

# Integración de Duo SAML SSO con Anyconnect Secure Remote Access mediante el estado de ISE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Flujo de tráfico](#)

[Configuraciones](#)

- [Configuración de Duo Admin Portal](#)

- [Configuración de gateway de acceso dúo \(DAG\)](#)

- [Configuración de ASA](#)

- [Configuración de ISE](#)

[Verificación](#)

[Experiencia de usuario](#)

[Troubleshoot](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe un ejemplo de configuración para integrar Duo SAML SSO con acceso de Cisco AnyConnect Secure Mobility Client del dispositivo de seguridad adaptable (ASA) que aprovecha Cisco ISE para una evaluación detallada del estado. Duo SAML SSO se implementa mediante Duo Access Gateway (DAG), que se comunica con Active Directory para la autenticación inicial del usuario y, a continuación, se comunica con Duo Security (Cloud) para la autenticación de varios factores. Cisco ISE se utiliza como servidor de autorización para proporcionar verificación de terminales mediante la evaluación de estado.

Colaboración de Dinesh Moudgil y Pulkit Saxena, ingeniero de HTTS de Cisco.

## Prerequisites

### Requirements

Este documento asume que ASA está completamente operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) o la Interfaz de línea de comandos (CLI) realicen cambios en la configuración.

Cisco recomienda que tenga conocimiento sobre estos temas:

- Fundamentos de Duo Access Gateway y Duo Security
- Conocimiento básico de la configuración de VPN de acceso remoto en ASA
- Conocimientos básicos de ISE y servicios de estado

## Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software Cisco Adaptive Security Appliance Versión 9.12(3)12
- Gateway de acceso doble
- Seguridad Duo
- Cisco Identity Services Engine versión 2.6 y posteriores
- Microsoft Windows 10 con AnyConnect versión 4.8.03052

---

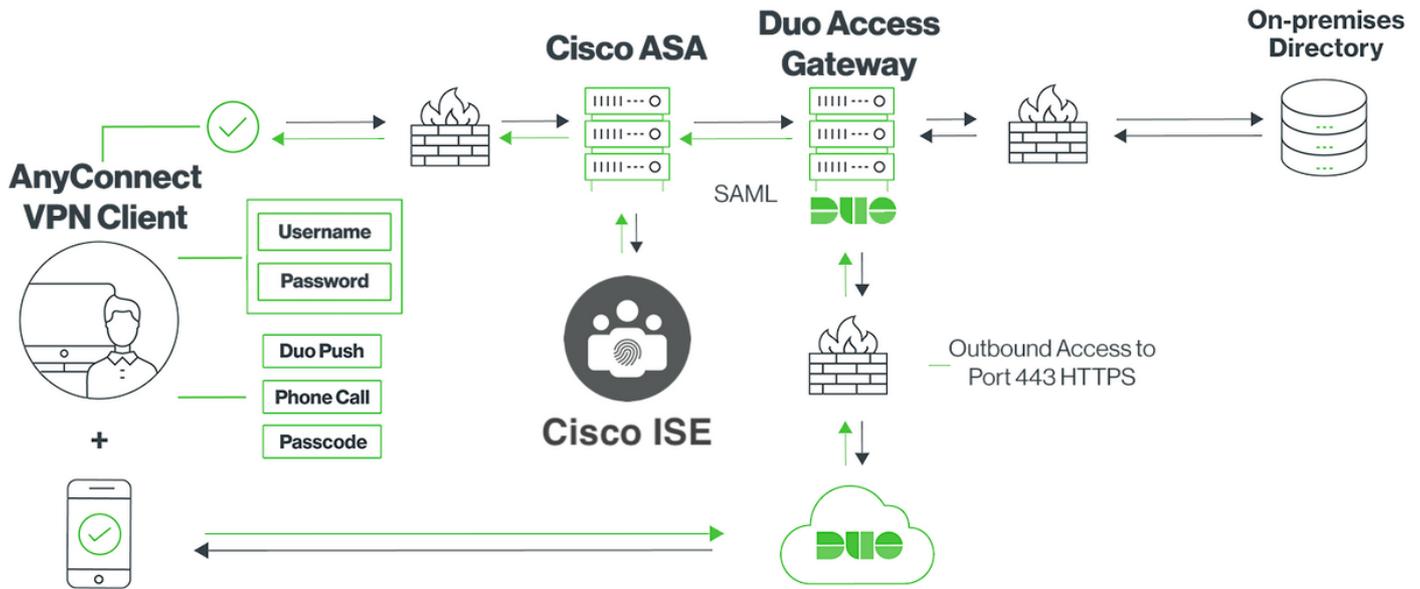
 Nota: el explorador integrado Anyconnect, utilizado en esta implementación, requiere ASA en las versiones 9.7(1)24, 9.8(2)28, 9.9(2)1 o superior de cada versión, y AnyConnect versión 4.6 o posterior.

---

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

## Configurar

### Diagrama de la red



## Flujo de tráfico

1. El cliente Anyconnect inicia una conexión VPN SSL con Cisco ASA
2. Cisco ASA, configurado para la autenticación principal con Duo Access Gateway (DAG), redirige el explorador integrado en el cliente Anyconnect a DAG para la autenticación SAML
3. El cliente Anyconnect se redirige al gateway de acceso Duo
4. Una vez que el cliente AnyConnect ingresa las credenciales, se genera una solicitud de autenticación SAML y se emite desde Cisco ASA a Duo Access Gateway
5. Duo Access Gateway aprovecha la integración con Active Directory in situ para realizar la autenticación principal para el cliente Anyconnect
6. Una vez que la autenticación primaria es exitosa, Duo Access Gateway envía una solicitud a Duo Security sobre el puerto TCP 443 para comenzar la autenticación de dos factores
7. El cliente AnyConnect ha presentado "Duo Interactive Prompt" y el usuario completa la autenticación Duo de dos factores utilizando su método preferido (push o passcode)
8. Duo Security recibe una respuesta de autenticación y devuelve la información al gateway de acceso Duo
9. En función de la respuesta de autenticación, Duo Access Gateway crea una respuesta de autenticación SAML que contiene una afirmación SAML y responde al cliente Anyconnect
10. El cliente Anyconnect autentica correctamente la conexión VPN SSL con Cisco ASA
11. Una vez que la autenticación es satisfactoria, Cisco ASA envía una solicitud de autorización a Cisco ISE



Nota: Cisco ISE solo está configurado para la autorización, ya que Duo Access Gateway proporciona la autenticación necesaria

12. Cisco ISE procesa la solicitud de autorización y, dado que el estado del cliente es Desconocido, devuelve la redirección de estado con acceso limitado al cliente Anyconnect a través de Cisco ASA
13. Si el cliente Anyconnect no tiene un módulo de cumplimiento, se le solicitará que lo descargue para continuar con la evaluación de estado
14. Si el cliente Anyconnect tiene un módulo de cumplimiento, establece una conexión TLS con Cisco ASA y se inicia el flujo de estado
15. En función de las condiciones de estado configuradas en ISE, se realizan comprobaciones de estado y se envían detalles desde el cliente Anyconnect a Cisco ISE
16. Si el estado del cliente cambia de Desconocido a Conforme, se envía una solicitud de cambio de autorización (CoA) desde Cisco ISE a Cisco ASA para conceder acceso completo al cliente y se establece VPN completamente

## Configuraciones

### - Configuración de Duo Admin Portal

En esta sección, configure la aplicación ASA en el Duo Admin Portal.

1. Inicie sesión en "Duo Admin Portal" y navegue hasta "Applications > Protect an Application", y busque "ASA" con tipo de protección "2FA with Duo Access Gateway, self-hosting". Haga clic en "Proteger" en el extremo derecho para configurar Cisco ASA

The screenshot shows the Duo Admin Portal interface. The breadcrumb navigation is "Dashboard > Applications > Protect an Application". The search bar contains "ASA". The table below shows the following applications:

Application	2FA	Single Sign-On (if available)	Documentation	Action
Asana	2FA	Duo Access Gateway (self-hosted)	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco ASA	2FA	Duo Access Gateway (self-hosted)	<a href="#">Documentation</a>	<a href="#">Protect</a>
Cisco ASA	2FA	Single Sign-On (hosted by Duo)	<a href="#">Documentation</a>	<a href="#">Configure</a>

2. Configure los siguientes atributos en "Proveedor de servicios" para la aplicación protegida, ASA

URL base	firebird.cisco.com
Grupo de Túnel	TG_SAML
Atributo de correo	sAMAccountName,mail

Haga clic en "Guardar" al final de la página

The screenshot shows the 'Cisco ASA - Duo Access Gateway' configuration page. The left sidebar contains navigation options like 'Device Insight', 'Policies', 'Applications', 'Users', 'Groups', 'Endpoints', '2FA Devices', 'Administrators', 'Reports', 'Settings', and 'Billing'. The main content area is titled 'Configure Cisco ASA' and includes a 'Reset Secret Key' button. A message box states: 'To set up this application, install the Duo Access Gateway and then configure your service provider. View Cisco ASA SAML SSO instructions. Next step: Download your configuration file'. The 'Service Provider' section contains the following fields:

- Base URL:** firebird.cisco.com (with a note: 'Enter the Cisco ASA Base URL.')
- Tunnel Group:** TG\_SAML (with a note: 'Enter the Tunnel Group you are protecting with SSO.')
- Custom attributes:** A checked checkbox with the text 'Use this setting if your Duo Access Gateway authentication source uses non-standard attribute names.'
- Mail attribute:** sAMAccountName,mail (with a note: 'The attribute containing the email address of the user.')

A 'Save Configuration' button is located at the bottom of the configuration section.

En este documento, el resto de la configuración utiliza parámetros predeterminados pero se pueden establecer en función de los requisitos del cliente.

En este momento se pueden ajustar ajustes adicionales para la nueva aplicación SAML, como cambiar el nombre de la aplicación del valor predeterminado, habilitar el autoservicio o asignar una directiva de grupo.

3. Haga clic en el enlace "Download your configuration file" (Descargar su archivo de configuración) para obtener los parámetros de la aplicación Cisco ASA (como archivo JSON). Este archivo se carga en la puerta de enlace de acceso doble en pasos posteriores

Device Insight

Policies

**Applications**

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Administrators

Reports

Settings

Billing

**Need Help?**

[Chat with Tech Support](#)

[Email Support](#)

Call us at 1-855-386-2884

**Account ID**

2010-1403-48

**Deployment ID**

DU057

**Helpful Links**

[Documentation](#)

## Cisco ASA - Duo Access Gateway

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

[Reset Secret Key](#)

### Configure Cisco ASA

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

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

#### Service Provider

**Base URL**

Enter the Cisco ASA Base URL.

---

**Tunnel Group**

Enter the Tunnel Group you are protecting with SSO.

---

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

---

**Mail attribute**

The attribute containing the email address of the user.

[Save Configuration](#)

4. En "Panel > Aplicaciones", la aplicación ASA recién creada se ve como se muestra en la siguiente imagen:

admin-77d04ebc.duosecurity.com/applications

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

**DUO**

Dashboard

Device Insight

Policies

**Applications**

Protect an Application

Single Sign-On

Users

Groups

Endpoints

2FA Devices

Dashboard > Applications

Cisco | ID: 2010-1403-48

## Applications

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

Export

Search

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

1 total

5. Navegue hasta "Usuarios > Agregar usuario" como se muestra en la imagen:

Cree un usuario denominado "duouser" para utilizarlo en la autenticación de acceso remoto de Anyconnect y active Duo Mobile en el dispositivo del usuario final

The screenshot shows the Duo Admin console interface. On the left is a dark sidebar with the Duo logo and a menu containing: Dashboard, Device Insight, Policies, Applications, **Users** (highlighted), **Add User** (highlighted), Pending Enrollments, Bulk Enroll Users, Import Users, Directory Sync, Bypass Codes, Groups, and Endpoints. The main content area has a search bar at the top with the text "Search for users, groups, applications, or devices". Below it is a breadcrumb trail: Dashboard > Users > Add User. The main heading is "Add User". A sub-heading "Adding Users" is followed by the text "Most applications allow users to enroll themselves after they complete primary authentication." and a link "Learn more about adding users". The "Username" field contains the text "duouser" and has a note below it: "Should match the primary authentication username." At the bottom of the form is a blue "Add User" button.

Para agregar el número de teléfono como se muestra en la imagen, seleccione la opción "Agregar teléfono".

The screenshot shows the Duo Admin console interface for adding a phone. The sidebar is the same as in the previous image, but the breadcrumb trail is: Dashboard > Users > duouser > Add Phone. The main heading is "Add Phone". A link "Learn more about Activating Duo Mobile" is present. The "Type" field has two radio buttons: "Phone" (selected) and "Tablet". The "Phone number" field contains a dropdown menu showing the flag for India and the text "+91 9xxx-xxx-xxx", followed by a link "Show extension field". Below the field is the text "Optional. Example: '+91 91234 56789'". At the bottom of the form is a blue "Add Phone" button.

Activar "Duo Mobile" para el usuario concreto

## Device Info

[Learn more about Activating Duo Mobile](#)



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



**Model**  
Unknown



**OS**  
Generic Smartphone



Nota: Asegúrese de tener "Duo Mobile" instalado en el dispositivo del usuario final.

[Instalación manual de la aplicación Duo para dispositivos IOS](#)

[Instalación manual de la aplicación Duo para dispositivos Android](#)

Seleccione "Generar Duo Mobile Activation Code" como se muestra en la imagen:

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48 | ciscoduobl

Dashboard > Phone: [redacted] > Activate Duo Mobile

### Activate Duo Mobile

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

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

Phone: [redacted]

Expiration: 24 hours after generation

[Generate Duo Mobile Activation Code](#)

Seleccione "Enviar instrucciones por SMS" como se muestra en la imagen:

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

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

# Activate Duo Mobile

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

Phone [REDACTED]

## Installation instructions

Send installation instructions via SMS

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

## Activation instructions

Send activation instructions via SMS

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

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

Haga clic en el enlace de la aplicación SMS y Duo se vinculará a la cuenta de usuario en la sección Device Info (Información del dispositivo), como se muestra en la imagen:

Dashboard

Device Insight

Policies

Applications

Users

Groups

Endpoints

**2FA Devices**

Phones

Hardware Tokens

WebAuthn & U2F

Administrators

Reports

Settings

Billing

Need Help?  
Chat with Tech Support

Search for users, groups, applications, or devices

Cisco | ID: 2010-1403-48

Duo Mobile instructions SMS'ed to +91 [redacted]

Dashboard > Phones > Phone: +91 [redacted]

+91 [redacted] Send SMS Passcodes...

**Shared phone**  
This phone is attached to multiple users.

duouser +91 [redacted] testing 123 +91 [redacted] Attach a user

Authentication devices can share multiple users

**Device Info**  
Learn more about Activating Duo Mobile

Using Duo Mobile  
Reactivate Duo Mobile

Model  
Unknown

OS  
Generic Smartphone

## - Configuración de gateway de acceso dúo (DAG)

### 1. Implementación de Duo Access Gateway (DAG) en un servidor de la red

 Nota: Siga estos documentos para la implementación:

Gateway de acceso Duo para Linux

<https://duo.com/docs/dag-linux>

Puerta de enlace de acceso Duo para Windows

<https://duo.com/docs/dag-windows>

2. En la página de inicio de Duo Access Gateway, navegue hasta "Authentication Source"

3. En "Configurar orígenes", introduzca los siguientes atributos para su Active Directory y haga clic en "Guardar parámetros"

## Configure Sources

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

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

4. En "Set Active Source", seleccione el tipo de origen como "Active Directory" y haga clic en "Set Active Source"

### Set Active Source

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

Source type

5. Navegue hasta "Aplicaciones", en el submenú "Agregar aplicación", cargue el archivo .json descargado desde Duo Admin Console dentro de la sección "Archivo de configuración". El archivo .json correspondiente se descargó en el paso 3 en Duo Admin Portal Configuration

## Applications

### Add Application

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

Configuration file

6. Una vez agregada correctamente la aplicación, aparece en el submenú "Aplicaciones"

### Applications

Name	Type	Logo	
Cisco ASA - Duo Access Gateway	Cisco ASA		<input type="button" value="Delete"/>

7. En el submenú "Metadatos", descargue los metadatos XML y el certificado IdP y anote las siguientes URL que se configuran en el ASA más adelante

1. URL DE SSO
2. URL de desconexión
3. ID de entidad
4. URL de error

Metadata Recreate Certificate

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

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

Expiration: 2030-04-30 18:57:14

SHA-1 Fingerprint: [REDACTED]

SHA-256 Fingerprint: [REDACTED]

SSO URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
Logout URL	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutSer</a>
Entity ID	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
Error URL	<a href="https://explorer.cisco.com/dag/module.php/duosecurity/du">https://explorer.cisco.com/dag/module.php/duosecurity/du</a>

## - Configuración de ASA

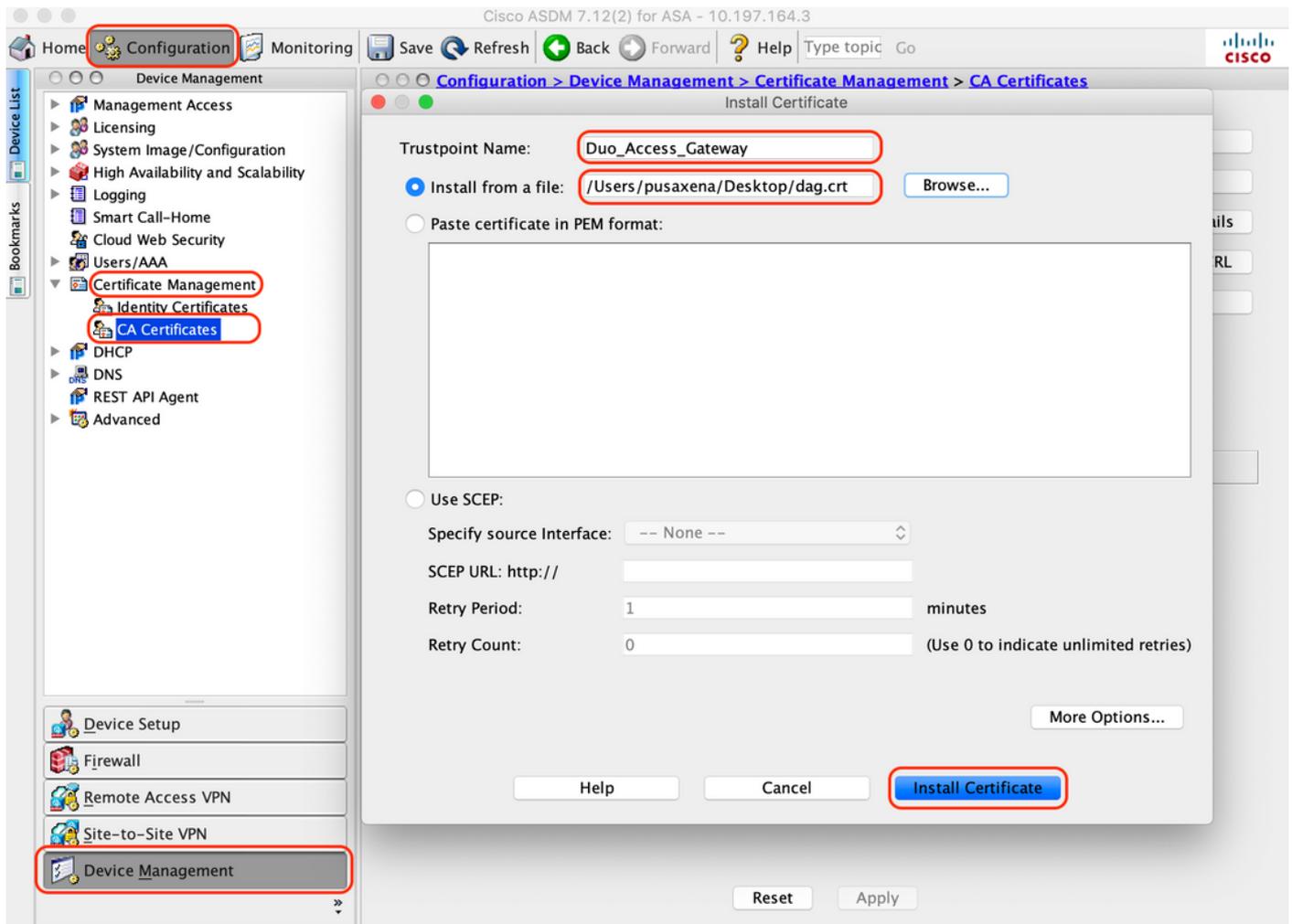
Esta sección proporciona información para configurar ASA para la autenticación IDP de SAML y la configuración básica de AnyConnect. El documento proporciona los pasos de configuración de ASDM y la configuración de ejecución de CLI para la descripción general.

### 1. Cargar certificado de gateway de acceso Duo

A. Navegue hasta "Configuración > Administración de dispositivos > Administración de certificados > Certificados de CA", haga clic en "Agregar"

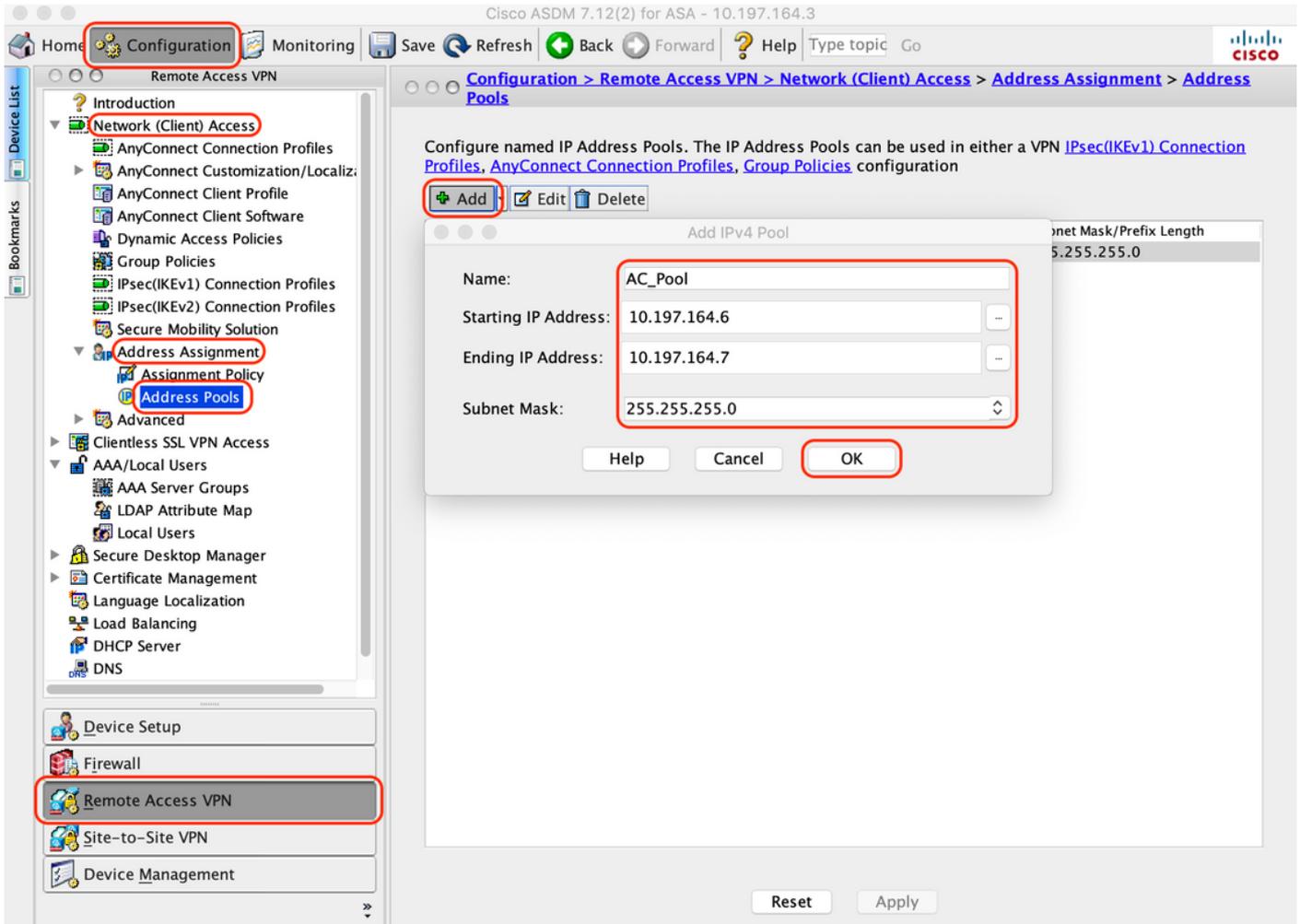
B. En la "Página de instalación del certificado", configure el nombre del punto de confianza: Duo\_Access\_Gateway

C. Haga clic en "Examinar" para seleccionar la ruta asociada al certificado DAG y, una vez seleccionado, haga clic en "Instalar certificado"



## 2. Crear pool local de IP para usuarios de AnyConnect

Vaya a "Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools" y haga clic en "Add"



### 3. Configuración del Grupo de Servidores AAA

R. En esta sección, configure el grupo de servidores AAA y proporcione detalles del servidor AAA específico que realiza la autorización

B. Navegue hasta "Configuración > VPN de acceso remoto > AAA/Usuarios locales > Grupos de servidores AAA", haga clic en "Agregar"

The screenshot shows the Cisco configuration interface for Remote Access VPN. The left sidebar has a tree view with 'AAA Server Groups' selected. The main content area displays the 'AAA Server Groups' configuration page. A modal dialog box titled 'Add AAA Server Group' is open, showing the following configuration:

- AAA Server Group: ISE
- Protocol: RADIUS
- Accounting Mode: Single (selected)
- Reactivation Mode: Depletion (selected)
- Dead Time: 10 minutes
- Max Failed Attempts: 3
- Enable interim accounting update
  - Update Interval: 24 Hours
- Enable Active Directory Agent mode
- ISE Policy Enforcement
  - Enable dynamic authorization
    - Dynamic Authorization Port: 1700
  - Use authorization only mode (no common password configuration required)
- VPN3K Compatibility Option: [Dropdown]

Buttons: Help, Cancel, OK (highlighted)

C. En la misma página, en la sección "Servidores del grupo Seleccionado", haga clic en "Agregar" y proporcione los detalles de la dirección IP del servidor AAA

Cisco ASDM 7.12(2) for ASA - 10.197.164.3

Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ISE	RADIUS	Single	Depletion	10	3
LOCAL	LOCAL				

Add AAA Server

Server Group: ISE

Interface Name: outside

Server Name or IP Address: 10.106.44.77

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: [Redacted]

Common Password: [Redacted]

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable:

SDI Messages

Message Table

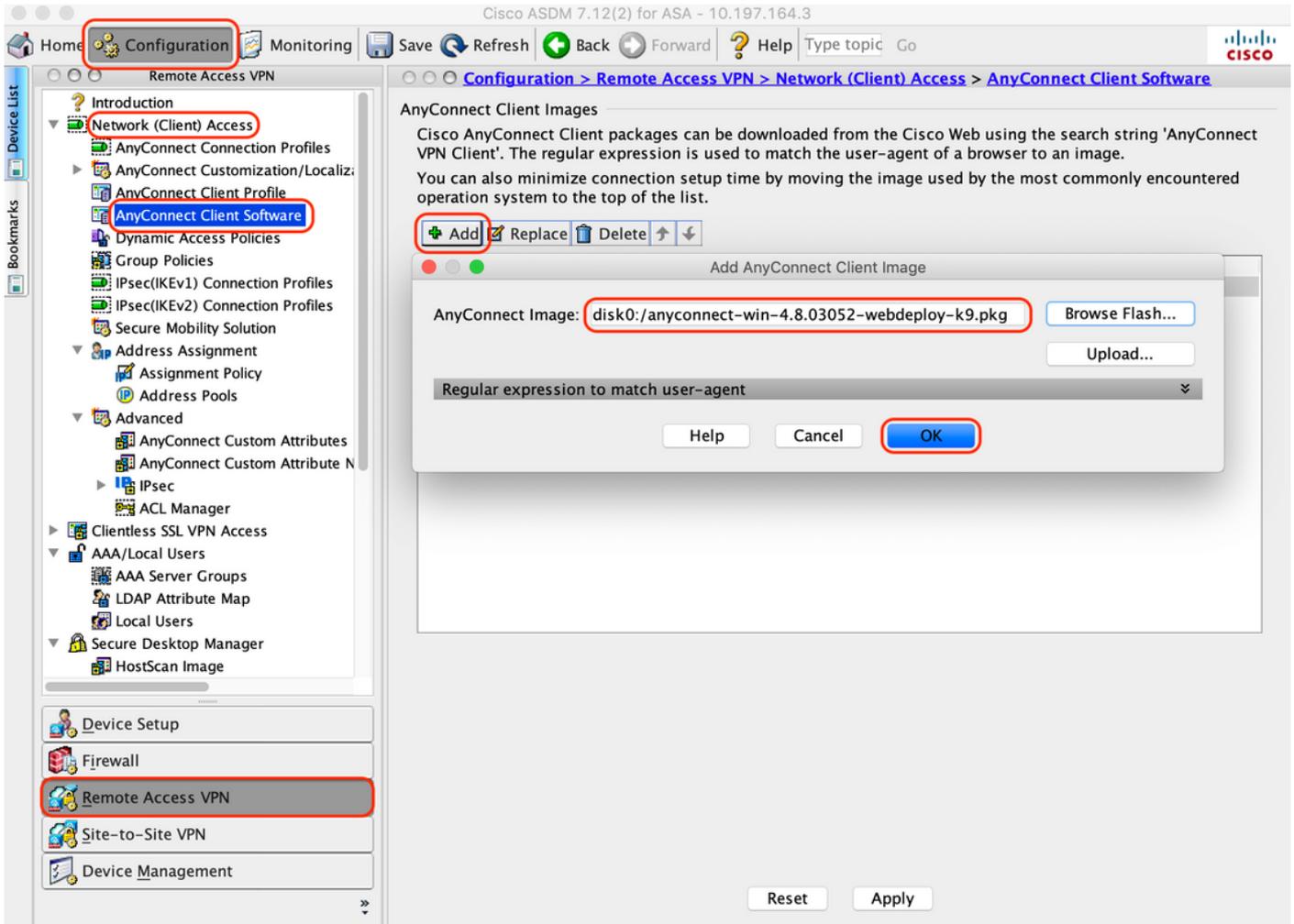
Help Cancel OK

Reset Apply

#### 4. Asignar software cliente AnyConnect

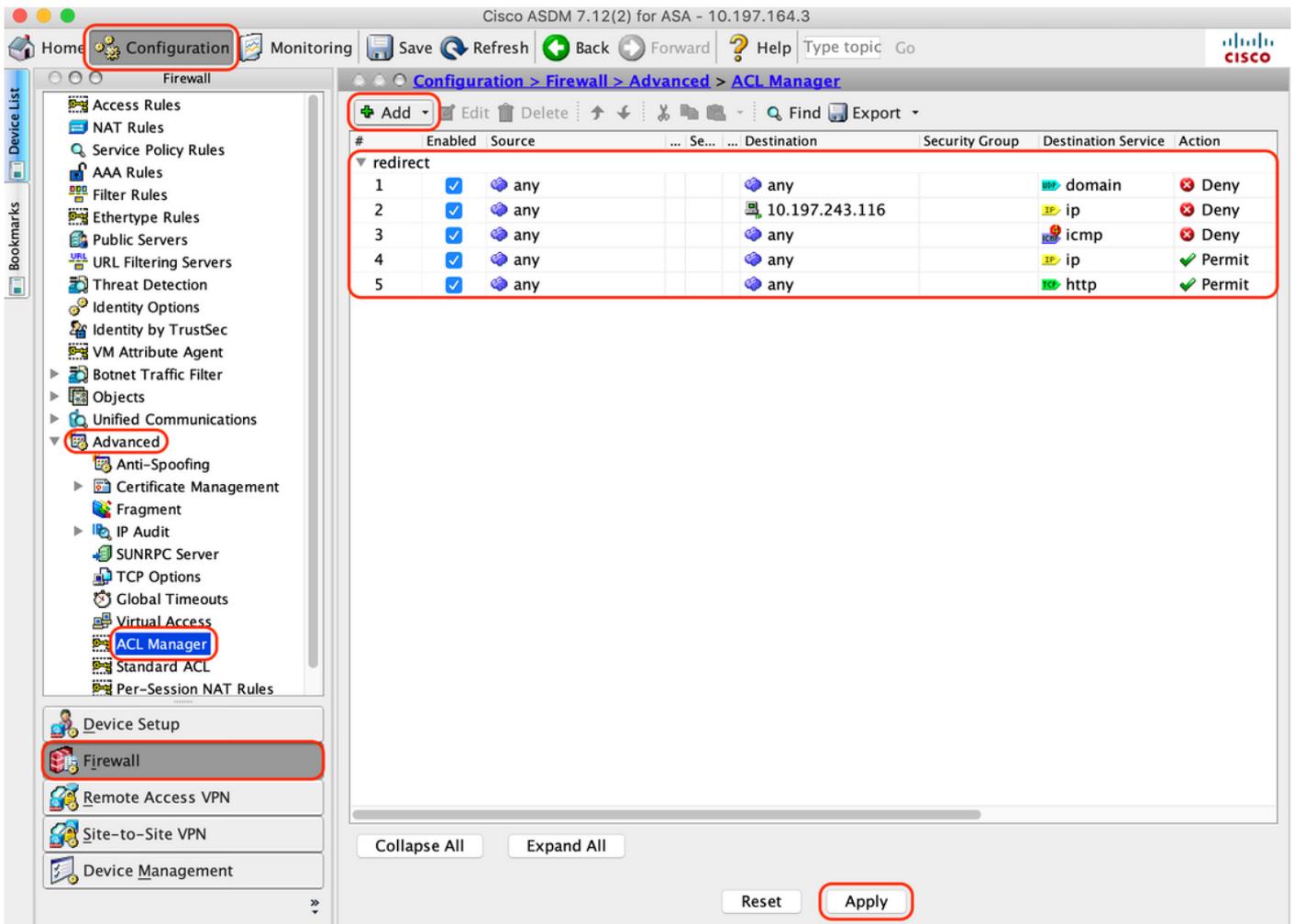
A. Asigne la imagen de implementación web del software cliente AnyConnect 4.8.03052 para las ventanas que se utilizarán para WebVPN

B. Vaya a "Configuración > VPN de acceso remoto > Acceso (cliente) de red > Software de cliente AnyConnect" y haga clic en "Agregar"



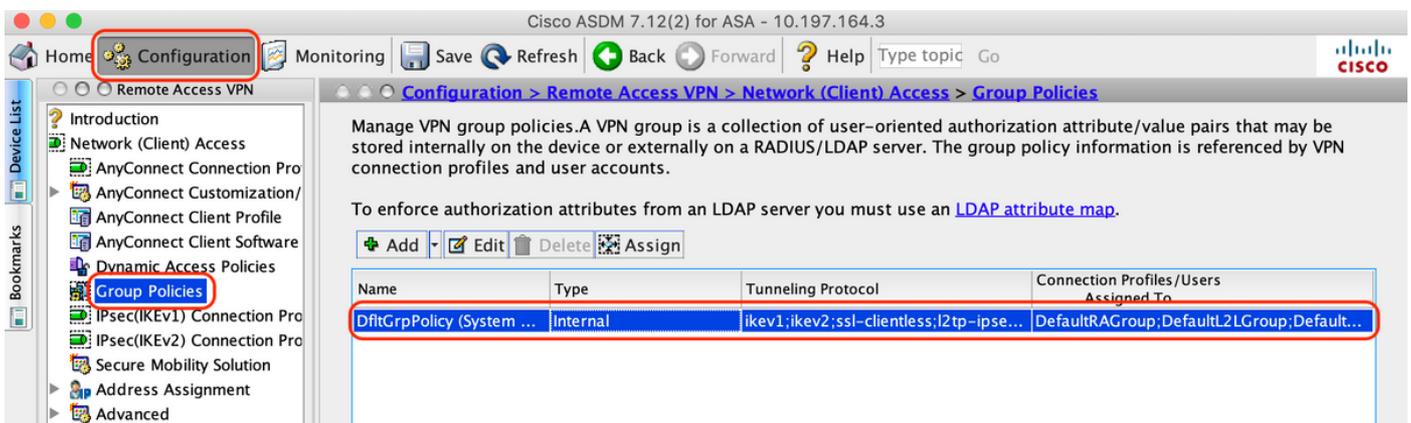
5. Configure la ACL de redirección que se envía como resultado de ISE

A. Navegue hasta "Configuration > Firewall > Advanced > ACL Manager", haga clic en Add para agregar la ACL de redirección. Las entradas, una vez configuradas, tienen el siguiente aspecto:



## 6. Validar la directiva de grupo existente

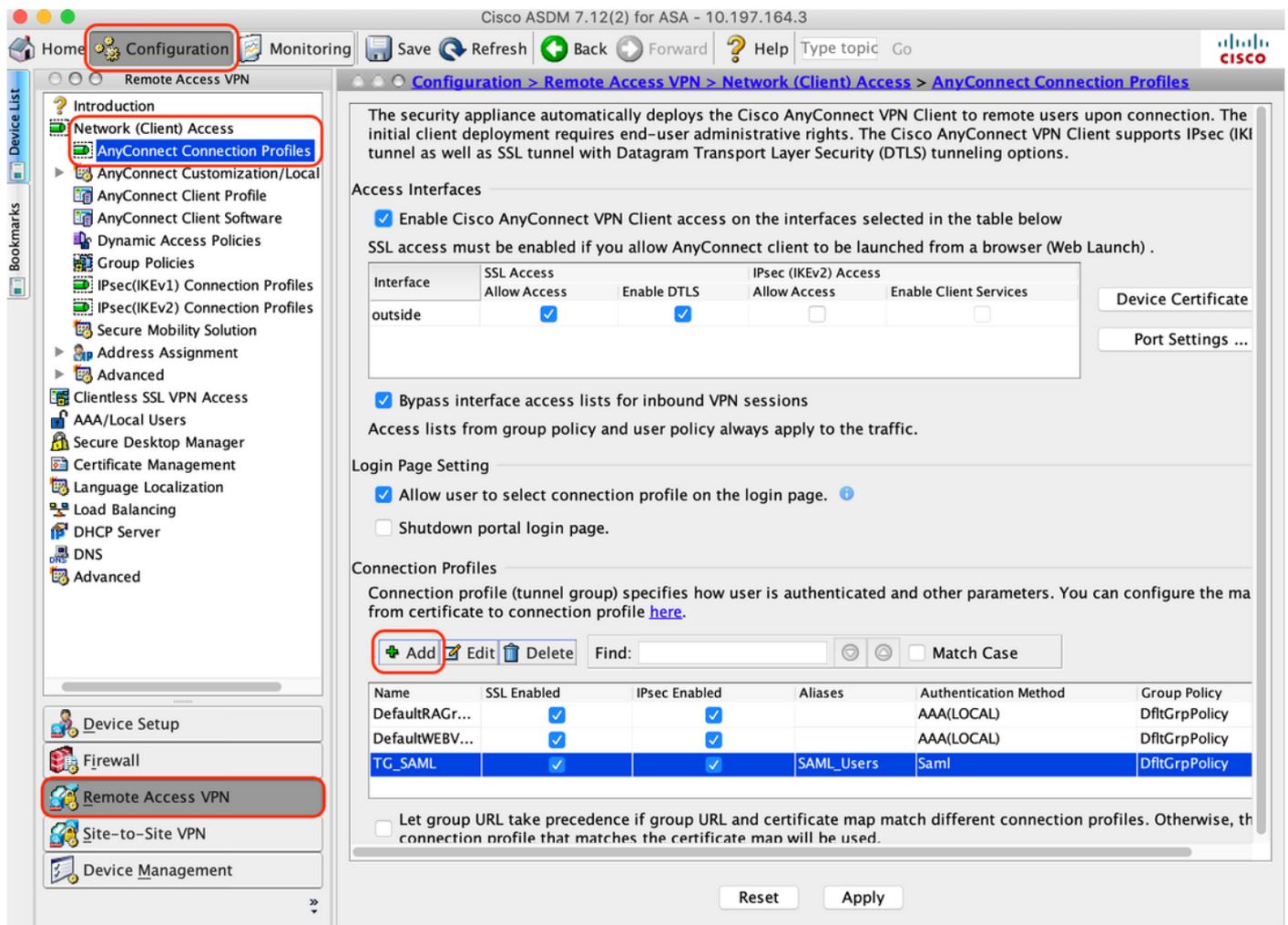
R. Esta configuración utiliza la política de grupo predeterminada y se puede ver en:  
 "Configuración > VPN de acceso remoto > Acceso (cliente) de red > Políticas de grupo"



## 7. Configuración del perfil de conexión

A. Crear un nuevo perfil de conexión al que se conecten los usuarios de AnyConnect

B. Vaya a "Configuración > VPN de acceso remoto > Acceso (cliente) de red > Perfiles de conexión de Anyconnect" y haga clic en "Agregar"



C. Configure los siguientes detalles asociados con el perfil de conexión:

Nombre	TG_SAML
Alias	Usuarios_SAML
Método	SAML
Grupo de servidores AAA	Local
Conjuntos de direcciones de cliente	AC_Pool
Directiva de grupo	DfltGrpPolicy

Basic  
▶ Advanced

Name: TG\_SAML

Aliases: SAML\_Users

Authentication

Method: SAML

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

SAML Identity Provider

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

Client Address Assignment

DHCP Servers:

None  DHCP Link  DHCP Subnet

Client Address Pools: AC\_Pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: DfltGrpPolicy Manage...

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

Enable SSL VPN client protocol

Enable IPsec(IKEv2) client protocol

DNS Servers:

WINS Servers:

Domain Name:

Find: Next Previous

Help Cancel OK

D. En la misma página, configure los detalles del proveedor de identidad SAML que se muestran a continuación:

ID de entidad IDP	<a href="https://explorer.cisco.com/dag/saml2/idp/metadata.php">https://explorer.cisco.com/dag/saml2/idp/metadata.php</a>
URL de inicio de sesión	<a href="https://explorer.cisco.com/dag/saml2/idp/SSOService.php">https://explorer.cisco.com/dag/saml2/idp/SSOService.php</a>
URL de cierre de sesión	<a href="https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cis">https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cis</a>
URL	<a href="https://firebird.cisco.com">https://firebird.cisco.com</a>

base

E. Haga clic en "Administrar > Agregar"

Add SSO Server

IDP Entity ID:

Settings

Sign In URL:

Sign Out URL:

Base URL:

Identity Provider Certificate:

Service Provider Certificate:

Request Signature:

Request Timeout:  seconds (1-7200)

Enable IdP only accessible on Internal Network

Request IdP re-authentication at login

F. En la sección Avanzadas del perfil de conexión, defina el servidor AAA para la autorización

Vaya a "Avanzado > Autorización" y haga clic en "Agregar"

Edit AnyConnect Connection Profile: TG\_SAML

Basic

Advanced

General

Client Addressing

Authentication

Secondary Authentication

**Authorization**

Accounting

Group Alias/Group L

Authorization Server Group

Server Group:

Users must exist in the authorization database to connect

Interface-specific Authorization Server Groups

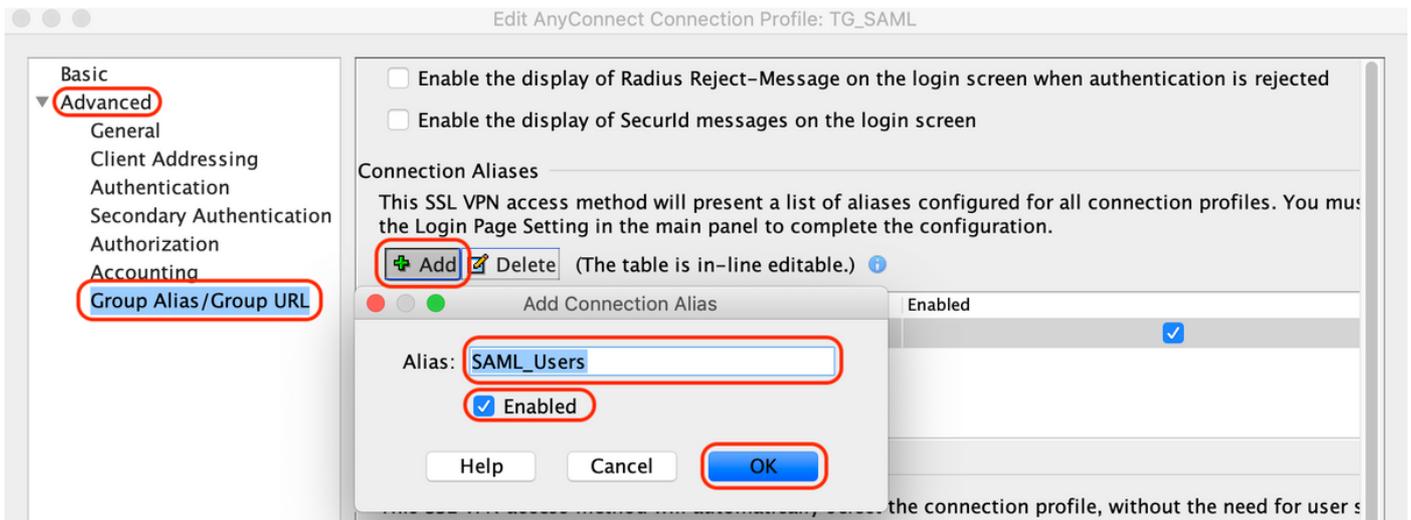
Assign Authorization Server Group to Interface

Interface:

Server Group:

G. En Alias de grupo, defina el alias de conexión

Vaya a "Avanzado > Alias de grupo/URL de grupo" y haga clic en "Agregar"



H. Esto completa la configuración de ASA, lo mismo que se ve a continuación en la interfaz de línea de comandos (CLI)

```

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

```

```

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

```

## -Configuración de ISE

### 1. Agregue Cisco ASA como dispositivo de red

En "Administration > Network Resources > Network Devices", haga clic en "Add".

Configure el nombre del dispositivo de red, la dirección IP asociada y, en "Configuración de autenticación de RADIUS", configure la "Clave secreta compartida" y haga clic en "Guardar"

Network Devices

\* Name   
Description

IP Address  /

\* Device Profile    
Model Name   
Software Version

\* Network Device Group

Location    
IPSEC    
Device Type



▼ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**  
\* Shared Secret    
Use Second Shared Secret    
  
CoA Port

RADIUS DTLS Settings

DTLS Required    
Shared Secret    
CoA Port    
Issuer CA of ISE Certificates for CoA    
DNS Name

General Settings

Enable KeyWrap    
\* Key Encryption Key    
\* Message Authenticator Code Key    
Key Input Format  ASCII  HEXADECIMAL



▶ TACACS Authentication Settings



▶ SNMP Settings



▶ Advanced TrustSec Settings

## 2. Instalar las últimas actualizaciones de estado

Vaya a "Administración > Sistema > Configuración > Estado > Actualizaciones" y haga clic en "Actualizar ahora"

### Posture Updates

Web  Offline

\* Update Feed URL

Proxy Address  ⓘ

Proxy Port  HH MM SS

Automatically check for updates starting from initial delay    every  hours ⓘ

### Update Information

Last successful update on	2020/05/07 15:15:05 ⓘ
Last update status since ISE was started	No update since ISE was started. ⓘ
Cisco conditions version	224069.0.0.0
Cisco AV/AS support chart version for windows	171.0.0.0
Cisco AV/AS support chart version for Mac OSX	91.0.0.0
Cisco supported OS version	41.0.0.0

## 3. Cargue el módulo de cumplimiento y el paquete de implementación de cabecera de AnyConnect en ISE

Vaya a "Política > Elementos de Política > Resultados > Aprovisionamiento de Cliente > Recursos". Haga clic en "Agregar" y seleccione "Recursos de agente del disco local" o "Recursos de agente del sitio de Cisco" en función de si los archivos se van a recuperar desde la estación de trabajo local o desde el sitio de Cisco.

En este caso, para cargar archivos desde la estación de trabajo local en Categoría, seleccione "Paquetes proporcionados por Cisco", haga clic en "Examinar", seleccione los paquetes necesarios y haga clic en "Enviar".

Este documento utiliza "anyconnect-win-4.3.1012.6145-isecomcompliance-webdeploy-k9.pkg"

como módulo de cumplimiento y "anyconnect-win-4.8.03052-webdeploy-k9.pkg" como paquete de implementación de cabecera de AnyConnect.

[Agent Resources From Local Disk](#) > [Agent Resources From Local Disk](#)

### Agent Resources From Local Disk

Category  ⓘ

Browse...

#### ▼ AnyConnect Uploaded Resources

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

#### 4. Crear un perfil de postura de AnyConnect

A. Vaya a "Política > Elementos de Política > Resultados > Aprovisionamiento de Cliente > Recursos". Haga clic en "Agregar" y seleccione "Perfil de postura de AnyConnect".

B. Introduzca el nombre del perfil de postura de Anyconnect y configure el nombre del servidor como "\*" en Reglas de nombre de servidor y haga clic en "Guardar"

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

\* Name:

Description:

#### Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	<input type="text" value="120"/> secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	<input type="text" value="60"/> secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	<input type="text" value="4"/>	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host	<input type="text"/>	IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	The server that the agent should connect to
Server name rules	<input type="text" value="*"/>	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List	<input type="text"/>	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	<input type="text" value="30"/> secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

## 5. Crear configuración de Anyconnect

A. Vaya a "Política > Elementos de Política > Resultados > Aprovisionamiento de Cliente > Recursos". Haga clic en "Agregar" y seleccione "Configuración de AnyConnect"

B. Seleccione el paquete de AnyConnect, introduzca el nombre de la configuración y seleccione el módulo de cumplimiento necesario

C. En "Selección de módulo AnyConnect", marque "Herramienta de diagnóstico e informes"

D. En "Selección de perfil", seleccione Perfil de postura y haga clic en "Guardar"

\* Select AnyConnect Package **AnyConnectDesktopWindows 4.8.3052.0** ▼

\* Configuration Name **AnyConnect Configuration**

Description:

**DescriptionValue**

\* Compliance Module **AnyConnectComplianceModuleWindows 4.3.1250.614** ▼

Notes

**AnyConnect Module Selection**

ISE Posture

VPN

Network Access Manager

Web Security

AMP Enabler

ASA Posture

Network Visibility

Umbrella Roaming Security

Start Before Logon

**Diagnostic and Reporting Tool**

**Profile Selection**

\* ISE Posture **Anyconnect Posture Profile** ▼

VPN ▼

Network Access Manager ▼

Web Security ▼

AMP Enabler ▼

Network Visibility ▼

Umbrella Roaming Security ▼

Customer Feedback ▼

6. Crear política de aprovisionamiento de clientes

A. Vaya a "Política > Aprovisionamiento de clientes"

B. Haga clic en "Editar" y seleccione "Insertar regla arriba"

C. Introduzca el nombre de la regla, seleccione el sistema operativo necesario y, en Resultados (en "Agente" > "Configuración de agente" ), seleccione "Configuración de AnyConnect" que se creó en el paso 5 y haga clic en "Guardar"

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

Policy Sets Profiling Posture Client Provisioning Policy Elements

### Client Provisioning Policy

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

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

Save Reset

## 7. Crear una condición de postura

A. Vaya a "Política > Elementos de Política > Condiciones > Condición > Condición de Archivo"

B. Haga clic en "Agregar" y configure el nombre de la condición "VPN\_Posture\_File\_Check", el sistema operativo requerido como "Windows 10(All)", el tipo de archivo como "FileExistence", la ruta de acceso del archivo como "ABSOLUTE\_PATH" y la ruta de acceso completa y el nombre del archivo como "C:\custom.txt", seleccione File Operator as "Exists" (Operador de archivos)

C. Este ejemplo utiliza la presencia de un archivo denominado "custom.txt" bajo C: drive como condición del archivo

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

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

### File Conditions List > VPN\_Posture\_File\_Check

#### File Condition

\* Name: VPN\_Posture\_File\_Check

Description:

\* Operating System: Windows 10 (All)

Compliance Module: Any version

\* File Type: FileExistence

\* File Path: ABSOLUTE\_PATH

\* File Operator: Exists

C:\custom.txt

Save Reset

## 8. Crear acción de remediación de postura

Vaya a "Política > Elementos de política > Resultados > Postura > Acciones de remediación" para crear la acción de remediación de archivo correspondiente. Este documento utiliza "Message Text Only" (Sólo texto del mensaje) como Acciones de remediación que se configuran en el paso siguiente.

## 9. Crear regla de requisito de condición

A. Vaya a "Política > Elementos de Política > Resultados > Postura > Requisitos"

B. Haga clic en "Editar" y seleccione "Insertar nuevo requisito"

C. Configure el nombre de condición "VPN\_Posture\_Requirement", el sistema operativo requerido como "Windows 10(All)", el módulo de cumplimiento como "4.x o posterior" y el tipo de condición como "Anyconnect"

D. Condiciones como "VPN\_Posture\_File\_Check" (creado en el paso 7) y en Acciones de remediación, seleccione Acción como "Sólo texto de mensaje" e introduzca el mensaje personalizado para Usuario agente

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

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

Save Reset

## 10. Crear una política de estado

A. Vaya a "Políticas > Condición"

B. Configure el nombre de la regla como "VPN\_Posture\_Policy\_Win", el sistema operativo requerido como "Windows 10(All)", el módulo de cumplimiento como "4.x o posterior", el tipo de postura como "Anyconnect" y los requisitos como "VPN\_Posture\_Requirement" como se configuraron en el paso 9

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

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

Save Reset

## 11. Crear ACL dinámicas (DACL)

Vaya a "Política > Elementos de política > Resultados > Autorización > ACL descargables" y cree las DACL para diferentes estados de estado.

Este documento utiliza las siguientes DACL.

A. Condición desconocida: permite el tráfico a DNS, PSN, HTTP y HTTPS

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Downloadable ACL List > PostureUnknown

**Downloadable ACL**

\* Name: PostureUnknown

Description: [Empty]

IP version:  IPv4  IPv6  Agnostic

\* DACL Content:

```

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

```

Check DACL Syntax

Save Reset

B. Estado no conforme: deniega el acceso a las subredes privadas y solo permite el tráfico de Internet

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Dictionaries > Conditions > Results

Downloadable ACL List > PostureNonCompliant

**Downloadable ACL**

\* Name: PostureNonCompliant

Description: [Empty]

IP version:  IPv4  IPv6  Agnostic

\* DACL Content:

```

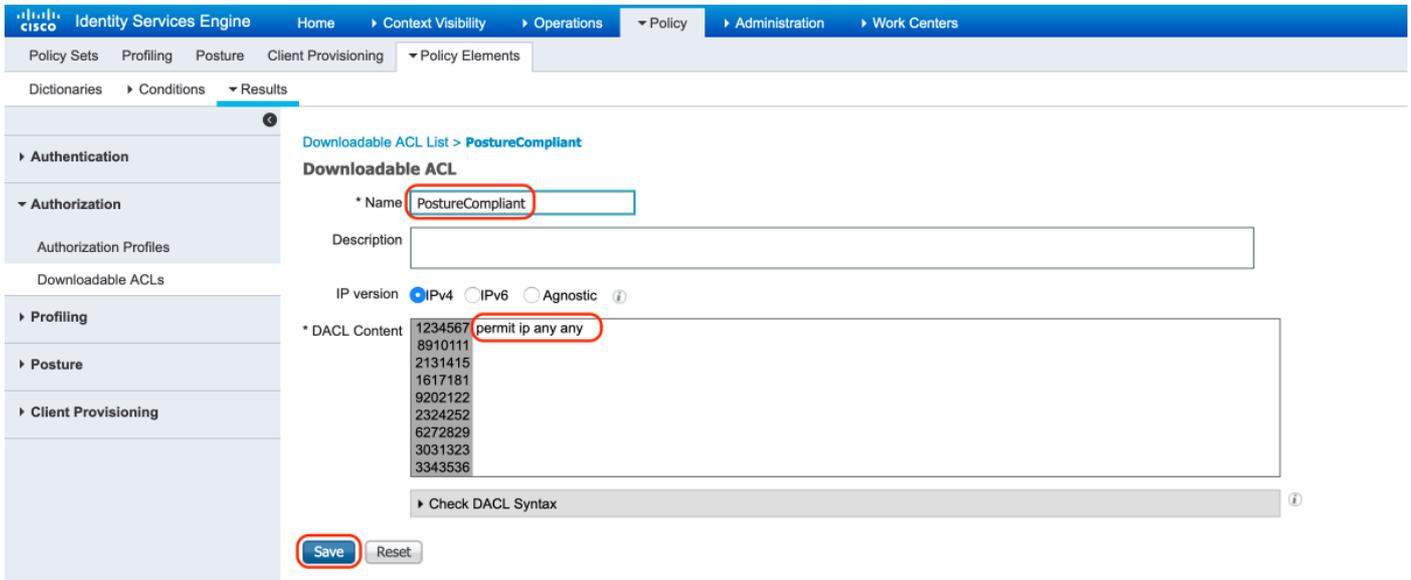
1234567 deny ip any 10.0.0.0 255.0.0.0
8910111 deny ip any 172.16.0.0 255.240.0.0
2131415 deny ip any 192.168.0.0 255.255.0.0
1617181 permit ip any any
9202122
2324252
6272829
3031323
3343536

```

Check DACL Syntax

Save Reset

C. Conforme a la condición: permite todo el tráfico para los usuarios finales que cumplen la condición

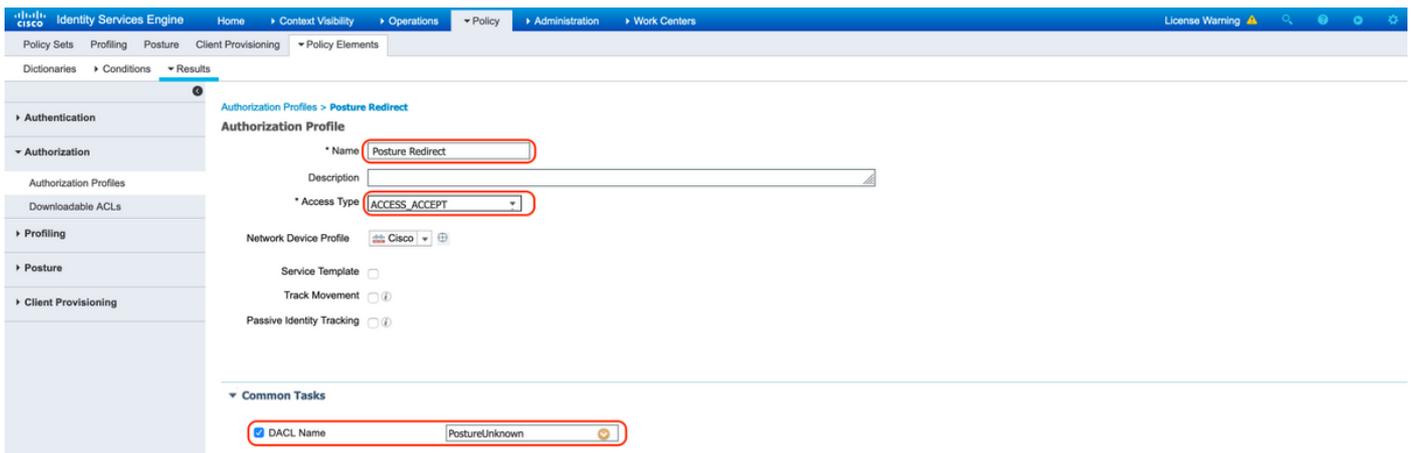


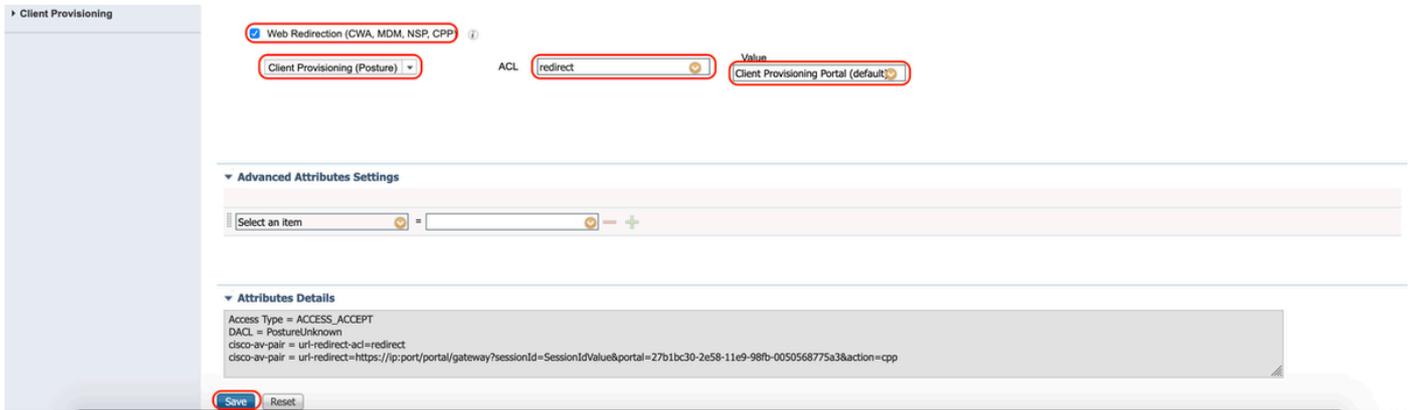
## 12. Crear perfiles de autorización

Vaya a "Política > Elementos de Política > Resultados > Autorización > Perfiles de Autorización".

### A. Perfil de autorización para postura desconocida

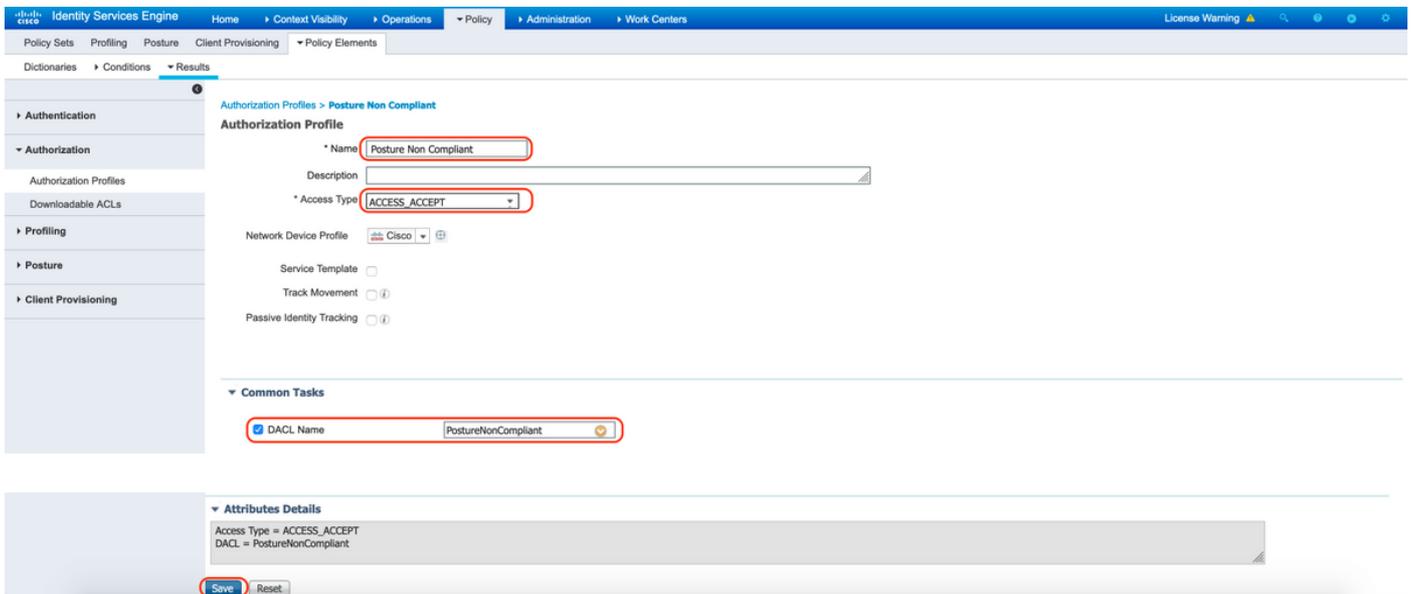
Seleccione DACL "PostureUnknown", marque Web Redirection (Redirección web), seleccione Client Provisioning (Posture) (Aprovisionamiento de clientes), configure Redirect ACL name "redirect" (Redirigir nombre de ACL) (que se configurará en ASA) y seleccione el portal Client Provisioning (Aprovisionamiento de clientes) (predeterminado)





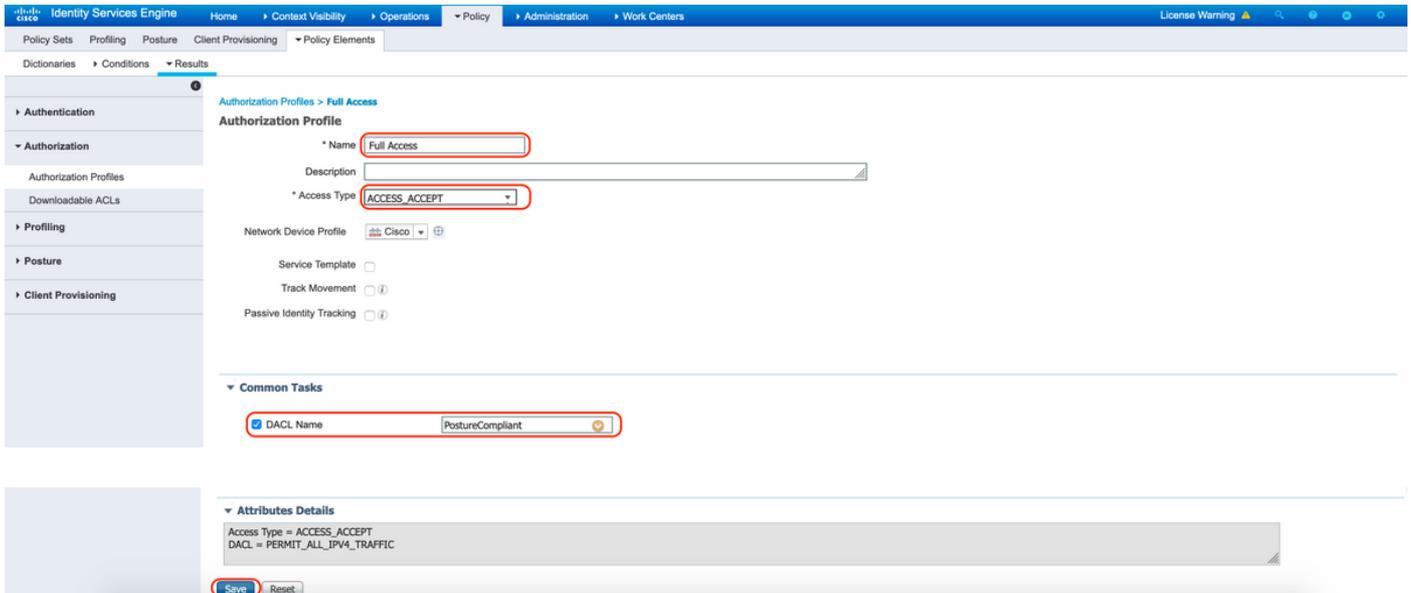
## B. Perfil de autorización para postura no conforme

Seleccione DACL "PostureNonCompliant" para limitar el acceso a la red



## C. Perfil de autorización para el cumplimiento del estado

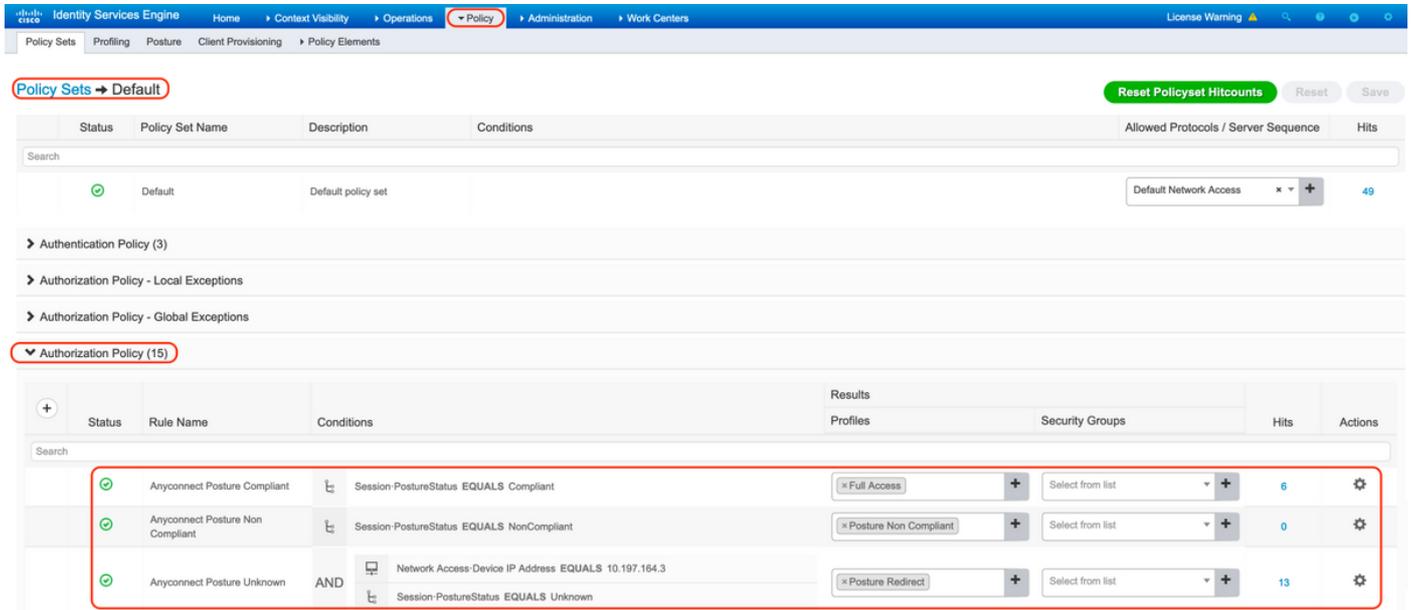
Seleccione DACL "PostureCompliant" para permitir el acceso completo a la red



## 12. Configurar políticas de autorización

Utilice los perfiles de autorización configurados en el paso anterior para configurar 3 políticas de autorización para Posture Compliant, Posture Non-Compliant y Posture Unknown.

La condición común "Session: Posture Status" se utiliza para determinar los resultados de cada política



## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Para verificar si el usuario se autenticó correctamente, ejecute el siguiente comando en ASA.

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

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

TG\_SAML

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

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

AnyConnect-Parent:

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

SSL-Tunnel:

Tunnel ID : 125.2  
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 57248  
TCP Dst Port : 443 Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes

Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
Bytes Tx : 7973 Bytes Rx : 0  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Filter Name : #ACSACL#-IP-PostureUnknown-5ee45b05

DTLS-Tunnel:

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

#ACSACL#-IP-PostureUnknown-5ee45b05

ISE Posture:

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

Una vez finalizada la evaluación de estado, el acceso del usuario cambia a acceso completo, como se observa en la DACL introducida en el campo "Nombre del filtro"

<#root>

firebird(config)#

show vpn-sess detail anyconnect

Session Type: AnyConnect Detailed

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

TG\_SAML

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

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

AnyConnect-Parent:

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

SSL-Tunnel:

Tunnel ID : 125.2  
Assigned IP : explorer.cisco.com Public IP : 10.197.243.143  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 57248  
TCP Dst Port : 443 Auth Mode : SAML  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.8.03052  
Bytes Tx : 7973 Bytes Rx : 0  
Pkts Tx : 6 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Filter Name : #ACSACL#-IP-PERMIT\_ALL\_IPV4\_TRAFFIC-57f6b0d3

DTLS-Tunnel:

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

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

Para comprobar si la autorización se ha realizado correctamente en ISE, vaya a "Operaciones > RADIUS > Registros en directo"

Esta sección muestra la información relevante asociada al usuario autorizado, es decir, la identidad, el perfil de autorización, la política de autorización y el estado.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentica...	Authorizati...	Authorization Pro...	Posture St...	IP Address	Network Device
Jun 14, 2020 07:44:59.975 AM			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				#ACSACL#-IP-PERMI...	10.197.243.143			Anyconnect ...	Full Access	Compliant		ASA
Jun 14, 2020 07:44:59.975 AM				#ACSACL#-IP-Posture...								ASA
Jun 14, 2020 07:44:34.963 AM												ASA
Jun 14, 2020 07:44:34.958 AM				_585b5291f01484dfd1...	00:50:56:A0:D6:97	Windows10-...	Default	Default >> A...	Posture Redirect	Pending		ASA

Nota: para obtener información adicional sobre la validación del estado de ISE, consulte la siguiente documentación:

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

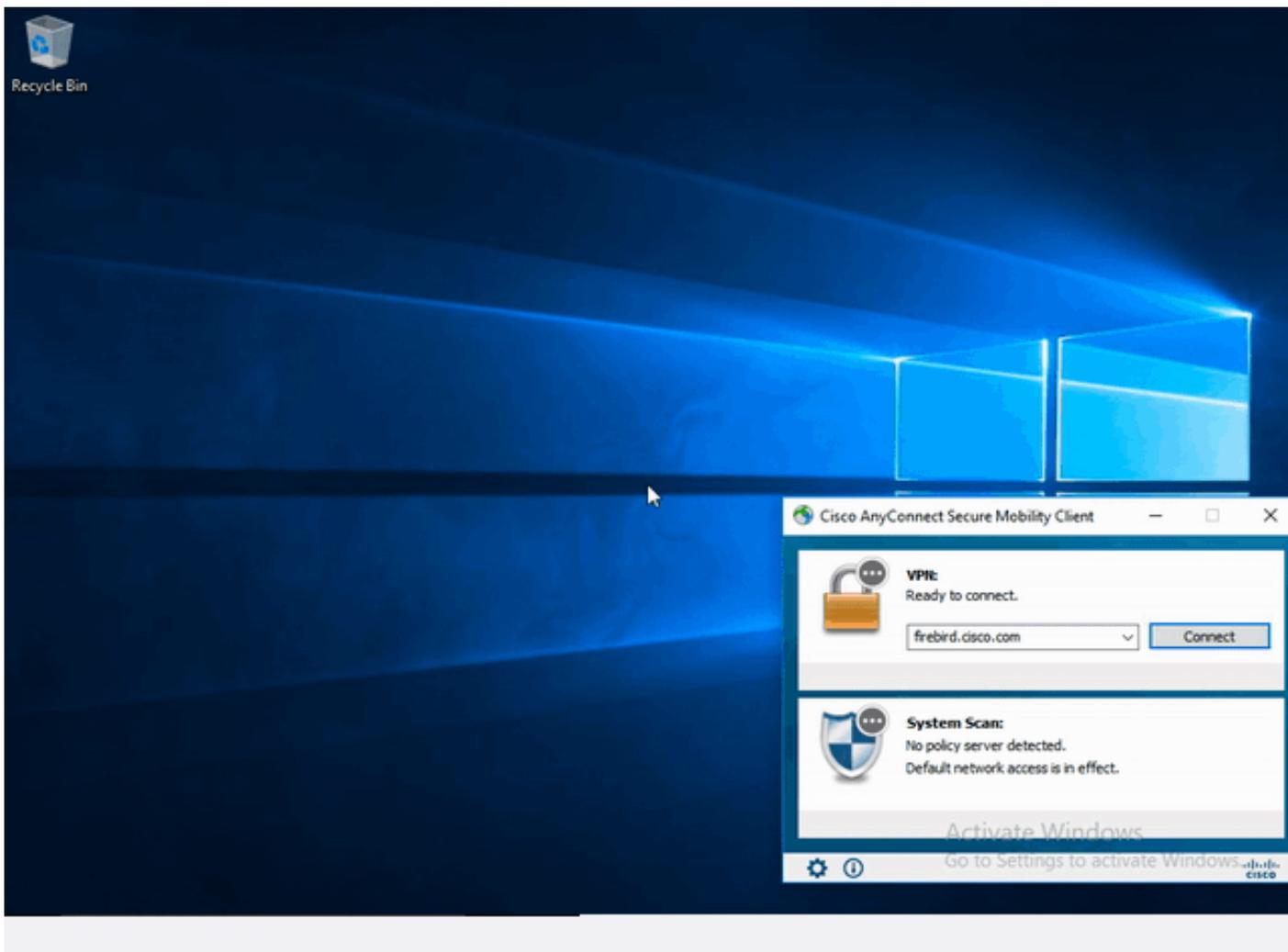
Para verificar el estado de autenticación en Duo Admin Portal, haga clic en "Informes" en el lado izquierdo del Panel de administración que muestra el Registro de autenticación.

Más información: <https://duo.com/docs/administration#reports>

Para ver el registro de depuración para el gateway de acceso dúo, utilice el siguiente enlace:

[https://help.duo.com/s/article/1623?language=en\\_US](https://help.duo.com/s/article/1623?language=en_US)

## Experiencia de usuario



## Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

---

 **Nota:** Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

---

 **Precaución:** En ASA, puede establecer varios niveles de depuración; de forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, puede aumentar la verbosidad de los depuradores. Hágalo con precaución, especialmente en entornos de producción.

---

La mayoría de la resolución de problemas de SAML implicará un error de configuración que se puede encontrar al verificar la configuración de SAML o ejecutar depuraciones.

"debug webvpn saml 255" se puede utilizar para resolver la mayoría de los problemas; sin embargo, en escenarios donde esta depuración no proporciona información útil, se pueden ejecutar depuraciones adicionales:

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

Para resolver problemas de autenticación y autorización en ASA, utilice los siguientes comandos debug:

```
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)
```



Nota: para obtener información detallada sobre el flujo de estado y la resolución de problemas de AnyConnect e ISE, consulte el siguiente enlace:

[Comparación del estilo de postura de ISE para versiones anteriores y posteriores a la 2.2](#)

Para interpretar y resolver problemas de los registros de depuración del gateway de acceso dúo

[https://help.duo.com/s/article/5016?language=en\\_US](https://help.duo.com/s/article/5016?language=en_US)

---

## Información Relacionada

<https://www.youtube.com/watch?v=W6bE2GTU0Is&>

<https://duo.com/docs/cisco#asa-ssl-vpn-using-saml>

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

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).