ةيلال اعياوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت

- يئانثال نامأل ازيمو وئيئانثال لوصول اوب ايساسأ
- ASA لعل دعب نع لوصول لل VPN نيوكتب ايساسأ افرعم
- Posture و ISE تامدخب ايساسأ افرعم

ةمدختسملا تانوكملا

ةيلائل اجماربال تارادصإ لىل دنننسملا اذه في ةدراول تامولعمل دننست:

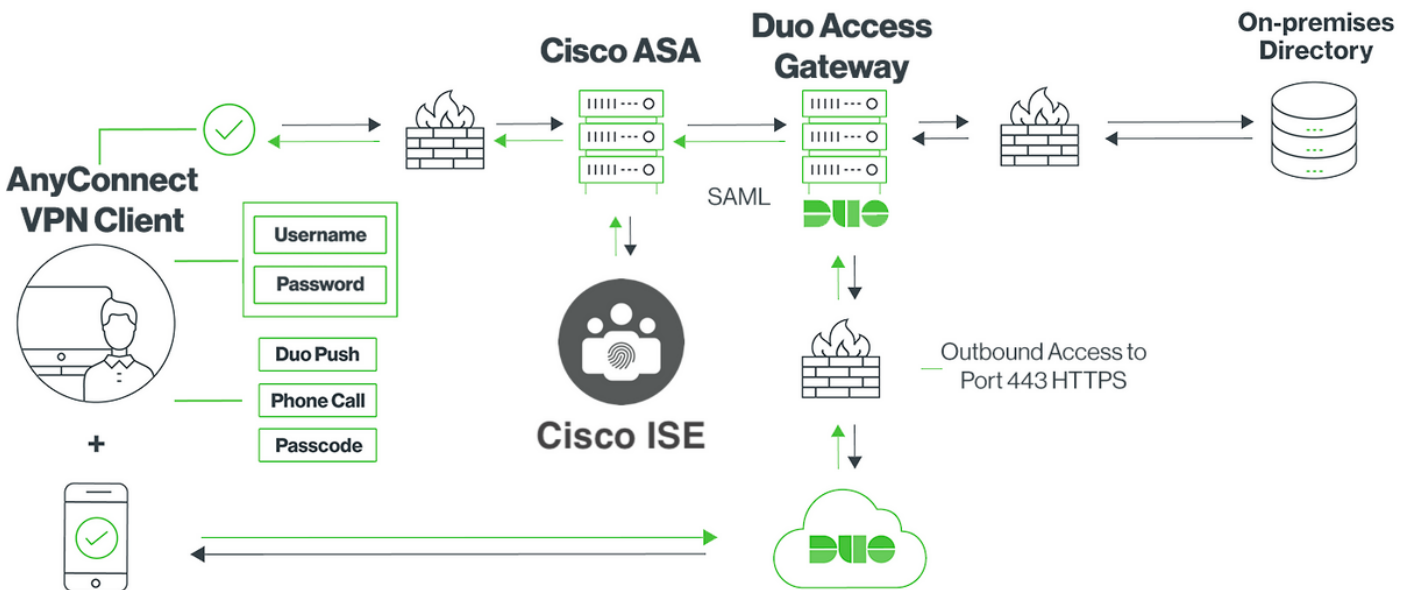
- Cisco، نمد فيكثلل لباقول نامأل زاا جمانرب 9.12(3)12 رادصإل
- Duo Access Gateway
- يئانثال نامأل
- Cisco Identity Services Engine، رادصإل او 2.6 رادصإل
- AnyConnect نمد 4.8.03052 رادصإل عم Microsoft Windows 10

✍ ASA، ذي فنننلا اذه في ممدختسملا، AnyConnect نمدضملا ضرعتسملا بلطتي: ةظالم AnyConnect و رادصإل لك نمد دحأ رادصإل وأ 9.9(2)1 و 9.8(2)28 و 9.7(1)24 رادصإل لعل دحأ رادصإل وأ 4.6 رادصإل.


ةصاخ ايلمعم ةئيبي في ةدوجوملا ةزهجال نمدنننسملا اذه في ةدراول تامولعمل عاشنإ مت نناك اذإ. (يضا رتفا) حوسمم نيوكتب دنننسملا اذه في ممدختسملا ةزهجال عيمج تادب رما يال لمحمل ريثائل كمهف نمدكأتف، ةرشابم كتكبش.

نيوكتلا

ةكبشلل يطيختلا مسرلا



رورملا ةكرح قفدت

1. Cisco ASA لىل SSL VPN لاصتا ةئيهت ب AnyConnect ليمع موقوي
 2. لوصول ةرابع مادختساب ةيساسأل ةقداصلل هنيوكت مت يذال، Cisco ASA موقوي DAG لىل AnyConnect Client يف نمضمل ضرعتسملل هيحوت ةداعإب، (DAG) ةئانثلا SAML ةقداصلل
 3. ةئانثلا لوصول ةرابع لىل AnyConnect ليمع هيحوت ةداعإ تمت
 4. SAML ةقداصلم بلط عاشنإ متي، دامتعالا تانايب لىل AnyConnect ليمع لوخد درجمب Cisco نم Duo لىل ASA لوصول ةرابع نم ردصيو
 5. عقوملا يف Active Directory ةمدخ عم لمالكثلا ةدايز لىل ةئانثلا لوصول ةرابع لمعت AnyConnect ليمعل ةيساسأل ةقداصلل ءارجال
 6. لىل بلط لاسراب ةئانثلا لوصول ةرابع موقت، ةيساسأل ةقداصلل حاجن درجمب لماول ةئانث ةقداصلل ءدبل 443 مقرر TCP ذفنم ربع ةئانثلا نامأل
 7. لمكيو "ةئانثلا ةيلعافتلا ةبلاطملا" مادختساب AnyConnect ليمع ميذقت مت (وأ طغضلا) هيذلة لصفملا ةقيرطال مادختساب لماعلا ةئانثلا ةقداصلل مدختسملل (رورملا زمر)
 8. ةئانثلا لوصول ةرابع لىل تامولعملل ديءيو ةقداصلم ةباجتسا Duo Security ملتسي
 9. ةباجتسا عاشنإب ةئانثلا لوصول ةرابع موقت، ةقداصلل ةباجتسا لىل اذانتسا AnyConnect ليمع عم بواجتتو SAML ديكاأت لىل ءوتحت SAML ةقداصلم
 10. Cisco ASA مادختساب SSL VPN لاصتال حاجن ب AnyConnect client ةقداصلم
 11. Cisco ISE لىل ضيوفت بلط Cisco ASA لسري، ةقداصلل حاجن درجمب
-
-  ةئانثلا لوصول ةرابع نأل ارظن لىل ءوختلل طقف Cisco ISE نيوكت متي: ةظحالمة مزاللا ةقداصلل رفوت
-
12. ءفورعم ريغ ليمعلل ءضو ءلاح نأ امبو ضيوفتلا بلط ءعالعمب Cisco ISE موقوي، Cisco ASA ربع AnyConnect client لىل دودحم لوصول عم Posture Redirect ءجريف
 13. هلبيزنتب هتبلاطم متت، ةيظمن قفاوت ءدحو AnyConnect ليمع لىل نكي مل اذال ءضولل مييقت ءعباتمل
 14. عم TLS لاصتال سسؤي هنإف، ةيظمن قفاوت ءدحو لىل ءوتحتي AnyConnect client ناك اذال ءاضوالل قفدت أدببو Cisco ASA
 15. متي ءضولل تاصوحن ءارجال متي، ISE لىل ءهنيوكت مت يذال ءضولل طورش لىل ءانب Cisco ISE لىل AnyConnect ليمع نم لىل صافتلا لاسرا

16. ريغت بلط لاسرا متيسف، قفاوتم لى فورعم ريغ نم ليمعلا عضو لاج تريغت اذا. اشن او ليمعلا لى لمالك لوصول حنم ل Cisco ASA لى Cisco ISE نم (CoA) ضيوفت ل لمالك اب VPN ةكبش

تانيوكتل

Duo لوؤسم لخدم نيوكت -

Duo لوؤسم لخدم لى ع ASA قيبطت نيوكتب مق، مسقلا اذه يف

1. شحبل او، "قيبطت ةيامح > تاقيبطت" لى لقننتل او "Duo Admin Portal" لى لوخدل ليجست. 1. "ةيامح" قوف رونا. "ايتاذ ةفاضتسم ل، Duo لوصول ةباب عم 2FA" ةيامح عونب "ASA" نع Cisco نم ASA نيوكتل نيمل لى صقأ لى ع

The screenshot shows the Duo Admin Portal interface. The search bar contains 'ASA'. The table lists applications:

Application	2FA	Single Sign-On (if available)	Documentation	Action
Asana	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
Cisco ASA	2FA	Duo Access Gateway (self-hosted)	Documentation	Protect
Cisco ASA	2FA	Single Sign-On (hosted by Duo)	Documentation	Configure

2. ASA، يمحمل قيبطت لل "مخدلا دوزم تحت ةيلالت تامس ل نيوكتب مق.

يساسأل URL	firebird.cisco.com
قافنألة وعومجم	tg_saml
ديربللة مس	sAMAccountName,mail

ةحفصل لفسأ يف "ظفح" لى ع رونا

Device Insight
Policies
Applications
Protect an Application
Single Sign-On
Users
Groups
Endpoints
2FA Devices
Administrators
Reports
Settings
Billing

Need Help?
Chat with Tech Support
Email Support
Call us at 1-855-386-2884

Account ID
2010-1403-48

Deployment ID
DU057

Helpful Links
Documentation

Cisco ASA - Duo Access Gateway

Authentication Log | Remove Application

Configure Cisco ASA

Reset Secret Key

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)
Next step: [Download your configuration file](#)

Service Provider

Base URL

firebird.cisco.com

Enter the Cisco ASA Base URL.

Tunnel Group

TG_SAML

Enter the Tunnel Group you are protecting with SSO.

Custom attributes

Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute

sAMAccountName.mail

The attribute containing the email address of the user.

Save Configuration

هه نيين عت نكمي نكلو ةيضا رتفا تام لعم نيوكتل ي قبا م دخت ست ، دن تس م الا ذه في
م س ا ر ي غ ت ل ث م ، ي ل ا ح ل ت ق و ل ا ي ف د ي د ج ل SAML ق ي ب ط ل ة ي ف ا ض ا ل ا ا د ا د ع ا ل ا ط ب ض ن ك م ي
ة و ع م ج ه ن ن ي ع ت و ا ، ة ي ا ذ ل ا ة م د خ ل ن ي ك م ت و ا ، ة ي ض ا ر ت ف ا ل ا ة م ي ق ل ا ن م ق ي ب ط ل ا

3. Cisco ASA ق ي ب ط ت ا د ا د ع ا ل ا ل و ص ح ل ل " ن ي و ك ت ل ا ف ل م ل ي ز ن ت " ط ا ب ت ر ا ل ا ق و ف ر ق ن ا .
ة ق ح ا ل ل ا و ط خ ل ا ي ف ة ي ا ن ث ل ل و ص و ل ا ة ر ا ب ع ا ل ا ف ل م ل ا ا ذ ه ل ي م ح ت م ت ي . (JSON ف ل م ك)

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Settings

Billing

Need Help?

Chat with Tech Support

Email Support

Call us at 1-855-386-2884

Account ID

2010-1403-48

Deployment ID

DU057

Helpful Links

Documentation

Cisco ASA - Duo Access Gateway

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

[Reset Secret Key](#)

Configure Cisco ASA

To set up this application, install the Duo Access Gateway and then configure your service provider. [View Cisco ASA SAML SSO instructions](#)

Next step: [Download your configuration file](#)

Service Provider

Base URL
Enter the Cisco ASA Base URL.

Tunnel Group
Enter the Tunnel Group you are protecting with SSO.

Custom attributes Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.

Mail attribute
The attribute containing the email address of the user.

[Save Configuration](#)

وه امك اشي دح هؤاشن| مت يذلا ASA قيبطت ودبي ، "تاقيبطت لل > تامولعمل اة حول تحت 4. هاندا ةروصل ايف حضورم

admin-77d04ebc.duosecurity.com/applications

Cisco Study | Cisco Tools | Mix | SourceFire | VPN | AAA | ASA | IFT 6.7

DUO

Dashboard

Device Insight

Policies

Applications

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduoblir

[Dashboard](#) > [Applications](#)

Applications

[SSO Setup Guide](#) | [Protect an Application](#)

[Export](#) |

Name	Type	Application Policy	Group Policies
Cisco ASA - Duo Access Gateway	Cisco ASA - Duo Access Gateway		

1 total

ةروصل ايف حضورم وه امك "مدختسم ةفاض| > نيمدختسم يل لقتنا 5.

دعب نع لوصولل AnyConnect ةقداصل هم ادختسال "duouser" يمسم مدختسم عاشن| يئاهنلل مدختسم ل زاهج يلع Duo Mobile طيشنتو

DUO

Dashboard

Device Insight

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

Search for users, groups, applications, or devices

Dashboard > Users > Add User

Add User

Adding Users

Most applications allow users to enroll themselves after they complete primary authentication.

[Learn more about adding users](#)

Username

Should match the primary authentication username.

Add User

"فتاه ةفاضل" راځل ددح، ةروصلل ي ف حضوم وه امك فتاهل مقرر ةفاضل.

DUO

Dashboard

Device Insight

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

Endpoints

2FA Devices

Search for users, groups, applications, or devices

Dashboard > Users > duouser > Add Phone

Add Phone

[Learn more about Activating Duo Mobile](#)

Type Phone Tablet

Phone number [Show extension field](#)

Optional. Example: "+91 91234 56789"

Add Phone

ني عملل مدخت سملل "Duo Mobile" طيشنت

Device Info

Learn more about Activating Duo Mobile [↗](#).



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone

يئاهنللا مدختسملا زاغ ىلع "Duo Mobile" تيبتت نم دكأت :ةظحالم
[IOS ةزهجال Duo قيبتتل يوديلا تيبتتلا](#)
[Android ةزهجال Duo قيبتتل يوديلا تيبتتلا](#)

ةروصللا يف حضوم وه امك "Duo Mobile" طيشنت زمر عاشنلا دح

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscodeubl

Dashboard > Phone: [redacted] > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone: [redacted]

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

ةروصللا يف حضوم وه امك "SMS" ربع تاميلعت لاسرا" دح

- Dashboard
- Device Insight
- Policies
- Applications
- Users
- Groups
- Endpoints
- 2FA Devices**
- Phones
- Hardware Tokens
- WebAuthn & U2F
- Administrators
- Reports
- Settings
- Billing
- Need Help?
- [Chat with Tech Support](#)
- [Email Support](#)
- Call us at 1-855-386-2884

[Dashboard](#) > [Phone: +91](#) > [Activate Duo Mobile](#)

Activate Duo Mobile

A new Duo Mobile activation code has been generated, and any old credentials have been invalidated. activation instructions to the user by SMS.

Phone [REDACTED]

Installation instructions

Send installation instructions via SMS

Welcome to Duo! Please install Duo Mobile from your app store.

Activation instructions

Send activation instructions via SMS

*To activate the app, tap and open this link with Duo Mobile:
<https://m-77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT>*

[Send Instructions by SMS](#) or [skip this step](#)

م س ق ي ف م د خ ت س م ل ا ب ا س ح ب Duo ق ي ب ط ت ط ب ر م ت ي و ، SMS ي ف د و ج و م ل ا ط ا ب ت ر ا ل ا ق و ف ر ق ن ا ة ر و ص ل ا ي ف ح ض و م و ه ا م ك ، ز ا ه ج ل ا ت ا م و ل ع م :

Dashboard > Phones > Phone: +91...
+91... Send SMS Passcodes... | []

Shared phone
This phone is attached to multiple users.

duouser +91... testing 123 +91... Attach a user
Authentication devices can share multiple users

Device Info
Learn more about Activating Duo Mobile []

Using Duo Mobile Reactivate Duo Mobile Model: Unknown OS: Generic Smartphone

- (DAG) يئانثلا لوصولا ةرابع نيوكت

1. كتكبش ي ف مداخ ىلع (DAG) ةيئانثلا لوصولا ةرابع رشن

✎ رشنلل ةيئانثلا لوصولا عبتا: ةظالم

Linux ليغشتلا ماظنل ةيئانثلا لوصولا ةرابع
<https://duo.com/docs/dag-linux>

Duo Access Gateway J Windows
<https://duo.com/docs/dag-windows>

2. "ةقداصلما ردصم ىلإ لقتنا، يئانثلا لوصولا ةرابع ل ةيسيئرلا ةحفصل ي ف"

3. ظفح" قوف رقناو Active Directory ل ةيئانثلا تامسلا لخدأ، "رداصلما نيوكت تحت
تاداعلا"

Configure Sources

Configure authentication source settings below. Changes made to non-active authentication sources will take effect when made active.

Source type	<input type="text" value="Active Directory"/> Specify the authentication source to configure.
Status:	<input checked="" type="checkbox"/> LDAP Bind Succeeded <input checked="" type="checkbox"/> ldap://10.197.243.110
Server	<input type="text" value="10.197"/> <input type="text" value="389"/> Hostname and port of your Active Directory. The port is typically 389 for cleartext LDAP and STARTTLS, and 636 for LDAPS. Hostnames can be comma separated for failover functionality. For example: ad1.server.com,ad2.server.com,10.1.10.150
Transport type	<input checked="" type="radio"/> CLEAR <input type="radio"/> LDAPS <input type="radio"/> STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.
Attributes	<input type="text" value="sAMAccountName,mail"/> Specify attributes to retrieve from the AD server. For example: sAMAccountName,mail.
Search base	<input type="text" value="CN=Users,DC=dmoudgil,DC=local"/> The DNs which will be used as a base for the search. Enter one per line. They will be searched in the order given.
Search attributes	<input type="text" value="sAMAccountName"/> Specify attributes the username should match against. For example: sAMAccountName,mail.
Search username	<input type="text" value="iseadmin"/> The username of an account that has permission to read from your Active Directory. We recommend creating a service account that has read-only access.
Search password	<input type="password" value="•••••"/> The password corresponding to the search username specified above.
<input type="button" value="Save Settings"/>	

4. نېيټ " قوف روناو "Active Directory" ك ردصم لاون دوح، "طشن ردصم نېيټ تحت
"طشن ردصم"

Set Active Source

Specify the source that end-users will use for primary authentication.

Source type

Active Directory

Set Active Source

5. فلم لي محتب مق ، "قوي بطت ةفاضل" ةيعرفل ةمئاقل نمض ، "تاقوي بطت لى لقتنا .json لي زنت مت . "نيوكتل فلم" مسق لخاد Duo لوؤسم مكحت ةدحو نم هلي زنت مت يذل .json فلم Duo لوؤسم لخدم نيوكت نمض 3 ةوطخل ي ف قباطم ال .json فلم

Applications

Add Application

Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here.



Configuration file

Browse... Cisco ASA - Duo Access Gateway.json

Upload

6. "تاقوي بطت" ةيعرفل ةمئاقل نمض رهظي ، حاجنب قوي بطت لى ةفاضل درجم ب .

Applications

Name	Type	Logo	
Cisco ASA - Duo Access Gateway	Cisco ASA		 Delete

7. ةداهش و XML فيرعت تانايب لي زنت مق ، "فيرعتل تانايب" ةيعرفل ةمئاقل تحت اقحال ASA لىل عاهنيوكت مت يتل ةيلال URL نيوانع ظحال و IdP

1. URL ب صاخل SSO
2. جورخل ليجستل URL ناونع
3. نايكل فرعم
4. أطخلل URL ناونع

Information for configuring applications with Duo Access Gateway. [Download XML metadata](#)

Certificate /C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. [Download certificate](#)

Expiration 2030-04-30 18:57:14

SHA-1 Fingerprint

SHA-256 Fingerprint

SSO URL <https://explorer.cisco.com/dag/saml2/idp/SSOService.php>

Logout URL <https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer>

Entity ID <https://explorer.cisco.com/dag/saml2/idp/metadata.php>

Error URL <https://explorer.cisco.com/dag/module.php/duosecurity/du>

ASA نيوكت-

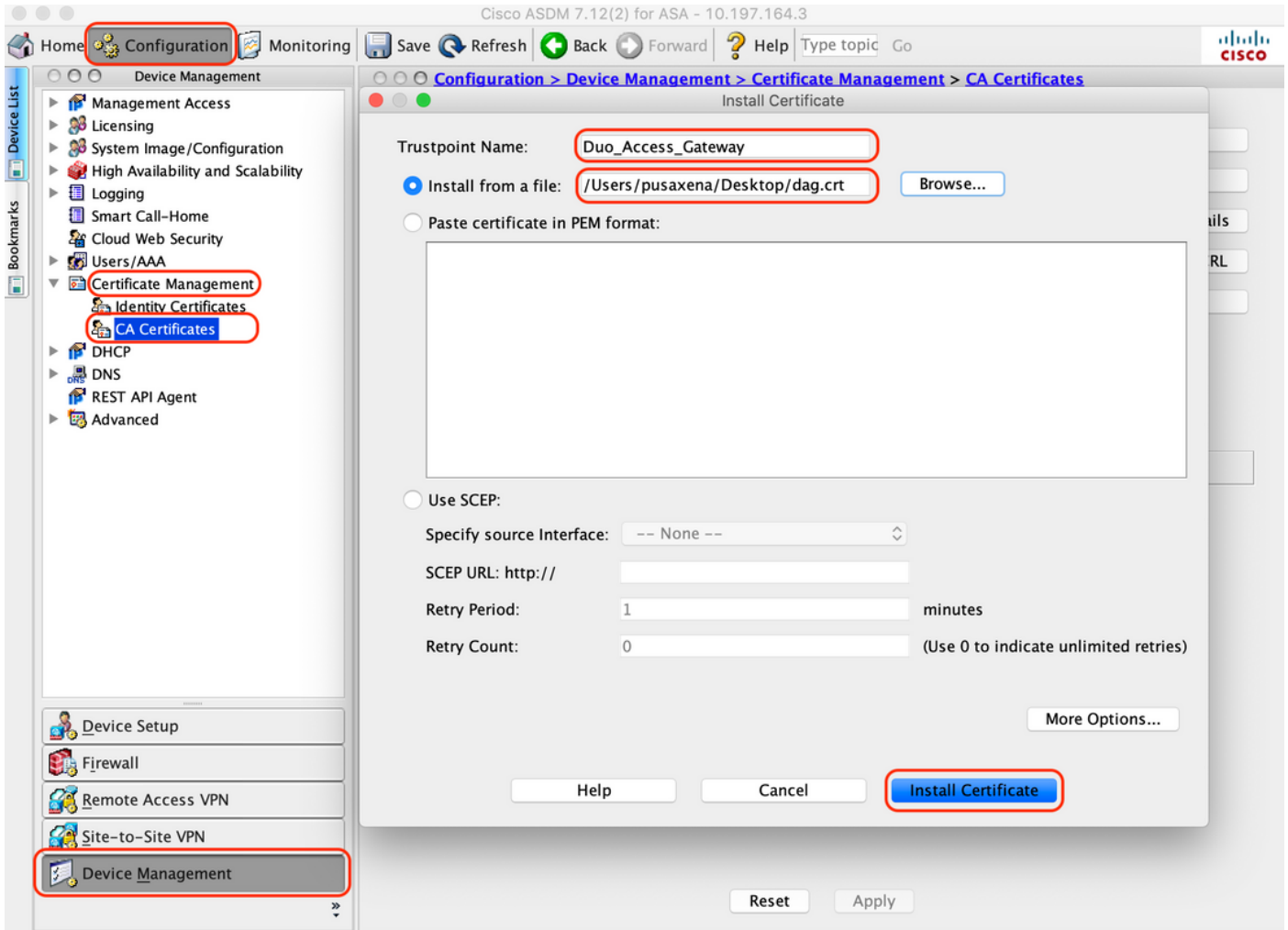
يستخدم الـ AnyConnect نيوكت و SAML IDP كإضافة لـ ASA نيوكت لتتم عملية تسجيل الـ AnyConnect نيوكت في الـ ASA نيوكت. يتم إعداد الـ AnyConnect نيوكت في الـ ASA نيوكت من خلال الـ ASDM و CLI و الـ ASA نيوكت.

1. إعداد الـ AnyConnect نيوكت في الـ ASA نيوكت

أ. قوف رقمنا، "قصد الـ AnyConnect نيوكت في الـ ASA نيوكت" > إعداد الـ AnyConnect نيوكت في الـ ASA نيوكت > إعداد الـ AnyConnect نيوكت في الـ ASA نيوكت

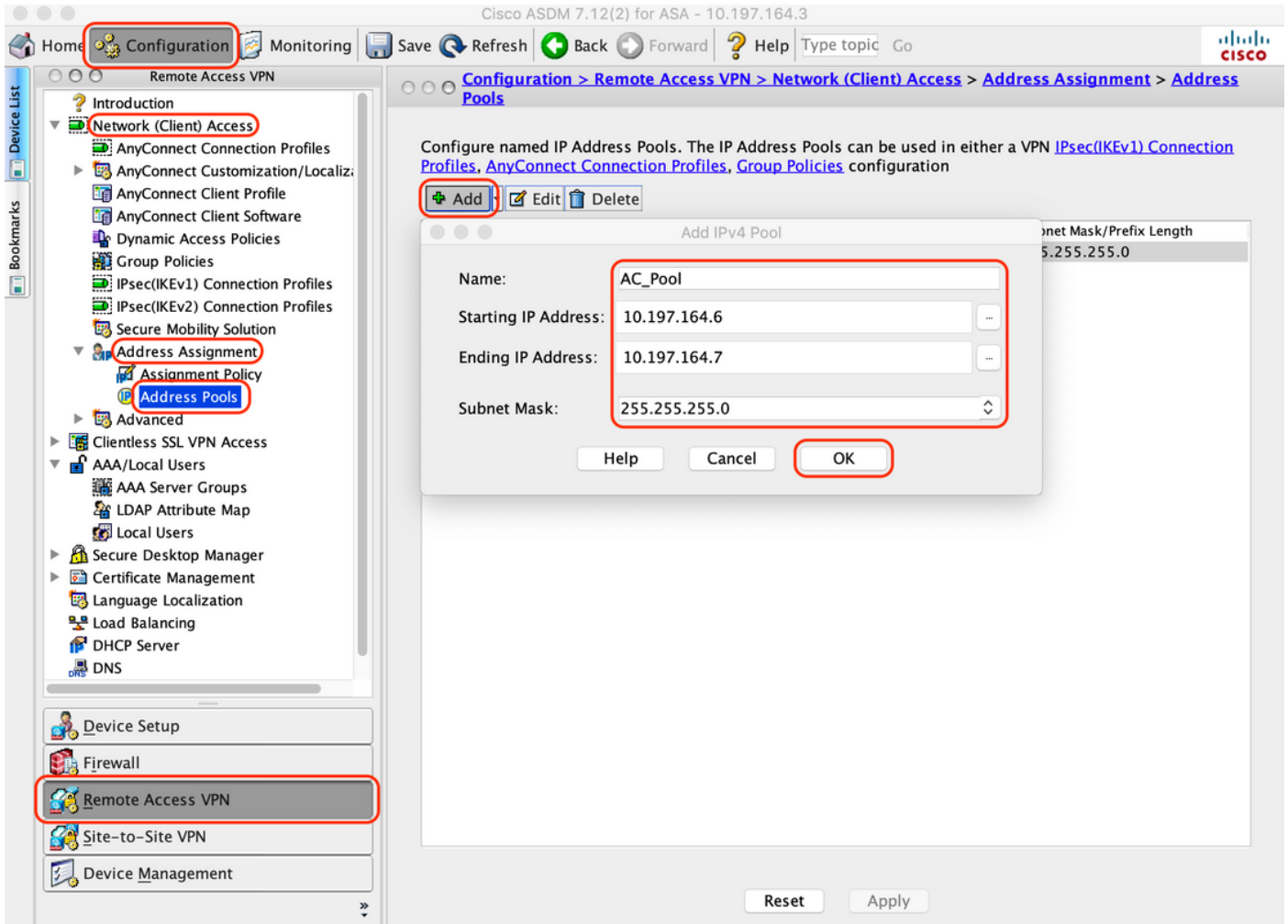
ب. TrustPoint: duo_access_gateway مسمي نيوكت في الـ ASA نيوكت، "إعداد الـ AnyConnect نيوكت في الـ ASA نيوكت" في الـ ASA نيوكت

ج. الـ AnyConnect نيوكت في الـ ASA نيوكت، "إعداد الـ AnyConnect نيوكت في الـ ASA نيوكت" في الـ ASA نيوكت



2. AnyConnect يمدخست سمل ي ل حمل ال IP عمجت عاشن ا

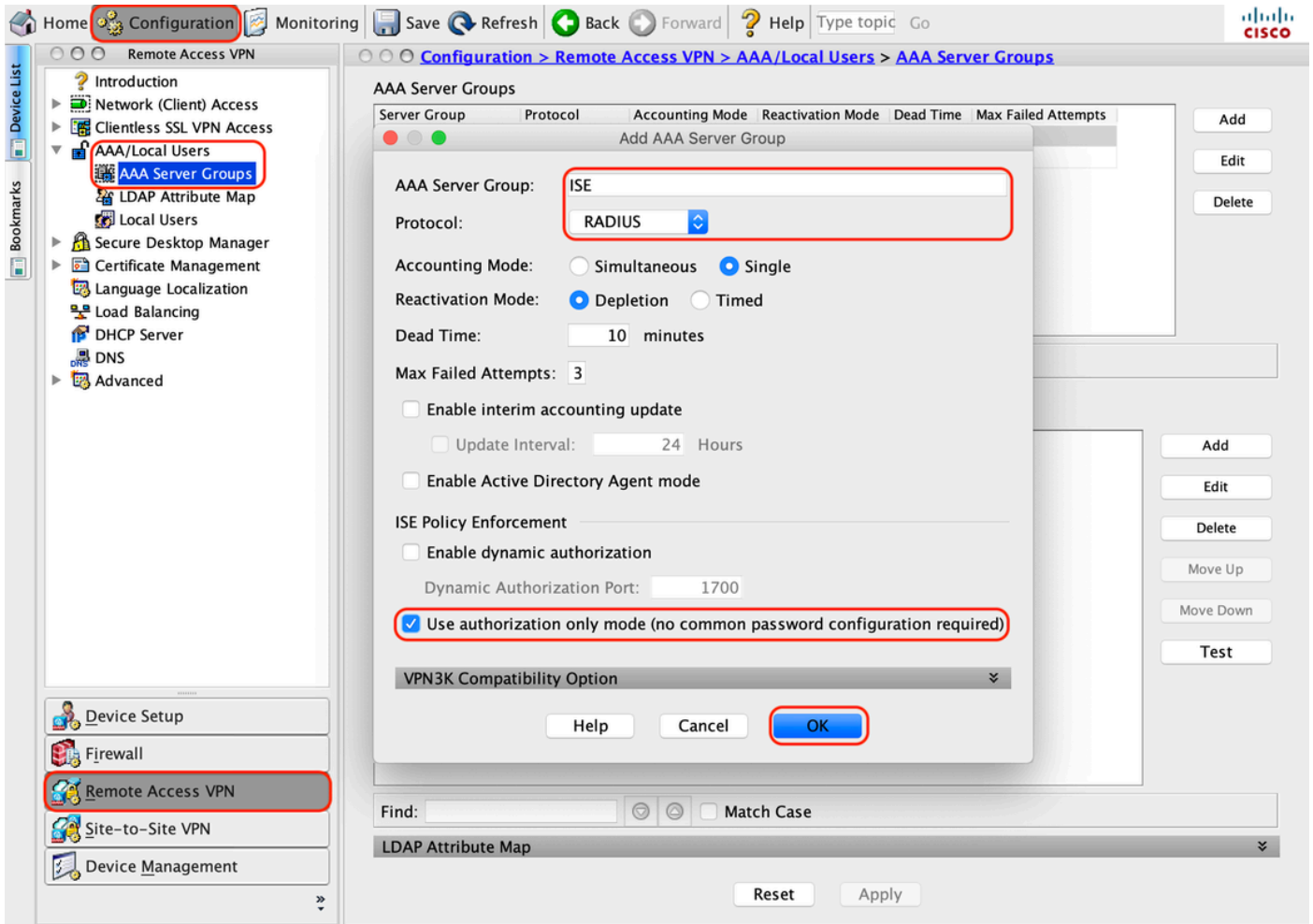
Remote Access VPN (النيوكت ال) > Network (اليمع ال) Access > Address Assignment (النيوانع ال النيي عت) ، "قوف رقونا" ، "قوف اضافا"



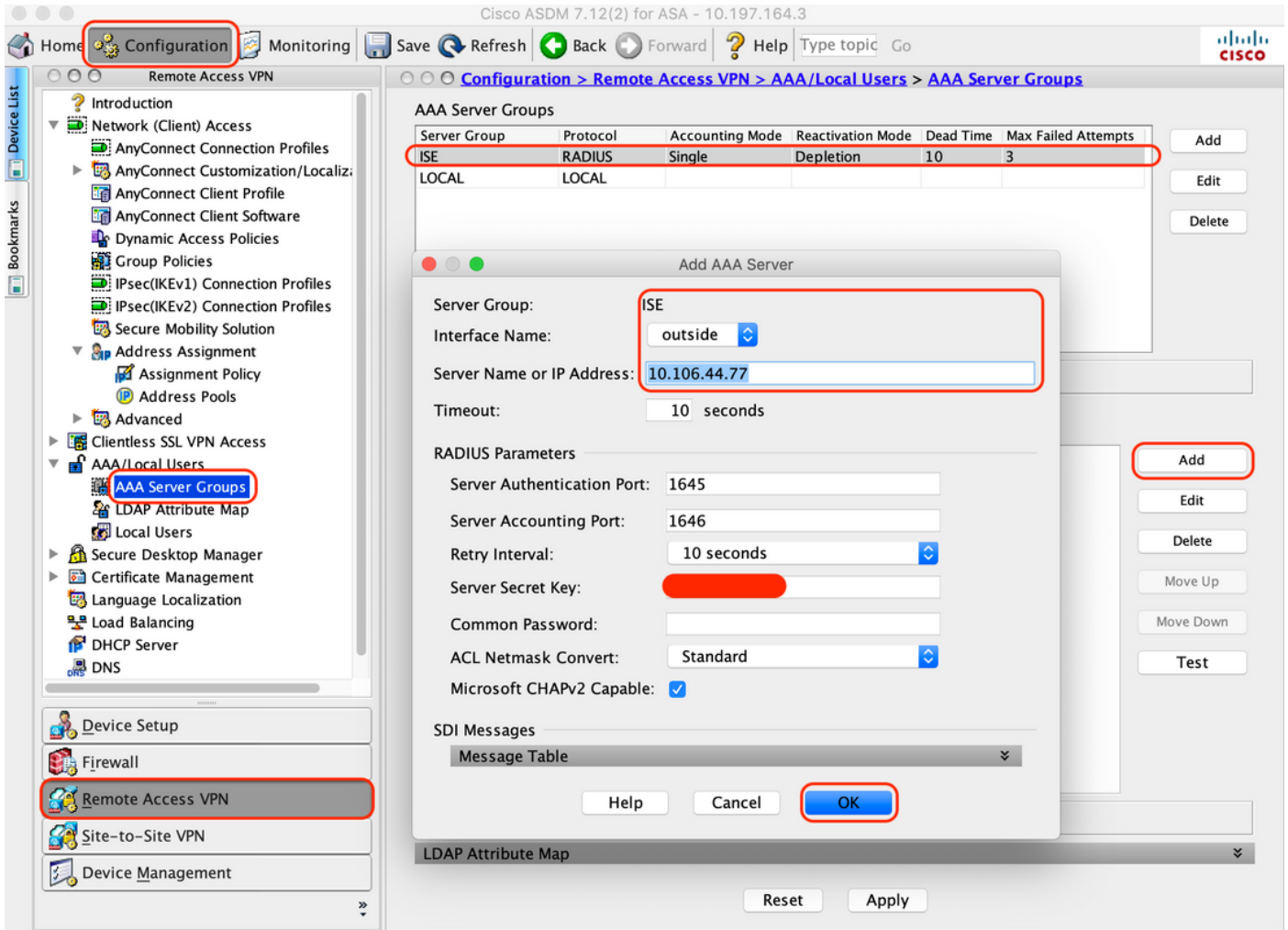
3. مداخل AAA وعومجم نيوكت

يذلل ددحمل ال AAA مداخل لوصافات مدقو ال AAA مداخل وعومجم نيوكتب مق، مسقلا اذف ف. ا
ضفوفتلا ذففنتب موقف

تاعومجم > نولحمل ال نومدختسمل ال AAA > VPN ال دعب نع لوصولا > نيوكت ال لقتنا ب.
"افاضا" قوف رقنا، "ال AAA مداخل"



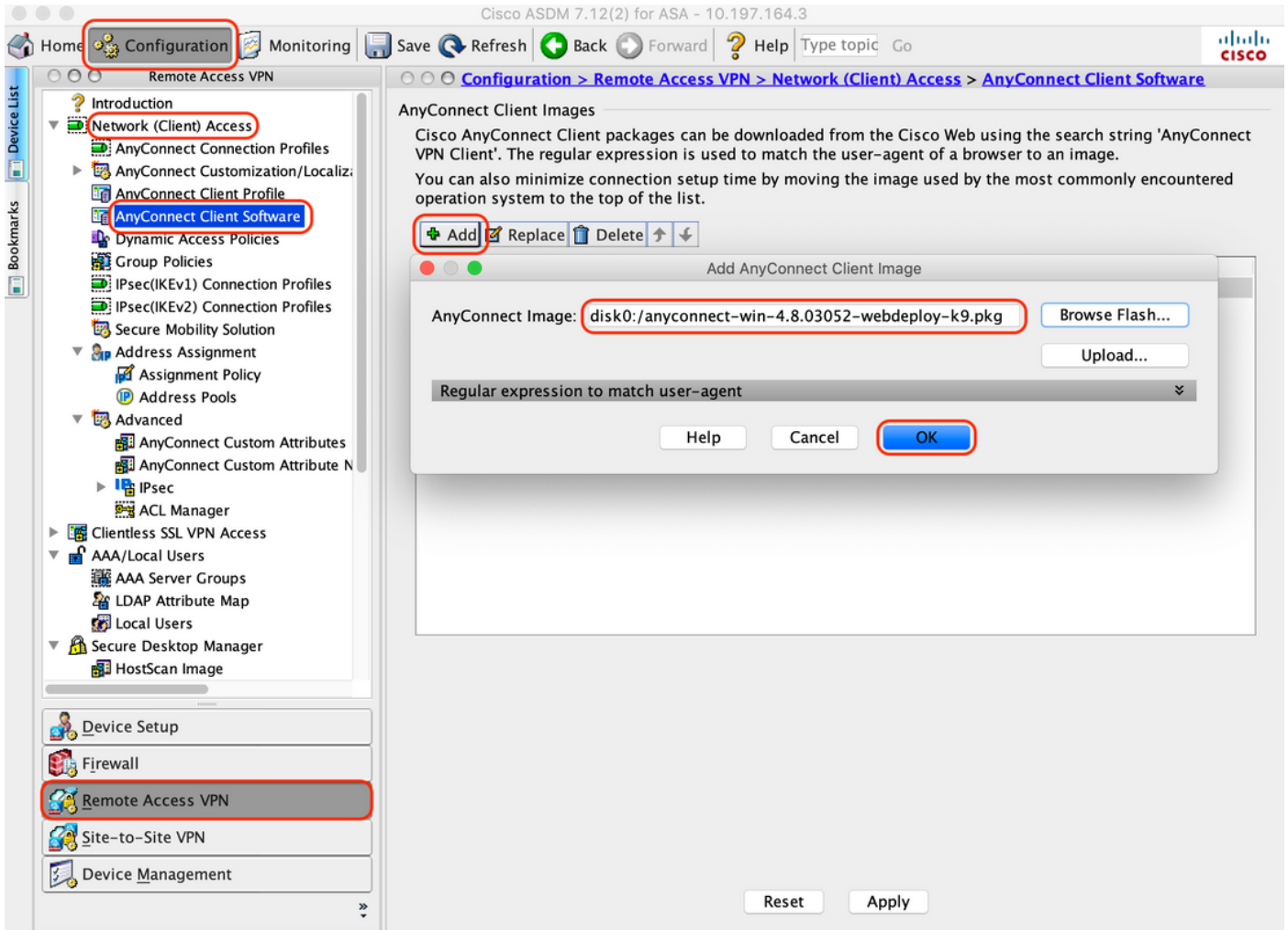
مقو "ةفاضإ" قوف رقنا، "ةدحمال ةومحمل ي ف مداوخل" مسقلا نمض، ةحفصلا سفن ي ف ج.
AAA مداخل IP ناوع ليصافت ريفوتب



4. AnyConnect Client چمانرب نييعت

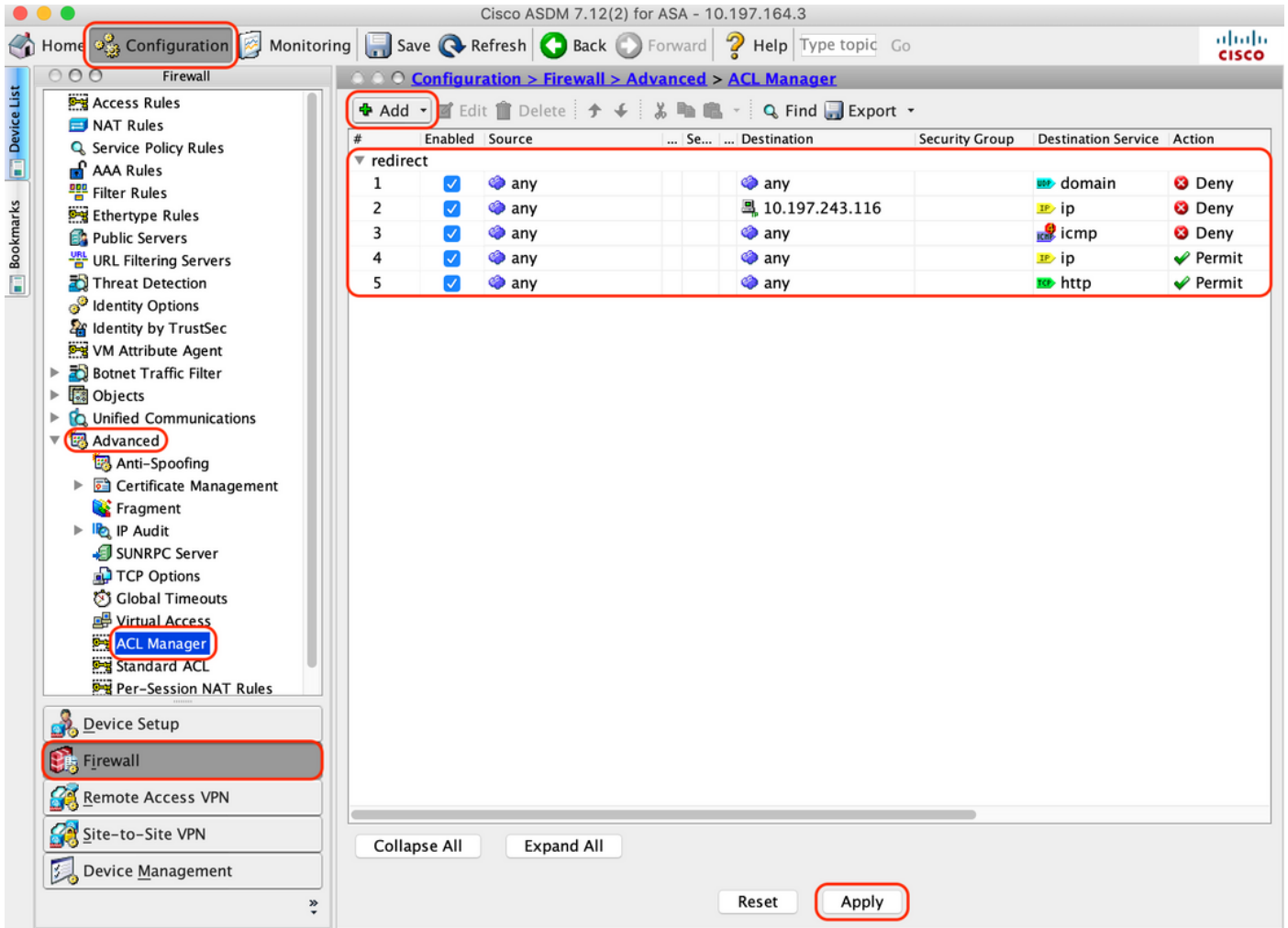
أ. همادختسإ متي Windows ل AnyConnect client 4.8.03052 چمانرب ل بيولا رشن ةروص نييعت أ. ل WebVPN

ب. چمانرب > (للمعالم) ةكبشلال لوصولو > VPN لوصولو > نيوكت لوصولو لقتنا ب. "ةفاضإ" قوف رقنا، "AnyConnect" للمع



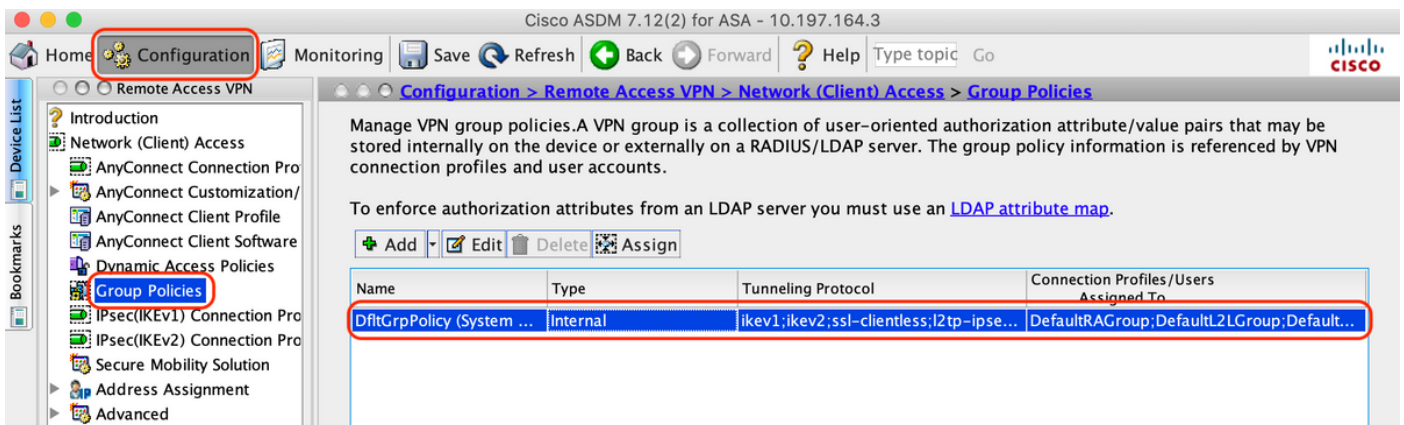
5. عجت نك اه عفد متي يتل اههيجوت داعم ال (ACL) لوصول ي ف مكحتل ا عمئاق ني وكت ب مق م ISE

أ. رونا (ACL) لوصول ي ف مكحتل ا عمئاق ا راد ا > مدقتم > ا عمئاق رادج > ني وكت ي ل لقتنا أ. تال ا خ دال رهظت. اههيجوت داعم ال (ACL) لوصول ي ف مكحتل ا عمئاق ا فاضال ا فاضال قوف، ان ا خضوم وه امك، ان ني وكت درجمب:



6. لي لاجل الة وعموم جمل جهن نم ققحت لآ

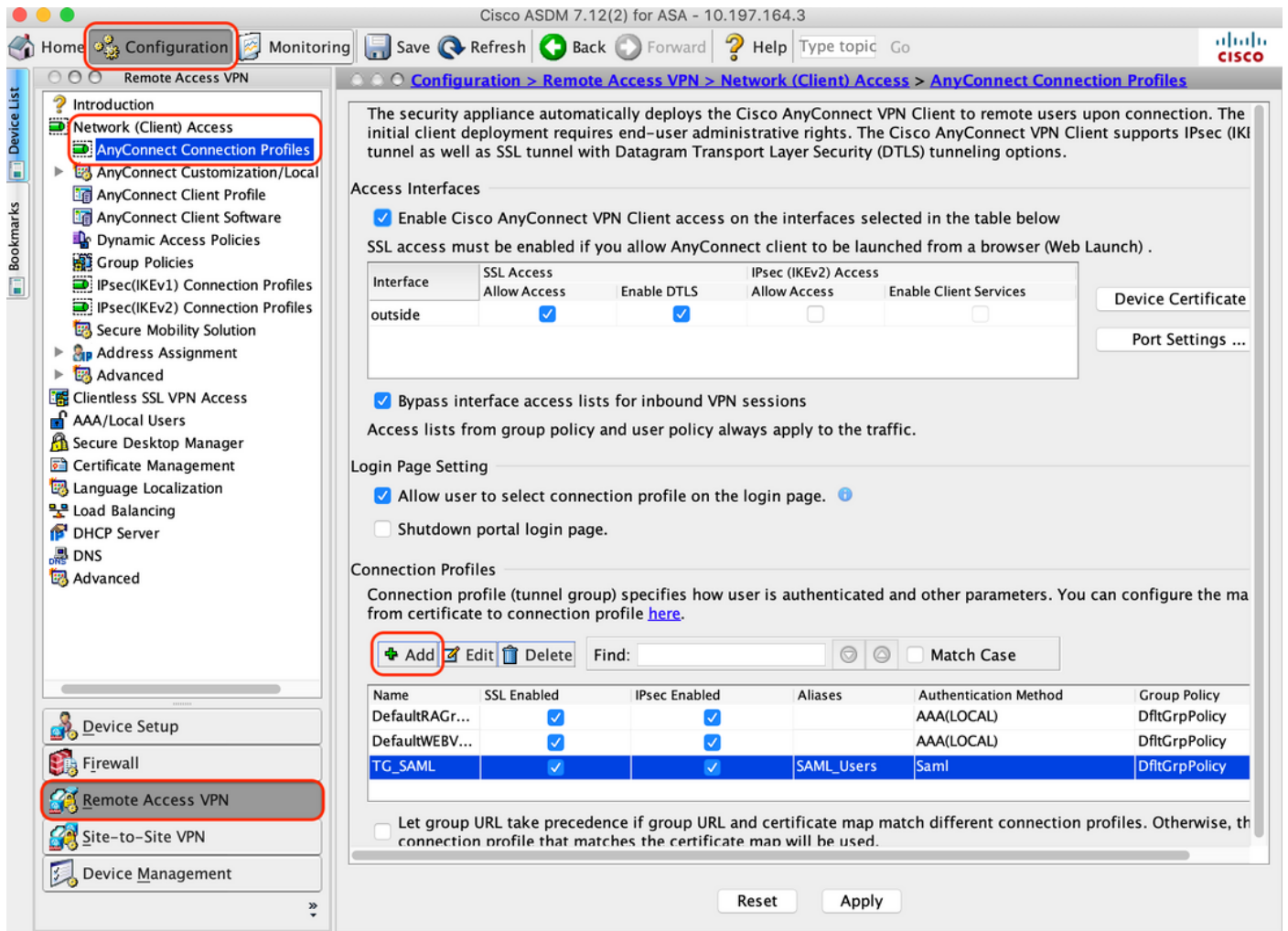
في هضرع نكمي يذلاو يضارت فالالة وعموم جمل جهن دادع إال اذه مدخت سي أ. Configuration > Remote Access VPN > Network (Client) Access > Group Policies"



7. لاصتالال فيرعت فلم نيوكت

AnyConnect وم دخت سم هب لاصتالال فيرعت فلم عاشن أ.

تافي صوت > (لي مكالمة) > VPN > لي دع ب نع لوصول > لي كشت لي لقتنا ب.
 "ةفاضل" لي ع رقنا ، "AnyConnect" لي صوت



لي صوت لي فيرعت فل م ب ة ط ب تر م ل ة لي ل ات ل لي ص اف ت ل ني و ك ت ب م ق ج:

م س ا ل ا	tg_saml
ة ر ا ع ت س م ء م س ا	SAML_Users
ة ق ي ر ط	ل م ا س
م د ا و خ ة ع و م ج م	ي ل ح م
ء ا ل م ع ل ا ن ي و ا ن ع ت ا ع م ت	AC_POOL
ة ع و م ج م ل ا ج ه ن	DfltGrpPolicy

Basic
Advanced

Name: TG_SAML

Aliases: SAML_Users

Authentication

Method: SAML

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider

SAML Server : <https://explorer.cisco.com/dag/saml2/idp/metadata.php> Manage...

Client Address Assignment

DHCP Servers:

None DHCP Link DHCP Subnet

Client Address Pools: AC_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

(Following fields are linked to attribute of the group policy selected above.)

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

Find: Next Previous

Help Cancel OK

حضوره و ه امك و دبت يت ال SAML ةي وه رفوم لي صافات ني و ك ت ب مق ، ة ح ف ص ل ا س ف ن ي ف د .
ه ا ن د ا :

فرعم نايك ني درشم الاي لخاد	https://explorer.cisco.com/dag/saml2/idp/metadata.php
ناونع URL ليجستل لوخدلا	https://explorer.cisco.com/dag/saml2/idp/SSOService.php
ناونع URL ليجستل جورخلا	https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer
URL يساسلا	https://firebird.cisco.com

"ةفاضإ > ةرادإ ىلع رقنا - ءاه

Add SSO Server

IDP Entity ID:

Settings

Sign In URL:

Sign Out URL:

Base URL:

Identity Provider Certificate:

Service Provider Certificate:

Request Signature:

Request Timeout: seconds (1-7200)

Enable IdP only accessible on Internal Network

Request IdP re-authentication at login

f. لىوختلل AAA مداخ فىرعتب مق ،لاصتالا فىرعت فللمل مدقتملا مسقلا نمض .

"ةفاضإ" قوف رقناو "ضىوفت > مدقتم ىلا لقتنا

Edit AnyConnect Connection Profile: TG_SAML

Basic

Advanced

General

Client Addressing

Authentication

Secondary Authentication

Authorization

Accounting

Group Alias/Group L

Authorization Server Group

Server Group:

Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

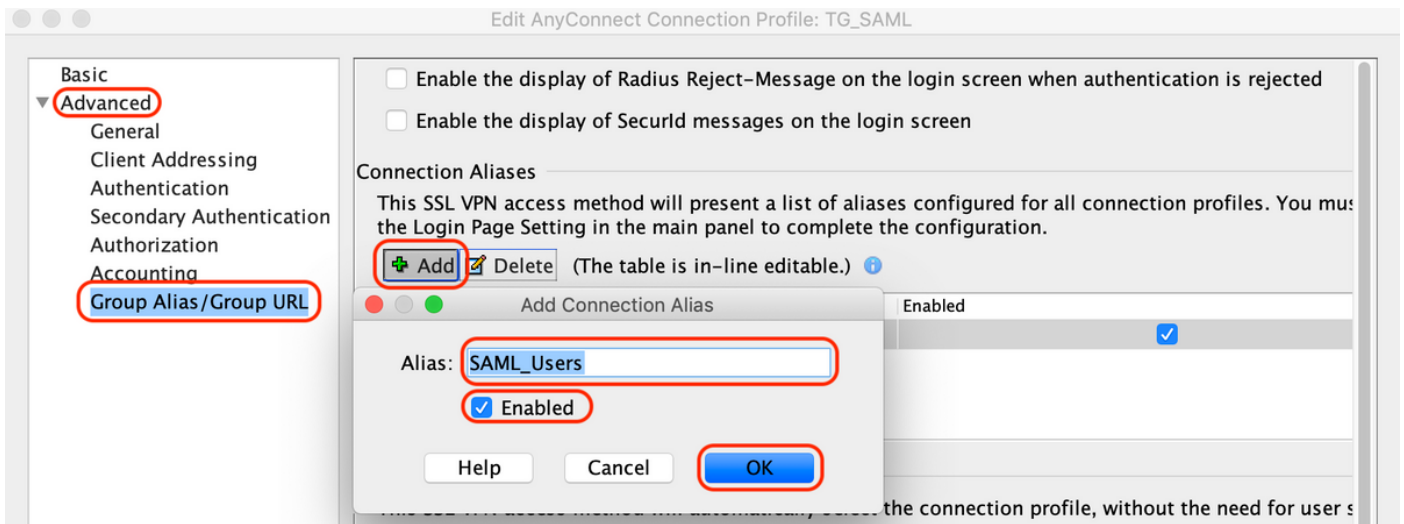
Assign Authorization Server Group to Interface

Interface:

Server Group:

G. لاصتالل راعتسملا مسالا فىرعتب مق ،ةوعومجملل راعتسملا مسالا تحت .

"ةفاضإ" قوف رقناو "ةوعومجملل راعتسملا مسالا > مدقتم ىلا لقتنا



(CLI) رماوأل رطس ةهجاو ىلع هاندأ لكشلا س فن وهو ASA، نيوكت لامتكأ ىلإ اذه يدؤي ح.

```

!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!-----Client pool configuration-----
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!-----Redirect Access-list-----
!
access-list redirect extended deny udp any any eq domain
access-list redirect extended deny ip any host 10.197.243.116
access-list redirect extended deny icmp any any
access-list redirect extended permit ip any any
access-list redirect extended permit tcp any any eq www
!
!-----AAA server configuration-----
!
aaa-server ISE protocol radius
  authorize-only
  interim-accounting-update periodic 1
  dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
  key *****
!
!-----Configure Trustpoint for Duo Access Gateway Certificate-----
!
crypto ca trustpoint Duo_Access_Gateway
  enrollment terminal
  crl configure
!
!-----Configure Trustpoint for ASA Identity Certificate-----
!
crypto ca trustpoint ID_CERT
  enrollment terminal
  fqdn firebird.cisco.com
  subject-name CN=firebird.cisco.com

```

```

ip-address 10.197.164.3
keypair ID_RSA_KEYS
no ca-check
cr1 configure
!
!-----Enable AnyConnect and configuring SAML authentication-----
!
webvpn
enable outside
hsts
enable
max-age 31536000
include-sub-domains
no preload
anyconnect image disk0:/anyconnect-win-4.8.03052-webdeploy-k9.pkg 1
anyconnect enable
saml idp https://explorer.cisco.com/dag/saml2/idp/metadata.php
url sign-in https://explorer.cisco.com/dag/saml2/idp/SSOService.php
url sign-out https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explor
base-url https://firebird.cisco.com
trustpoint idp Duo_Access_Gateway
trustpoint sp ID_CERT
no signature
no force re-authentication
timeout assertion 1200
tunnel-group-list enable
cache
disable
error-recovery disable
!
!-----Group Policy configuration-----
!
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
!
!-----Tunnel-Group (Connection Profile) Configuraiton-----
!
tunnel-group TG_SAML type remote-access
tunnel-group TG_SAML general-attributes
address-pool AC_Pool
authorization-server-group ISE
accounting-server-group ISE
tunnel-group TG_SAML webvpn-attributes
authentication saml
group-alias SAML_Users enable
saml identity-provider https://explorer.cisco.com/dag/saml2/idp/metadata.php
!

```

ISE نيوكت-

1. كېبش زاھجك Cisco ASA ةفاضل

"ةفاضل" قوف رقنا ، "ةكېبشللا ةزهجأ > ةكېبشللا دراوم > ةرادا تحت نيوكتو "RADIUS ةقداصم تادادع" تحت و نرتقملا IP ناونعو ةكېبشللا زاھج مسا نيوكت م ق "ظفح" ل ع رقناو "كرتشملا رسلا"

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

Use Second Shared Secret

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

DNS Name

General Settings

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL



▶ TACACS Authentication Settings



▶ SNMP Settings



▶ Advanced TrustSec Settings

Agent Resources From Local Disk

Category ⓘ

Browse...

▼ AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.8.30...	AnyConnectDesktopWindows	4.8.3052.0	AnyConnect Secure Mobility Clie...

4. AnyConnect Posture فيرعت فلم عاشنإ.

ىلع رقنا ". دراوملا > ليمعلا دادمإ > جئاتنلا > ةسايسلا رصانع > ةسايس ىلإ لقتنا أ.
"AnyConnect Posture فيصوت" ددحو "ةفاضإ"

مسا دعاوق تحت "" ك مداخل مسا نيوكتب مقو AnyConnect Posture فيرعت فلم مسا لخدأ ب.
"ظفح" قوف رقناو مداخل

ISE Posture Agent Profile Settings > Anyconnect Posture Profile

* Name:

Description:

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List		List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPAddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	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	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect 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

5. AnyConnect نيوكت ءاشن |

ىلع رونا . " دراوملا > ليمعلا دادم | > جئاتنلا > ءسايسلا رصانع > ءسايس ىلإ لوقت نا . أ
"AnyConnect نيوكت" دحو "ءافاضا"

ءبولطملا قفاوتلا ءحو دحو ، نيوكتلا مسا لخدأو ، AnyConnect ءمزح دحو . ب

"ريراقتلا دادعإو صيخششتلا ءادأ" نم ققحت ، "ءيطمنلا AnyConnect ءحو ديءحت" تحت . ج

"ظفح" قوف روناو ءعضولا فيرعت فلم دحو ، "فيرعتلا فلم ديءحت" تحت . د

* Select AnyConnect Package: AnyConnectDesktopWindows 4.8.3052.0

* Configuration Name: AnyConnect Configuration

Description:

DescriptionValue

* Compliance Module: AnyConnectComplianceModuleWindows 4.3.1250.614

Notes

AnyConnect Module Selection

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: Anyconnect Posture Profile

VPN

Network Access Manager

Web Security

AMP Enabler

Network Visibility

Umbrella Roaming Security

Customer Feedback

6. لي معالج ديوزتة سايس ءاشن ا.

أ. "لي معالج دادم > ءة سايس ل لقتنا ا.

ب. "هالعة ءءءاق ءارءا" دء مء "ريرءء" قوف رقنا ب.

ج. > "لي ءولا" نمض) ءءءاءنل ءءءو، بولطمل ليرغشءل لماظن دءو، ءءءاق ل مءسا لءءا ا. "ظفء" قوف رقنا او 5 ءوطلء ل ير هءاشن ا مء يءل "AnyConnect ني ءوكت" دء، ("لي ءولا ني ءوكت"

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Windows_10	If Any	and Windows 10 (All)	and Condition(s)	then AnyConnect Configuration
Windows	If Any	and Windows All	and Condition(s)	then CiscoTemporalAgentWindows 4.7.00135 And WinSPWizard 2.5.0.1 And Cisco-ISE-NSP
MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOS X 4.7.00135 And MacOsXSPWizard 2.1.0.42 And Cisco-ISE-NSP
Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Save Reset

7. ةلا ءاشناب مق

فلم ةلا ءاشناب مق > ةلا ءاشناب مق > ةلا ءاشناب مق > ةلا ءاشناب مق

ماظن م، "VPN_Posture_File_CHECK" طرشلل مسا نيوك ت مق و "ةفاضل" قوف رقنا ب. ك فلملا راسمو، "FilePresence" ك فلملا عونو، "Windows 10(All)" ك بولطملا ليغشتلا ك فلملا لغشم ددحو، "C:\custom.txt" ك فلملا مساو لمكلا راسملا م، "ABSOLUTE_PATH" "دوجوم"

فلم طرشك صارقألا كرحم C: نمض "custom.txt" مسا ب فلم دوجو لاثملا اذم مدختسي ج.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Library Conditions Smart Conditions Time and Date Profiling Posture Anti-Malware Condition Anti-Spyware Condition Anti-Virus Condition Application Condition Compound Condition Disk Encryption Condition File Condition

File Conditions List > VPN_Posture_File_Check

File Condition

* Name: VPN_Posture_File_Check

Description:

* Operating System: Windows 10 (All)

Compliance Module: Any version

* File Type: FileExistence

* File Path: ABSOLUTE_PATH

* File Operator: Exists

C:\custom.txt

Save Reset

8. ءصولا ءالصا ءارجا ءاشناب

عارجا عاشنال "عجالعم تاءارجا" > عيعضو > جئاتن > عسايس رصانع > عسايس ىل لقتنا مت حالصا تاءارجا "طقف ةلاسرلا صن" دن تسمل اذه مدختسي. قفاوتم فلم عجالعم ةيلا ل ةوطخلال يه انه نيوكت.

9. عضولا تابلطتم ةدعاق عاشنال

"تابلطتم > عيعضو > جئاتن > عسايس رصانع > عسايس ىل لقتنا أ.

"ديج بطلطتم جاردا" ددح مٲ "ريحت" قوف رقنا ب.

ك بولطملا ليغشتلا ماظنو، "VPN_Posture_Requirements" طرشلل مسانيوكت ب مق ج. "AnyConnect" ك عضولا عونو، "ثدحأ رادصا" وأ "4.x" ك قفاوتلا ةدحوو، "Windows 10(All)"

تاءارجا تحتو (7 ةوطخلال يه اهؤاشنال مت يتيلا) "VPN_Posture_File_CHECK" ك طورش د. Agent User ل ةصصخملا ةلاسرلا لخدأو "طقف ةلاسرلا صن" ك عارجالا ددح، حالصالا

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
USB_Block_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if USB_Check	then Message Text Only
Any_AM_Installation_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Installation_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if ANY_am_mac_inst	then Message Text Only
Default_AppVis_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations
Default_AppVis_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations
Default_Hardware_Attributes_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Hardware_Attributes_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Win_Remediation_Win
Default_Firewall_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
VPN_Posture_Requirement	for Windows 10 (All)	using 4.x or later	using AnyConnect	met if VPN_Posture_File_Che...	then Message Text Only

Note: Remediation Action is filtered based on the operating system and stealth mode selection. Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.

10. عضولا عسايس عاشنال

"ةيعضو > عسايس ىل لقتنا أ.

ك بولطملا ليغشتلا ماظنو، "VPN_Posture_POLICY_WIN" ك ةدعاقلا مسانيوكت ب. "AnyConnect" ك عضولا عونو، "ثدحأ رادصا" وأ "4.x" ك قفاوتلا ةدحوو، "Windows 10(All)" ةوطخلال يه انه نيوكت مت امك "VPN_Posture_Require" ك تابلطتملاو

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements
⊙	Policy Options	Default_AppVis_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_AppVis_Requirement_Win
⊙	Policy Options	Default_AppVis_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppVis_Requirement_Win_temporal
⊙	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Mac
⊙	Policy Options	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal
⊙	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Firewall_Requirement_Win
⊙	Policy Options	Default_Firewall_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Win_temporal
⊙	Policy Options	Default_Hardware_Attributes_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and AnyConnect	and	then Default_Hardware_Attributes_Requirement_Mac
⊙	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Mac_temporal
⊙	Policy Options	Default_Hardware_Attributes_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then Default_Hardware_Attributes_Requirement_Win
⊙	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Win_temporal
⊙	Policy Options	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and AnyConnect	and	then USB_Block
⊙	Policy Options	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then USB_Block_temporal
⊙	Policy Options	VPN_Posture_Policy_Win	If Any	and Windows 10 (All)	and 4.x or later	and AnyConnect	and	then VPN_Posture_Requirement

Save Reset

11. (DACL) ءيكي مانيدل (ACL) لوصولو ي ف مكحتل مئوق عاشن.

ي ف مكحتل مئوق > ضيوفتال > چئاتنل > ءسايسل رصانع > ءسايسل ل لقتنل
 ذفنملاب ءصاخلا لوصولو ي ف مكحتل مئوق عاشناب مقو "ليزنلل ءلباقل (ACL) لوصولو
 ءعضولا تالاح فللخمل (DACL).

ءيالاتل (DACL) لوصولو ي ف مكحتل مئوق دننل سمل اذه مدختسي.

a. Posture رورم ءكح لىل رورم ءكح و PSN و HTTP و HTTPS رورم ريغ

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Downloadable ACL List > PostureUnknown

Downloadable ACL

* Name PostureUnknown

Description

IP version IPv4 IPv6 Agnostic

* DACL Content

```

1234567 permit udp any any eq domain
8910111 permit ip any host 10.106.44.77
2131415 permit tcp any any eq 80
1617181 permit tcp any any eq 443
9202122
2324252
6272829
3031323
3343536
  
```

Check DACL Syntax

Save Reset

ب. Posture NonCompliant: الة حمسي الوة صاخ الة عرف الة اك بش الة الة لوصول الة ضفري: Posture NonCompliant: تنرت الة رورم ة كرحب

The screenshot shows the configuration page for a Downloadable ACL named 'PostureNonCompliant'. The interface includes a navigation menu on the left with categories like Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled 'Downloadable ACL List > PostureNonCompliant' and contains the following fields:

- Name:** PostureNonCompliant
- Description:** (Empty text box)
- IP version:** IPv4 (selected), IPv6, Agnostic
- DACL Content:**

```

1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536

```
- Buttons:** Save, Reset

ج. ني قفاوتم الة ني ئاه الة ني م دخت سمل ل رورم الة كرح عي م جل حمسي: عضولل قباطم ج. عضولل

The screenshot shows the configuration page for a Downloadable ACL named 'PostureCompliant'. The interface is similar to the previous one, with the following fields:

- Name:** PostureCompliant
- Description:** (Empty text box)
- IP version:** IPv4 (selected), IPv6, Agnostic
- DACL Content:**

```

1234567 permit ip any any
8910111
2131415
1617181
9202122
2324252
6272829
3031323
3343536

```
- Buttons:** Save, Reset

12. لي وخت الة في رعت تافل مءاشن ا.

صي صخت تافل م > ضي وفت الة > جئ ات الة > ة سايس الة رصانع > ة سايس الة لقتنا "ضي وفت الة".

فورعلم الة ريغ عضولل لي وخت الة في رعت فلم ا.

مقو (Posture) ليم عمل دادع دحو، بيول هيجوت دواع نم ققحتو، "PostureUnknown" DACL دحو (ASA) (لعل هنيوكت متلي) "redirect" هيجوت ل دواع لوصولاب مكحتل ةمئاق مسا نيوكتب (يضارت فالال) ليم عمل دادم لخدم دحو

The screenshot shows the configuration page for an Authorization Profile named "Posture Redirect". The interface includes a left-hand navigation menu with categories like Authentication, Authorization, Profiling, Posture, and Client Provisioning. The main content area is titled "Authorization Profiles > Posture Redirect" and contains the following fields and sections:

- Authorization Profile:**
 - Name: Posture Redirect
 - Description: (empty)
 - Access Type: ACCESS_ACCEPT
 - Network Device Profile: Cisco
 - Service Template: (unchecked)
 - Track Movement: (unchecked)
 - Passive Identity Tracking: (unchecked)
- Common Tasks:**
 - DACL Name: PostureUnknown
 - Web Redirection (CWA, MDM, NSP, CPP): (checked)
 - Client Provisioning (Posture): (dropdown menu)
 - ACL: redirect
 - Value: Client Provisioning Portal (default)
- Advanced Attributes Settings:** (empty)
- Attributes Details:**
 - Access Type = ACCESS_ACCEPT
 - DACL = PostureUnknown
 - cisco-av-pair = uri-redirect-ac=redirect
 - cisco-av-pair = uri-redirect=https://ip:port/portal/gateway?sessionId=SessionId&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp

At the bottom of the page, there are "Save" and "Reset" buttons.

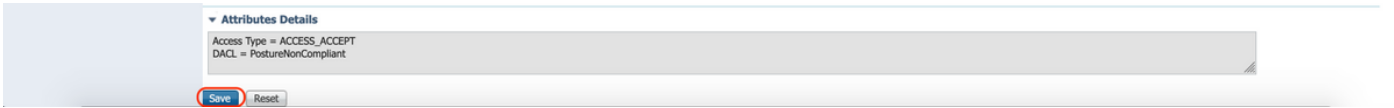
عضولل لاثتمالال مدعل ضيوفتلال فيرعت فلم - ءاب

ةكبشلال لوصولال نم دحلل "PostureNonCompliant" DACL دحو

The screenshot shows the configuration page for an Authorization Profile named "Posture Non Compliant". The interface is similar to the previous one, with a left-hand navigation menu and a main content area titled "Authorization Profiles > Posture Non Compliant". The configuration details are as follows:

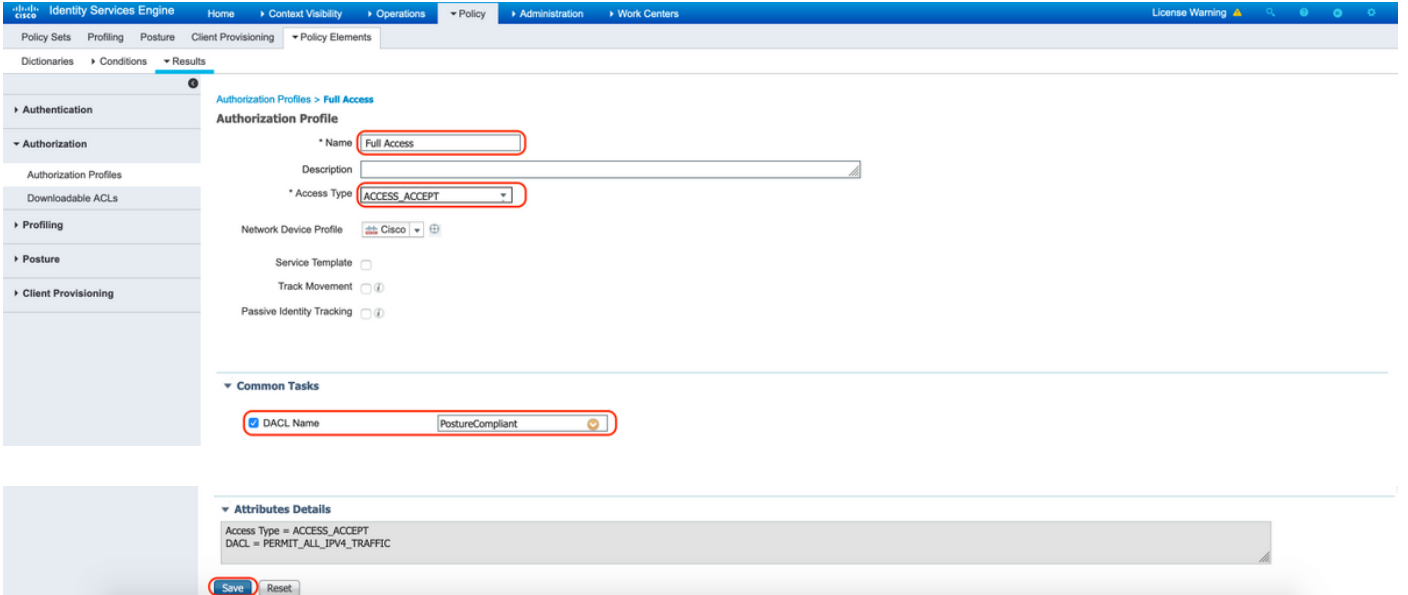
- Authorization Profile:**
 - Name: Posture Non Compliant
 - Description: (empty)
 - Access Type: ACCESS_ACCEPT
 - Network Device Profile: Cisco
 - Service Template: (unchecked)
 - Track Movement: (unchecked)
 - Passive Identity Tracking: (unchecked)
- Common Tasks:**
 - DACL Name: PostureNonCompliant

At the bottom of the page, there are "Save" and "Reset" buttons.



عضولاء عم قفاوتلاب صاخلا ليوختلا فيرعت فلم - ميج

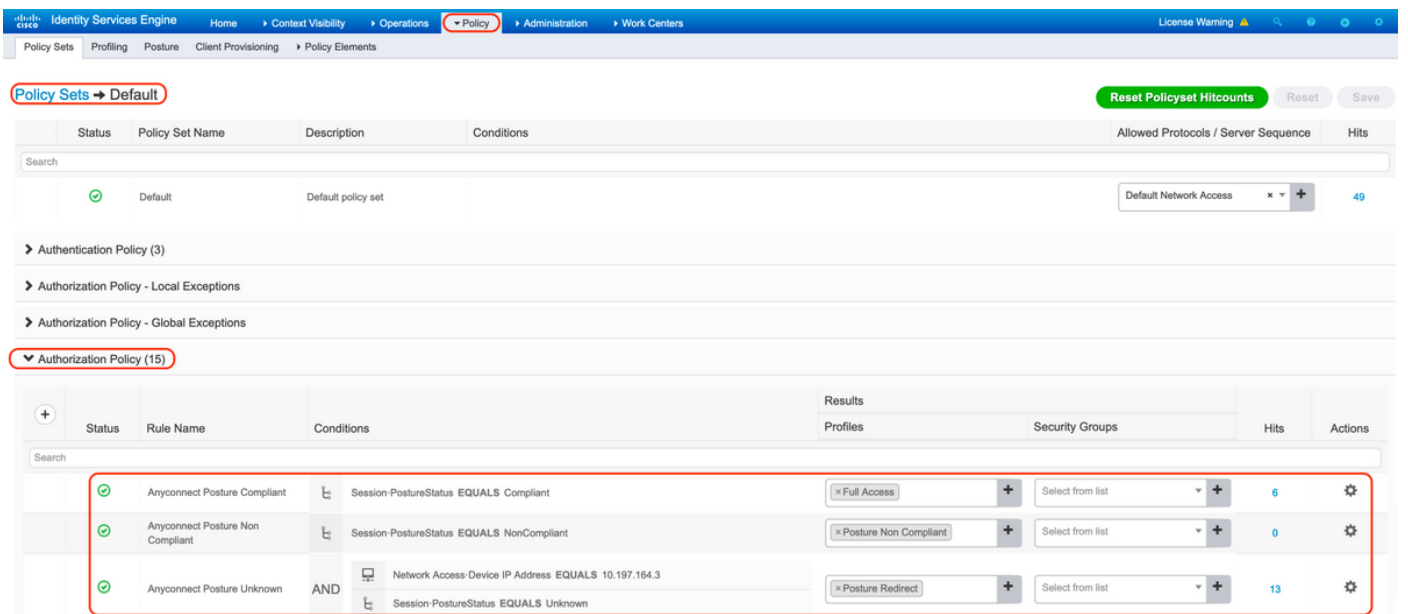
ةكبشلا لىلا لمكلا لوصولاب حامسلا ل "PostureCompliant" DACL دح



ضيوفتلا تاسايس نيوك 12.

3 نيوك تلة قبا سلا ةوطخلا في اه نيوك مت يتلا ليوختلا فيرعت افلم مدختسا ةفورعم ريغ ةيعوو، عضولا عم ةقفاوتم ريغو، عضولا عم ةقفاوتم ليوخت تاسايس.

جهن لك جئاتن ديدحتل "عضولا ةلاح: لمعلا ةسلج" كرتشملا طرشلما مدختسا متي



ةحصل ال نم ققحتل

ححص لكشب نيوكتل لمع ديكأتل مسقلا اذه مدختسا

ASA. لعل يلاتل رمألا ليغشتب مق ،حاجنب مدختسمل اةقداصم نم ققحتلل

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : _585b5291f01484dfd16f394be7031d456d314e3e62
Index : 125
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 16404 Bytes Rx : 381
Pkts Tx : 16 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

TG_SAML

Login Time : 07:05:45 UTC Sun Jun 14 2020
Duration : 0h:00m:16s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 125.1
Public IP : 10.197.243.143
Encryption : none Hashing : none
TCP Src Port : 57244 TCP Dst Port : 443
Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0

Pkts Tx Drop : 0

Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 57248
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:

Tunnel ID : 125.3
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 49175
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 458 Bytes Rx : 381
Pkts Tx : 4 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture:

Redirect URL : https://ise261.pusaxena.local:8443/portal/gateway?sessionId=0ac5a4030007d0005ee5cc49&p
Redirect ACL : redirect

وه امك لمالك لوصول الى مدخست سمل لوصول ريغي غت متي ،عضول المي يقيقت لامتك ادرج م
"حش رمل مسا" لقل ل اء ف د م ت ي ال (DACL) لوصول اب مكحت ل اء ف ي ف ظ حال م

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

Username : _585b5291f01484dfd16f394be7031d456d314e3e62
Index : 125

Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 16404 Bytes Rx : 381
Pkts Tx : 16 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group :

TG_SAML

Login Time : 07:05:45 UTC Sun Jun 14 2020
Duration : 0h:00m:36s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5a4030007d0005ee5cc49
Security Grp : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 125.1
Public IP : 10.197.243.143
Encryption : none Hashing : none
TCP Src Port : 57244 TCP Dst Port : 443
Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 125.2
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 57248
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 7973 Bytes Rx : 0
Pkts Tx : 6 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:

Tunnel ID : 125.3
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 49175
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows

Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052
Bytes Tx : 458 Bytes Rx : 381
Pkts Tx : 4 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Filter Name :

#ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

> RADIUS > تايللمع ىل لى لقتنا ،ISE ىل ع حاجنب ضىوفتلا ذىفنت مت اذا ام نم ققحتلل
ةىح تالاجس

نجوم وةىوهلا ى ،دمت عمل مدختس ملاب ةنرتقملا ةلصللا تاذا م ولعمل مسقلا اذ هضرع
عضولا ةلاحو لى وختلا جهنو لى وختلا فىرعت

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			0	_585b5291f01484d6d1...	00:50:56:A0:D6:97	Windows10-...	Default	Anyconnect ...	Full Access	Compliant	10.197.164.7	ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-PERMI...	10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:34.963 AM				#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484d6d1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA



ىل ع وجرلا ىجرى ،ISE ىل ع عضولا ةحص نم ققحتلل نم ديزم ىل ع لوصحلل :ةظالم
ةىلاتلا قىثولا

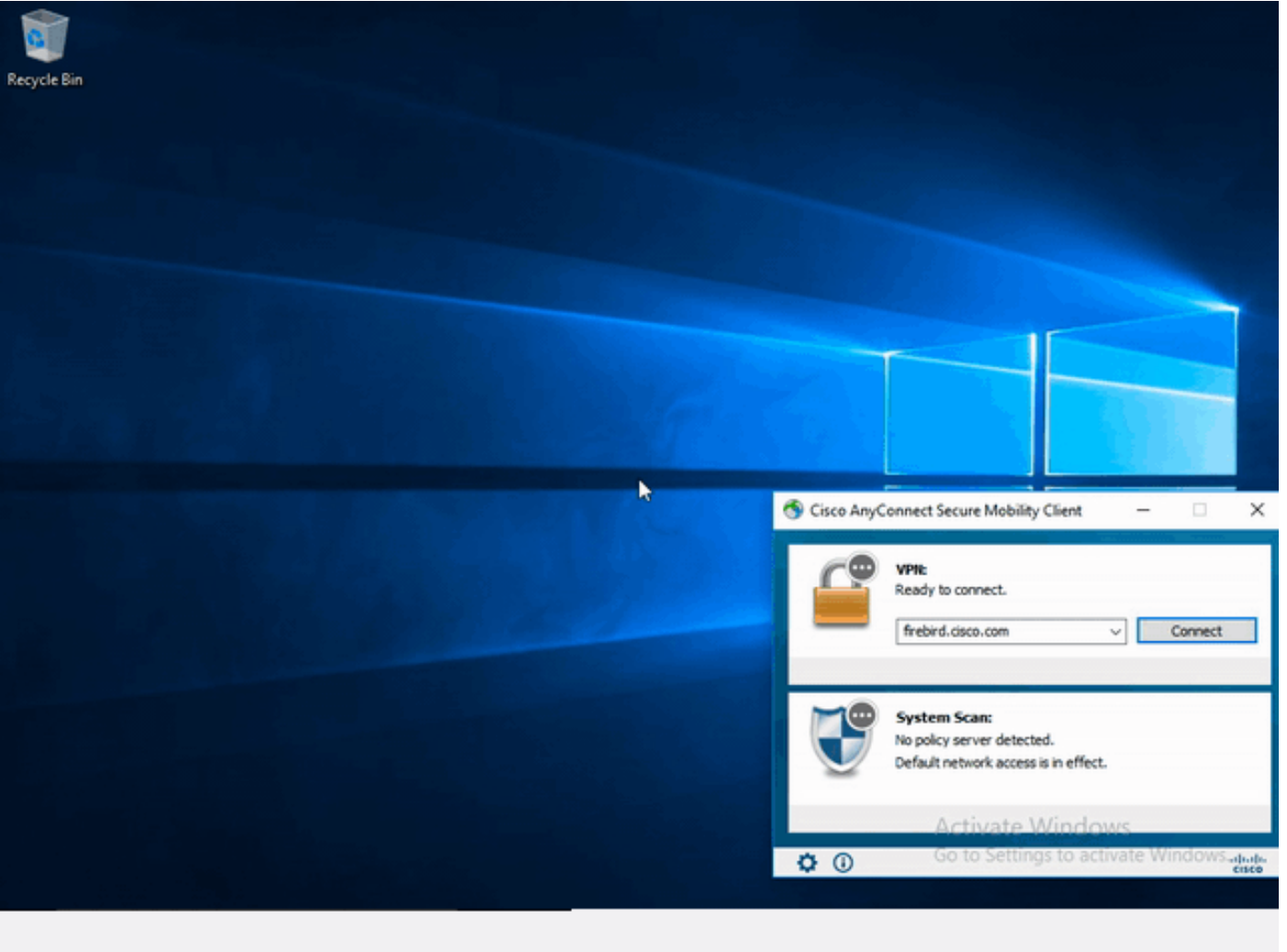
<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-acces.html#anc7>

ىل ع ةدوجوملا "ريراقتلا" ىل ع رقنا ،Duo لوؤسم لخدم ىل ع ةقداصلما ةلاحو نم ققحتلل
ةقداصلما لاجس رهظت ىتلا ةرادلا ةحول نم رسيال بناجال

لئىصافتلا نم ديزملا : <https://duo.com/docs/administration#reports>

ىلاتلا طابترال مدختسأ ،ةىئانثلا لوصول ةرابعل ءاطخألا حىحصت لىجست ضرعل
https://help.duo.com/s/article/1623?language=en_US


مدختس ملاب ةبرجت



اهحالصإو ءاطخأل فاشك ت سا

اهحالصإو نيوك ت ل ءاطخأ فاشك ت سا ل اهم ادخ ت سا ل كنكمي يت ل ا تام ول عمل ا مسق ل ا اذه رفوي

 debug رم او ا مدخ ت سا ل ب ق [حي حص ت ل ا رم او ل و ح ة مه م ت ا م و ل ع م](#) ي ل ا ع ج ر ا : ة ط خ ا ل م

 م ادخ ت سا م تي ؛ ة فل ت خ م ءاطخأ حي حص ت ت ا ي و ت س م ن ي ي ع ت ك ن ك م ي ، ASA ي ل ع : ه ي ب ن ت ة ج ر د د ي ا ز ت ت د ق ف ، ءاطخأل ا حي حص ت ي و ت س م ر ي ي غ ت ب ت م ق ا ذ ا . ا ي ض ا ر ت ف ا ل و ا ل ا ي و ت س م ل ا ج ا ت ن ا ل ا ت ا ي ب ي ف ة ص ا خ و ، ر ذ ح ب ك ل ذ ب م ق . ءاطخأل ا حي حص ت ع س و ت

ه ي ل ع ر و ث ع ل ا ن ك م ي ح ي ح ص ر ي غ ن ي و ك ت ا ه ح ا ل ص ا و SAML ءاطخأ فاشك ت سا م ط ع م ن م ض ت ي س ءاطخأل ا حي حص ت ل ي غ ش ت و ا SAML ن ي و ك ت ن م ق ق ح ت ل ا ل ا ل خ ن م


عمو، اهحال صإو لكاشم لالمظعم ءاطخأ فاشك تسال "debug webVPN saml 255" مادختسإ نكمي نكمي، ءديفم تامولعم اذه ءاطخأل احيحصت اهيف رفوي ال يتل تا هويرانيس لال يف كلذ ءيفاضإ تاحيحصت ليغشت

```
debug webvpn 255
debug webvpn anyconnect 255
debug webvpn session 255
debug webvpn request 255
```

احيحصت رمإو مدختسأ، اهحال صإو ASA ب ءقلعت م لاضيفوت لال ءقدا ص م لال ءاطخأ فاشك تسال ءيلال ءاطخأل:

```
debug radius all
debug aaa authentication
debug aaa authorization To troubleshoot Posture related issues on ISE, set the following attributes to
```

```
posture (ise-psc.log)
portal (guest.log)
provisioning (ise-psc.log)
runtime-AAA (prrt-server.log)
nsf (ise-psc.log)
nsf-session (ise-psc.log)
swiss (ise-psc.log)
```

 ISE و AnyConnect ءاطخأ فاشك تسال ءصلا ءفدت لىل ءلوصحلل: ءطالم ي: لالال طابترالال لال عرا، اهحال صإو [ISE Posture لال pre و post 2.2 طمن ءنراقم](#)

اهحال صإو اهئاطخأ فاشك تسال ءيئان لال لوصول ءرابع ءاطخأ احيحصت تالچس ءمچرتل https://help.duo.com/s/article/5016?language=en_US

ءلص تا ذ تامولعم

<https://www.youtube.com/watch?v=W6bE2GTU0Is&>
<https://duo.com/docs/cisco#asa-ssl-vpn-using-saml>

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html#anc0>

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا