# AnyConnect Secure عم Duo SAML SSO جمد Access مادختساب ISE Posture

## تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>نى وكتلا</u> <u>ةكبشلل يطيطختلا مسرلا</u> <u>رورملا ةكرح قفدت</u> <u>تانىوكتلا</u> <u>Duo لوؤسم لخدم نيوكت -</u> (DAG) يئانثلا لوصول قرابع نيوكت -<u>ASA نېوكت-</u> <u>ISE نىوكت-</u> <u>قحصابا نم ققحتايا</u> <u>مدختسملا ةبرجت</u> <u>امحال ص او ءاطخأل ا ف اش ك ت س ا</u> <u>ةلص تاذ تامولعم</u>

## ةمدقملا

فيكتلل لباقلا نامألا زامج عم Duo SAML SSO جمدل نيوكتلل الااثم دنتسملا اذه فصي مييقت ءارجإل Cisco AnyConnect Secure Mobility Client Access لغتسي يذلا (ASA) Cisco AnyConnect Secure Mobility Client Access لغتسي يخل (DAG) قيئانثلا لوصولا قرابع مادختساب 200 SAML SSO ذيفنت متي عضولل لصفم يئانثلا نامألاب لصتت مث مدختسملل قيلوألا ققداصملل Vacive Directory بلصتت يتلا ريفوتل ضيوفت مداخك ISco ISE مادختسإ متي لماوعلا قددعتم ققداصملل (قباحسلا) ريفوتل ضيوفت مداخك Samu مي من مي من مي من مي مي الماري الماري في مي

.Cisco HTTS سدنهم ،انيسكاس تيكلوبو ليجدوم شينيد اهيف مهاس

## ةيساسألا تابلطتملا

### تابلطتملا

ل حامسلل ەنيوكت متو لماكلا ليغشتلا ديق ASA نأ دنتسملا اذه ضرتفي Cisco Adaptive ل حامسلل اذه ضرتفي. نيوكتلا تارىيغت ءارجإب (CLI) رماوألا رطس ةەجاو وأ (ASDM) Security Device Manager

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- يئانثلا نامألا ةزيمو ةيئانثلا لوصولا ةباوب تايساسا •
- ASA ىلع دعب نع لوصولل VPN نيوكتب ةيساسأ ةفرعم 🛛 •
- Posture و ISE تامدخب ةيساسأ ةفرعم 🔹

ةمدختسملا تانوكملا

ةيلاتا جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Cisco، رادصإلا، Cisco نم فيكتلل لباقلا نامألا زاهج جمانرب
- Duo Access Gateway
- يئانثلا نامألا
- Cisco Identity Services Engine، اثدحألا تارادصإلاو 2.6 رادص ال
- Microsoft Windows 10 نم 4.8.03052 رادصإلا عم AnyConnect

الذيفنتال الذه يف مدختسمال ،Ask من مضمال ضرعتسمال بلطتي :ةظحالم Ask ،ذيفنتال الذه يف مدختسمال م و رادصإ لك نم ثدحأ رادصإ وأ 1(2)9.9 و 82(2)8.8 و 9.7(1)9.7 رادصإلا ىلع ثدحأ رادصإ وأ 4.6 رادصإلا

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

## نيوكتلا

### ةكبشلل يطيطختلا مسرلا



### رورملا ةكرح قفدت

- Cisco ASA كالصتا ةئيەتب AnyConnect ليمع موقي .1
- لوصولا ةرابع مادختساب ةيساسألا ةقداصملل ەنيوكت مت يذلا، Cisco ASA موقي .2 DAG ىلإ AnyConnect Client يف نمضملا ضرعتسملا ميجوت ةداعإب ،(DAG) ةيئانثلا قوداصمل SAML
- ةيئانثلا لوصولا ةرابع ىلإ AnyConnect ليمع هيجوت ةداعإ تمت .3
- 4. هقداصم بلط ءاشنإ متي ،دامتعالا تانايب ىلإ AnyConnect ليمع لوخد درجمب .4 نم Duo يلإ ASA لوصولا ةرابع نم ردصيو
- عقوملا يف Active Directory ةمدخ عم لماكتلا ةدايز ىلع ةيئانثلا لوصولا ةرابع لمعت .5 ليمعل ةيساسألا ةقداصملا ءارجإل
- ىلإ بلط لاسراب ةيئانثلا لوصولا ةرابع موقت ،ةيساسألا ةقداصملا حاجن درجمب .6 لماوعلا ةيئانث ةقداصملا عدبل 443 مقر TCP ذفنم ربع يئانثلا نامألا
- ليمع ميدقت مت .7 لمكيو "ةيئانثلا ةيلعافتلا ةبلاطملا" مادختساب AnyConnect ليمع ميدقت مت .7 وأ طغضلا) هيدل ةلضفملا ةقيرطلا مادختساب لماعلا ةيئانثلا ةقداصملا مدختسملا (رورملا زمر
- ةيئانثلا لوصولا ةرابع ىلإ تامولعملا ديعيو ةقداصم ةباجتسإ Duo Security ملتسي .8
- ةباجتسإ ءاشنإب ةيئانثلا لوصولا ةرابع موقت ،ةقداصملا ةباجتسإ ىلإ ادانتسا .9 AnyConnect ليمع عم بواجتتو SAML ديكأت ىلع يوتحت SAML ةقداصم
- Cisco ASA مادختساب SSL VPN لاصتال حاجنب Cisco ASA ةقداصم .10
- Cisco ISE ىلإ ضيوفت بلط Cisco ASA لسري ،ةقداصملا حاجن درجمب .11

ا ةيئانثلا لوصولا ةرابع نأل ارظن ليوختلل طقف Cisco ISE نيوكت متي :ةظحالم Sisco ISE نيوكت متي :ةظحالم 💊

- ،ةفورعم ريغ ليمعلا عضو ةلاح نأ امبو ضيوفتلا بلط ةجلاعمب Cisco ISE موقي .12 مريف AnyConnect client يل دودجم لوصو عم Posture Redirect عجريف
- ا ەليزنتب ەتبلاطم متت ،ةيطمن قفاوت ةدحو AnyConnect ليمع ىدل نكي مل اذإ .13 عضولا مييقت ةعباتمل
- عم TLS لاصتا سسؤي ەنإف ،ةيطمن قڧاوت ةدحو ىلع يوتحي AnyConnect client ناك اذإ .14 Cisco ASA عاضوألا قڧدت أدبيو
- متيو عضولا تاصوحف ءارجإ متي ،ISE ىلع اەنيوكت مت يتلا عضولا طورش ىلع ءانب .15 متيو عضولا تاصوحف عارج متي ،ISE كلي AnyConnect ليمع نم ليصافتلا لاسرا

رييغت بلط لاسرا متيسف ،قفاوتم ىلإ فورعم ريغ نم ليمعلا عضو ةلاح تريغت اذإ .16 عاشناو ليمعلا ىلإ لماكلا لوصولا حنمل Cisco ASA ىلإ Cisco ISE نم (CoA) ضيوفتلا لماكلاب VPN ةكبش

تانيوكتلا

Duo لوؤسم لخدم نيوكت -

.Duo لوؤسم لخدم ىلع ASA قيبطت نيوكتب مق ،مسقلاا اذه يف

1. ثحبلاو ،"قيبطت ةيامح < تاقيبطت" ىلإ لقنتلاو "Duo Admin Portal" ىلإ لوخدلا ليجست تهيامح" قوف رقنا ."ايتاذ ةفاضتسملا ،Duo لوصولا ةباوب عم 2FA" ةيامح عونب "ASA" نع تم ASA نيوكتل نيميلا ىصقأ ىلع

|      | admin-77d04ebc.duosecurity.com/applications/protect/types |                |   |           |    | ☆ 🖬                              |                          |               |  |
|------|---|----------------|---|-----------|----|----------------------------------|--------------------------|---------------|--|
| visc | Cisco Study 🗎 Cisco Tools [                               | Mix 🗎 S        | GourceFire 🗎 VPN 🗎 AAA 🗎 ASA                | 🗎 IFT 6.7 |    |                                  |                          |               |  |
|      | <b>DU</b> O   | ۹ Search       | n for users, groups, applications, or devic | ces       |    | a                                | Cisco   ID: 2010-1403-48 | ciscoduoblr 🗸 |  |
|      | Dashboard   | Dashboard      | > Applications > Protect an Application     |           |    |                                  |                          |               |  |
|      | Device Insight  | Prot           | ect an Applicatio                           | on        |    |                                  |                          |               |  |
|      | Policies  | (ASA)          |   |           |    |                                  |                          |               |  |
|      | Applications  |                |   |           |    |                                  |                          |               |  |
|      | Protect an Application                                    | Application    | n   | 28        | FA | Single Sign-On (if available)    | Documentation            | Action        |  |
|      | Single Sign-On<br>Users                                   | asana          | Asana                                       | 28        | FA | Duo Access Gateway (self-hosted) | Documentation E          | Protect       |  |
|      | Groups  |                |   |           |    |                                  |                          |               |  |
|      | Endpoints   | uhuhu<br>cisco | Cisco ASA                                   | 28        | FA | Duo Access Gateway (self-hosted) | Documentation ⊡          | Protect       |  |
|      | 2FA Devices   |                |   |           |    |                                  |                          |               |  |
|      | Administrators  | ahaha          | Cisco ASA                                   | 28        | FA | Single Sign-On (hosted by Duo)   | Documentation F          | Configure     |  |
|      | Reports   | cisco          |   |           |    |                                  |                          | guio          |  |

ASA ،يمحملا قيبطتلل "ةمدخلا دوزم تحت ةيلاتلا تامسلا نيوكتب مق .2

| يساسألا URL    | firebird.cisco.com  |  |
|----------------|---------------------|--|
| قافنألا ةعومجم | tg_saml             |  |
| ديربلا ةمس     | sAMAccountName،mail |  |

ةحفصلا لفسأ يف "ظفح" ىلع رقنا

| Device Insight<br>Policies  | Cisco ASA - Duo Access Gateway                          |   |  |  |  |
|---|---|---|--|--|--|
| Applications<br>Protect an Application  | Configure Cisco ASA Reset Secret Key                    |   |  |  |  |
| Single Sign-On<br>Users   | To set up this application,<br>Next step: Download your | To set up this application, install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions L'<br>Next step: Download your configuration file |  |  |  |
| Groups<br>Endpoints<br>2FA Devices  | Service Provider  |   |  |  |  |
| Administrators<br>Reports   | Base URL  | firebird.cisco.com  |  |  |  |
| Settings<br>Billing   | Tunnel Group  | TG_SAML<br>Enter the Tunnel Group you are protecting with SSO.  |  |  |  |
| Need Help?<br>Chat with Tech Support ਿੰ<br>Email Support<br>Call us at 1-855-386-2884 | Custom attributes                                       | Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.  |  |  |  |
| Account ID<br>2010-1403-48  | Mail attribute  | sAMAccountName,mail   |  |  |  |
| Deployment ID<br>DUO57 대  |   | The attribute containing the email address of the user.   |  |  |  |
| Helpful Links<br>Documentation 다  |   | Save Configuration  |  |  |  |

اەنييعت نكمي نكلو ةيضارتفا تاملعم نيوكتلا يقاب مدختست ،دنتسملا اذه يف ليمعلا تابلطتم ىلإ ادانتسا.

مسا رييغت لثم ،يلاحلا تقولا يف ديدجلا SAML قيبطتل ةيفاضإلا تادادعإلا طبض نكمي ةعومجم جەن نييعت وأ ،ةيتاذلا ةمدخلا نيكمت وأ ،ةيضارتفالا ةميقلا نم قيبطتلا.

Cisco ASA قيبطت تادادعإ ىلع لوصحلل "نيوكتلا فلم ليزنت" طابترالا قوف رقنا .3 ةقحاللا تاوطخلا يف ةيئانثلا لوصولا ةرابع ىلإ فلملا اذه ليمحت متي .(JSON فلمك)

| Device Insight<br>Policies                                     | Cisco ASA - Duo Access Gateway Authentication Log    Remove Application |   |  |  |  |
|--|---|---|--|--|--|
| Applications<br>Protect an Application                         | Configure Cisco ASA Reset Secret Key                                    |   |  |  |  |
| Single Sign-On<br>Users  | To set up this application, ins<br>Next step: Download your co          | stall the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions 🖄 |  |  |  |
| Groups<br>Endpoints  | Service Provider  |   |  |  |  |
| 2FA Devices<br>Administrators<br>Reports                       | Base URL  | firebird.cisco.com  |  |  |  |
| Settings<br>Billing  | Tunnel Group  | TG_SAML Enter the Tunnel Group you are protecting with SSO.   |  |  |  |
| Need Help?<br><u>Chat with Tech Support</u> C<br>Email Support | Custom attributes   | Vise this setting if your Duo Access Gateway authentication source uses non-standard attribute names.         |  |  |  |
| Call us at 1-855-386-2884<br>Account ID<br>2010-1403-48        | Mail attribute  | sAMAccountName,mail   |  |  |  |
| Deployment ID<br>DUO57 C<br>Helpful Links<br>Documentation C   |   | Save Configuration  |  |  |  |

4. وه امك اڻيدح هؤاشنا مت يذلا ASA قيبطت ودبي ،"تاقيبطتالا < تامولعمالا ةحول تحت هاندأ قروصلا يف حضوم:

| dmin-77d04ebc.duosecurity.com/applications |   |                                |                    |  |  |
|--|---|--------------------------------|--------------------|--|--|
| 🗎 Cisco Study 🗎 Cisco Tools                | 🗎 Mix 🗎 SourceFire 🗎 VPN 🗎 AAA                              | 🗎 ASA 📋 IFT 6.7                |                    |  |  |
| DUO  | <ul> <li>Search for users, groups, applications,</li> </ul> | or devices                     |                    | e Cisco   ID: 2010-1403-48 ciscoduoblr ∨ |  |
| Dashboard                                  | Dashboard > Applications                                    |                                |                    |  |  |
| Device Insight                             |   |                                |                    |  |  |
| Policies                                   | Applications  |                                |                    | SSO Setup Guide ☐ Protect an Application |  |
| Applications                               |   |                                |                    |  |  |
| Protect an Application                     |   |                                |                    | Export V Search                          |  |
| Single Sign-On                             |   |                                |                    |  |  |
| Users                                      | Name 🔺  | Туре                           | Application Policy | Group Policies                           |  |
| Groups                                     | Cisco ASA - Duo Access Gateway                              | Cisco ASA - Duo Access Gateway |                    |  |  |
| Endpoints                                  |   |                                |                    |  |  |
| 2FA Devices                                | 1 total   |                                |                    |  |  |

5. تەروصلا يف حضوم وە امك "مدختسم ةفاضإ < نيمدختسم ىلإ لقتنا:

دعب نع لوصولل AnyConnect ةقداصمل ەمادختسال "duouser" ىمسم مدختسم ءاشنإ يئاەنلا مدختسملا زاەج ىلع Duo Mobile طيشنتو



"فتاه ةفاضإ" رايخلا ددح ،ةروصلا يف حضوم وه امك فتاهلا مقر ةفاضإل.

|                     | ۹ Search for users, groups, a | applications, or devices             |
|---------------------|-------------------------------|--------------------------------------|
| Dashboard           | Dashboard > Users > duouser   | r > Add Phone                        |
| Device Insight      | Add Phone                     |                                      |
| Policies            | Add Flidile                   |                                      |
| Applications        | Learn more about Activatir    | ng Duo Mobile ⊡.                     |
| Users               |                               |                                      |
| Add User            |                               |                                      |
| Pending Enrollments | Туре                          | Phone                                |
| Bulk Enroll Users   |                               | Tablet                               |
| Import Users        |                               |                                      |
| Directory Sync      |                               |                                      |
| Bypass Codes        | Phone number                  | Show extension field                 |
| Groups              |                               | Optional. Example: "+91 91234 56789" |
| Endpoints           |                               |                                      |
| 2FA Devices         |                               | Add Phone                            |

نيعملا مدختسملل "Duo Mobile" طيشنت

#### **Device Info**

Learn more about Activating Duo Mobile 2.



ا يئاەنلا مدختسملا زاەج ىلع "Duo Mobile" تيبثت نم دكأت :ةظحالم IOS قزەجأل Duo قىبطتل يودىلا تيبثتلا مزەجأل Duo قىبطتل يودىلا تيبثتلا

:ةروصلا يف حضوم وه امك "Duo Mobile طيشنت زمر ءاشنإ" ددح

| DUO             | Q. Search for users, groups, applications, or devices ciscoduoblr ~   |
|-----------------|---|
| Dashboard       | Dashboard > Phone: > Activate Duo Mobile  |
| Device Insight  | Activate Due Mahile   |
| Policies        | Activate Duo Mobile   |
| Applications    | 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 |
| Users           | mobile device or authenticate via Duo Push.   |
| Groups          | Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.               |
| Endpoints       | Phone   |
| 2FA Devices     |   |
| Phones          |   |
| Hardware Tokens | Expiration 24 hours v after generation  |
| WebAuthn & U2F  |   |
| Administrators  | Generate Duo Mobile Activation Code   |
| Reports         |   |
| Settings        |   |

:ةروصلا يف حضوم وه امك "SMS ربع تاميلعت لاسرإ" ددح

| Dashboard                       | Dashboard > Phone: +91  | > Activate Duo Mobile  |  |  |  |
|---------------------------------|---|--|--|--|--|
| Device Insight                  | Activate Duo Mobile<br>A new Duo Mobile activation code has been generated, and any old credentials have been invalidated |  |  |  |  |
| Policies                        |   |  |  |  |  |
| Applications                    |   |  |  |  |  |
| Users                           | activation instructions to the  | user by SMS.   |  |  |  |
| Groups                          | Phone   |  |  |  |  |
| Endpoints                       |   |  |  |  |  |
| 2FA Devices                     | Installation instructions   | Send installation instructions via SMS                       |  |  |  |
| Phones                          |   | Welcome to Duo! Please install Duo Mobile from your app      |  |  |  |
| Hardware Tokens                 |   | store.   |  |  |  |
| WebAuthn & U2F                  |   |  |  |  |  |
| Administrators                  |   |  |  |  |  |
| Reports                         |   |  |  |  |  |
| Settings                        | Activation instructions   | Send activation instructions via SMS                         |  |  |  |
| Billing                         |   | To activate the app, tap and open this link with Duo Mobile: |  |  |  |
|                                 |   | 77d04ebc.duosecurity.com/activate/YB5ucEisJAq1YIBN5ZrT       |  |  |  |
| Need Help?                      |   |  |  |  |  |
| <u>Chat with Tech Support</u> 다 |   |  |  |  |  |
| Email Support                   |   |  |  |  |  |
| Call us at 1-855-386-2884       |   | Send Instructions by SMS br skip this step                   |  |  |  |
|                                 |   |  |  |  |  |

مسق يف مدختسملا باسحب Duo قيبطت طبر متيو ،SMS يف دوجوملا طابترالا قوف رقنا ةروصلا يف حضوم وه امك ،زاهجلا تامولعم:



(DAG) يئانثلا لوصولا ةرابع نيوكت -

كتكبش يف مداخ ىلع (DAG) ةيئانثلا لوصولاً ةرابع رشن .1



ليغشتلا ماظنل ةيئانثلا لوصولا ةباوب https://duo.com/docs/dag-linux

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

- "ةقداصملا ردصم ىلإ لقتنا ،يئانثلا لوصولا ةرابعل ةيسيئرلا ةحفصلا يف .2
- ظفح" قوف رقناو Active Directory ل ةيلاتلا تامسلا لخدأ ،"رداصملا نيوكت تحت .3 "تادادعإلا

#### **Configure Sources**

| onfigure authentication | a source settings below. Changes made to non-active authentication sources will take effect when made active.   |
|-------------------------|---|
| Source type             | Active Directory Specify the authentication source to configure.  |
| Status:                 | <ul> <li>✓ LDAP Bind Succeeded</li> <li>✓ Idap://10.197.243.110</li> </ul>  |
| Server                  | 10.197.       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          | CLEAR CLDAPS CLDAPS STARTTLS This setting controls whether the communication between Active Directory and the Duo Access Gateway is encrypted.  |
| Attributes              | SAMAccountName,mail<br>Specify attributes to retrieve from the AD server.<br>For example: sAMAccountName,mail.  |
| Search base             | CN=Users,DC=dmoudgil,DC=local   |
| Search attributes       | SAMAccountName<br>Specify attributes the username should match against.<br>For example: sAMAccountName,mail.  |
| Search username         | 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         | ••••• The password corresponding to the search username specified above.  |
|                         | Save Settings   |

نييعت" قوف رقناو "Active Directory" ك ردصملا عون ددح ،"طشن ردصم نييعت تحت 4. "طشن ردصم

| - | Set Active Source         |  |
|---|---------------------------|--|
|   | Specify the source that e | end-users will use for primary authentication. |
|   | Source type               | Active Directory                               |
|   |                           | Set Active Source                              |

فلم ليمحتب مق ،"قيبطت ةفاضإ" ةيعرفلا ةمئاقلا نمض ،"تاقيبطت ىلإ لقتنا .5 ليزنت مت ."نيوكتلا فلم" مسق لخاد Duo لوؤسم مكحت ةدحو نم هليزنت مت يذلا json. لوؤسم لخدم نيوكت نمض 3 ةوطخلا يف قباطملا json. فلم

## Applications

| Add Application  |  |  |  |  |  |
|--|--|--|--|--|--|
| Create a SAML application                              | Create a SAML application in the Duo Admin Panel. Then, download the provided configuration file and upload it here. |  |  |  |  |
| Configuration file Cisco ASA - Duo Access Gateway.json |  |  |  |  |  |
|  | Upload   |  |  |  |  |

"تاقيبطت" ةيعرفلا ةمئاقلا نمض رهظي ،حاجنب قيبطتلا ةفاضإ درجمب .6

| Applications                   |           |                 |        |  |  |  |
|--------------------------------|-----------|-----------------|--------|--|--|--|
| Name                           | Туре      | Logo            |        |  |  |  |
| Cisco ASA - Duo Access Gateway | Cisco ASA | dialia<br>cisco | Delete |  |  |  |

- ةداەشو XML فيرعت تانايب ليزنتب مق ،"فيرعتال تانايب" ةيعرفال ةمئاقال تحت .7 اقحال ASA ىلع اەنيوكت مت يتال ةيلاتال URL نيوانع ظحالو IdP
  - SSO ب صاخلا 1. URL
  - جورخلا ليجستل URL ناونع .2
  - نايكلا فرعم .3
  - أطخلل URL ناونع .4

| Metadata                                       |  | Recreate Certificate |
|--|--|----------------------|
| Information for configuring                    | applications with Duo Access Gateway. Download XML metadata.                             |                      |
| Certificate<br>Expiration<br>SHA-1 Fingerprint | /C=US/ST=MI/L=Ann Arbor/O=Duo Security, Inc. Download certificate<br>2030-04-30 18:57:14 |                      |
| SHA-256 Fingerprint                            |  | -                    |
| SSO URL  | https://explorer.cisco.com/dag/sam12/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-

يساسألا AnyConnect نيوكتو SAML IDP ةقداصمل ASA نيوكتل تامولعم مسقلا اذه رفوي. ةماعلا ةرظنلل نيوكتلا لغشت يتلا CLI و ASDM نيوكت تاوطخ دنتسملا رفوي.

ةيئانثلا لوصولا ةرابع ةداهش ليمحت .1

قوف رقنا ،"قدصملا عجرملا تاداەش < تاداەشلا ةرادا < ةزەجألا ةرادا < ليكشت ىلإ لقتنا .أ "ةفاضإ"

TrustPoint: duo\_access\_gateway مسا نيوكتب مق ،"ةداەشلا تيبثت ةحفص" يف .ب

ىلع رقنا ،اەديدحت درجمبو DAG ةداەشب طبترملا راسملا ديدحتل "ضارعتسإ" ىلع رقنا .ج "ةداەشلا تيبثت"

| Home       Configuration       Monitoring       Save       Refresh       Date:       Particle         Imagement       Device Management > Carclificate Management > CA Certificate Management > CA Certificate Management > CA Certificate       Install Certificate         Imagement       Management Access       Install Certificate       Install Certificate         Imagement       Management       Carcel       Install Certificate         Imagement       Management       Carcel       Install Certificate         Imagement       Management       Carcel       Imagement         Imagement       Carcel       Imagement       Carcel         Imagement       Carcel       Imagement       Imagement         Imagement       Carcel       Imagement  | ••   | Cisco ASDM   | 7.12(2) for ASA - 10.197.164.3  |                                  |            |
|--|--|--|---|----------------------------------|------------|
| Device Management       Install Certificate         Management Access       Install Certificate         System Image/Configuration       Install Certificate         Management Call-Home       Install from a file:       Uuc_Access_Gateway         System Image/Configuration       Install from a file:       Uuc_Access_Gateway         Install from a file:       Uuc_Access_Gateway       Browse         System Image/Configuration       Install from a file:       Uuc_Access_Gateway         Install from a file:       Uuc_Access_Gateway       Browse         System Image/Configuration       Install from a file:       Uuc_Access_Gateway         Install from a file:       Uuc_Access_Gateway       Paste certificate in PEM format:         Imagement Certificates       Paste certificate in PEM format:       Imagement         Imagement Certificates       Imagement       Imagement   | Home 🍕 Configuration 👰 Monitoring  | 🔚 Save 🔇 Refresh 🔇 1   | Back 🔘 Forward 🧳 Help Type to   | pic Go                           | c          |
| Install Certificate          Imagement Access       Install Certificate         Image/Configuration       Image/Configuration         Image/Configuration <t< td=""><td>O O Device Management</td><td>○ ○ ○ Configuration &gt; D</td><td>Device Management &gt; Certificate Ma</td><td>anagement &gt; CA Certificates</td><td></td></t<> | O O Device Management  | ○ ○ ○ Configuration > D  | Device Management > Certificate Ma  | anagement > CA Certificates      |            |
| Retry Period: 1     Retry Period: 1     Retry Count: 0     (Use 0 to indicate unlimited retries)     More Options     More Options     Help     Cancel   Install Certificate   | <ul> <li>Bevice Management</li> <li>Management Access</li> <li>Licensing</li> <li>System Image/Configuration</li> <li>High Availability and Scalability</li> <li>Logging</li> <li>Smart Call-Home</li> <li>Cloud Web Security</li> <li>Users/AAA</li> <li>Certificate Management</li> <li>Identity Certificates</li> <li>C Acertificates</li> <li>DHCP</li> <li>DNS</li> <li>REST API Agent</li> <li>Advanced</li> </ul> | Configuration > D Configuratio | evice Management > Certificate Milestall Certificate         Install Certificate         Duo_Access_Gateway         /Users/pusaxena/Desktop/dag.crt         ?EM format: | Browse                           | nils<br>RL |
| Retry Count: 0     (Use 0 to indicate unlimited retries)     More Options     More Options     More Options     More Options     More Options  |  | Retry Period:  | 1   | minutes                          |            |
| Device Setup   Image: Spice Setup   Image: Spice Setup   |  | Retry Count:   | 0   | (Use 0 to indicate unlimited ret | ries)      |
| Firewall       Image: Remote Access VPN  | Bevice Setup   |  |   | More Options                     |            |
| Remote Access VPN     Help     Cancel       Install Certificate  | 🗊 Firewall   |  |   |                                  |            |
| Site-to-Site VPN   | Remote Access VPN  |  | Help Cancel   | Install Certificate              |            |
|  | Site-to-Site VPN   |  |   |                                  |            |
| Device Management  | Device <u>M</u> anagement  |  |   |                                  |            |

AnyConnect يمدختسمل يلحملا IP عمجت ءاشنإ .2

ليمعلا) Access > Address (نيوكتال) Network (ليمعلا) Access > Address < (نيوانعلا) معلا) Access > Address Assignment (نيوانعلا نييعت) Address Pools (نيوانعلا نييعت)

|                           |      |   | Cisco ASDM 7.12(2) for ASA - 10.197.164.3  |       |
|---------------------------|------|---|--|-------|
|                           | Home | 🍇 Configuration 🧾 Monitoring 🖡  | 🚽 Save 🔇 Refresh 🔇 Back 🚫 Forward 🤗 Help Type topic Go   | cisco |
|                           | 00   | Remote Access VPN   | Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Ad  | dress |
| Bookmarks     Device List |      | Remote Access VPN         Introduction         Network (Client) Access         AnyConnect Connection Profiles         AnyConnect Client Profile         AnyConnect Client Profile         AnyConnect Client Profile         AnyConnect Client Profiles         Dynamic Access Policies         Group Policies         IPsec(IKEV1) Connection Profiles         IPsec(IKEV2) Connection Profiles         Secure Mobility Solution         Address Assignment         Address Pools         Advanced         Clientless SSL VPN Access         AAA/Local Users         Secure Desktop Manager         Certificate Management         Language Localization         Load Balancing         DHCP Server         DNS | Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Add<br>Pools<br>Configure named IP Address Pools. The IP Address Pools can be used in either a VPN IPsec(IKEv1) Connect<br>Profiles. AnyConnect Connection Profiles, Group Policies configuration | dress |
|                           |      | gite-to-Site VPN  |  |       |
|                           | ۵.   | Device <u>M</u> anagement   |  |       |
|                           |      | »<br>*  | Reset Apply  |       |

### AAA مداوخ ةعومجم نيوكت .3

يذلا ددحملا AAA مداخ ل.وح ل.يصافت مدقو AAA مداوخ ةعومجم ن.يوكتب مق ،مسقلا اذه يف .أ ضيوفتلا ذيفنتب موقي

تاعومجم < نويلحملا نومدختسملا/VPN > AAA دا نوصولا < نيوكت ىل لقتنا .ب "ةفاضا" قوف رقنا ،"AAA مداوخ

|           | Home 🖓 Configuration 🔯 Monitoring  | g 🔚 Save 🔇 Refresh 🔇 Back 💭 Forward 🦻 Help Type topic Go  | cisco          |
|-----------|--|---|----------------|
| 4         | O O O Remote Access VPN  | ○ ○ ○ Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups   |                |
| e Lis     | ? Introduction   | AAA Server Groups   |                |
| Devic     | <ul> <li>Interview (Client) Access</li> <li>Clientless SSL VPN Access</li> </ul>   | Server Group Protocol Accounting Mode Reactivation Mode Dead Time Max Failed Attempts   | Add            |
| Bookmarks | <ul> <li>AAA/Local Users</li> <li>AAA Server Groups</li> <li>LDAP Attribute Map</li> <li>Local Users</li> <li>Secure Desktop Manager</li> <li>Certificate Management</li> <li>Language Localization</li> <li>Load Balancing</li> <li>DHCP Server</li> <li>DHS</li> </ul> | AAA Server Group:   ISE     Protocol:   RADIUS     Accounting Mode:   Simultaneous     Simultaneous   Single     Reactivation Mode:   Depletion     Timed     Dead Time:   10 | Edit<br>Delete |
|           | Advanced   | Max Failed Attempts: 3  |                |
|           | ~  | Enable interim accounting update  |                |
|           |  | Update Interval: 24 Hours   | Add            |
|           |  | Fachla Astiva Directory Associationale  |                |
|           |  | Enable Active Directory Agent mode  | Edit           |
|           |  | ISE Policy Enforcement  | Delete         |
|           |  | Enable dynamic authorization  |                |
|           |  | Dynamic Authorization Port: 1700  | Move Up        |
|           |  | Use authorization only mode (no common password configuration required)   | Move Down      |
|           |  |   | Test           |
|           |  | VPN3K Compatibility Option *  |                |
|           | Pevice Setup   | Help Cancel OK  |                |
|           | 👬 Firewall   |   |                |
|           | Remote Access VPN  |   |                |
|           | Site-to-Site VPN   |   |                |
|           | Device Management  | LDAP Attribute Map  | *              |
|           | »  | <b>Reset</b> Apply  |                |

مقو "ةفاضإ" قوف رقنا ،"ةددحملا ةعومجملا يف مداوخلا" مسقلا نمض ،ةحفصلا سفن يف .ج مداخل IP ناونع ليصافت ريفوتب

|  | Save C Refresh   | Back C          | Forward 2 Help              | Type topic Co     |                  |                     | ab        |
|--|------------------|-----------------|-----------------------------|-------------------|------------------|---------------------|-----------|
| Remote Access V/PN   | Jave Kellesi     |                 | Torward S Help              | Type copie do     |                  | <b>C</b>            | CIS       |
|  | Configura        | tion > Remot    | <u>e Access VPN &gt; A/</u> | AA/Local Users    | > <u>AAA Ser</u> | ver Groups          |           |
| Network (Client) Access  | AAA Server Group | )S              |                             |                   |                  |                     | 1         |
| AnyConnect Connection Profiles   | Server Group     | RADIUS          | Accounting Mode<br>Single   | Reactivation Mode | Dead Time        | Max Failed Attempts | Add       |
| AnyConnect Customization/Localization  | LOCAL            | LOCAL           |                             |                   |                  |                     | Edit      |
| AnyConnect Client Profile  |                  |                 |                             |                   |                  |                     |           |
|  |                  |                 |                             |                   |                  |                     | Delete    |
| Group Policies   |                  |                 | Add AAA Serve               | r                 |                  |                     |           |
| <ul> <li>IPsec(IKEV1) Connection Profiles</li> <li>IPsec(IKEv2) Connection Profiles</li> </ul> | Server Group:    | ſ               | SE                          |                   |                  |                     |           |
| B Secure Mobility Solution   | Interface Name   | e:              | outside ᅌ                   |                   |                  |                     |           |
| Address Assignment   | Comme Norma a    |                 | 10 100 44 77                |                   |                  |                     |           |
| Assignment Policy     Address Pools  | Server Name o    | r IP Address:   | 10.106.44.77                |                   |                  |                     |           |
| Advanced   | Timeout:         |                 | 10 seconds                  |                   |                  |                     |           |
| Clientless SSL VPN Access  | RADIUS Param     | eters           |                             |                   |                  | (                   | Add       |
| AAA/Local Users  | Server Authe     | entication Port | : 1645                      |                   |                  | C C                 | Auu       |
| LDAP Attribute Map   | Senver Accou     | unting Port     | 1646                        |                   |                  |                     | Edit      |
| 🕼 Local Users  | Derver Accor     | inting Port.    | 1040                        |                   |                  |                     | Delete    |
| Gertificate Management   | Retry Interva    | u:              | 10 seconds                  |                   |                  |                     | Maus IIn  |
| anguage Localization   | Server Secre     | t Key:          |                             |                   |                  |                     | Move up   |
| Sector Contractions  | Common Pa        | ssword:         |                             |                   |                  |                     | Move Down |
| DHCP Server  | ACL Netmas       | k Convert:      | Standard                    |                   | 0                |                     | Test      |
|  | Microsoft Cl     | HAPv2 Capable   | e: 🔽                        |                   |                  |                     |           |
| A Device Setup   | SDI Messages     |                 |                             |                   |                  |                     |           |
| Firewall   | Message Ta       | able            |                             |                   |                  | *                   |           |
| <u>R</u> emote Access VPN  |                  | Help            | Cancel                      | ОК                |                  |                     |           |
| Site-to-Site VPN   |                  | Man             |                             |                   |                  |                     |           |
| Device Management  | LDAF Attribute   | nap             |                             |                   |                  |                     |           |
| »  |                  |                 | Res                         | et Apply          |                  |                     |           |

AnyConnect Client جمانرب نييعت .4

أ، ممادختسإ متيل Windows ل AnyConnect client 4.8.03052 جمانربل بيولا رشن ةروص نييعت أ ل WebVPN

جمانرب < (ليمعلا) ةكبشلا ىلإ لوصولا < VPN ىلإ دعب نع لوصولا < نيوكت ىلإ لقتنا .ب تةفاضإ" قوف رقنا ،"AnyConnect ليمع



5. ةجيتنك اهعفد متي يتلا اههيجوت داعملا (ACL) لوصولا يف مكحتلا ةمئاق نيوكتب مق iSE نم

رقنا ،(ACL) لوصولا يف مكحتلا ةمئاق ةرادإ < مدقتم < ةيامح رادج < نيوكت ىلإ لقتنا .أ ،تالاخدالا رەظت .اەەيجوت داعملا (ACL) لوصولا يف مكحتلا ةمئاق ةفاضإل ةفاضإ قوف :ەاندأ حضوم وە امك ،اەنيوكت درجمب

| •     |             |                           | La    | _      |   | Cisco ASDM 7.12(2) fo | or ASA - 10.             | 197.164.3         |                |                     |          |
|-------|-------------|---------------------------|-------|--------|---|-----------------------|--------------------------|-------------------|----------------|---------------------|----------|
| ð     | Home        | 🍕 Configuration 🦉 Monitor | ing 🔓 | - Sav  | e 💽 R   | efresh 🔇 Back 🔘       | Forward                  | Help Type topic G | D              |                     | cisco    |
| t     | 00          | O Firewall                |       | 00     | onfigur   | ation > Firewall > A  | <mark>lvanced</mark> > , | ACL Manager       |                |                     |          |
| Ce Li |             | Access Rules              | 4     | Add ·  | • 🖬 Edi   | t 📋 Delete 👌 🗲        | አ 🖻 🛍                    | - 🔍 Find 調 Export | -              |                     |          |
| Devi  |             | Service Policy Rules      | #     |        | Enabled   | Source                | Se                       | . Destination     | Security Group | Destination Service | Action   |
|       | , a         | AAA Rules                 | ▼ r   | edirec | t   |                       |                          |                   |                |                     |          |
|       |             | Filter Rules              | 1     | 1      | <ul> <li>Image: A set of the set of the</li></ul> | any                   |                          | any               |                | 👐 domain            | 🕴 Deny   |
| arks  | <b>0</b> -9 | Ethertype Rules           | 1     | 2      |   | any                   |                          | 🖳 10.197.243.116  |                | ₽ ip                | Oeny     |
| - k   |             | Public Servers            | 3     | 3      | <ul> <li>Image: A start of the start of</li></ul> | any                   |                          | any               |                | 💕 icmp              | Oeny     |
| Bo    |             | URL Filtering Servers     | 4     | 4      |   | any                   |                          | any               |                | <u>₽</u> ip         | 🖌 Permit |
|       | 2           | Threat Detection          |       | 5      |   | 🧼 any                 |                          | 🧼 any             |                | 🐵 http              | 🖌 Permit |
|       | ૢૻ          | ' Identity Options        |       |        |   |                       |                          |                   |                |                     |          |
|       | 4           | M Attribute Agent         |       |        |   |                       |                          |                   |                |                     |          |
|       | ▶ 55        | Botnet Traffic Filter     |       |        |   |                       |                          |                   |                |                     |          |
|       | ▶ 🗖         | Objects                   |       |        |   |                       |                          |                   |                |                     |          |
|       | Þ 🙆         | Unified Communications    |       |        |   |                       |                          |                   |                |                     |          |
|       | <b>v (B</b> | Advanced                  |       |        |   |                       |                          |                   |                |                     |          |
|       |             | Anti-Spoofing             |       |        |   |                       |                          |                   |                |                     |          |
|       | ►           | Certificate Management    |       |        |   |                       |                          |                   |                |                     |          |
|       |             | Stragment                 |       |        |   |                       |                          |                   |                |                     |          |
|       | P           |                           |       |        |   |                       |                          |                   |                |                     |          |
|       |             | TCP Options               |       |        |   |                       |                          |                   |                |                     |          |
|       |             | 🖏 Global Timeouts         |       |        |   |                       |                          |                   |                |                     |          |
|       |             | Printial Access           |       |        |   |                       |                          |                   |                |                     |          |
|       |             | ACL Manager               |       |        |   |                       |                          |                   |                |                     |          |
|       |             | Standard ACL              |       |        |   |                       |                          |                   |                |                     |          |
|       |             | Per-Session NAT Rules     |       |        |   |                       |                          |                   |                |                     |          |
|       | <u>_</u>    | <u>D</u> evice Setup      |       |        |   |                       |                          |                   |                |                     |          |
|       |             | F <u>i</u> rewall         |       |        |   |                       |                          |                   |                |                     |          |
|       | <b>3</b>    | Remote Access VPN         |       |        |   |                       |                          |                   |                |                     |          |
|       | <b>8</b>    | Site-to-Site VPN          |       | Collap | se All  | Expand All            |                          |                   |                |                     |          |
|       | 3           | Device <u>M</u> anagement |       |        |   |                       |                          |                   |                |                     |          |
|       |             | »<br>*                    |       |        |   |                       |                          | Reset Apply       | )              |                     |          |

- يلاحلا ةعومجملا جەن ةحص نم قىقى ا.
- أ. يف مضرع نكمي يذلاو يضارتفالا اقعومجملا جهن دادعإلاا اذه مدختسي. Remote Access VPN > Network (Client) Access > Group Policies"



- لاصتالا فيرعت فلم نيوكت .7
- AnyConnect ومدختسم هب لصتي ديدج لاصتا فيرعت فلم ءاشنإ .أ

### تافيصوت < (ليمعلا) ةكبشلا لوصو < VPN ىلإ دعب نع لوصولا < ليكشت ىلإ لقتنا .ب "ةفاضإ" ىلع رقنا ،"AnyConnect ليصوت

|  |   | Refresh 🖸 Bac   | k 💟 Forward 📔  | Help Type topic   | Go  | ci   |
|--|---|---|--|---|---|--|
| O O O Remote Access VPN  | ○ ○ ○ Configu   | ration > Remote   | e Access VPN > N   | letwork (Client) Ac   | cess > AnyConnect Conne   | ction Profiles   |
| <ul> <li>Introduction</li> <li>Network (Client) Access</li> <li>AnyConnect Connection Profiles</li> <li>AnyConnect Customization/Local</li> <li>AnyConnect Client Profile</li> </ul> | The security a<br>initial client d<br>tunnel as well<br>Access Interface  | ppliance automat<br>eployment requir<br>as SSL tunnel wit                       | tically deploys the<br>res end-user admi<br>th Datagram Trans  | e Cisco AnyConnect<br>nistrative rights. Th<br>sport Layer Security | VPN Client to remote users<br>le Cisco AnyConnect VPN Cli<br>(DTLS) tunneling options.  | upon connection. Th<br>ient supports IPsec (   |
| AnyConnect Client Software   | 🗹 Enable Ci   | sco AnyConnect \  | /PN Client access  | on the interfaces se  | elected in the table below  |  |
| Uphamic Access Policies  | SSL access mi   | ust be enabled if   | you allow AnyCon   | nect client to be lau   | inched from a browser (Web  | Launch) .  |
| IPsec(IKEv1) Connection Profiles   | Interface   | SSL Access  |  | IPsec (IKEv2) Acces   | S   |  |
| IPsec(IKEv2) Connection Profiles   |   | Allow Access  | Enable DTLS  | Allow Access  | Enable Client Services  | Device Certificat  |
| Secure Mobility Solution   | outside   |   |  |   |   |  |
| Address Assignment   |   |   |  |   |   | Port Settings  |
| Advanced   |   |   |  |   |   |  |
| DHCP Server  | Shutdown  | portal login page   | 2.   |   |   |  |
| 뤊 DNS<br>졨 Advanced  | Connection Prof   | lies  |  |   |   |  |
| 屦 DNS<br>蹘 Advanced  | Connection Prof<br>Connection pu<br>from certificat   | rofile (tunnel grou<br>te to connection   | up) specifies how profile <u>here</u> .  | user is authenticate  | d and other parameters. You   | ı can configure the r  |
| 愿 DNS<br>정 Advanced  | Connection Prof<br>Connection prof<br>from certificat   | rofile (tunnel grou<br>te to connection<br>dit <u>î</u> Delete                  | up) specifies how<br>profile <u>here</u> .<br>Find:  | user is authenticate  | and other parameters. You   | ı can configure the r  |
| DNS Advanced   | Connection Prof<br>Connection pu<br>from certificat   | rofile (tunnel grou<br>te to connection<br>Edit î Delete                        | up) specifies how<br>profile <u>here</u> .<br>Find:<br>IPsec Enabled   | user is authenticate  | d and other parameters. You Match Case Authentication Method  | can configure the r  |
| DNS Advanced   | Connection Prof<br>Connection pi<br>from certificat<br>Add 2 E  | rofile (tunnel grou<br>te to connection<br>Edit î Delete<br>SSL Enabled         | up) specifies how<br>profile <u>here</u> .<br>Find:<br>IPsec Enabled   | user is authenticate  | d and other parameters. You Match Case Authentication Method AAA(LOCAL)   | a can configure the r<br>Group Policy<br>DfltGrpPolicy   |
| Advanced   | Connection Prof<br>Connection pi<br>from certificat<br>Add 2 t<br>Name<br>DefaultRAGr<br>DefaultWEBV            | rofile (tunnel groi<br>te to connection<br>Edit î Delete                        | up) specifies how<br>profile <u>here</u> .<br>Find:<br>IPsec Enabled   | Aliases   | d and other parameters. You Match Case Authentication Method AAA(LOCAL) AAA(LOCAL)  | a can configure the a<br>Group Policy<br>DfltGrpPolicy<br>DfltGrpPolicy  |
| DNS Advanced  Device Setup  Firewall   | Connection Prof<br>Connection pu<br>from certificat<br>Add 2 I<br>Name<br>DefaultRAGr<br>DefaultWEBV<br>TG_SAML | Trofile (tunnel groi<br>te to connection<br>Edit 👚 Delete I<br>SSL Enabled<br>V | up) specifies how<br>profile <u>here</u> .<br>Find:<br>IPsec Enabled<br>V  | USER IS AUTHENTICATE  | d and other parameters. You         Match Case         Authentication Method         AAA(LOCAL)         AAA(LOCAL)         Sami | can configure the r<br>Group Policy<br>DfltGrpPolicy<br>DfltGrpPolicy<br>DfltGrpPolicy                           |
| DNS<br>Advanced Device Setup Firewall Site-to-Site VPN   | Connection Prof<br>Connection p<br>from certifical<br>Add I I<br>Name<br>DefaultRAGr<br>DefaultWEBV<br>TG_SAML  | URL take preceden   | up) specifies how<br>profile <u>here</u> .<br>Find:<br>IPsec Enabled<br>ence if group URL<br>tches the certifica | Aliases<br>SAML_Users<br>and certificate map<br>te map will be used | and other parameters. You         Match Case         Authentication Method         AAA(LOCAL)         AAA(LOCAL)         Sami   | a can configure the a<br>Group Policy<br>DfltGrpPolicy<br>DfltGrpPolicy<br>DfltGrpPolicy<br>profiles. Otherwise, |

### ليصوتلا فيرعت فلمب ةطبترملا ةيلاتلا ليصافتلا نيوكتب مق ج:

| مسالا                 | tg_saml       |
|-----------------------|---------------|
| ةراعتسم ءامسأ         | SAML_Users    |
| ةقيرط                 | لماس          |
| AAA مداوخ ةعومجم      | يلحم          |
| ءالمعلا نيوانع تاعمجت | AC_POOL       |
| ةعومجملا جەن          | DfltGrpPolicy |

|                   |                              |   | _        |
|-------------------|------------------------------|---|----------|
| Basic<br>Advanced | Name:                        | TG_SAML   |          |
| Advanced          | 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 clien         | t protocol  |          |
|                   | ✓ Enable IPsec(IKEv2) c      | lient protocol  |          |
|                   | DNS Servers:                 |   |          |
|                   | WINS Servers:                |   |          |
|                   | Domain Name:                 |   |          |
|                   |                              |   |          |
|                   |                              |   |          |
| Find:             |                              | Next Previous   |          |
|                   |                              | Help Cancel OK  |          |
|                   |                              |   |          |

حضوم وه امك ودبت يتلا SAML ةيوه رفوم ليصافت نيوكتب مق ،ةحفصلا سفن يف .د هاندأ:

| فرعم<br>نايك<br>نيدرشملا<br>ايلخاد | https://explorer.cisco.com/dag/saml2/idp/metadata.php                                     |
|------------------------------------|---|
| ناونع<br>URL<br>ليجستل<br>لوخدلا   | https://explorer.cisco.com/dag/saml2/idp/SSOService.php                                   |
| ناونع<br>URL<br>ليجستل<br>جورخلاا  | https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explore |
| URL<br>يساسألا                     | https://firebird.cisco.com  |

|  | Add SSO Server  |
|--|---|
| IDP Entity ID:                                 | https://explorer.cisco.com/dag/saml2/idp/metadata.php       |
| Settings                                       |   |
| Sign In URL:                                   | https 📀 :// explorer.cisco.com/dag/saml2/idp/SSOService.php |
| Sign Out URL:                                  | https ᅌ :// explorer.cisco.com/dag/saml2/idp/SingleLogoutSe |
| Base URL                                       | https 📀 :// firebird.cisco.com                              |
| Identity Provider Certificate                  | Duo_Access_Gateway:o=Duo Security Inc., I=Ann Ar            |
| Service Provider Certificate:                  | ID_CERT:cn=firebird.cisco.com:cn=SHERLOCK-CA, dc=c          |
| Request Signature:                             | None 📀  |
| Request Timeout:                               | 1200 seconds (1-7200)                                       |
| Enable IdP only accessible on Internal Network |   |
| Request IdP re-authentication at login         |   |
| Help   | Cancel  |

ليوختلل AAA مداخ فيرعتب مق ،لاصتالا فيرعت فلمل مدقتملا مسقلا نمض f.

"ةفاضإ" قوف رقناو "ضيوفت < مدقتم ىلإ لقتنا

| Basic  | Authorization Server Group  |
|--|---|
| <ul> <li>Advanced</li> <li>General</li> </ul>      | Server Group: ISE 🗘 Manage  |
| Client Addressing<br>Authentication                | Users must exist in the authorization database to connect   |
| Secondary Authentic<br>Authorization<br>Accounting | Interface-specific Authorization Server Groups   Add Edit Delete   Assign Authorization Server Group to Interface |
| Group Anas/Group C                                 | Interface: Outside O<br>Server Group: ISE O Manage  |
|  | Help Cancel OK  |

لاصتالل راعتسملا مسالا فيرعتب مق ،ةعومجملل راعتسملا مسالا تحت .G

"ةفاضإ" قوف رقناو "URL/ةعومجملل راعتسملا مسالا < مدقتم ىلإ لقتنا

Edit AnyConnect Connection Profile: TG\_SAML

| Basic<br>▼ (Advanced)<br>General   | <ul> <li>Enable the display of Radius Reject-Messa</li> <li>Enable the display of Securld messages or</li> </ul>   | ge on the login screen when authentication is rejected  |
|--|--|---|
| Client Addressing<br>Authentication<br>Secondary Authentication<br>Authorization<br>Accounting | Connection Aliases<br>This SSL VPN access method will present a list<br>the Login Page Setting in the main panel to co<br>Add Delete (The table is in-line edita | of aliases configured for all connection profiles. You mus mplete the configuration.<br>ble.) 1 |
| Group Allas/Group UKL  | Add Connection Alias   |   |
|  | Help Cancel OK   | , the connection profile, without the need for user s   |

(CLI) رماوألا رطس ةەجاو ىلع ەاندأ لكشلا سفن وەو ،ASA نيوكت لامتكا ىلإ اذە يدؤي .ح

```
1
hostname firebird
domain-name cisco.com
1
1
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
Т
!-----Client pool configuration------Client
I
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
I
1 -
   -----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
I
!-----AAA server configuration-----
Т
aaa-server ISE protocol radius
authorize-only
 interim-accounting-update periodic 1
 dynamic-authorization
aaa-server ISE (outside) host 10.106.44.77
key *****
L
!----Configure Trustpoint for Duo Access Gateway Certificate----
L
crypto ca trustpoint Duo_Access_Gateway
enrollment terminal
crl configure
1
!-----Configure Trustpoint for ASA Identity Certificate-----
I
crypto ca trustpoint ID_CERT
 enrollment terminal
 fqdn firebird.cisco.com
 subject-name CN=firebird.cisco.com
```

0 0 0

```
ip-address 10.197.164.3
 keypair ID_RSA_KEYS
no ca-check
crl configure
I
!-----Enable AnyConnect and configuring SAML authentication-----
1
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/sam12/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
1
 -----Group Policy configuration------Group Policy
I
ļ
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
ļ
    -----Tunnel-Group (Connection Profile) Configuraiton-----
1
T
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
i
```

ISE نيوكت-

ةكبش زاهجك Cisco ASA ةفاضإ .1

```
ة الما تراوم < قرادا تحت".
نيوكتو "RADIUS ققداصم تادادعا" تحتو نرتقملا IP ناونعو قكبشلا زاهج مسا نيوكتب مق
"ظفح" ىلع رقناو "كرتشملا رسلا"
```

| Notwor | A Devices   |   |
|--------|---|---|
| Networ |   |   |
|        |   |   |
|        |   |   |
|        |   |   |
|        | IP Address • IP : 10.197.164.3  | / 32  |
|        |   |   |
|        | * Device Profile  |   |
|        |   |   |
|        | Software Version  |   |
|        |   |   |
|        | * Network Device Group  |   |
|        | Location All Locations 📀 Set To Default   |   |
|        | IPSEC No Set To Default   |   |
|        | Device Type All Device Types 📀 Set To Default   |   |
|        |   |   |
|        |   |   |
|        |   |   |
|        | RADIUS UDP Settings   |   |
|        | Protocol  | RADIUS  |
|        | * Shared Secret   | ••••• Show  |
|        |   |   |
|        | Use Second Shared Secret  |   |
|        | Use Second Shared Secret  | Show  |
|        | Use Second Shared Secret<br>CoA Port  | Image: Show       Image: Show       Image: Show       Set To Default  |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)  | Image: Show       1700       Set To Default   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)<br>DTLS Required<br>Shared Secret  | Image: Show       Image: Show <t< th=""></t<>   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (2)<br>DTLS Required<br>Shared Secret<br>CoA Port  | Image: Constraint of the second se                     |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA   | Image: Show   Image: Show </th  |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings 7<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name   | Image: Show   Image: Show </th  |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name   | Image: Show   Image: Show   Image: Image: Show   Image: Image: Image: Show   Image: Ima   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings   | Image: Show   Image: Show   Image: Image: Show   Image: Image: Show   Image: Image: Show   Image: Image: Image: Image: Image: Show   Image: Im   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key   | Image: Show   1700   Set To Default   Image: Set To Default   Image: Set To Default   Select if required (optional)   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings ()<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key<br>* Message Authenticator Code Key  | Image: Show   Image: Image: Image: Show   Image: Imag                                     |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings ()<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key<br>* Message Authenticator Code Key<br>Key Input Format  | Image: Show   Image: I                   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings ()<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key<br>* Message Authenticator Code Key<br>Key Input Format  | Image: Constraint of the second s |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings ()<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key<br>* Message Authenticator Code Key<br>Key Input Format  | Image: Show   Image: I                   |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings (i)<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key<br>* Message Authenticator Code Key<br>Key Input Format   | Image: Show   Image: Show </th  |
|        | Use Second Shared Secret<br>CoA Port<br>RADIUS DTLS Settings ()<br>DTLS Required<br>Shared Secret<br>CoA Port<br>Issuer CA of ISE Certificates for CoA<br>DNS Name<br>General Settings<br>Enable KeyWrap<br>* Key Encryption Key<br>* Message Authenticator Code Key<br>Key Input Format<br>• TACACS Authentication Settings<br>• SNMP Settings | image: show   1700   Set To Default   image: show   Show   Show   ASCII   HEXADECIMAL   |

#### عضولا تاثيدحت رخآ تيبثت .2

#### "نآلا ثيدجت" قوف رقناو "تاثيدجت < ةيعضو < تادادعإ < ماظن < ةرادإ يلإ لقتنا

| Posture Updates                       |   |   |  |  |  |  |  |  |
|---------------------------------------|---|---|--|--|--|--|--|--|
| • Web                                 | O Offline   |   |  |  |  |  |  |  |
| * Update Feed URL                     | https://www.cisco.com/web                               | /secure/spa/posture-update.xml Set to Default |  |  |  |  |  |  |
| Proxy Address                         | 72.163.217.104  |   |  |  |  |  |  |  |
| Proxy Port                            | 80  | HH MM SS                                      |  |  |  |  |  |  |
| Automatically che                     | ck for updates starting from i                          | nitial delay 06 - 00 - 18 - every 2 hours     |  |  |  |  |  |  |
| Save                                  | date Now Reset  |   |  |  |  |  |  |  |
| _                                     |   |   |  |  |  |  |  |  |
|                                       |   |   |  |  |  |  |  |  |
| ▼ Update Informa                      | ation   |   |  |  |  |  |  |  |
| Last successful upd                   | ate on  | 2020/05/07 15:15:05                           |  |  |  |  |  |  |
| Last update status s                  | since ISE was started                                   | No update since ISE was started.              |  |  |  |  |  |  |
| Cisco conditions version 224069.0.0.0 |   |   |  |  |  |  |  |  |
| Cisco AV/AS suppor                    | Cisco AV/AS support chart version for windows 171.0.0.0 |   |  |  |  |  |  |  |
| Cisco AV/AS suppor                    | Cisco AV/AS support chart version for Mac OSX 91.0.0.0  |   |  |  |  |  |  |  |
| Cisco supported OS                    | version   | 41.0.0.0                                      |  |  |  |  |  |  |

ISE ىلع AnyConnect نم ثبلاو لابقتسالاا ةدحو رشن ةمزحو قفاوتالا ةدحو ليمحت .3

قوف رقنا ."دراوملا < ليمعلا دادمإ < جئاتنلا < ةسايسلا رصانع < ةسايس ىلإ لقتنا "ىل ادانتسا "Cisco عقوم نم ليكولا دراوم" وأ "يلحملا صرقلا نم ليكولا دراوم" ددحو "ةفاضإ عقوم وأ ةيلحملا لمعلا قطحم نم تافلملا راضحإ متيس ناك اذإ ام

نم ةمدقملا مزحلا" ددح ،ةئفلا نمض ةيلحملا لمعلا ةطحم نم تافلم ليمحتل ،ةلاحلا هذه يف Cisco"، الاسرا" قوف رقناو ةبولطملا مزحلا ددحو "ضارعتسإ" قوف رقناو".

دنتسملا اذه مدختسي "AnyConnect-win-4.3.1012.6145-isecompliance-webdeploy-k9.pkg" و لاثتما ةدحوك "AnyConnect-win-4.8.03052-webdeploy-k9.pkg"و ل نم ثبلاو AnyConnect.

#### Agent Resources From Local Disk > Agent Resources From Local Disk

Agent Resources From Local Disk

| Category | Cisco Provided Packages Browse anyconnect-win-4.8.03 | 3052-webdeploy-k9.pkg    |            |                                 |
|----------|--|--------------------------|------------|---------------------------------|
|          | <ul> <li>AnyConnect Uploaded Resource</li> </ul>     | S                        |            |                                 |
|          | Name   | Туре                     | Version    | Description                     |
|          | AnyConnectDesktopWindows 4.8.30                      | AnyConnectDesktopWindows | 4.8.3052.0 | AnyConnect Secure Mobility Clie |



AnyConnect Posture فيرعت فلم ءاشنإ .4

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

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

### ISE Posture Agent Profile Settings > Anyconnect Posture Profile

| * Name:     | Anyconnect Posture Profile |     |
|-------------|----------------------------|-----|
| Description | :                          |     |
|             |                            | 11. |

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<br>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<br>without port must be comma-separated and with<br>colon in between the IP address/FQDN and the<br>port. Example: IPaddress/FQDN:Port (Port<br>number should be the same, specified in the<br>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<br>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<br>supported range is between 10s - 600s.  | Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously<br>connected PSNs) by sending the discovery packets till this max time limit is reached |

#### AnyConnect نيوكت ءاشنإ .5

ىلع رقنا ."دراوملا < ليمعلا دادمإ < جئاتنلا < ةسايسلا رصانع < ةسايس ىلإ لقتنا .أ تيوكت" ددحو "ةفاضإ"

ةبولطملا قفاوتلا ةدجو ددجو ،نيوكتلا مسا لخدأو ،AnyConnect ةمزح ددح .ب

"ريراقتلا دادعإو صيخشتلا ةادأ" نم ققحت ،"ةيطمنلا AnyConnect ةدحو ديدحت" تحت .ج

"ظفح" قوف رقناو عضولا فيرعت فلم ددح ،"فيرعتلا فلم ديدجت" تحت .د

#### AnyConnect Configuration > AnyConnect Configuration



#### 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 🔹 🔻 | D |
| VPN                       | <b>*</b>                       |   |
| Network Access Manager    | •                              |   |
| Web Security              | •                              |   |
| AMP Enabler               | *                              | ] |
| Network Visibility        | *                              | 1 |
| Umbrella Roaming Security | *                              | ] |
| Customer Feedback         | *                              | 1 |

ليمعلا ديوزت ةسايس ءاشنإ .6

"ليمعلا دادمإ < ةسايس ىلإ لقتنا .أ

"ەالءأ ةدعاق جاردإ" ددح مث "ريرحت" قوف رقنا .ب

"ليكولا" نمض) جئاتنلا تحتو ،بولطمل ليغشتل ماظن ددحو ،ةدعاقل مسا لخدا .ج
 "ظفح" قوف رقناو 5 ةوطخلا يف مؤاشنإ مت يذلا "AnyConnect نيوكت" ددح ،("ليكول نيوكت"

| dent                     | tity Services Engine                                   | Home                                   | Context Visibili                             | ty       | Operations                               | ▼ Policy                  | Administration   | Work Centers |      |  | License Warning 🔺 | ् ( | 0        |
|--------------------------|--|--|--|----------|--|---------------------------|------------------|--------------|------|--|-------------------|-----|----------|
| olicy Sets               | Profiling Posture                                      | Client Provis                          | ioning + Policy E                            | lements  | 3  |                           |                  |              |      |  |                   |     |          |
| ent Provi                | isioning Policy<br>nt Provisioning Policy t            | to determine wh                        | at users will receive                        | upon log | gin and user sess                        | ion initiation:           |                  |              |      |  |                   |     |          |
| Agent Conf<br>Native Sup | figuration: version of ago<br>plicant Configuration: v | gent, agent profi<br>wizard profile an | le, agent compliance<br>d/or wizard. Drag an | d drop r | e, and/or agent co<br>rules to change th | ustomization<br>ne order. | package.         |              |      |  |                   |     |          |
|                          | Rule Name  |  | Identity Groups                              |          | Operating Syst                           | iems                      | Other Condition  | ons          |      | Results  |                   |     |          |
|                          | IOS  | ł                                      | Any  | and      | Apple iOS All                            | 1                         | and Condition(s) |              | then | Cisco-ISE-NSP  |                   |     | Edit   • |
|                          | Android  | 1                                      | Any  | and      | Android                                  | 1                         | and Condition(s) |              | then | Cisco-ISE-NSP  |                   |     | Edit   • |
| 1                        | Windows_10   | 1                                      | Any  | and      | Windows 10 (/                            | All) i                    | and Condition(s) |              | then | AnyConnect<br>Configuration  |                   |     | Edit   🔻 |
|                          | Windows  | 1                                      | Any  | and      | Windows All                              | 1                         | and Condition(s) |              | then | CiscoTemporalAgentWi<br>ndows 4.7.00135 And<br>WinSPWizard 2.5.0.1<br>And Cisco-ISE-NSP    |                   |     | Edit   🔻 |
|                          | MAC OS   | 1                                      | Any  | and      | Mac OSX                                  | 1                         | Ind Condition(s) |              | then | CiscoTemporalAgentOS<br>X 4.7.00135 And<br>MacOxXSPWizard<br>2.10.42 And Cisco-ISE-<br>NSP |                   |     | Edit   🔻 |
| <b>~</b>                 | Chromebook   | 1                                      | Any  | and      | Chrome OS A                              |                           | and Condition(s) |              | then | Cisco-ISE-Chrome-NSP   |                   |     | Edit   • |
|                          |  |  |  |          |  |                           |                  |              |      |  |                   |     |          |
| ve Res                   | set  |  |  |          |  |                           |                  |              |      |  |                   |     |          |

#### ةلاح ءاشنإب مق .7

فلم ةلاح < ةيعضو < طورش < ةسايس رصانع < ةسايس ىلإ لقتنا .أ

ماظن مث ،"VPN\_Posture\_File\_CHECK" طرشلاا مسا نيوكتب مقو "ةفاضإ" قوف رقنا .ب ك فلملا راسمو ،"FilePresence" ك فلملا عونو ،"Windows 10(All) ك بولطملا ليغشتلا "ABSOLUTE\_PATH" ك فلملا مساو لماكلا راسملا مث ،"ABSOLUTE\_PATH" "دوجوم"

فلم طرشك صارقألاا كرحم :C نمض "custom.txt" مساب فلم دوجو لاثملاا اذه مدختسي .ج

| cisco Identity Services Engine   | Home   | ➤ Operations ▼ Policy | Administration | ➤ Work Centers |
|--|--|-----------------------|----------------|----------------|
| Policy Sets Profiling Posture Cl                                       | lient Provisioning - Policy Element  | ts                    |                |                |
| Dictionaries - Conditions - Result                                     | ts   |                       |                |                |
| C Library Conditions<br>Smart Conditions<br>Time and Date<br>Profiling | File Conditions List > VPN_Postu<br>File Condition<br>* Name VPN_<br>Description<br>* Operating System Win | Posture_File_Check    |                |                |
| Posture  | Compliance Module Any v  | ersion                |                |                |
| Anti-Maiware Condition   | * File Type  | ixistence 🔹           | ۲              |                |
| Anti-Virus Condition   | * File Path  | OLUTE_PATH            | C:\custom.txt  |                |
| Application Condition  | * File Operator Exist  | rs 🔹                  |                |                |
| Compound Condition   | Save   |                       |                |                |
| Disk Encryption Condition  |  |                       |                |                |
| File Condition   |  |                       |                |                |

عضولا حالصإ ءارجإ ءاشنإ .8

ءارجإ ءاشنال "ةجلاعم تاءارجإ < ةيعضو < جئاتن < ةسايس رصانع < ةسايس ىل لقتنا مت حالصإ تاءارجإك "طقف ةلاسرلا صن" دنتسملا اذه مدختسي .قفاوتم فلم ةجلاعم .قيلاتا ةوطخلا يف اهنيوكت

عضولا تابلطتم ةدعاق ءاشنإ .9

"تابلطتم < ةيعضو < جئاتن < ةسايس رصانع < ةسايس ىلإ لقتنا .أ

"ديدج بلطتم جاردإ" ددح مث "ريرحت" قوف رقنا .ب

ك بولطملا ليغشتلا ماظنو ،"VPN\_Posture\_Requirements" طرشلا مسا نيوكتب مق .ج "AnyConnect" ك عضولا عونو ،"ثدحأ رادصإ وأ 4.x" ك قفاوتلا ةدحوو ،"(All)Windows 10

تاءارجا تحتو (7 ةوطخلا يف اهؤاشنا مت يتلا) "VPN\_Posture\_File\_CHECK" ك طورش .د ل قصصخملا قلاسرلا لخدأو "طقف قلاسرلا صن" ك ءارجإلا ددح ،حالصإل

| cisco Identity Services Engine          | Home   | Operations     Policy   | Administration  |   |  | License Warning 🔺                         | ୍ ତ | •        | φ. |
|---|--|---|---|---|--|---|-----|----------|----|
| Policy Sets Profiling Posture Cl        | ient Provisioning  Policy Element                          | ents  |   |   |  |   |     |          |    |
| Dictionaries                            | s  |   |   |   |  |   |     |          |    |
| 0                                       |  |   |   |   |  | (w  |     |          | ٩  |
| Authentication                          | Requirements   |   |   |   |  |   |     |          |    |
| h Authorization                         | quirement_win  | Operating System  | Compliance Module   | Posture Type                                  | Conditions                                 | Remediations Actions                      |     |          |    |
| > Ruthingation                          | Default_Hardware_Attri<br>quirement_Mac                    | butes_Re for Mac OSX  | using 4.x or later  | using AnyConnect                              | met if Hardware_Attributes_Ch<br>eck       | then Select Remediations                  |     | Edit   🔻 |    |
| Profiling                               | Default_Firewall_Requir                                    | rement_W for Windows All  | using 4.x or later  | using AnyConnect                              | met if Default_Firewall_Conditi<br>on_Win  | then Default_Firewall_Remedi<br>ation_Win |     | Edit   🕶 |    |
| (* Posture                              | Default_Firewall_Requir<br>ac                              | rement_M for Mac OSX  | using 4.x or later  | using AnyConnect                              | met if Default_Firewall_Conditi<br>on_Mac  | then Default_Firewall_Remedi<br>ation_Mac |     | Edit   🕶 |    |
| <ul> <li>Remediation Actions</li> </ul> | USB_Block_temporal   | for Windows All   | using 4.x or later  | using Temporal Agent                          | met if USB_Check                           | then Message Text Only                    |     | Edit   🔻 |    |
| Requirements                            | Any_AM_Installation_W<br>ral                               | fin_tempo for Windows All   | using 4.x or later  | using Temporal Agent                          | met if ANY_am_win_inst                     | then Message Text Only                    |     | Edit   🕶 |    |
| Client Provisioning                     | Any_AM_Installation_M<br>ral                               | lac_tempo for Mac OSX   | using 4.x or later  | using Temporal Agent                          | met if ANY_am_mac_inst                     | then Message Text Only                    |     | Edit   🕶 |    |
|   | Default_AppVis_Requir<br>n_temporal                        | ement_Wi for Windows All  | using 4.x or later  | using Temporal Agent                          | met if Default_AppVis_Conditio<br>n_Win    | then Select Remediations                  |     | Edit   🕶 |    |
|   | Default_AppVis_Requir<br>ac_temporal                       | ement_M for Mac OSX   | using 4.x or later  | using Temporal Agent                          | met if Default_AppVis_Conditio<br>n_Mac    | then Select Remediations                  |     | Edit   🔻 |    |
|   | Default_Hardware_Attri<br>quirement_Win_tempor             | butes_Re for Windows All<br>al  | using 4.x or later  | using Temporal Agent                          | met if Hardware_Attributes_Ch<br>eck       | then Select Remediations                  |     | Edit   🕶 |    |
|   | Default_Hardware_Attri<br>quirement_Mac_tempor             | butes_Re for Mac OSX<br>ral   | using 4.x or later  | using Temporal Agent                          | met if Hardware_Attributes_Ch<br>eck       | then Select Remediations                  |     | Edit   🕶 |    |
|   | Default_Firewall_Requi<br>in_temporal                      | rement_W for Windows All  | using 4.x or later  | using Temporal Agent                          | met if Default_Firewall_Conditi<br>on_Win  | then Default_Firewall_Remedi<br>ation_Win |     | Edit   🕶 |    |
|   | Default_Firewall_Requi<br>ac_temporal                      | rement_M for Mac OSX  | using 4.x or later  | using Temporal Agent                          | met if Default_Firewall_Conditi<br>on_Mac  | then Default_Firewall_Remedi<br>ation_Mac |     | Edit   🕶 |    |
|   | VPN_Posture_Requirer                                       | ment for Windows 10 (All)   | using 4.x or later  | using AnyConnect                              | met if VPN_Posture_File_Chec               | then Message Text Only                    |     | Edit   🕶 |    |
|   | Note: Remediation Action is fil<br>Remediation Actions are | tered based on the operating system<br>e not applicable for Application Condi | and stealth mode selection.<br>ions (configured using the Provision B | y Category or Provision By Everything options | s), Hardware Conditions, and External Data | source conditions.                        |     |          |    |
|   | Save Reset   |   |   |   |  |   |     |          |    |

عضولا ةسايس ءاشنإ .10

"ةيعضو < تاسايس ىلإ لقتنا .أ

```
ك بولطملا ليغشتلا ماظنو ،"VPN_Posture_POLICY_WIN" ك ةدعاقلا مسا نيوكت .ب
"Windows 10(All" ك عضولا عونو ،"ثدحأ رادصإ وأ 4.x" ك قفاوتلا ةدحوو ،"Windows 10(All"
9 ةوطخلا يف اهنيوكت مت امك "VPN_Posture_Require" ك تابلطتملاو
```

| cisco    | Identity Se  | ervices Engin    | e Home                             | <ul> <li>Context Vis</li> </ul> | ibility > Ope     | rations 🔽  | Policy      | Administration | •      | Work Centers     |     |                |                 |    |    | License Warning 🔺  |      |          |
|----------|--------------|------------------|------------------------------------|---------------------------------|-------------------|------------|-------------|----------------|--------|------------------|-----|----------------|-----------------|----|----|--|------|----------|
| Policy   | Sets Prof    | filing Posture   | Client Provisio                    | oning + Polic                   | y Elements        |            |             |                |        |                  |     |                |                 |    |    |  |      |          |
|          |              |                  |                                    |                                 |                   |            |             |                |        |                  |     |                |                 |    |    |  |      |          |
| Postur   | re Policy    |                  |                                    |                                 |                   | No.        |             |                |        |                  |     |                |                 |    |    | -  | <br> | 0        |
| Define t | ne Posture P | olicy by contigu | ring rules based of                | n operating syst                | em and/or other c | onditions. |             |                |        |                  |     |                |                 |    |    | (  |      |          |
| •        | Ctatue       | Policy Options   | Pule Name                          |                                 | Identify Grou     | ne         | Operating S | wiene          | 0      | omnliance Module |     | Posture Tune   | Other Condition |    |    | Requirements   |      |          |
|          | 0            | Policy Options   | Default AppVis                     | Policy Win                      | If Any            | and        | Windows Al  | l a            | ind 4. | x or later a     | ind | AnyConnect     | and             | 17 | en | Default AppVis Requir  |      |          |
|          | -            | roney options    |                                    |                                 |                   |            |             |                |        |                  |     |                |                 |    |    | ement_Win  |      | Edit   * |
|          | 0            | Policy Options   | Default_AppVis_<br>mporal          | Policy_Win_te                   | If Any            | and        | Windows Al  | 1 8            | and 4. | x or later a     | ind | Temporal Agent | and             | 17 | en | Default_AppVis_Requir<br>ement_Win_temporal                  |      | Edit   👻 |
|          | 0            | Policy Options   | Default_Firewall_                  | Policy_Mac                      | If Any            | and        | Mac OSX     | 8              | ind 4. | x or later a     | ind | AnyConnect     | and             | 0  | en | Default_Firewall_Requir<br>ement_Mac                         |      | Edit   👻 |
|          | 0            | Policy Options   | Default_Firewall_<br>emporal       | Policy_Mac_t                    | If Any            | and        | Mac OSX     | 8              | and 4. | x or later a     | ind | Temporal Agent | and             | 0  | en | Default_Firewall_Requir<br>ement_Mac_temporal                |      | Edit   + |
|          | 0            | Policy Options   | Default_Firewall_                  | Policy_Win                      | If Any            | and        | Windows Al  | l a            | and 4. | x or later a     | and | AnyConnect     | and             | 17 | en | Default_Firewall_Requir<br>ement_Win                         |      | Edit   • |
|          | 0            | Policy Options   | Default_Firewall_<br>mporal        | Policy_Win_te                   | If Any            | and        | Windows Al  | 1 8            | ind 4. | x or later a     | and | Temporal Agent | and             | 17 | en | Default_Firewall_Requir<br>ement_Win_temporal                |      | Edit   🕶 |
|          | 0            | Policy Options   | Default_Hardwar<br>olicy_Mac       | re_Attributes_P                 | If Any            | and        | Mac OSX     | 8              | and 4. | x or later a     | ind | AnyConnect     | and             | tř | en | Default_Hardware_Attri<br>butes_Requirement_Ma<br>c          |      | Edit   • |
|          | 0            | Policy Options   | Default_Hardwar<br>olicy_Mac_tempo | re_Attributes_P<br>oral         | If Any            | and        | Mac OSX     | 8              | and 4. | x or later a     | ind | Temporal Agent | and             | tr | en | Default_Hardware_Attri<br>butes_Requirement_Ma<br>c_temporal |      | Edit   • |
|          | 0            | Policy Options   | Default_Hardwar<br>olicy_Win       | re_Attributes_P                 | If Any            | and        | Windows Al  | l a            | and 4. | x or later a     | and | AnyConnect     | and             | tr | en | Default_Hardware_Attri<br>butes_Requirement_Wi<br>n          |      | Edit   • |
|          | 0            | Policy Options   | Default_Hardwar<br>olicy_Win_tempo | re_Attributes_P<br>oral         | If Any            | and        | Windows Al  | l a            | and 4. | x or later a     | ind | Temporal Agent | and             | tr | en | Default_Hardware_Attri<br>butes_Requirement_Wi<br>n_temporal |      | Edit   • |
|          | 0            | Policy Options   | Default_USB_Bk                     | ock_Policy_Wi                   | If Any            | and        | Windows Al  | l a            | and 4. | x or later a     | and | AnyConnect     | and             | 0  | en | USB_Block  |      | Edit   + |
|          | 0            | Policy Options   | Default_USB_Blo<br>n_temporal      | ock_Policy_Wi                   | If Any            | and        | Windows Al  | 1 8            | and 4. | x or later a     | and | Temporal Agent | and             | 17 | en | USB_Block_temporal   |      | Edit   • |
| <u></u>  | <b>~</b>     | Policy Options   | VPN_Posture_Po                     | olicy_Win                       | If Any            | and        | Windows 10  | e (All) a      | and 4. | x or later a     | and | AnyConnect     | and             | tř | en | VPN_Posture_Require ment                                     |      | Edit   🕶 |
| Save     | Reset        |                  |                                    |                                 |                   |            |             |                |        |                  |     |                |                 |    |    |  |      |          |

(DACL) ةيكيمانيدلا (ACL) لوصولا يف مكحتلا مئاوق ءاشنإ .11

يف مكحتلا مئاوق < ضيوفتلا < جئاتنلا < ةسايسلا رصانع < ةسايس ىلإ لقتنا ذفنملاب ةصاخلا لوصولا يف مكحتلا مئاوق ءاشنإب مقو "ليزنتلل ةلباقلا (ACL) لوصولا عضولا تالاح فلتخمل (DACL).

.ةيلاتلا (DACL) لوصولا يف مكحتلا مئاوق دنتسملا اذه مدختسي

HTTPS و HTTP و PSN و DNS رورم ةكرح ىلإ رورملا ةكرحب حمسي :فورعم ريغ ALTPS

| cisco Identity Services Engine  | Home   Context Visibility   Operations   Policy   Administration   Work Centers                                   |
|---------------------------------|---|
| Policy Sets Profiling Posture C | lient Provisioning  Policy Elements   |
| Dictionaries                    |   |
| Authentication                  | Downloadable ACL List > PostureUnknown Downloadable ACL   |
| - Authorization                 | * Name PostureUnknown   |
| Authorization Profiles          | Description   |
| Downloadable ACLs               | IP version IPv4 Annostic  |
| ▶ Profiling                     | * DACL Content 1234567 permit udp any any eq domain   |
| ▶ Posture                       | 2131415 permit tip any nost 10.105.44.77<br>2131415 permit tcp any any eq 80<br>1617181 permit tcp any any eq 443 |
| Client Provisioning             | 9202122<br>2324252<br>6272829<br>3031323<br>3343536<br>> Check DACL Syntax  |
|                                 | Save Reset  |

ب Posture NonCompliant: الإ حمسي الو ةصاخلا ةيعرفلا تاكبشلا ىلإ لوصولا ضفري تنرتنإلا رورم ةكرحب

| cisco Identity Services Engine      | Home → Context Visibility → Operations → Policy → Administration → Work Centers |
|-------------------------------------|---|
| Policy Sets Profiling Posture Clie  | ent Provisioning   Policy Elements  |
| Dictionaries   Conditions   Results |   |
| Authentication                      | Downloadable ACL List > PostureNonCompliant Downloadable ACL                    |
| - Authorization                     | * Name PostureNonCompliant  |
| Authorization Profiles              | Description   |
| Downloadable ACLs                   |   |
| ▶ Profiling                         | * DACL Content 1234567 deny jp any 10.0.0.0 255.0.0.0                           |
| ▶ Posture                           | 2131415 deny ip any 1/2.168.0.0 255.256.0.0<br>1817181 permit ip any any        |
| ▶ Client Provisioning               | 9202122<br>2324252<br>6272829<br>3031323  |
|                                     | 3343535   |
|                                     | Save Reset  |

عم نيقفاوتملا نييئاەنلا نيمدختسملل رورملا ةكرح عيمجل حمسي :عضولل قباطم .ج عضولا

| Identity Services Engine                 | Home → Context Visibility → Operations ▼Policy → Administration → Work Centers                  |
|--|---|
| Policy Sets Profiling Posture C          | Client Provisioning   Policy Elements   |
| Dictionaries + Conditions - Resu         | dts   |
| Authentication Authorization             | Downloadable ACL List > PostureCompliant Downloadable ACL   · Name PostureCompliant Description |
| Authorization Profiles Downloadable ACLs |   |
| ▶ Profiling                              | * DACL Content 1234567 permit ip any any  |
| ▶ Posture                                | 2131415<br>1617181  |
| Client Provisioning                      | 3224252       6272829         3031323       3343636         • Check DACL Syntax       0         |
|  | Save Reset  |

ليوختلا فيرعت تافلم ءاشنإ .12

صيصخت تافلم < ضيوفتلا < جئاتنلا < ةسايسلا رصانع < ةسايس ىلإ لقتنا ضيوفتلا.

فورعملا ريغ عضولل ليوختلا فيرعت فلم .أ

ددح DACL "PostureUnknown"، مقو ،(Posture) ليمعلاا دادعإ ددحو ،بيولا ميجوت ةداعإ نم ققحتو ، (PostureUnknown ددح (يصولاب مكحتلا ةمئاق مسا نيوكتب (ASA ىلع ەنيوكت متيل) "redirect" ميجوتلا ةداعإل لوصولاب مكحتلا قمئاق مسا نيوكتب (يضارتفالا) ليمعلا دادمإ لخدم ددحو

| dentity Services Engine            | Home   Context Visibility   Operations   Policy   Administration   Work Centers   | License Warning 🔺 🔍 🐵 🗳 |
|------------------------------------|---|-------------------------|
| Policy Sets Profiling Posture C    | Ient Provisioning   Policy Elements   |                         |
| Dictionaries + Conditions - Result | ls  |                         |
| 0                                  |   |                         |
| Authentication                     | Authorization Profile   |                         |
| - Authorization                    | * Name Posture Redirect   |                         |
| Authorization Profiles             | Description   |                         |
| Downloadable ACLs                  | * Access Type Access_Accept   |                         |
| Profiling                          | Network Device Profile 🗰 Cisco 💌 🕀  |                         |
| ▶ Posture                          | Service Template  |                         |
| Client Provisioning                | Track Movement 💿 🕡  |                         |
|                                    | Passive Identity Tracking 🗌 👔   |                         |
|                                    |   |                         |
|                                    |   |                         |
|                                    | ▼ Common Tasks  |                         |
|                                    | DACL Name PostureUnknown  |                         |
|                                    |   |                         |
|                                    |   |                         |
| Client Provisioning                |   |                         |
|                                    | B Web Redirection (CWA, MDM, NSP, CPP)  |                         |
|                                    | Client Provisioning (Posture)   |                         |
|                                    |   |                         |
|                                    |   |                         |
|                                    |   |                         |
|                                    | ▼ Advanced Attributes Settings  |                         |
|                                    |   |                         |
|                                    | Select an item 📀 = 💽 🔿 — 🕂  |                         |
|                                    |   |                         |
|                                    |   |                         |
|                                    | ▼ Attributes Details  |                         |
|                                    | Access Type = ACCESS_ACCEPT<br>DACL = PostureUnknown  |                         |
|                                    | cisco-av-pair = url-redirect=acl=redirect<br>cisco-av-pair = url-redirect=https://p:port/portal/gateway/sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050566775a3&action=cpp |                         |
|                                    |   | li.                     |
|                                    | Sive Reset  |                         |

عضولل لاثتمالا مدعل ضيوفتلا فيرعت فلم - ءاب

ةكبشلا ىلإ لوصولا نم دحلل "DACL "PostureNonCompliant ددح

| dentity Services Engine          | Home   Context Visibility   Operations   Policy   Administration   Work Centers | License Warning 🔺 | ۹, | 0 ( | 0 |
|----------------------------------|---|-------------------|----|-----|---|
| Policy Sets Profiling Posture Cl | ent Provisioning    Policy Elements   |                   |    |     |   |
| Dictionaries                     |   |                   |    |     |   |
| 0                                |   |                   |    |     |   |
| Authentication                   | Authorization Profile Authorization Profile                                     |                   |    |     |   |
| - Authorization                  | * Name Posture Non Compliant  |                   |    |     |   |
| Authorization Profiles           | Description   |                   |    |     |   |
| Downloadable ACLs                | * Access Type Access ACCEPT *   |                   |    |     |   |
| Profiling                        | Network Device Profile 🗰 Cisco 💌 🕀  |                   |    |     |   |
| Posture                          | Service Template  |                   |    |     |   |
| Client Provisioning              | Track Movement 🗇 🛈  |                   |    |     |   |
|                                  | Passive Identity Tracking 🔹 🕢   |                   |    |     |   |
|                                  |   |                   |    |     |   |
|                                  |   |                   |    |     |   |
|                                  | * Common Tasks  |                   |    |     |   |
|                                  | DACL Name     PostureNonCompliant   |                   |    |     |   |

| ✓ Attributes Details                                      |  |
|---|--|
| Access Type = ACCESS_ACCEPT<br>DACL = PostureNonCompliant |  |
| Comp. Reads   |  |

#### عضولا عم قفاوتلاب صاخلا ليوختلا فيرعت فلم - ميج

ةكبشلا ىلإ لماكلا لوصولاب حامسلل "DACL "PostureCompliant ددح

| dentity Services Engine            | Home  Context Visibility  Operations  Policy  Administration  Work Centers | License Warning 🔺 | ् ( | • | 0 |
|------------------------------------|--|-------------------|-----|---|---|
| Policy Sets Profiling Posture C    | Ilent Provisioning  Policy Elements  |                   |     |   |   |
| Dictionaries + Conditions + Result |  |                   |     |   |   |
| 0                                  |  |                   |     |   |   |
| Authentication                     | Authorization Profiles > Full Access Authorization Profile                 |                   |     |   |   |
| - Authorization                    | * Name Full Access   |                   |     |   |   |
| Authorization Profiles             | Description  |                   |     |   |   |
| Downloadable ACLs                  | * Access Type Access ACCEPT T  |                   |     |   |   |
| Profiling                          | Network Device Profile dt Clisco v 🕀                                       |                   |     |   |   |
| Posture                            | Service Template   |                   |     |   |   |
| Client Provisioning                | Track Movement 🗇 🕖   |                   |     |   |   |
|                                    | Passive Identity Tracking 🗌 🕢  |                   |     |   |   |
|                                    |  |                   |     |   |   |
|                                    |  |                   |     |   |   |
|                                    | ▼ Common Tasks   |                   |     |   |   |
|                                    |  |                   |     |   |   |
|                                    | C DACL Name PostureCompliant   |                   |     |   |   |
|                                    |  |                   |     |   |   |
|                                    |  |                   |     |   |   |
|                                    | ✓ Attributes Details   |                   |     |   |   |
|                                    | Access Type = ACCESS_ACCEPT<br>DACL = PERMIT_ALL_IPV4_TRAFFIC              |                   |     |   |   |
|                                    |  |                   | In. |   |   |
|                                    | Save Reset   |                   |     |   |   |

ضيوفتلا تاسايس نيوكت .12

3 نيوكتل ةقباسلا ةوطخلا يف اهنيوكت مت يتلا ليوختلا فيرعت تافلم مدختسأ .ةفورعم ريغ ةيعضوو ،عضولا عم ةقفاوتم ريغو ،عضولا عم ةقفاوتم ليوخت تاسايس

جەن لك جئاتن دىدحتل "عضولا ةلاح :لمعلا ةسلج" كرتشملا طرشلا مادختسا متي

| cisco Ide  | ntity Service | es Engine Home > Conte              | ext Visibility               | y Derations           | Policy     Administration    | Work Centers |                         |   |                  | License Warning         | <u> </u>     |         |
|------------|---------------|-------------------------------------|------------------------------|-----------------------|------------------------------|--------------|-------------------------|---|------------------|-------------------------|--------------|---------|
| Policy Set | Profiling     | Posture Client Provisioning         | <ul> <li>Policy E</li> </ul> | lements               |                              |              |                         |   |                  |                         |              |         |
|            |               | <u></u>                             |                              |                       |                              |              |                         |   |                  |                         |              |         |
| Policy S   | iets → De     | fault                               |                              |                       |                              |              |                         |   |                  | Reset Policyset Hitcour | ts Res       | et Save |
|            | Status        | Policy Set Name                     | Descrip                      | ption                 | Conditions                   |              |                         |   |                  | Allowed Protocols / Sen | ver Sequence | Hits    |
| Search     |               |                                     |                              |                       |                              |              |                         |   |                  |                         |              |         |
|            | $\odot$       | Default                             | Default                      | policy set            |                              |              |                         |   |                  | Default Network Access  | x • +        | 49      |
|            |               |                                     |                              |                       |                              |              |                         |   |                  |                         | _            |         |
| > Authe    | ntication Po  | licy (3)                            |                              |                       |                              |              |                         |   |                  |                         |              |         |
| > Autho    | rization Poli | cy - Local Exceptions               |                              |                       |                              |              |                         |   |                  |                         |              |         |
| > Autho    | vization Poli | av - Clobal Exceptions              |                              |                       |                              |              |                         |   |                  |                         |              |         |
| * Addie    | nization Foil | cy - Global Exceptions              |                              |                       |                              |              |                         |   |                  |                         |              |         |
| ✓ Author   | rization Poli | cy (15)                             |                              |                       |                              |              |                         |   |                  |                         |              |         |
|            |               |                                     |                              |                       |                              |              | Results                 |   |                  |                         |              |         |
| +          | Status        | Rule Name                           | Cond                         | litions               |                              |              | Profiles                |   | Security Group   | is                      | Hits         | Actions |
| Search     |               |                                     |                              |                       |                              |              |                         |   |                  |                         |              |         |
|            | 0             | Anyconnect Posture Compliant        | ĥ                            | Session PostureStatu: | s EQUALS Compliant           |              | Full Access             | + | Select from list | · +                     | 6            | ۵       |
|            | ø             | Anyconnect Posture Non<br>Compliant | ĥ                            | Session PostureStatur | s EQUALS NonCompliant        |              | × Posture Non Compliant | + | Select from list | × +                     | 0            | ٥       |
|            |               |                                     |                              | Network Acc           | ess-Device IP Address EQUALS | 10.197.164.3 |                         |   |                  |                         |              |         |
|            | $\odot$       | Anyconnect Posture Unknown          | AND                          | έ Session-Pos         | tureStatus EQUALS Unknown    |              | × Posture Redirect      | + | Select from list | · +                     | 13           | ¢       |

## ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

.ASA ىلع يلاتلا رمألا ليغشتب مق ،حاجنب مدختسملا ةقداصم 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 : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel Protocol License : AnyConnect Premium : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Encryption Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 : 16404 Bytes Rx : 381 Bytes Tx Pkts Tx : 16 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG SAML : 07:05:45 UTC Sun Jun 14 2020 Login Time : 0h:00m:16s Duration 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 : win Client OS Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052 : 7973 : 0 Bytes Tx Bytes Rx Pkts Tx : 6 Pkts Rx : 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 : 7973 Bytes Tx Bytes Rx : 0 : 6 Pkts Tx Pkts Rx : 0 Pkts Rx Drop : 0 Pkts Tx 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 :

Pkts Rx Drop : 0

#ACSACL#-IP-PostureUnknown-5ee45b05

Pkts Tx Drop : 0

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

وه امك لماكلا لوصولا ىلٍ مدختسملا لوصو رييغت متي ،عضولا مييقت لامتكا درجمب حشرملا مسا" لقحلا يف اهعفد مت يتلا (DACL) لوصولاب مكحتلا ةمئاق يف ظحالم"

#### <#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 : AnyConnect Premium License : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Hashing : 16404 : 381 Bytes Tx Bytes Rx Pkts Tx : 16 Pkts Rx : 6 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : DfltGrpPolicy Tunnel Group : TG\_SAML : 07:05:45 UTC Sun Jun 14 2020 Login Time Duration : 0h:00m:36s : 0h:00m:00s Inactivity 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 : none Hashing TCP Dst Port : 443 TCP Src Port : 57244 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 : Cisco AnyConnect VPN Agent for Windows 4.8.03052 Client Ver Bytes Tx : 7973 : 0 Bytes Rx Pkts Tx Pkts Rx : 6 : 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 : AES-GCM-256 : SHA384 Encryption Hashing 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 Public IP Assigned IP : explorer.cisco.com : 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 : SAML Auth Mode 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   | Windo | Swe | 5 4.8.03052 |
| Bytes Tx     | : | 458              |     | Byte  | es R> | (     | :   | 381         |
| Pkts Tx      | : | 4                |     | Pkts  | 5 Rx  |       | :   | 6           |
| Pkts Tx Drop | : | 0                |     | Pkts  | s Rx  | Drop  | :   | 0           |
| Filter Name  | : |                  |     |       |       |       |     |             |

#ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

< RADIUS < تايلمع ىلإ لقتنا ،ISE ىلع حاجنب ضيوفتلا ذيفنت مت اذإ ام نم ققحتلل ةيح تالجس

زجومو ةيوهلا يأ ،دمتعملا مدختسملاب ةنرتقملا ةلصلا تاذ تامولعملا مسقلا اذه ضرعي عضولاا ةلااحو ليوختايا جەنو ليوختايا فيرعت.

|   |   |          |          |        |                     |                   |                |                | Refresh       | Never •                | Show Latest 20 | records 👻 Within | Las | st 24 hours 🔹  |
|---|---|----------|----------|--------|---------------------|-------------------|----------------|----------------|---------------|------------------------|----------------|------------------|-----|----------------|
| c | <sup>©</sup> Refersh <sup>©</sup> Reset Repeat Counts <sup>™</sup> Filter |          |          |        |                     |                   |                |                |               |                        |                |                  |     |                |
|   | Time  | Status   | Details  | Repeat | Identity            | Endpoint ID       | Endpoint P     | Authenticat    | Authorizati   | Authorization Pro      | Posture St     | IP Address       |     | Network Device |
| × |   | •        |          |        | Identity            | Endpoint ID       | Endpoint Profi | Authentication | Authorization | Authorization Profiles | Posture Statu: | IP Address       | ٠   | Network Device |
|   | Jun 14, 2020 07:44:59.975 AM  | 0        | 0        | 0      | _585b5291f01484dfd1 | 00:50:56:A0:D6:97 | Windows10      | Default        | Anyconnect    | Full Access            | Compliant      | 10.197.164.7     |     |                |
|   | Jun 14, 2020 07:44:59.975 AM  |          | <u>a</u> |        |                     | 10.197.243.143    |                |                | Anyconnect    | Full Access            | Compliant      |                  |     | ASA            |
|   | Jun 14, 2020 07:44:59.975 AM  |          | <u>o</u> |        | #ACSACL#-IP-PERMI   |                   |                |                |               |                        |                |                  |     | ASA            |
|   | Jun 14, 2020 07:44:34.963 AM  |          | 0        |        | #ACSACL#-IP-Posture |                   |                |                |               |                        |                |                  |     | ASA            |
|   | Jun 14, 2020 07:44:34.958 AM  | <b>~</b> | 0        |        | _585b5291f01484dfd1 | 00:50:56:A0:D6:97 | Windows10      | Default        | Default >> A  | Posture Redirect       | Pending        |                  |     | ASA            |
|   |   |          |          |        |                     |                   |                |                |               |                        |                |                  |     |                |

ىلاٍ عوجرلا ىجري ،ISE ىل ع عضولا ةحص نم ق ق حتلا نم ديزم ىل ع لوصحلل :ةظحالم 📎 اتىلات تەركات تەركە تەركى ت

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

ىلع ةدوجوملا "ريراقتلا" ىلع رقنا ،Duo لوؤسم لخدم ىلع ةقداصملا ةلاح نم ققحتلل ةقداصملا لجس رەظت يتلا ةرادإلا ةحول نم رسيألا بناجلا. لىصافتال نم دىزمالا: <u>https://duo.com/docs/administration#reports</u>

: إيلات العابترال مدختساً ،ةيئانثلا لوصولا ةرابعل ءاطخالا حيحصت ليجست ضرعل https://help.duo.com/s/article/1623?language=en\_US

مدختسملا ةبرجت



## اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسإ كنكمي يتلا تامولعملا مسقلا اذه رفوي.

.debug رماوأ مادختسإ لبق <u>حيحصتلا رماوأ لوح ةمهم تامولعم</u> ىلإ عجرا :ةظحالم 💊

مادختسا متي ؛ةفلتخم ءاطخأ حيحصت تايوتسم نييعت كنكمي ،ASA ىلع :هيبنت 🗥 ةجرد ديازتت دقف ،ءاطخألا حيحصت ىوتسم رييغتب تمق اذإ .اًيضارتفا لوألا ىوتسملا جاتنإلاا تائيب يف ًةصاخو ،رذحب كلذب مق .ءاطخألاا حيحصت عسوت

هيلع روثعلا نكمي حيحص ريغ نيوكت امحالصإو SAML ءاطخاً فاشكتساً مظعم نمضتيس ءاطخاُلا حيحصت ليغشت وأ SAML نيوكت نم ققحتلا لالخ نم. مادختسإ نكمي debug webVPN saml كمو ،امحالصإو لكاشملا مظعم ءاطخأ فاشكتسال "debug webVPN saml كمو ، نكمي ،ةديفم تامولعم اذه ءاطخألا حيحصت اميف رفوي ال يتلا تامويرانيسلا يف كلذ ةيفاضإ تاحيحصت ليغشت:

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

```
حيحصت رماوأ مدختساً ،اەحالصإو ASA ب ةقلعتملا ضيوفتلاو ةقداصملا ءاطخاً فاشكتسال
ةيلاتلا ءاطخالا:
```

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)



ا و AnyConnect ءاطخأ فاشكتساو يليصفتلا عضولا قفدت ىلع لوصحلل :ةظحالم AnyConnect ءاطخأ فاشكتساو يليصفتلا عضولا قفدت ال يل اتل اطابترال اىل عجرا ،اەحالصاو : <u>و post 2.2 طمن قنراقم ISE Posture مال ا</u>

اهحالصاو اهﺉاطخأ فاشڬتساو ةيﺉانثلا لوصولا ةرابع ءاطخأ حيحصت تالجس ةمجرتل https://help.duo.com/s/article/5016?language=en\_US

ةلص تاذ تامولءم

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-postureover-anyconnect-remote-acces.html#anc0

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما