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

## Contenido



## 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

---

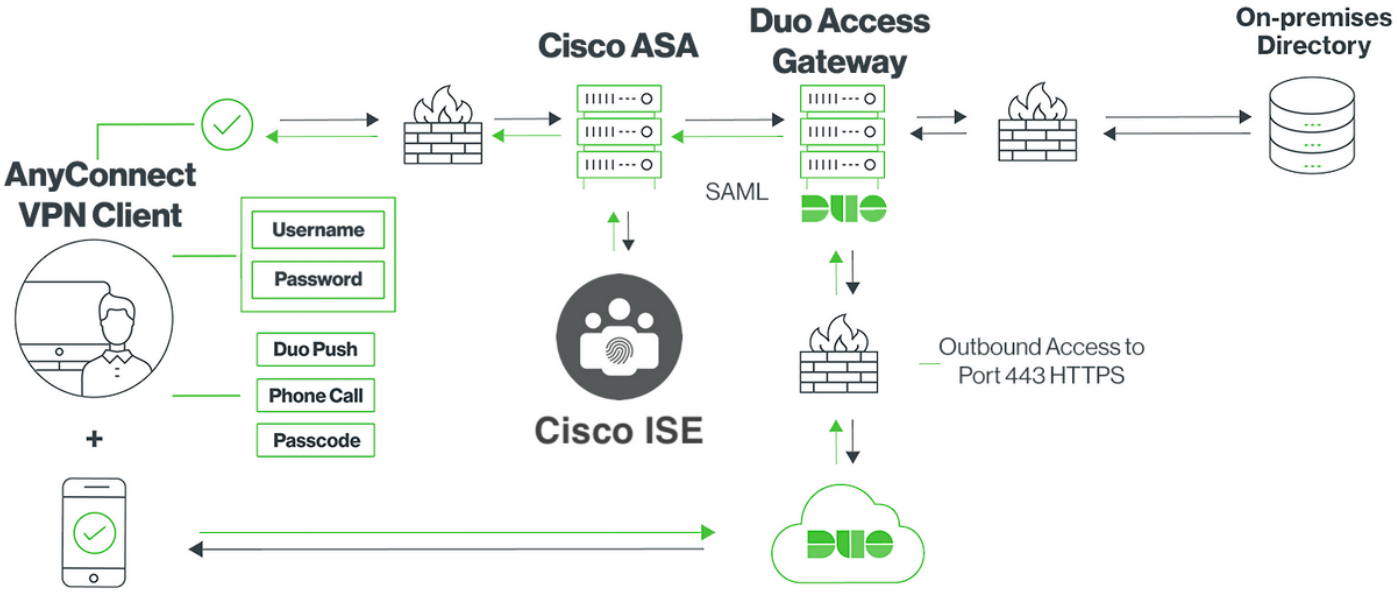
Nota: el explorador integrado Anyconnect, utilizado en esta implementación, requiere ASA en las versiones 9.7(1)24, 9.8(2)28, 9.9(2)1 o superior de cada versión, y AnyConnect versión 4.6 o posterior.

---

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

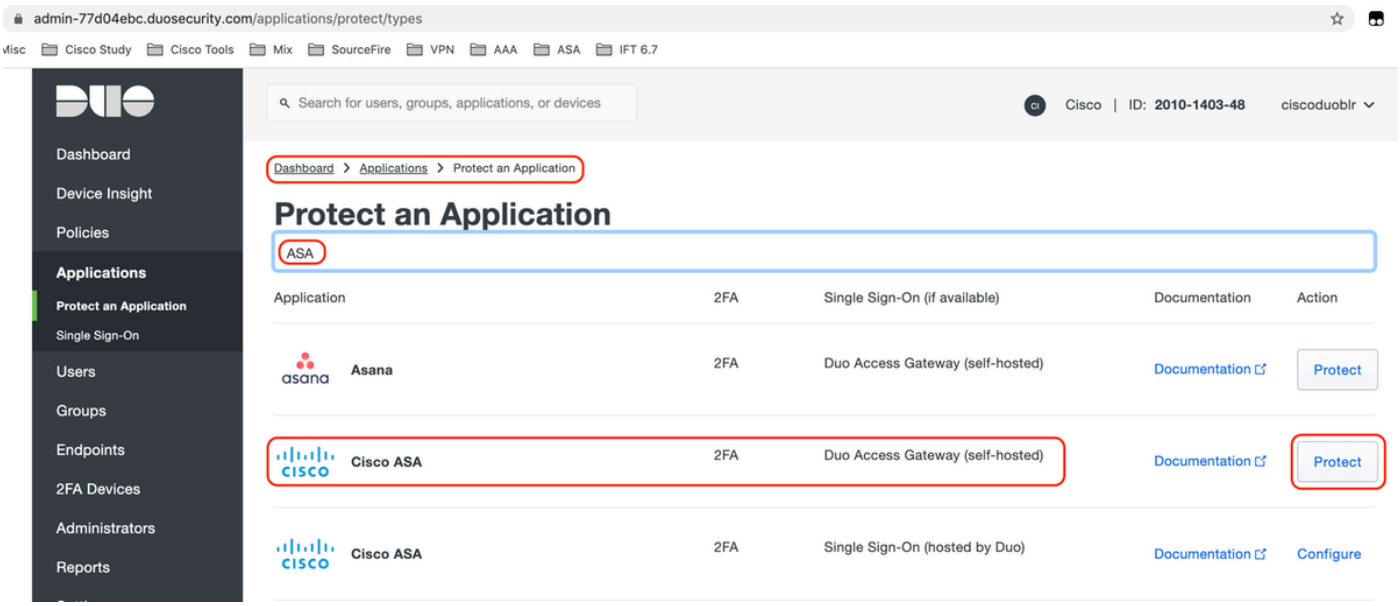
16. Si el estado del cliente cambia de Desconocido a Conforme, se envía una solicitud de cambio de autorización (CoA) desde Cisco ISE a Cisco ASA para conceder acceso completo al cliente y se establece VPN completamente

## Configuraciones

### - Configuración de Duo Admin Portal

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

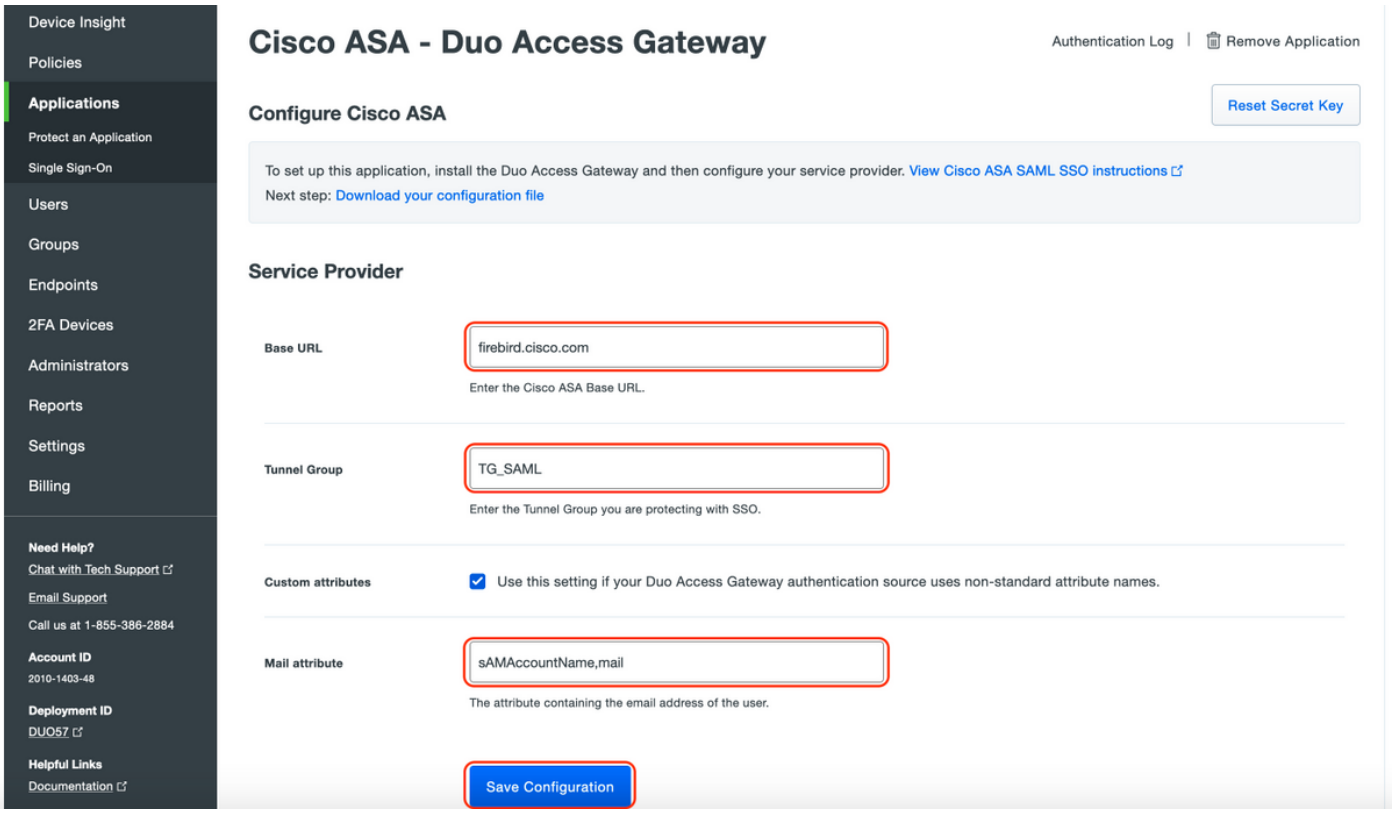
1. Inicie sesión en "Duo Admin Portal" y navegue hasta "Applications > Protect an Application", y busque "ASA" con tipo de protección "2FA with Duo Access Gateway, self-hosting". Haga clic en "Proteger" en el extremo derecho para configurar Cisco ASA



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

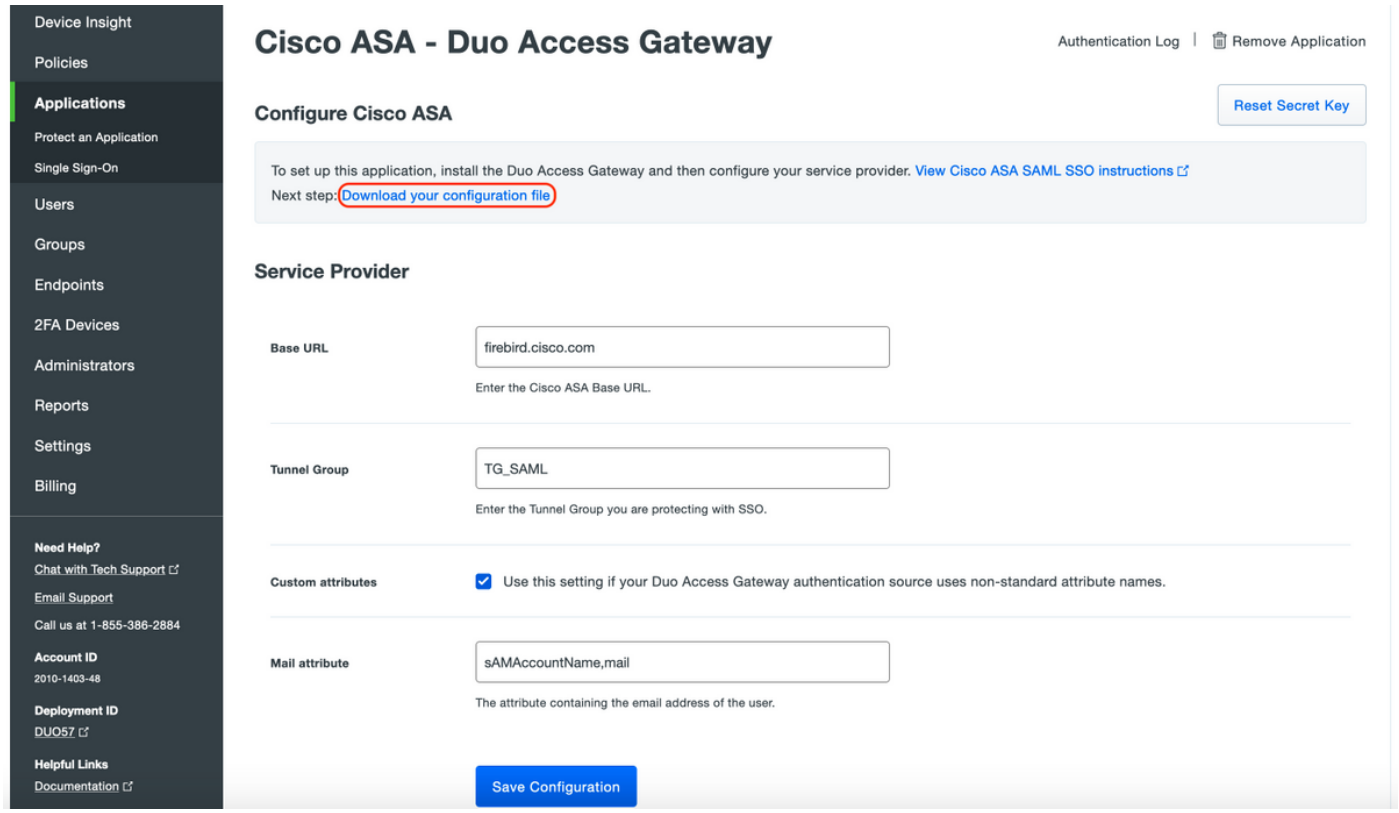
| | |
|---|---|
| URL base | firebird.cisco.com |
| Grupo de Túnel | TG_SAML |
| Atributo de correo | sAMAccountName,mail |

Haga clic en "Guardar" al final de la página

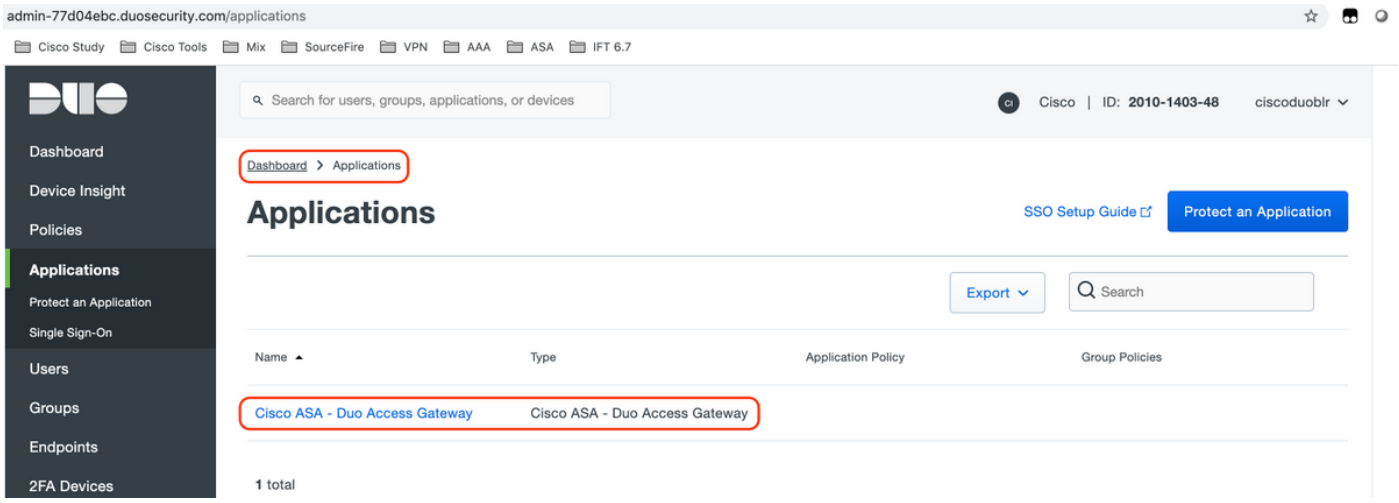



En este documento, el resto de la configuración utiliza parámetros predeterminados pero se pueden establecer en función de los requisitos del cliente.
En este momento se pueden ajustar ajustes adicionales para la nueva aplicación SAML, como cambiar el nombre de la aplicación del valor predeterminado, 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

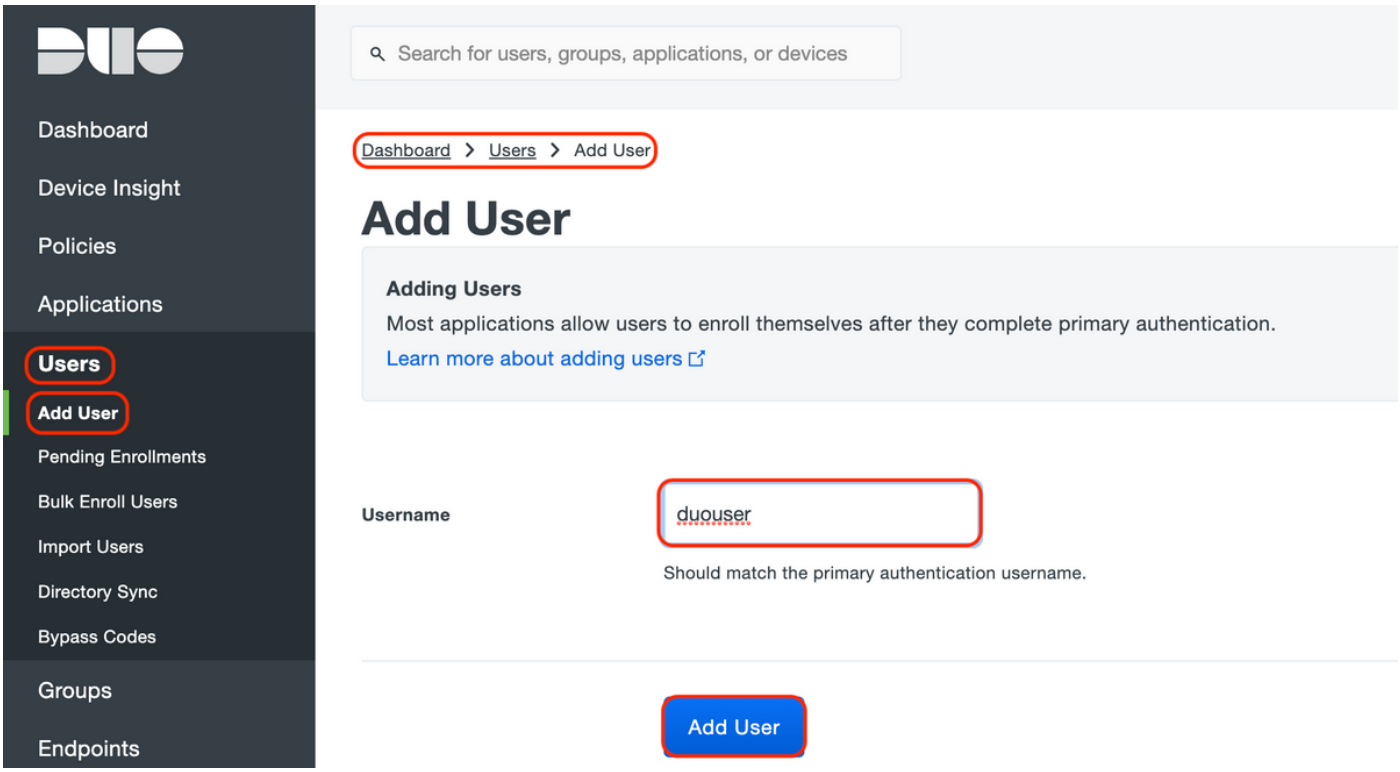



4. En "Panel > Aplicaciones", la aplicación ASA recién creada se ve como se muestra en la siguiente imagen:

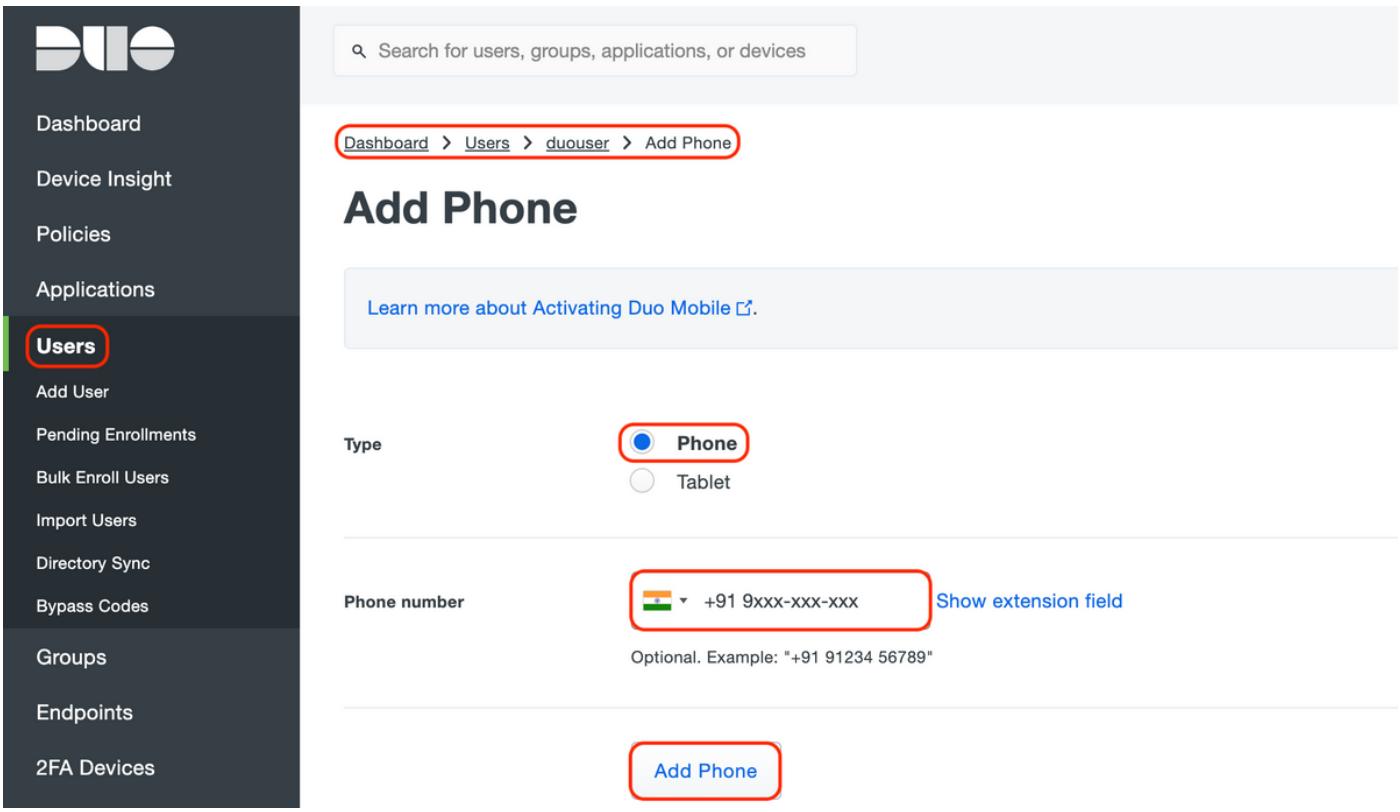



5. Navegue hasta "Usuarios > Agregar usuario" como se muestra en la imagen:

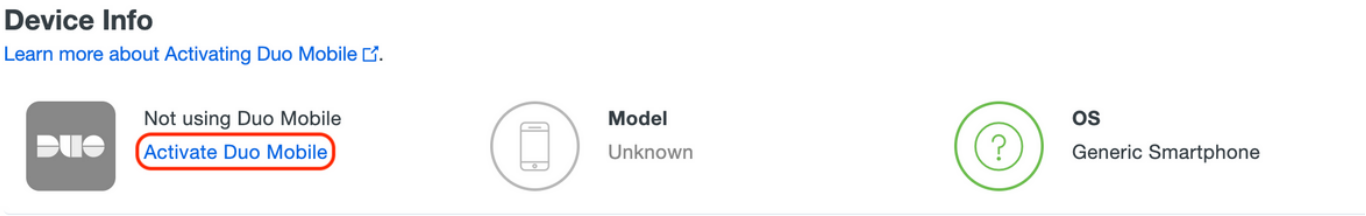
Cree un usuario denominado "duouser" para utilizarlo en la autenticación de acceso remoto de Anyconnect y active Duo Mobile en el dispositivo del usuario final




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

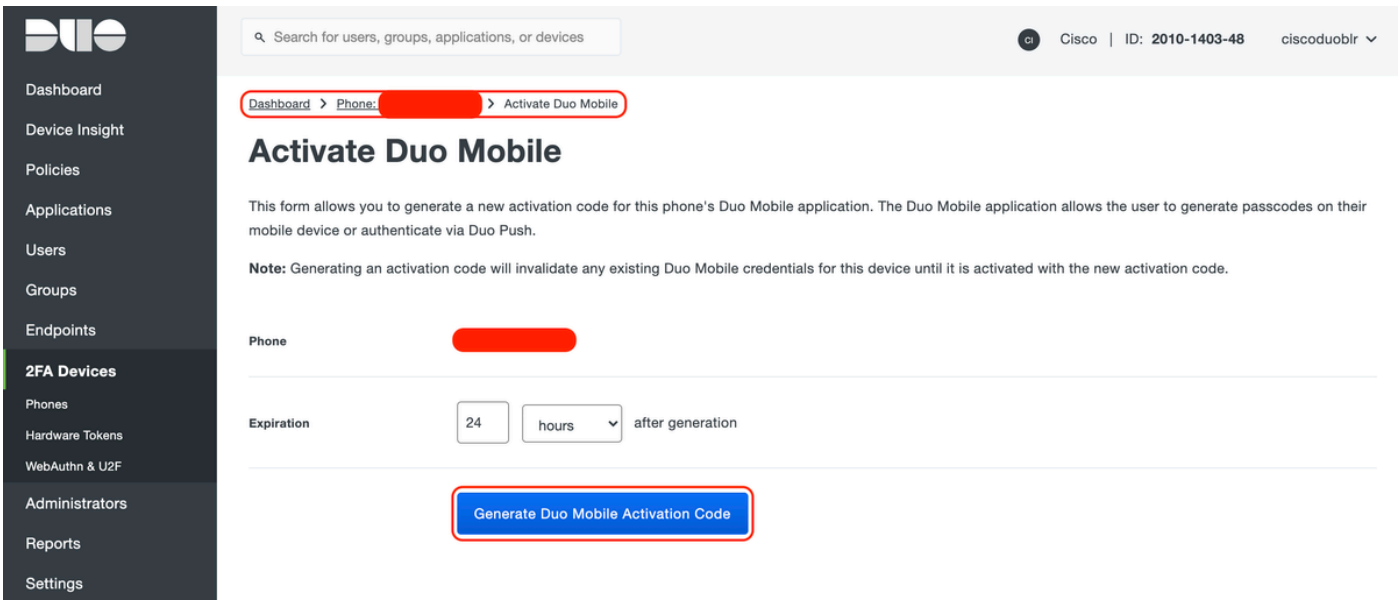



Activar "Duo Mobile" para el usuario concreto

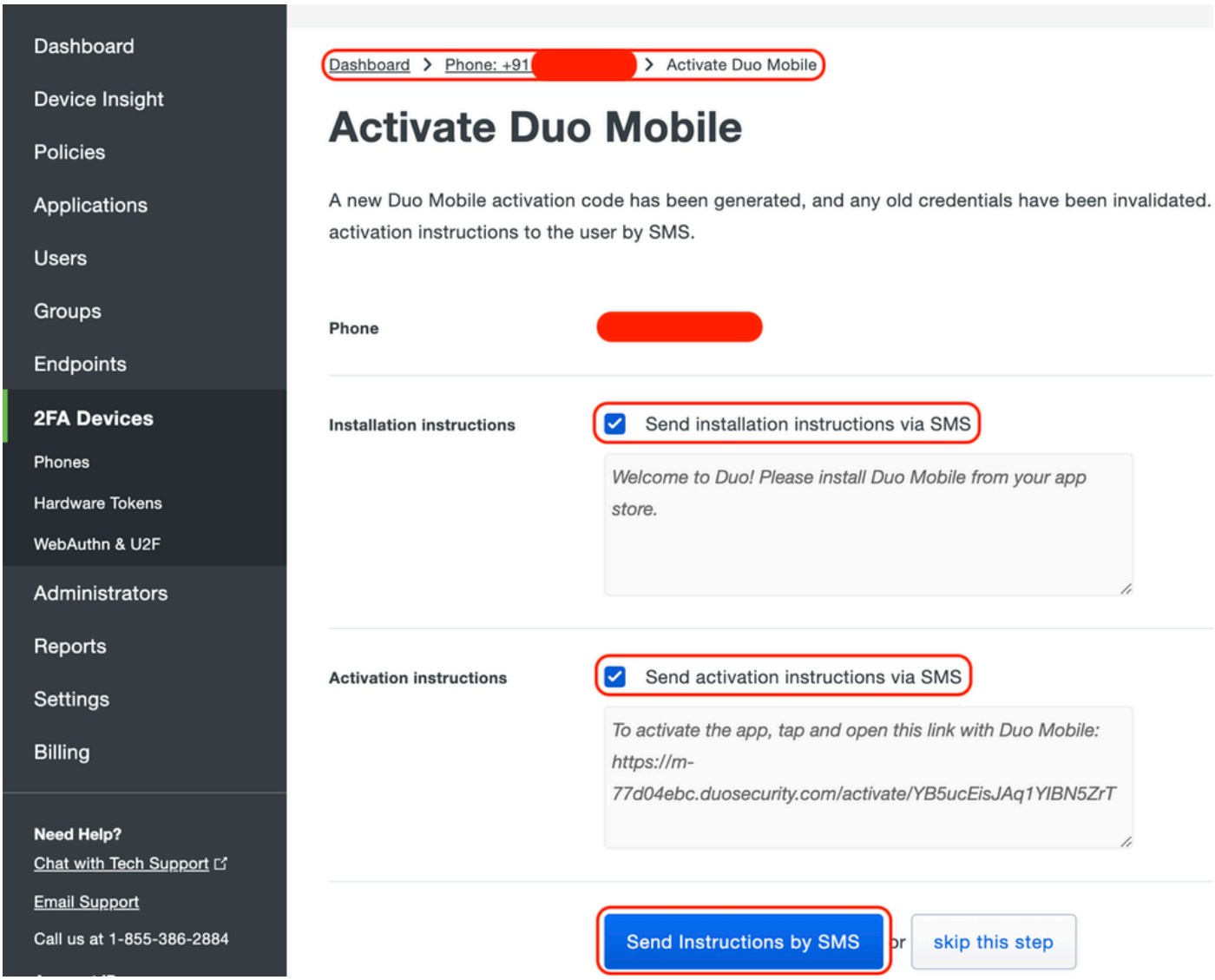



Nota: Asegúrese de tener "Duo Mobile" instalado en el dispositivo del usuario final.
Instalación manual de la aplicación Duo para dispositivos IOS
Instalación manual de la aplicación Duo para dispositivos Android

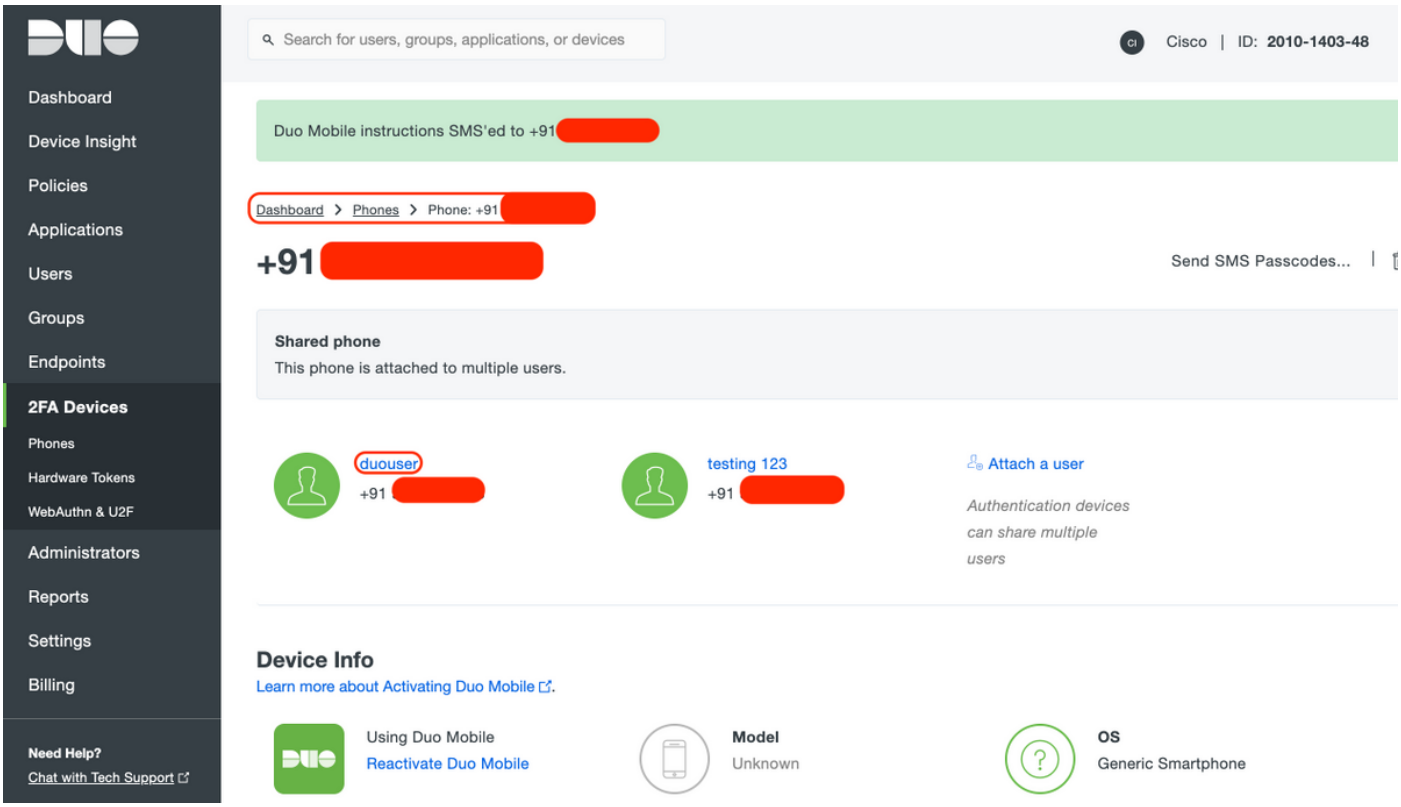
Seleccione "Generar Duo Mobile Activation Code" como se muestra en la imagen:




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




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:




- 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:

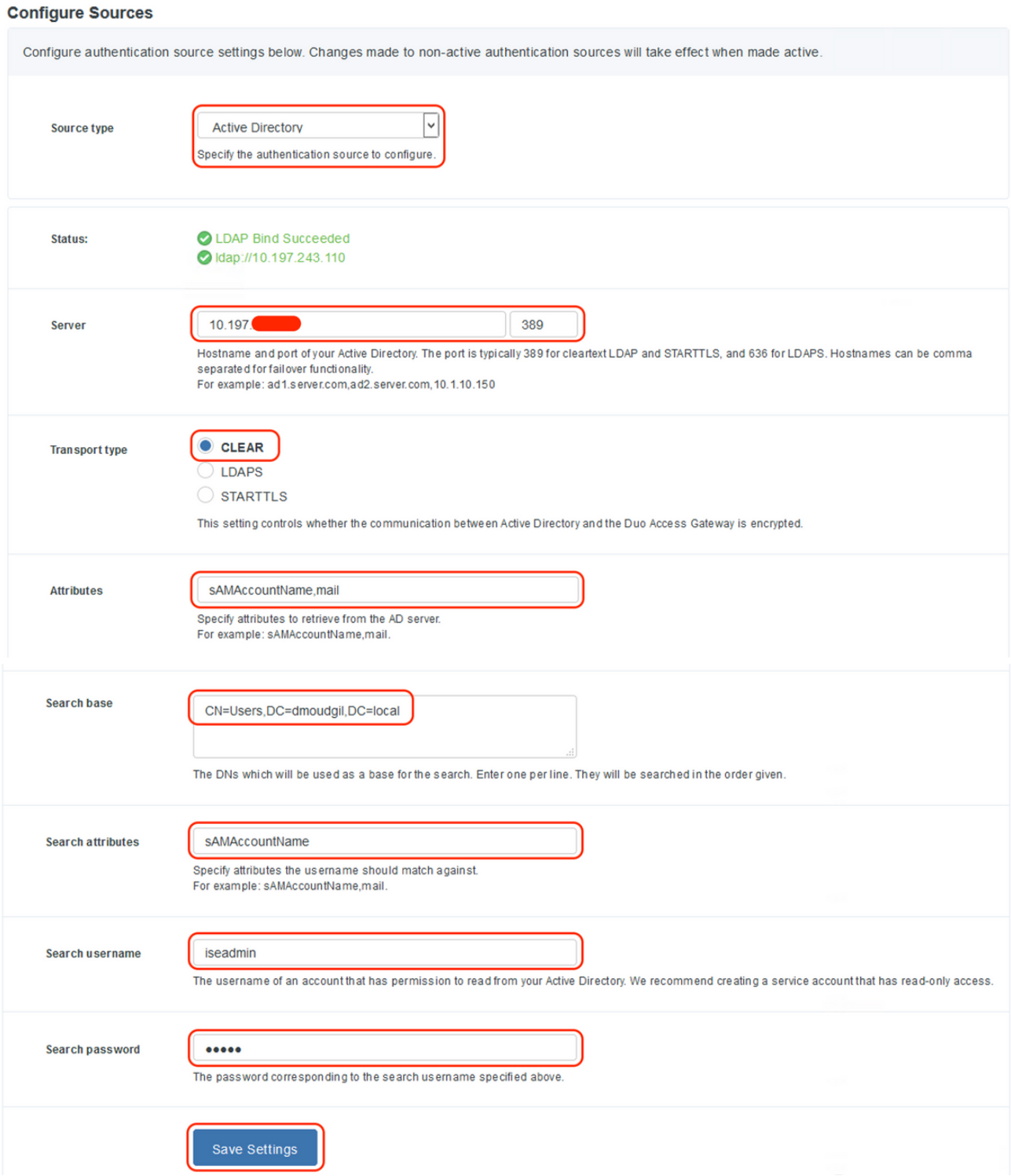
Gateway de acceso Duo para Linux
https://duo.com/docs/dag-linux

Puerta de enlace de acceso Duo para Windows
https://duo.com/docs/dag-windows

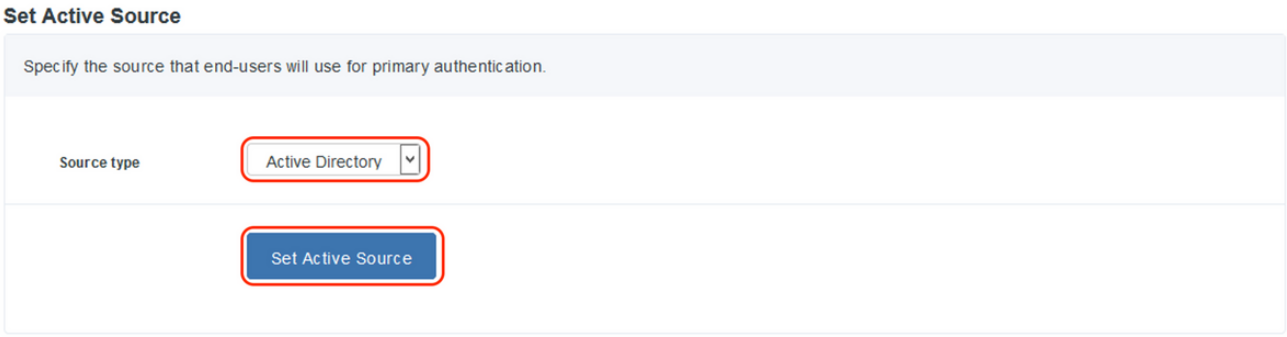
---

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

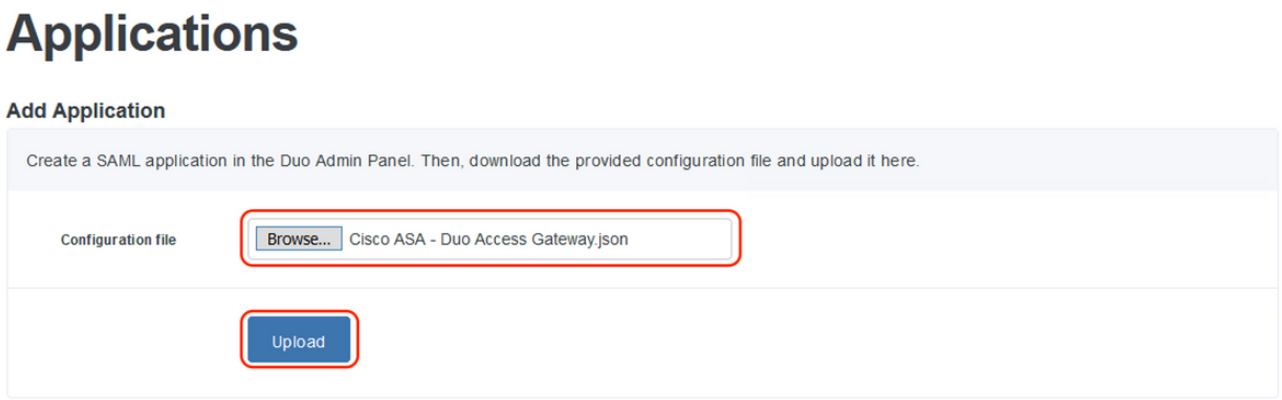
3. En "Configurar orígenes", introduzca los siguientes atributos para su Active Directory y haga clic en "Guardar parámetros"



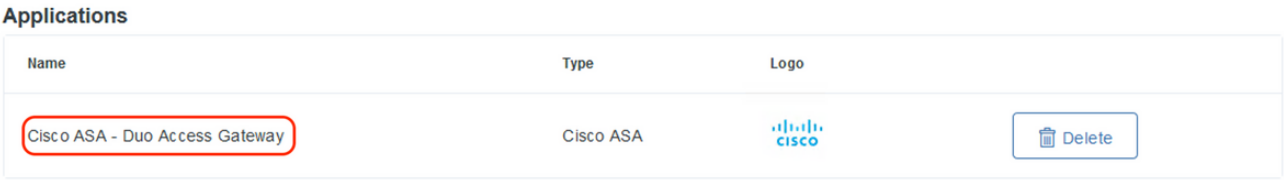

4. En "Set Active Source", seleccione el tipo de origen como "Active Directory" y haga clic en "Set Active Source"




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

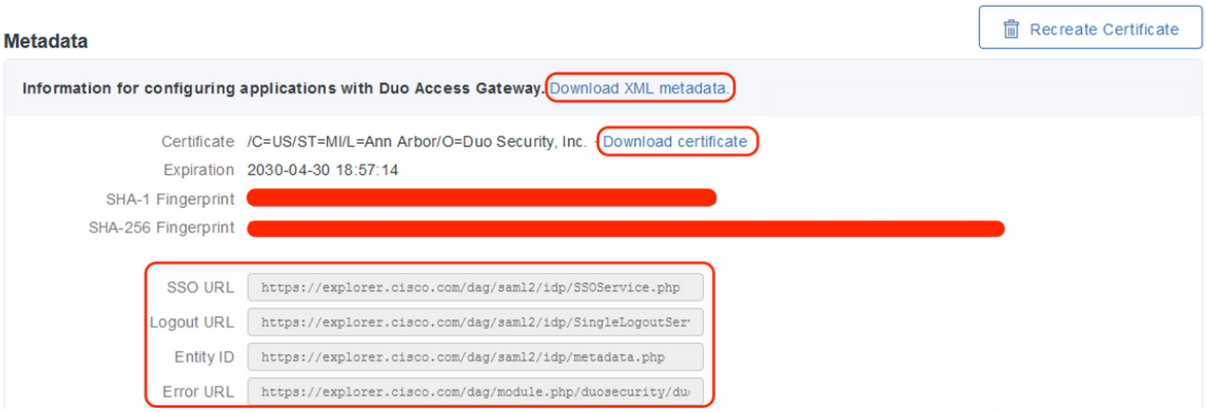



6. Una vez agregada correctamente la aplicación, aparece en el submenú "Aplicaciones"




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




## - Configuración de ASA

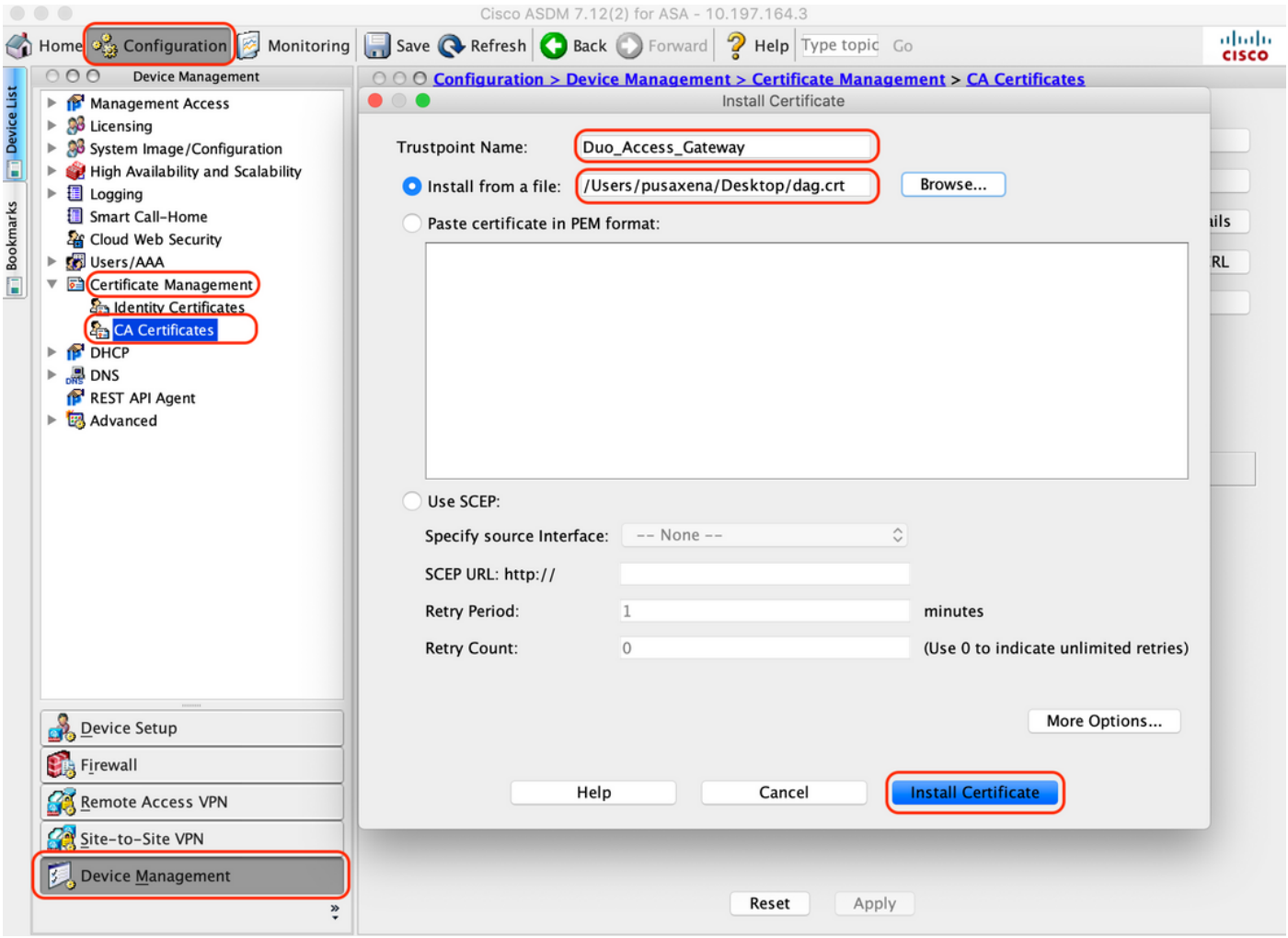
Esta sección proporciona información para configurar ASA para la autenticación IDP de SAML y la configuración básica de AnyConnect. El documento proporciona los pasos de configuración de ASDM y la configuración de ejecución de CLI para la descripción general.

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"

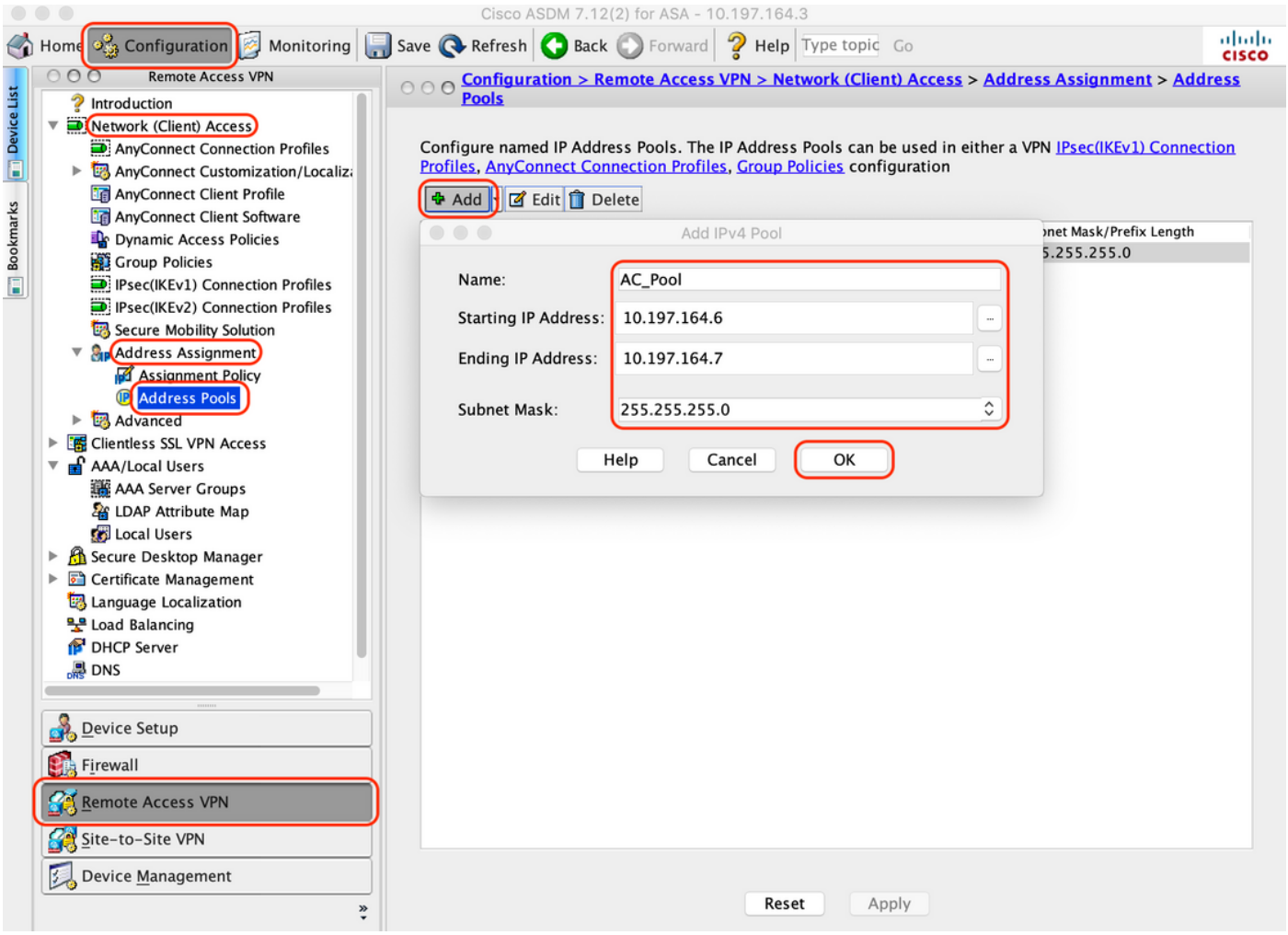
B. En la "Página de instalación del certificado", configure el nombre del punto de confianza: Duo_Access_Gateway

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

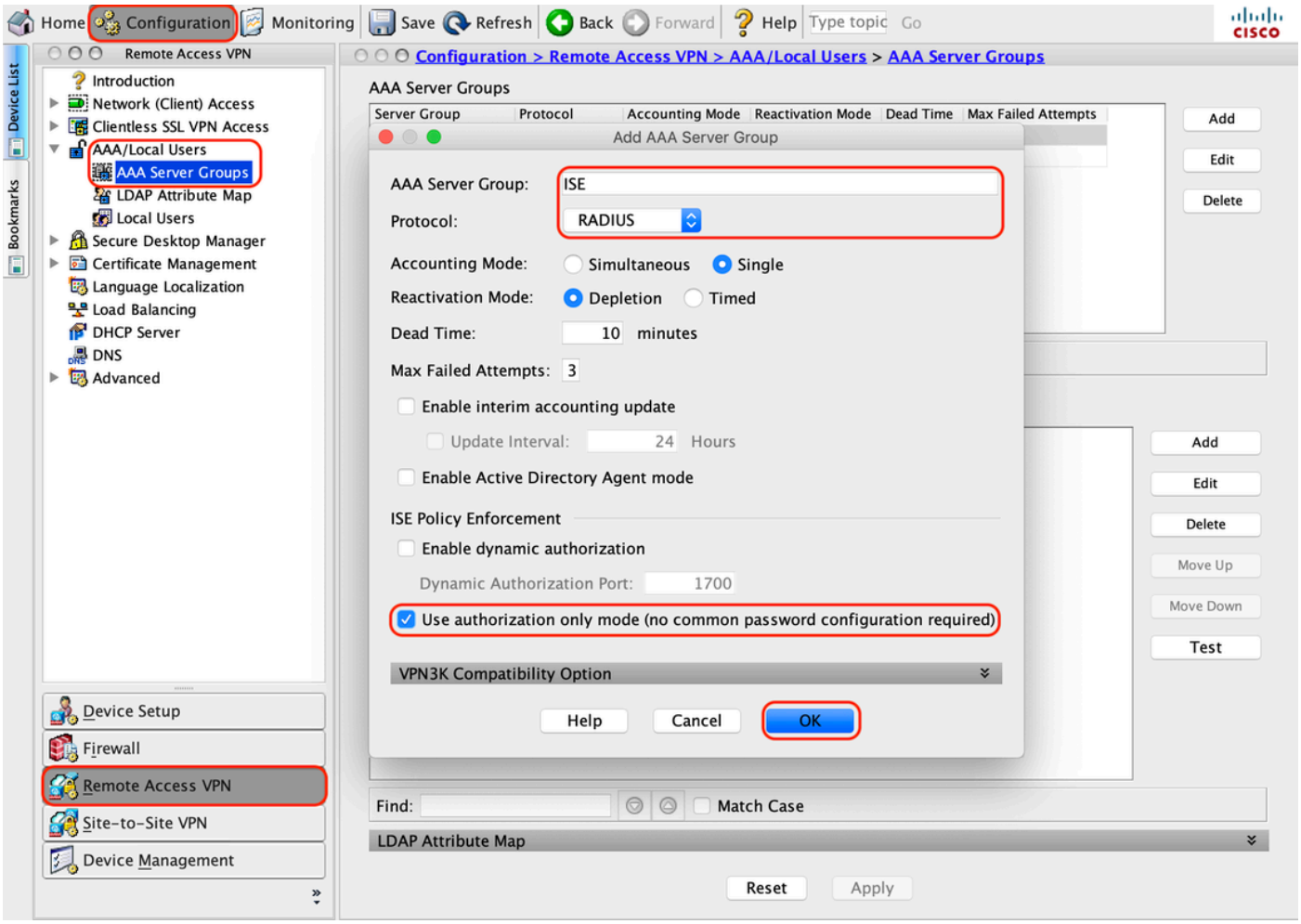
Vaya a "Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools" y haga clic en "Add"



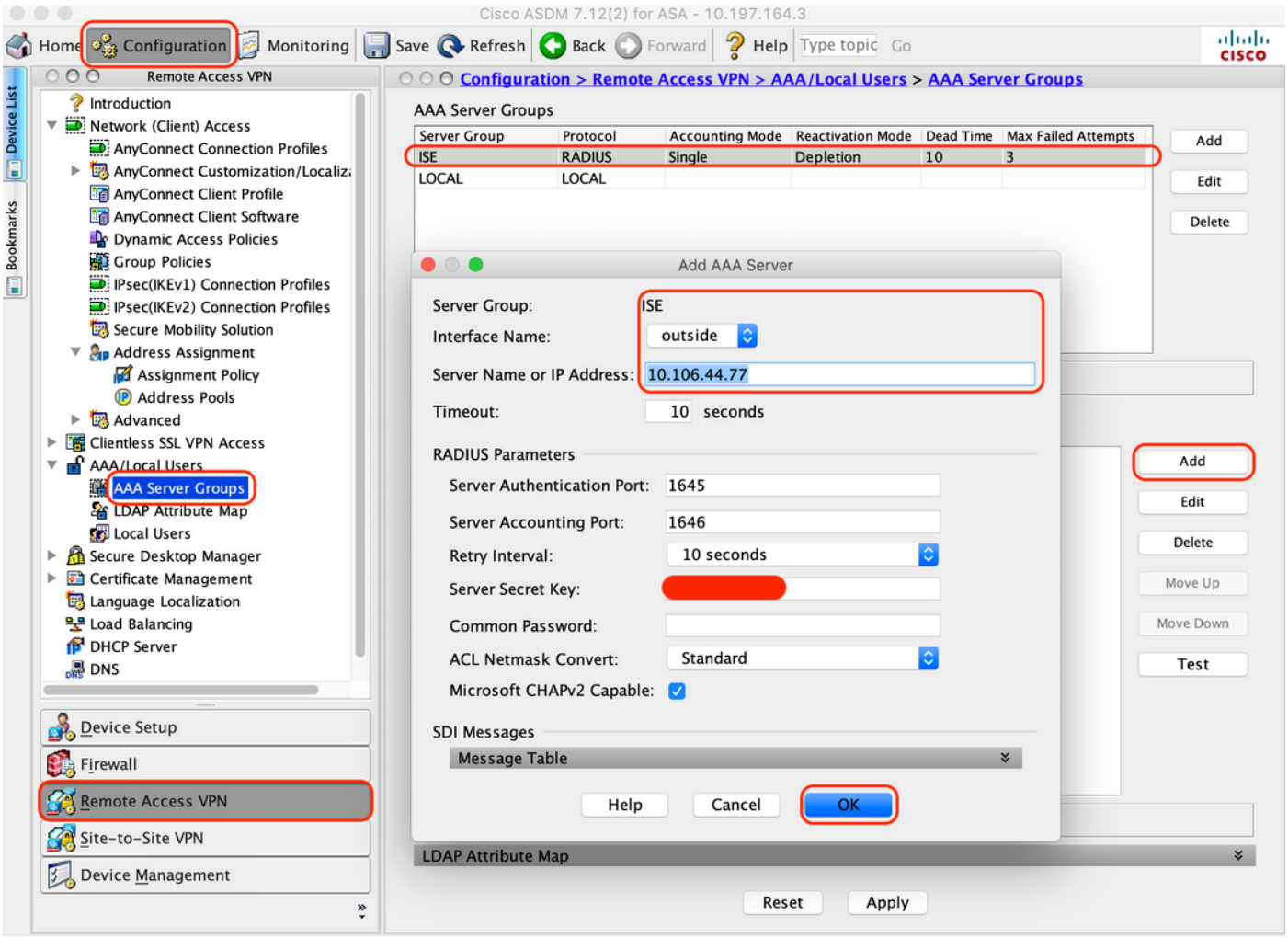

3. Configuración del Grupo de Servidores AAA

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"



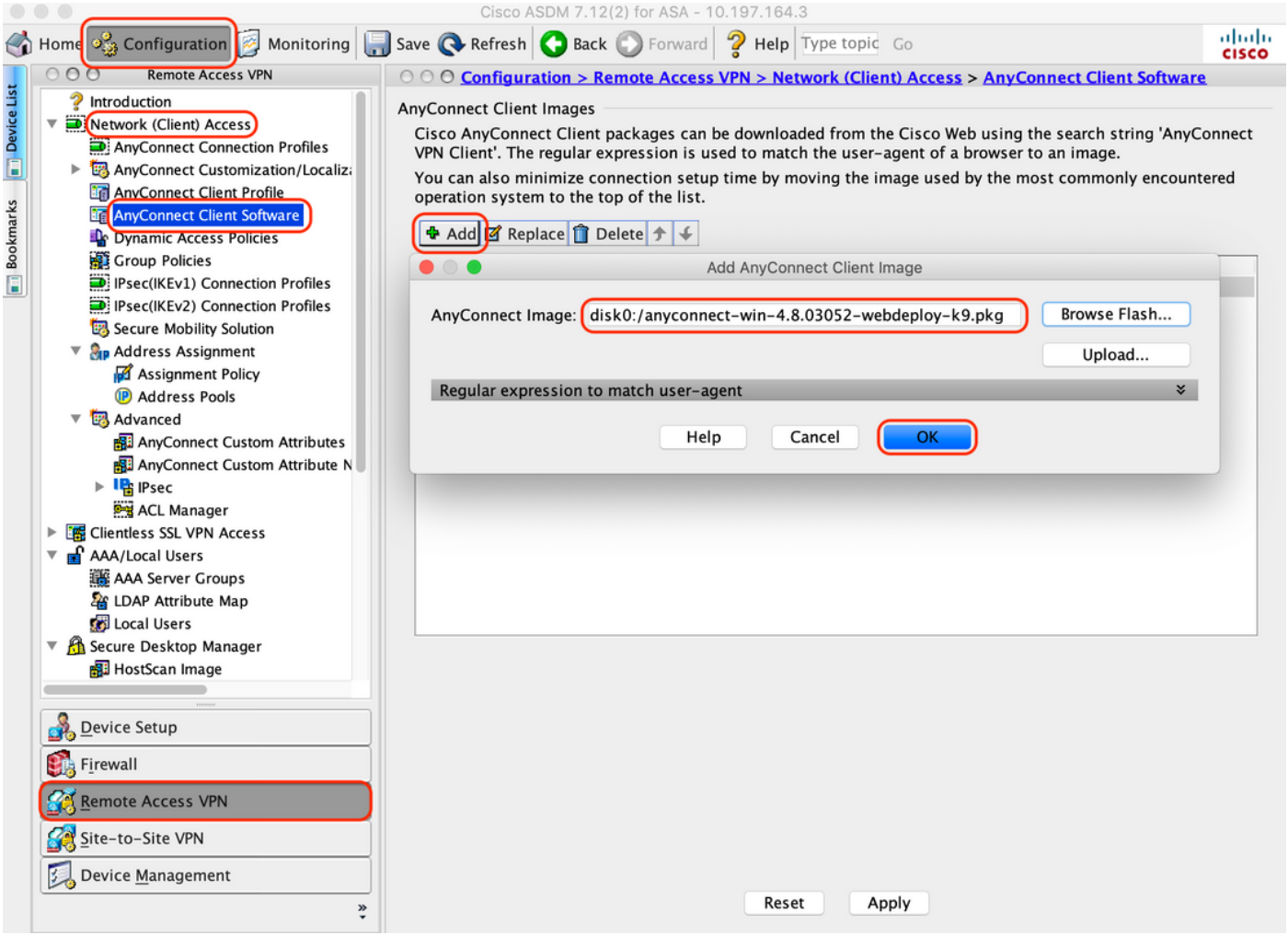

C. En la misma página, en la sección "Servidores del grupo Seleccionado", haga clic en "Agregar" y proporcione los detalles de la dirección IP del servidor AAA




4. Asignar software cliente AnyConnect

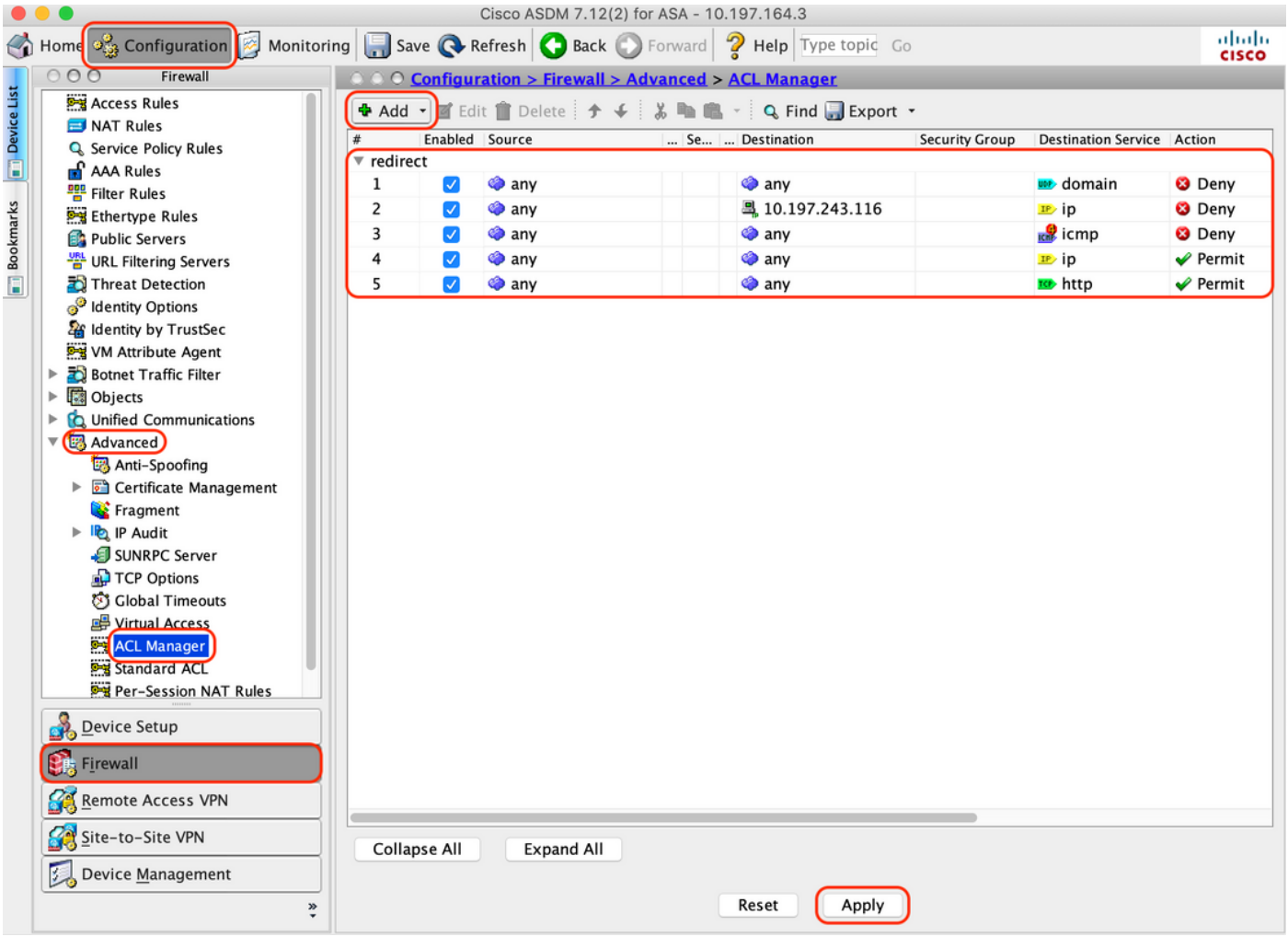
A. Asigne la imagen de implementación web del software cliente AnyConnect 4.8.03052 para las ventanas que se utilizarán para WebVPN

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



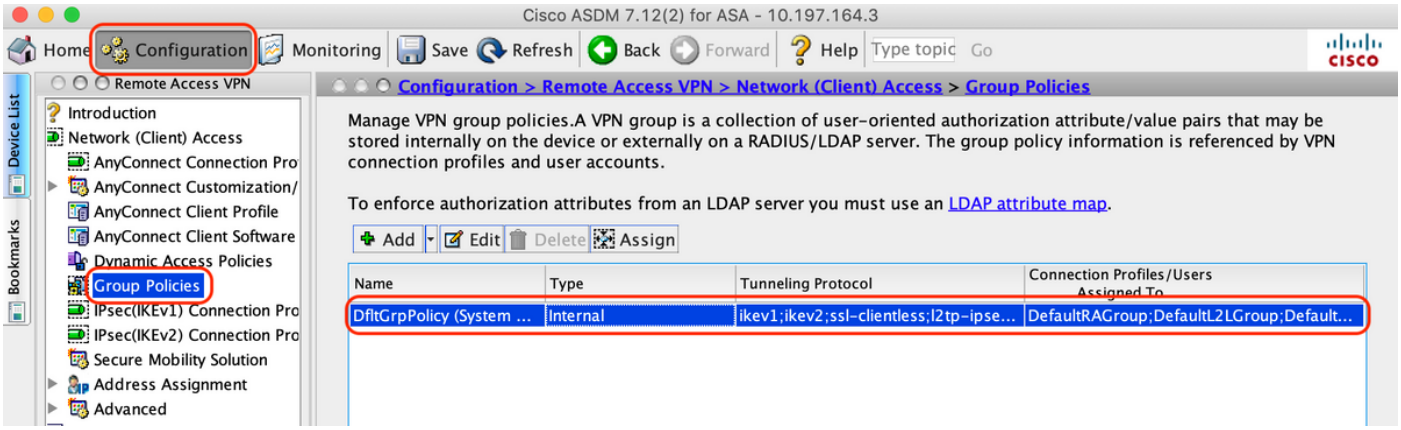

5. Configure la ACL de redirección que se envía como resultado de ISE

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

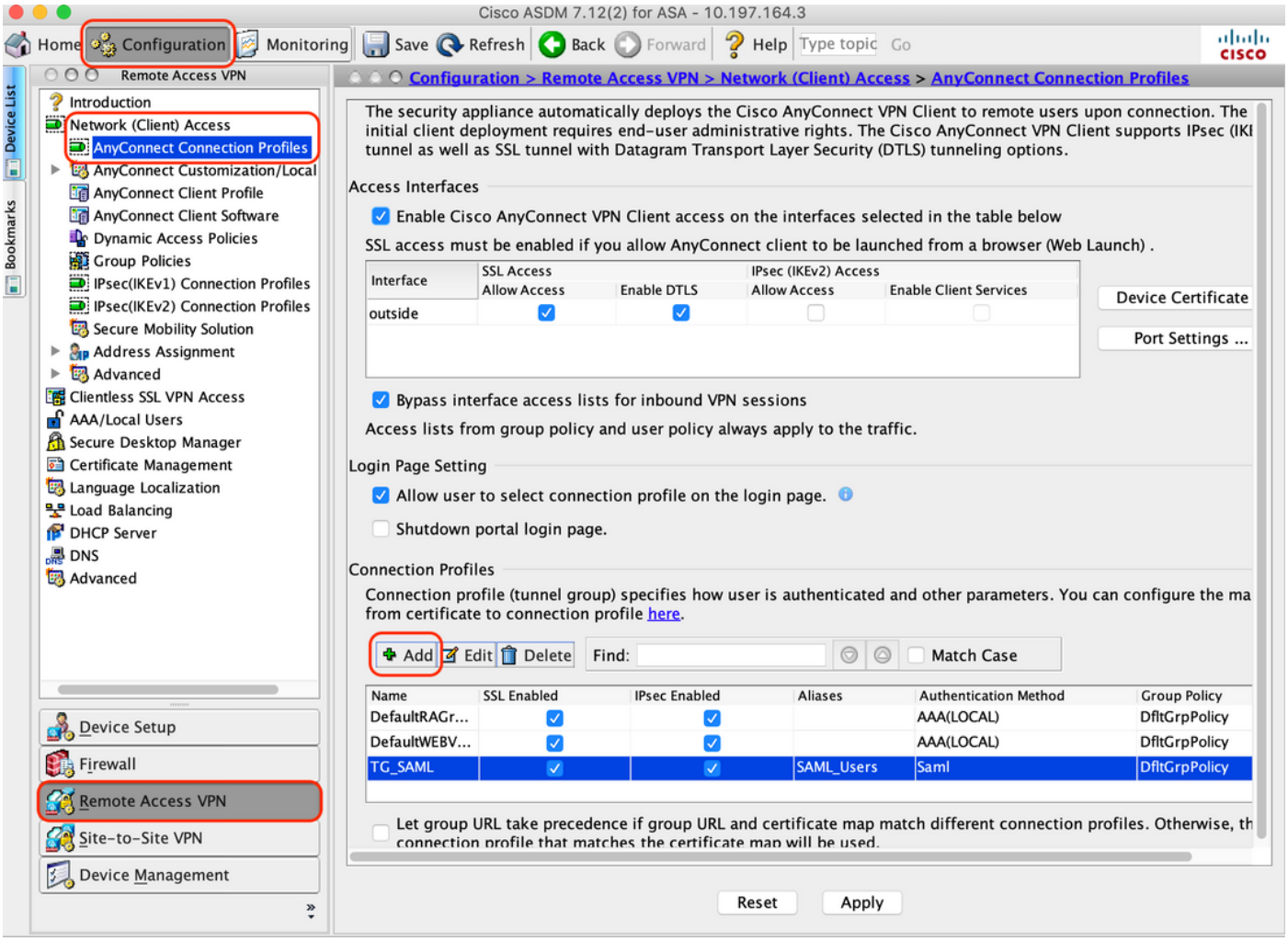
R. Esta configuración utiliza la política de grupo predeterminada y se puede ver en: "Configuración > VPN de acceso remoto > Acceso (cliente) de red > Políticas de grupo"




7. Configuración del perfil de conexión

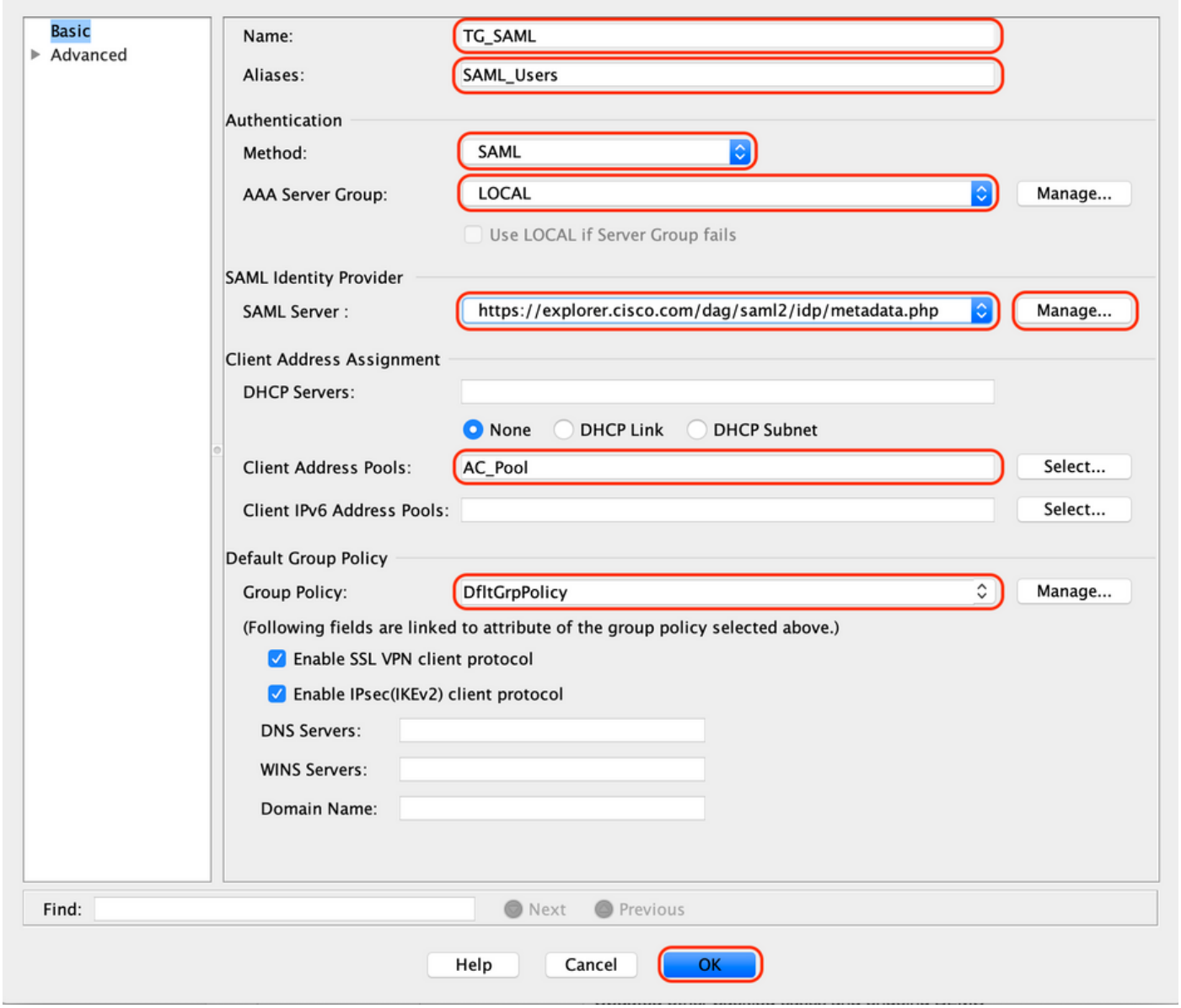
A. Crear un nuevo perfil de conexión al que se conecten los usuarios de AnyConnect

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 |

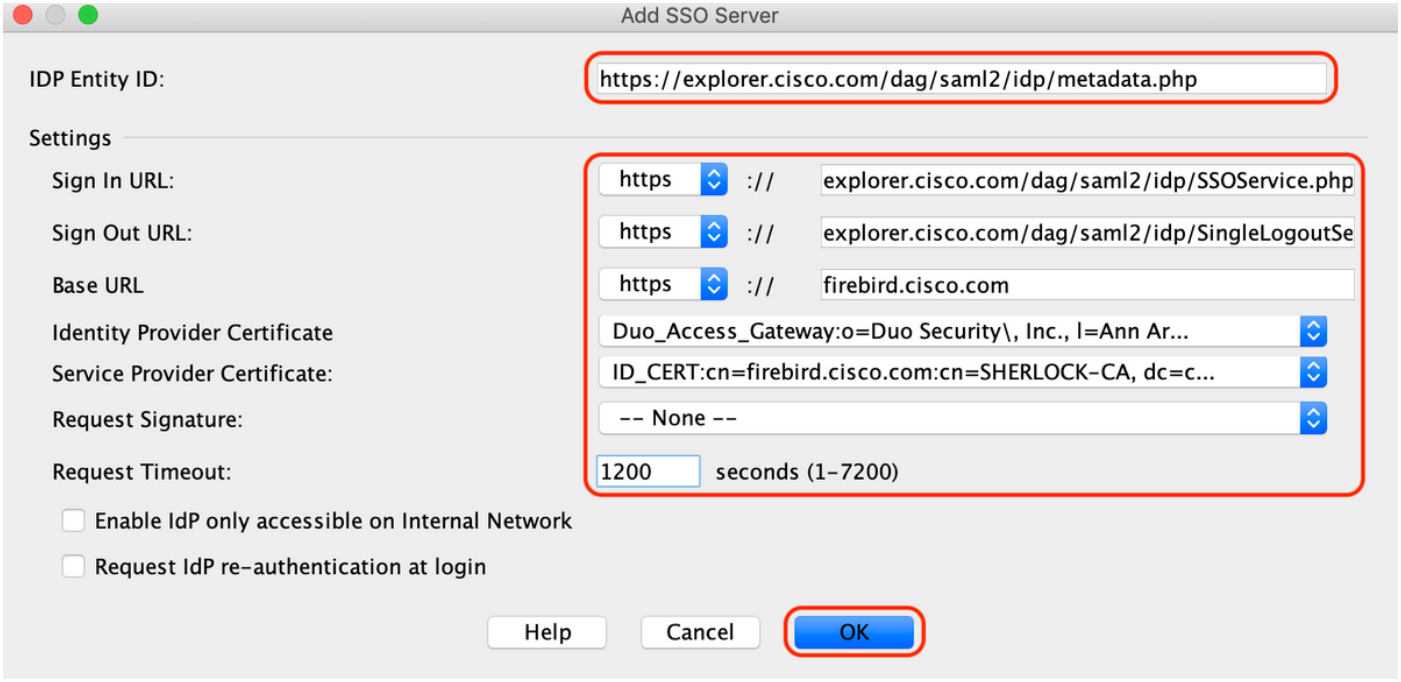



D. En la misma página, configure los detalles del proveedor de identidad SAML que se muestran a continuación:

| | |
|---|---|
| ID de entidad IDP | https://explorer.cisco.com/dag/saml2/idp/metadata.php |
| URL de inicio de sesión | https://explorer.cisco.com/dag/saml2/idp/SSOService.php |
| URL de cierre de sesión | https://explorer.cisco.com/dag/saml2/idp/SingleLogoutService.php?ReturnTo=https://explorer.cis |
| URL | https://firebird.cisco.com |

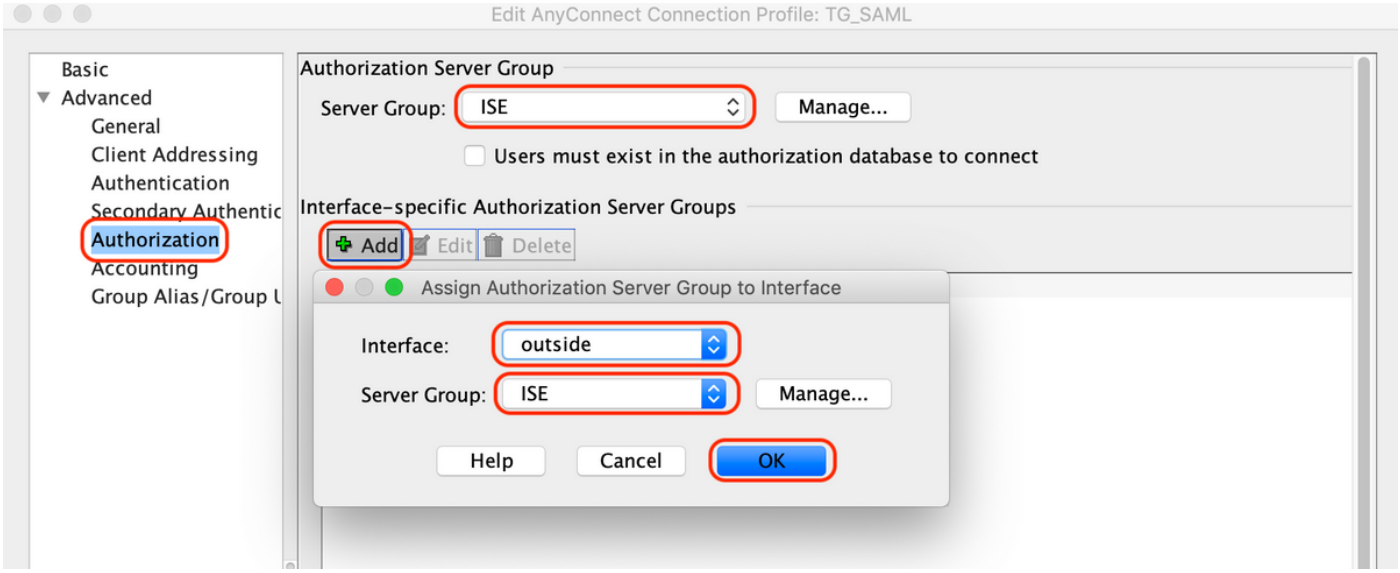
| | |
|---|---|
| base | |

E. Haga clic en "Administrar > Agregar"



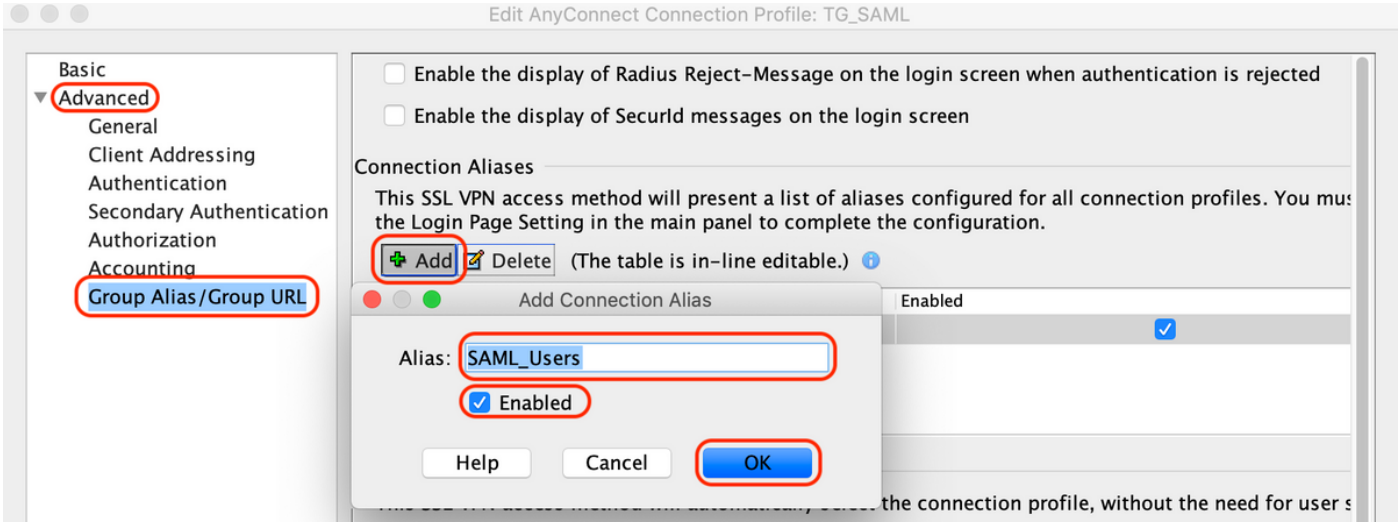

F. En la sección Avanzadas del perfil de conexión, defina el servidor AAA para la autorización

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




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)

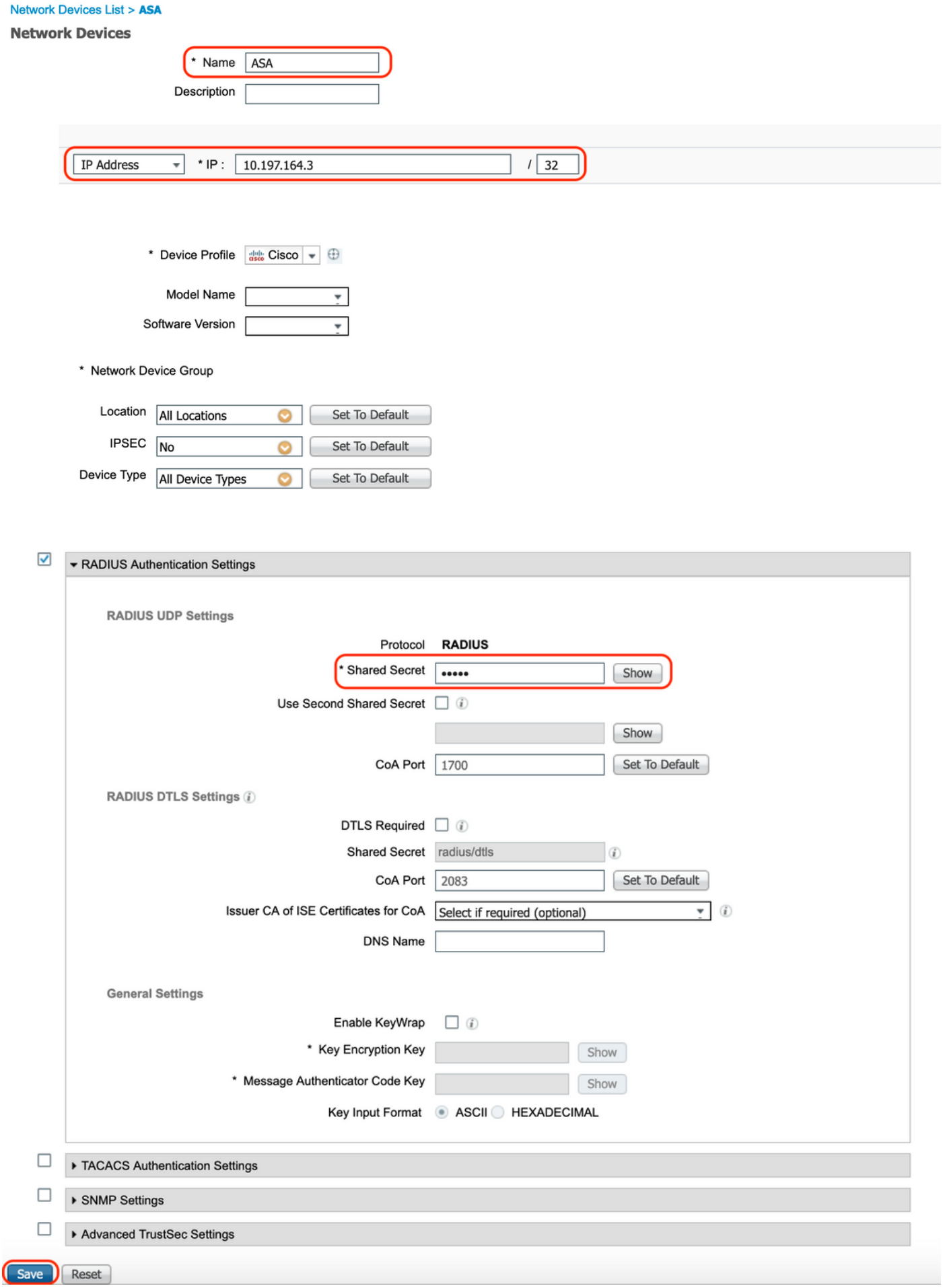
```
!
hostname firebird
domain-name cisco.com
!
!
name 10.197.164.7 explorer.cisco.com
name 10.197.164.3 firebird.cisco.com
!
!--------------------Client pool configuration--------------------
!
ip local pool AC_Pool 10.197.164.6-explorer.cisco.com mask 255.255.255.0
!
!--------------------Redirect Access-list-------------------------
!
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
 crl 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

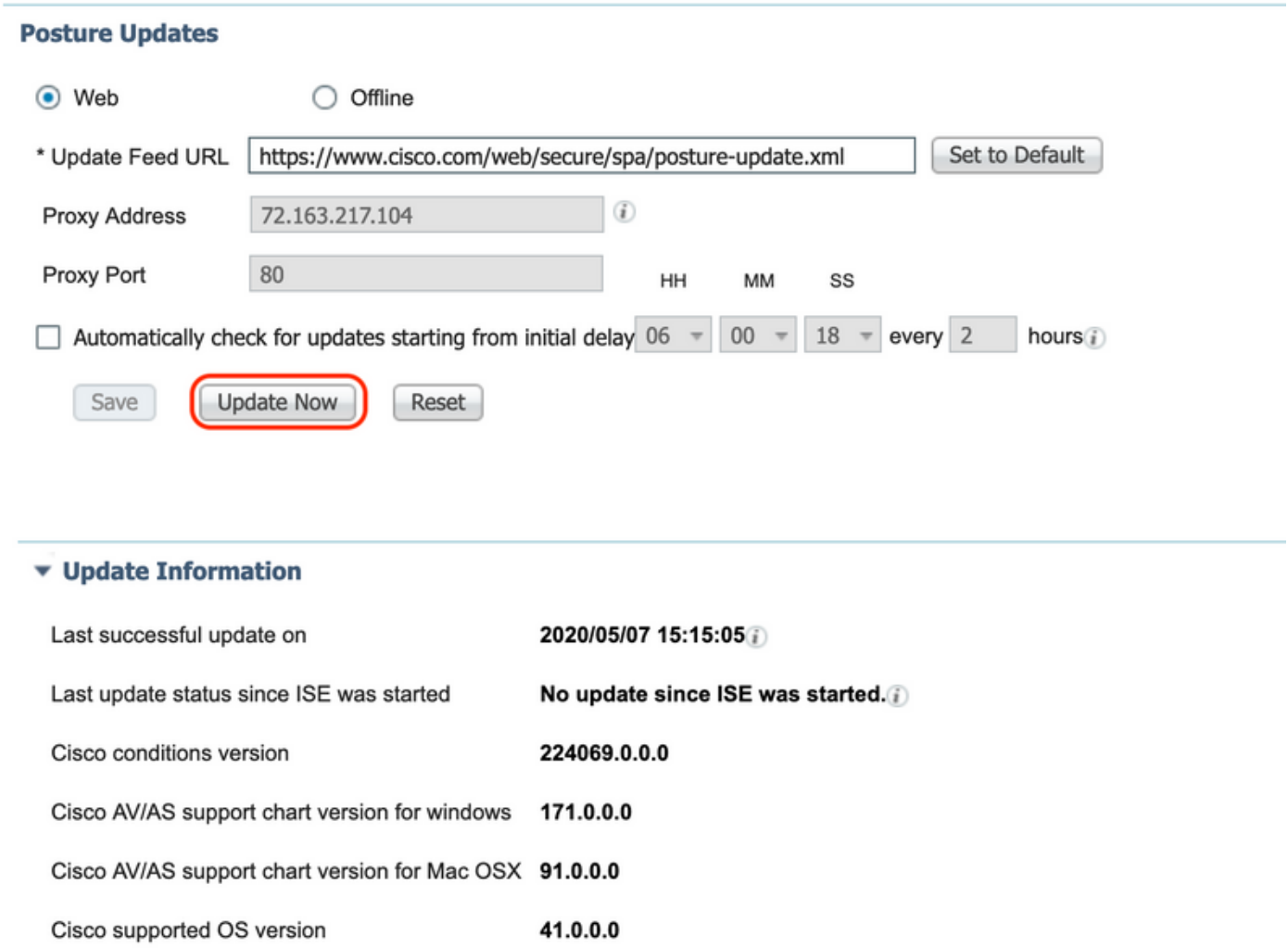
1. Agregue Cisco ASA como dispositivo de red

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 List > ASA
Network Devices
* Name
ASA
Description
IP Address
* IP :
10.197.164.3
/ 32
* Device Profile
Cisco
Model Name
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 Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
* Shared Secret
Show
Use Second Shared Secret
Show
CoA Port
1700
Set To Default
RADIUS DTLS Settings
DTLS Required
Shared Secret
radius/dtls
CoA Port
2083
Set To Default
Issuer CA of ISE Certificates for CoA
Select if required (optional)
DNS Name
General Settings
Enable KeyWrap
* Key Encryption Key
Show
* Message Authenticator Code Key
Show
Key Input Format
ASCII
HEXADECIMAL
TACACS Authentication Settings
SNMP Settings
Advanced TrustSec Settings
Save
Reset

2. Instalar las últimas actualizaciones de estado

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



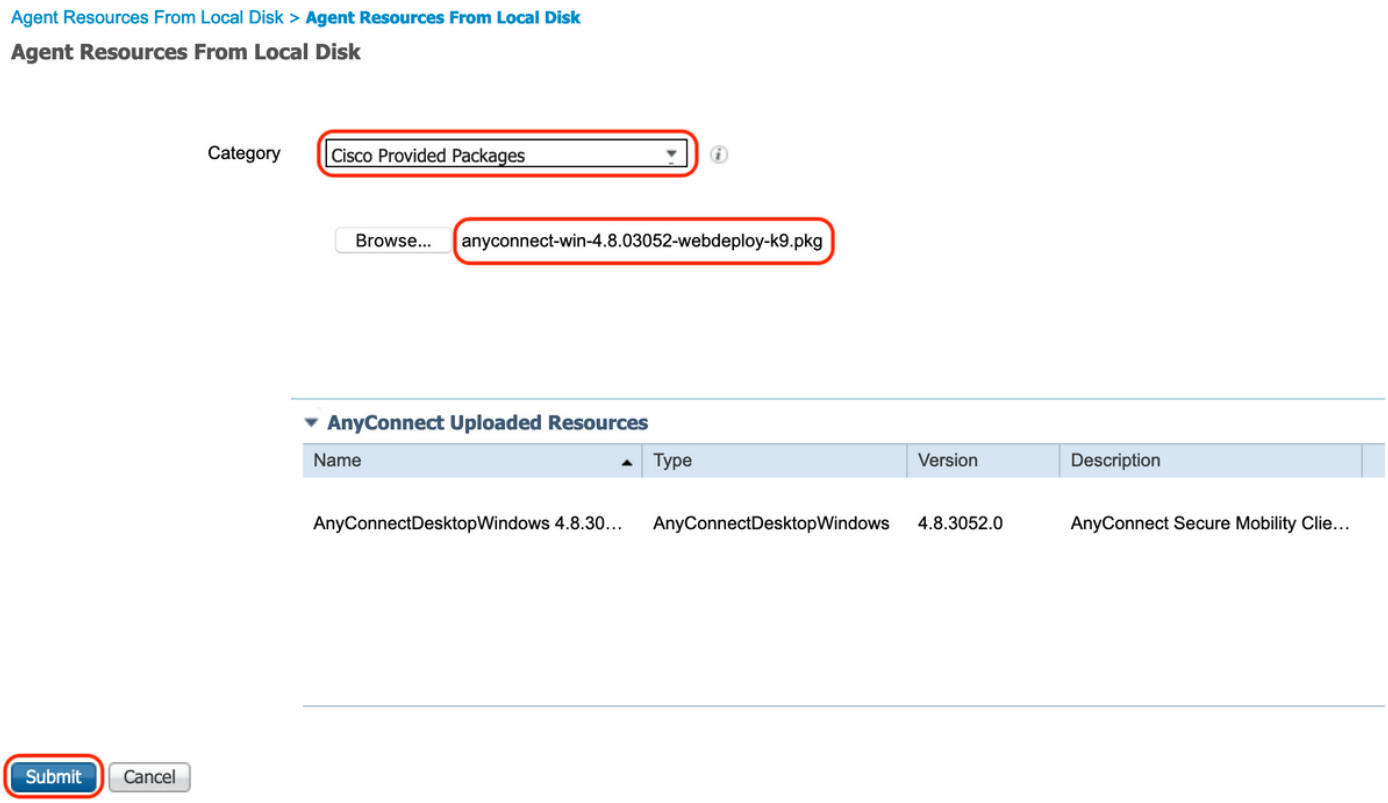

3. Cargue el módulo de cumplimiento y el paquete de implementación de cabecera de AnyConnect en ISE

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"

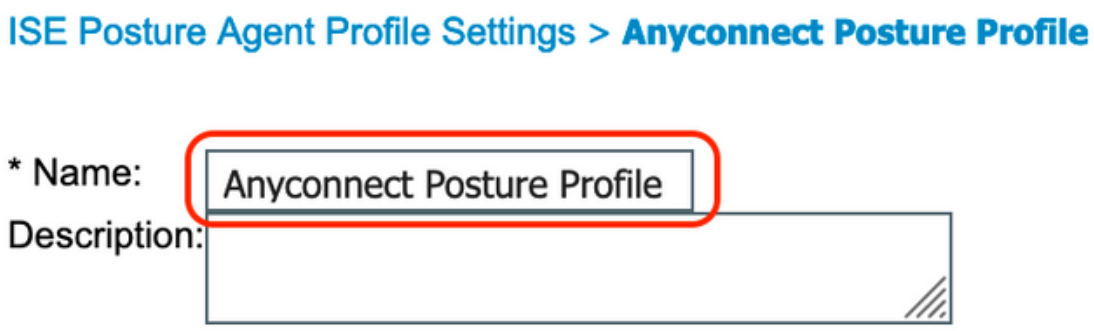
como módulo de cumplimiento y "anyconnect-win-4.8.03052-webdeploy-k9.pkg" como paquete de implementación de cabecera de AnyConnect.




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"



Posture Protocol

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

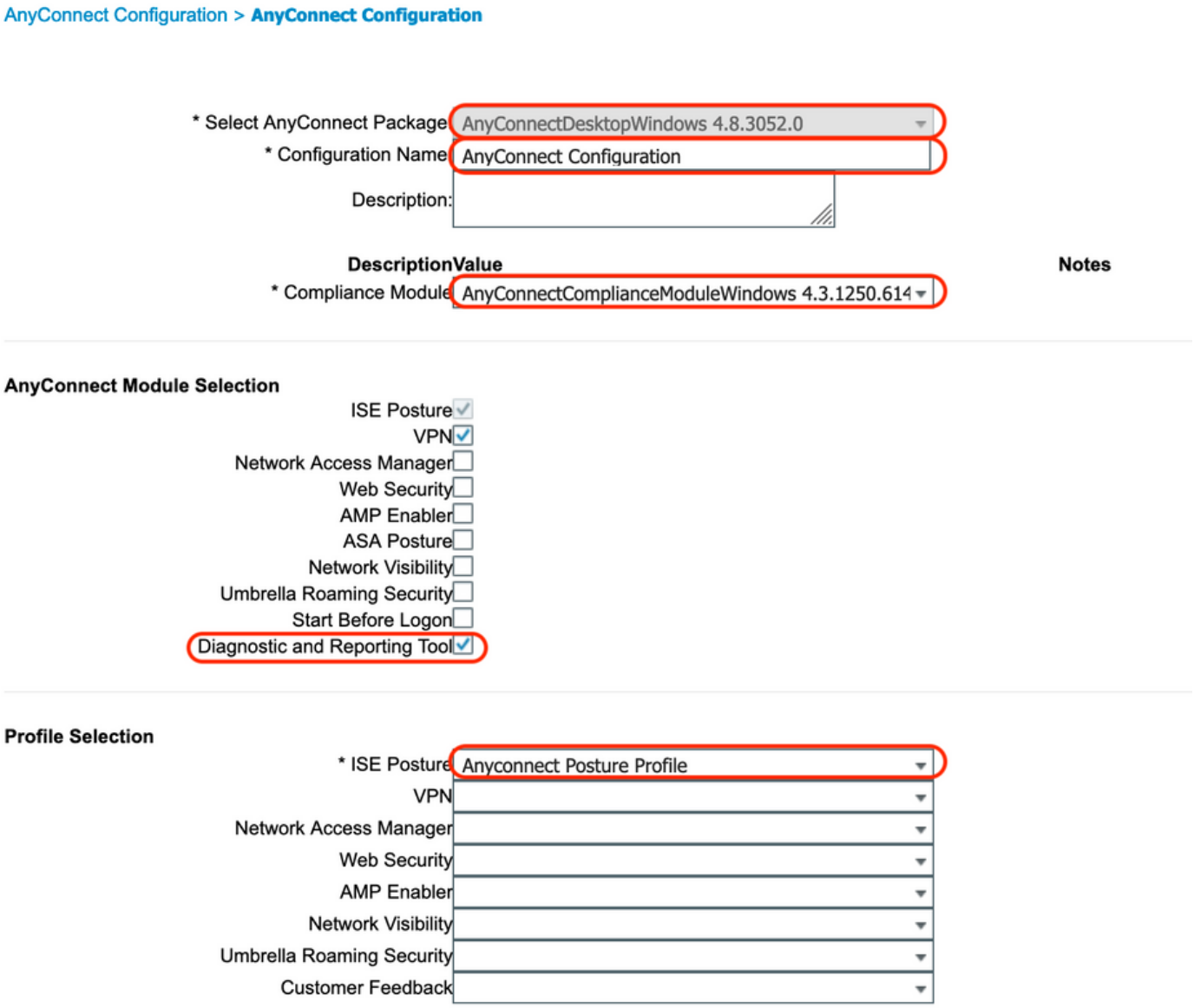
5. Crear configuración de Anyconnect

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"

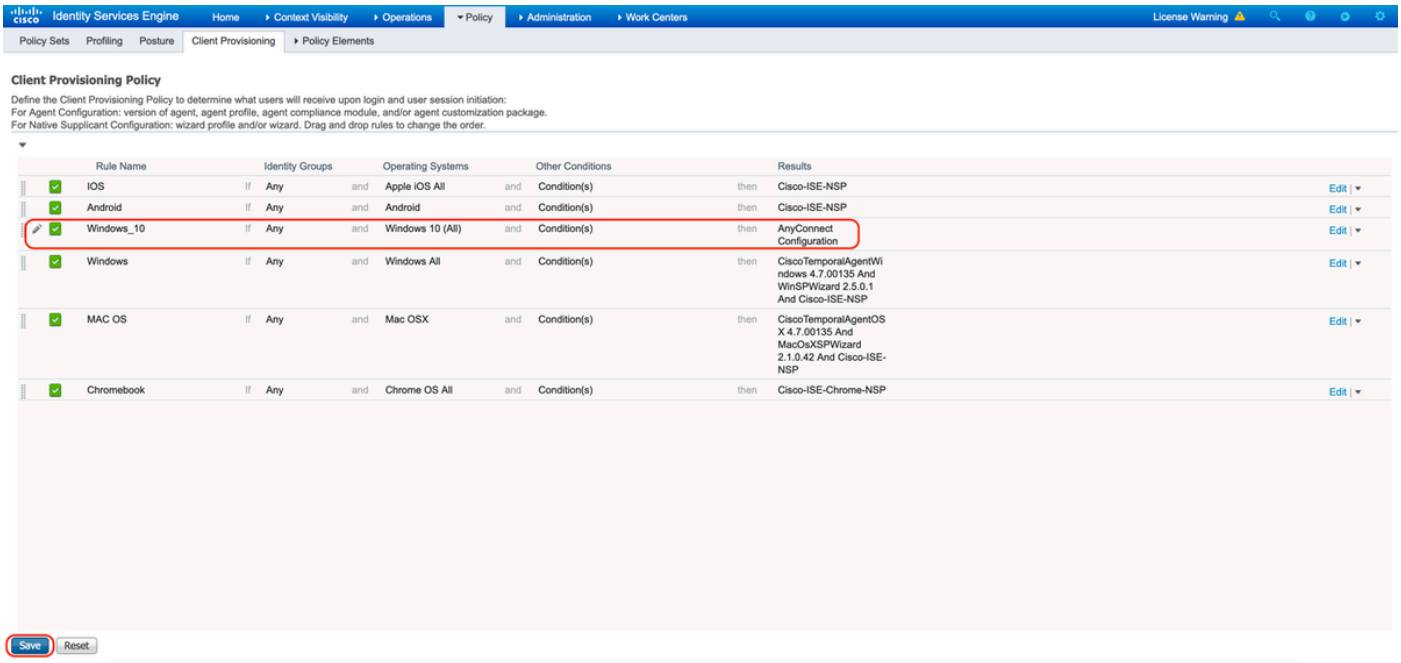



6. Crear política de aprovisionamiento de clientes

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"

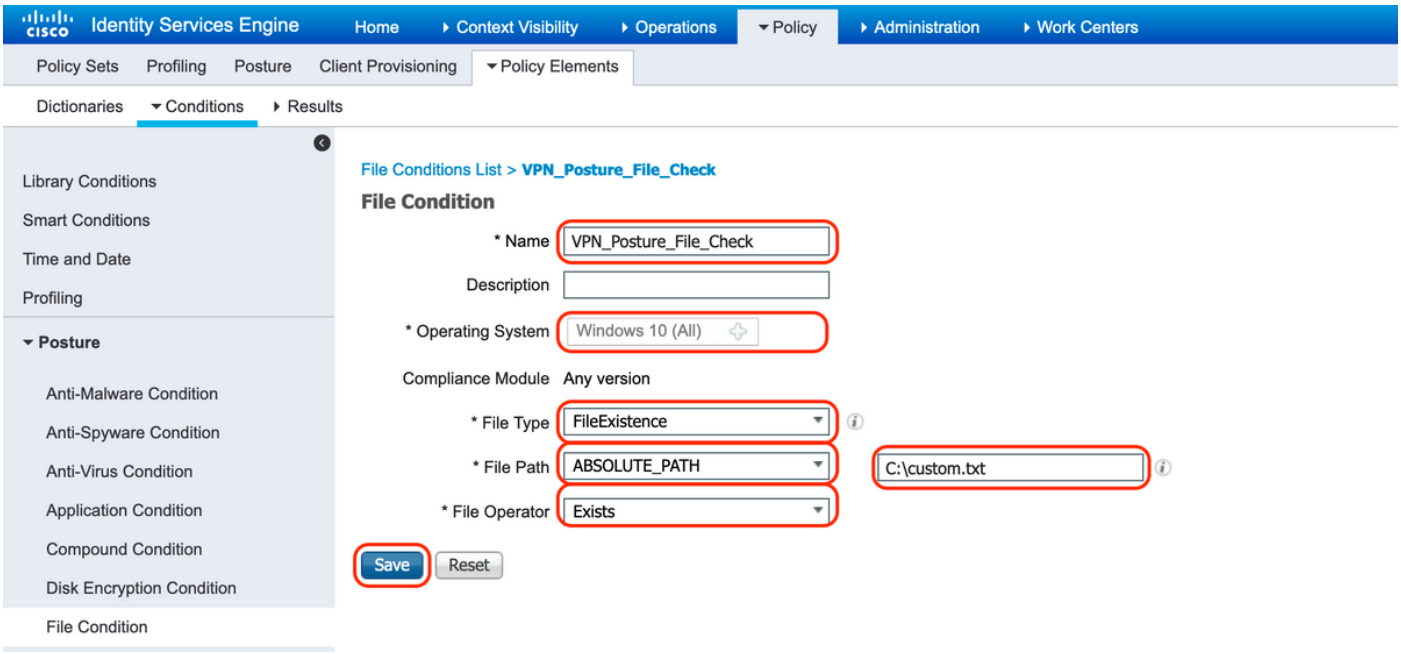



7. Crear una condición de postura

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



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.

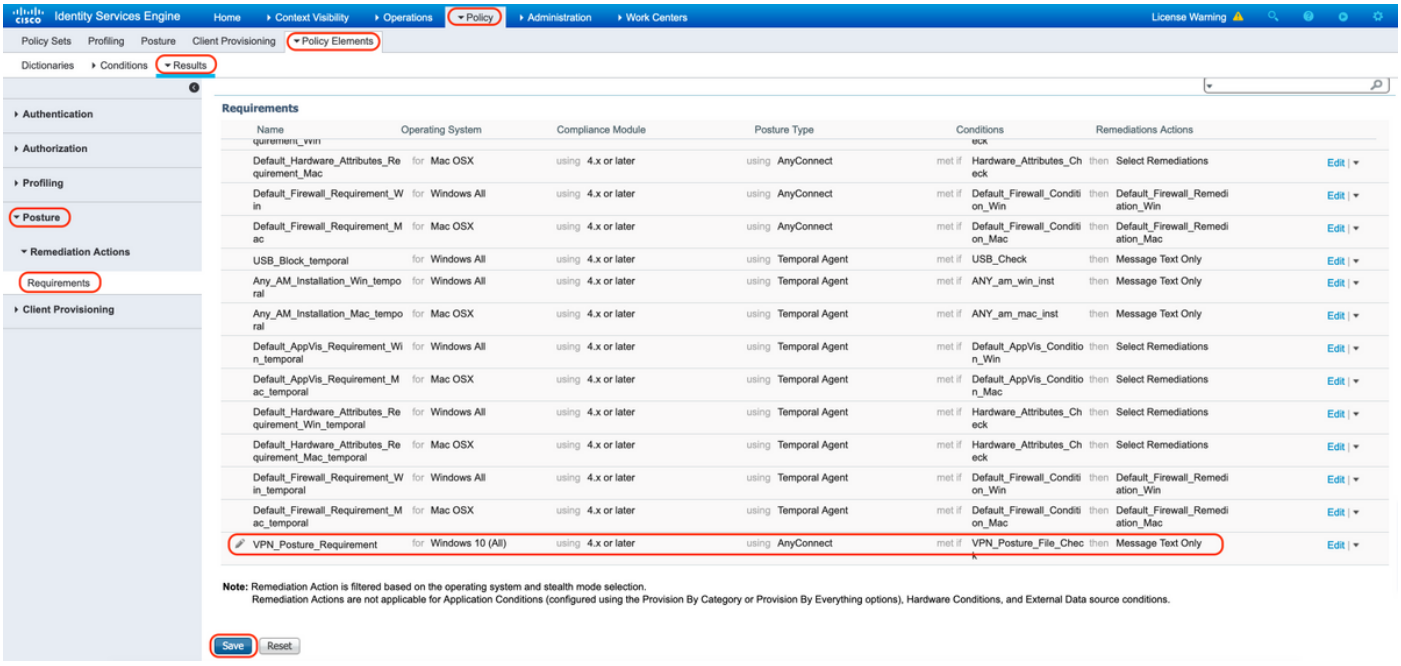
9. Crear regla de requisito de condición

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"

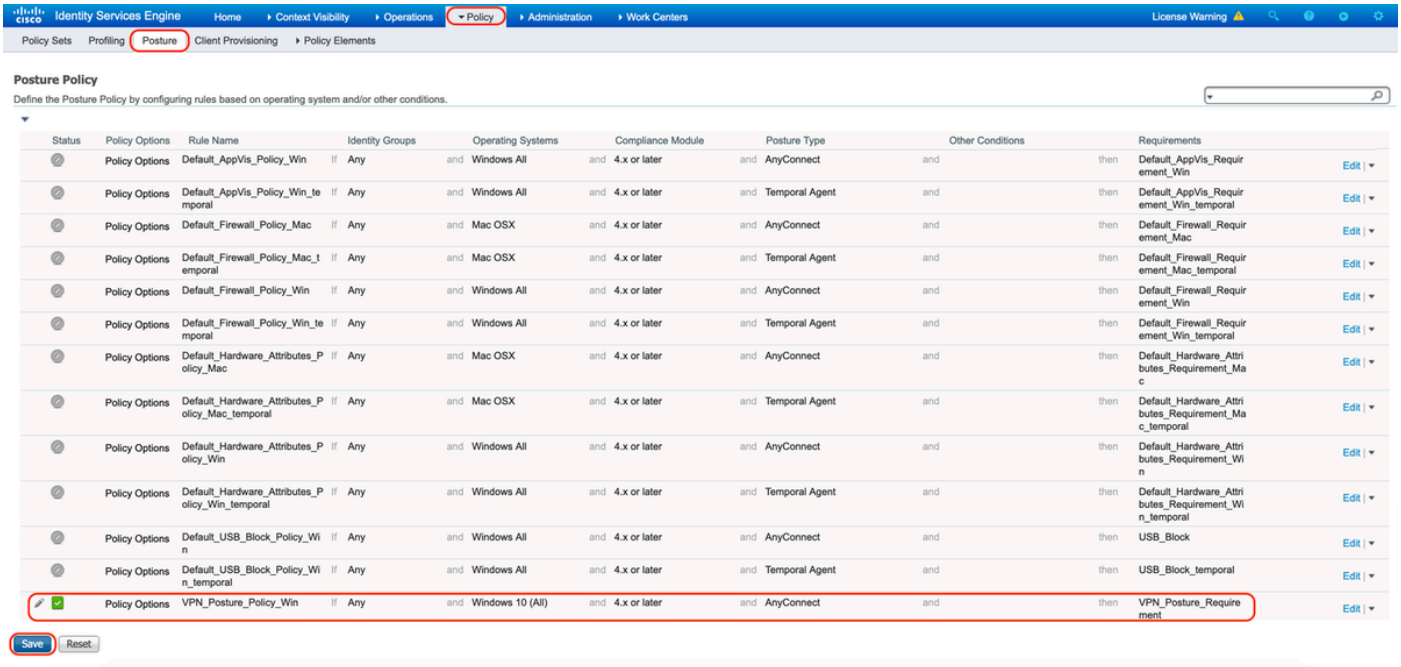
D. Condiciones como "VPN_Posture_File_Check" (creado en el paso 7) y en Acciones de remediación, seleccione Acción como "Sólo texto de mensaje" e introduzca el mensaje personalizado para Usuario agente




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

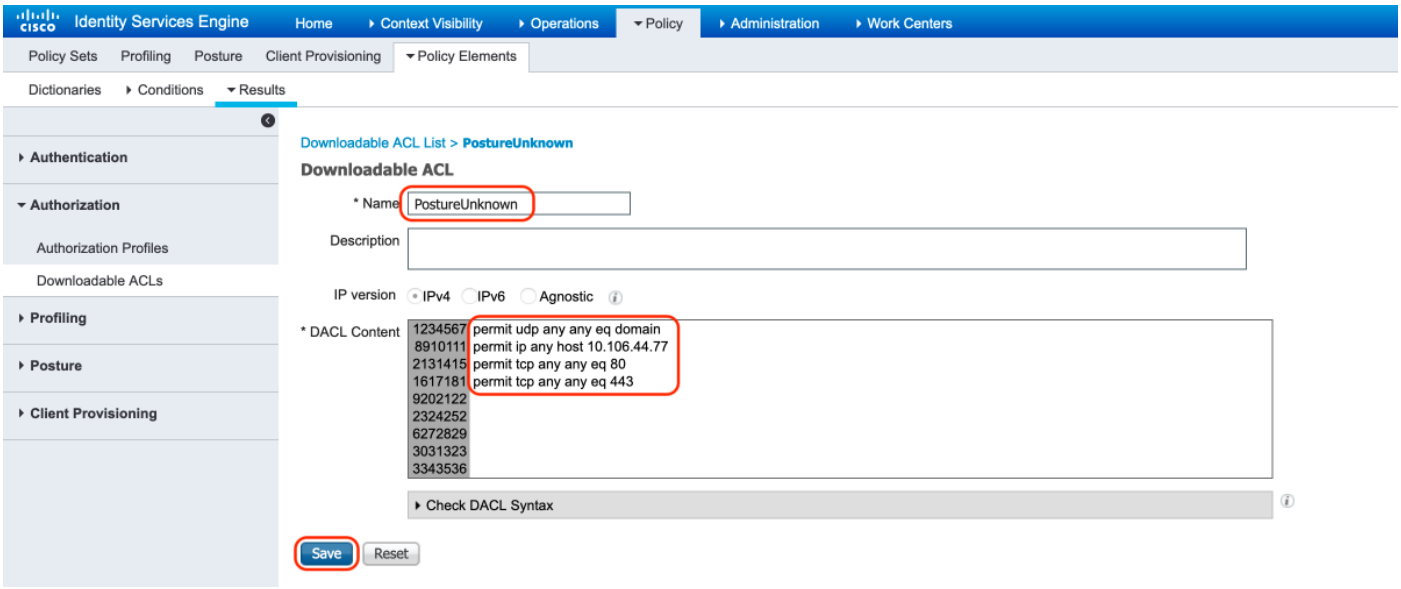



11. Crear ACL dinámicas (DACL)

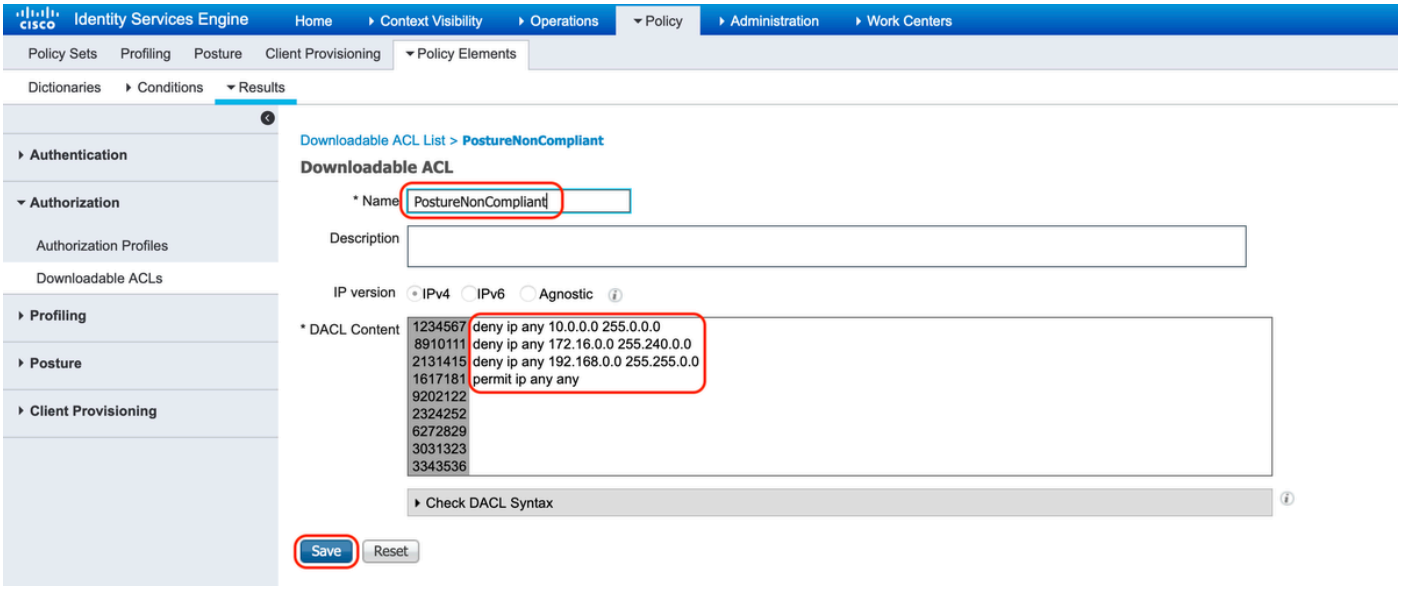
Vaya a "Política > Elementos de política > Resultados > Autorización > ACL descargables" y cree las DACL para diferentes estados de estado.

Este documento utiliza las siguientes DACL.

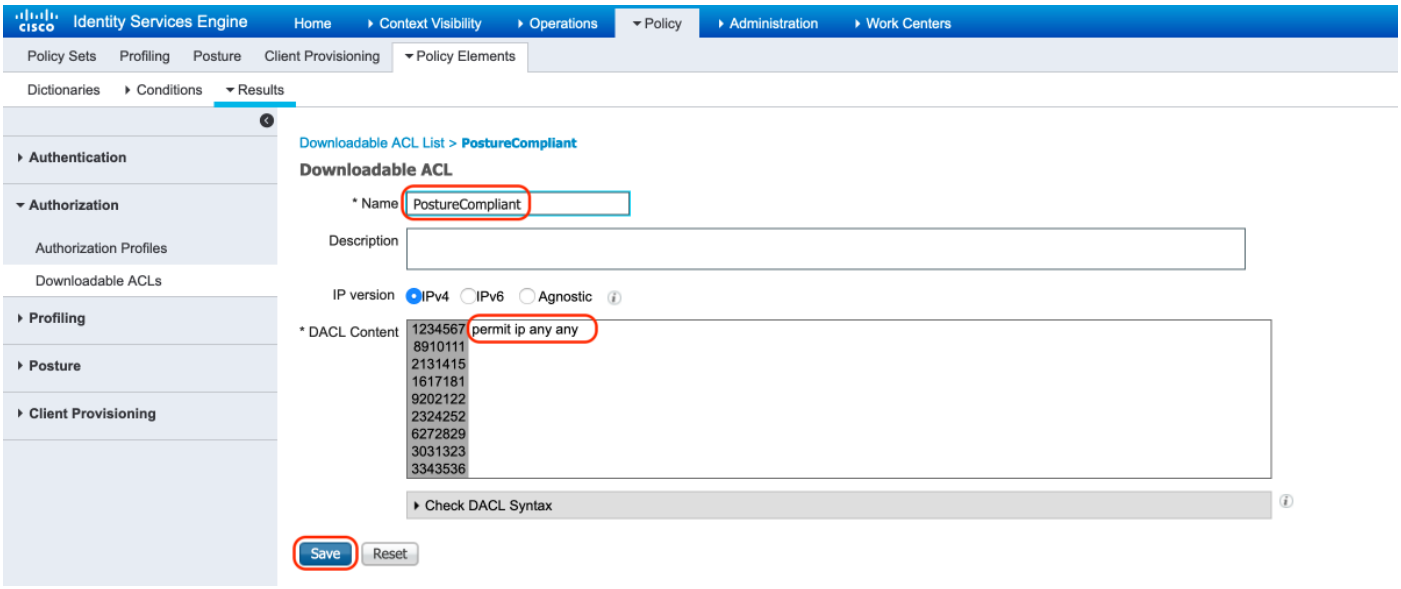
A. Condición desconocida: permite el tráfico a DNS, PSN, HTTP y HTTPS




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




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

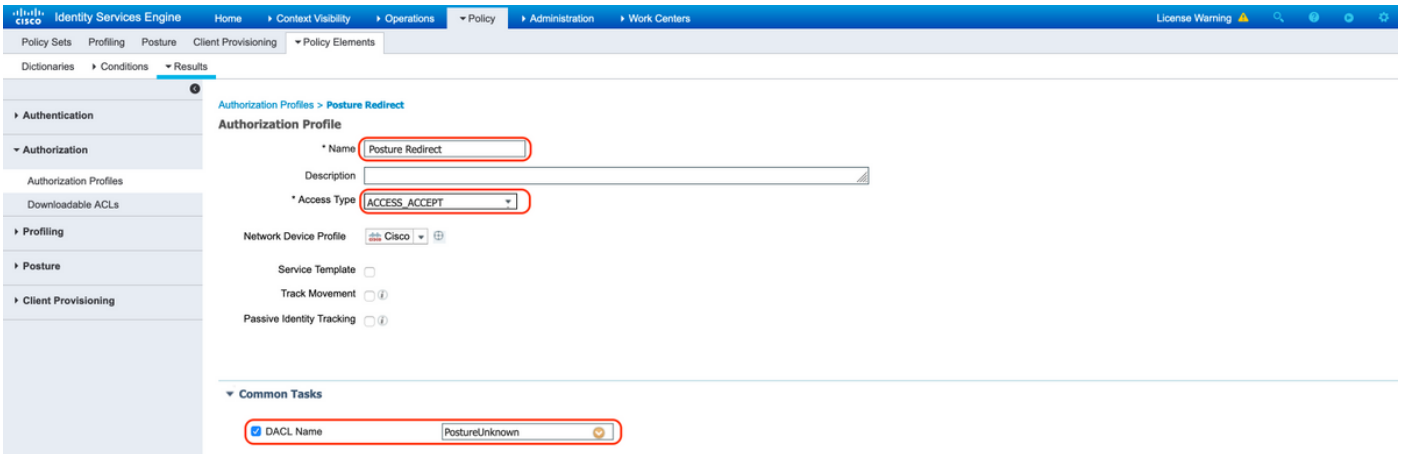


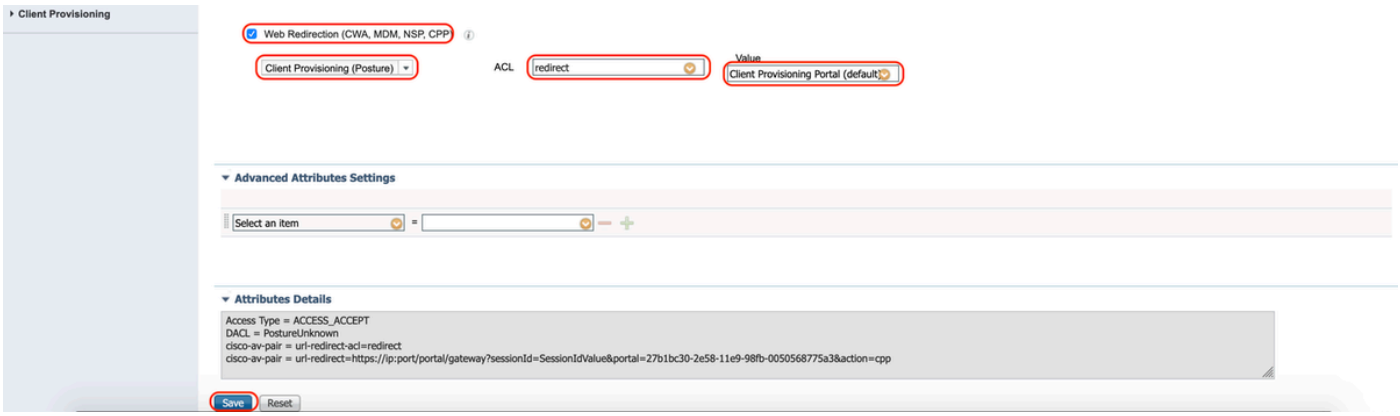

12. Crear perfiles de autorización

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

A. Perfil de autorización para postura desconocida

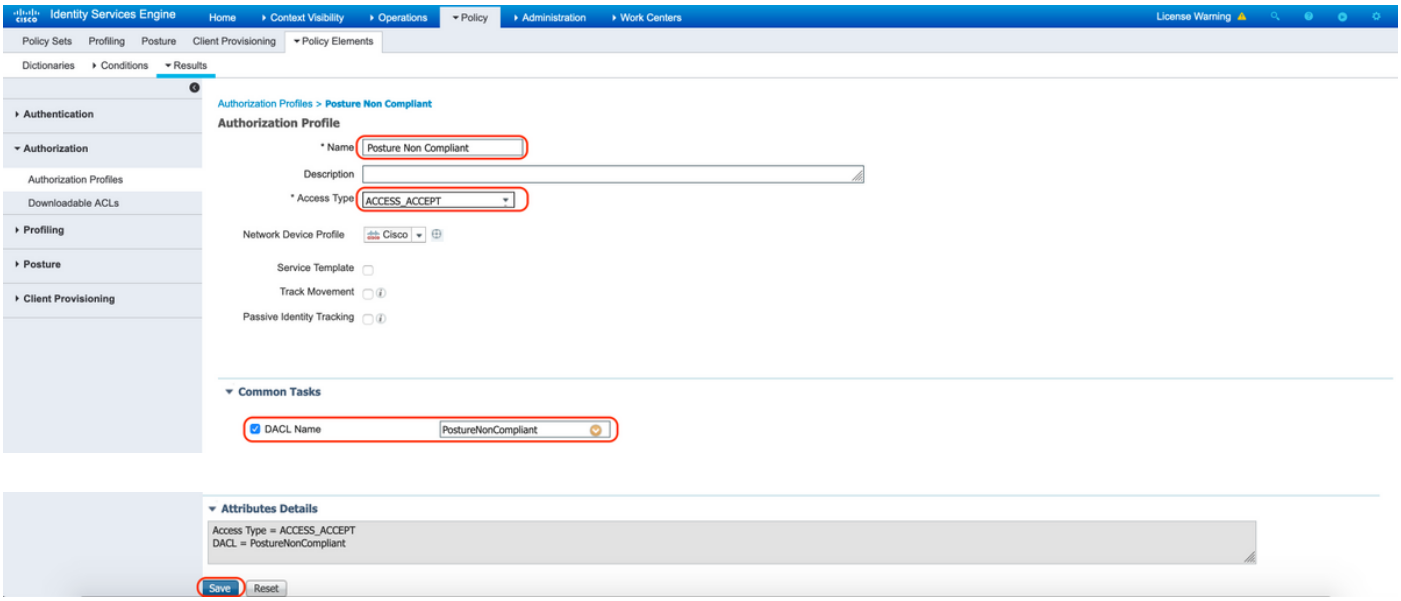
Seleccione DACL "PostureUnknown", marque Web Redirection (Redirección web), seleccione Client Provisioning (Posture) (Aprovisionamiento de clientes), configure Redirect ACL name "redirect" (Redirigir nombre de ACL) (que se configurará en ASA) y seleccione el portal Client Provisioning (Aprovisionamiento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





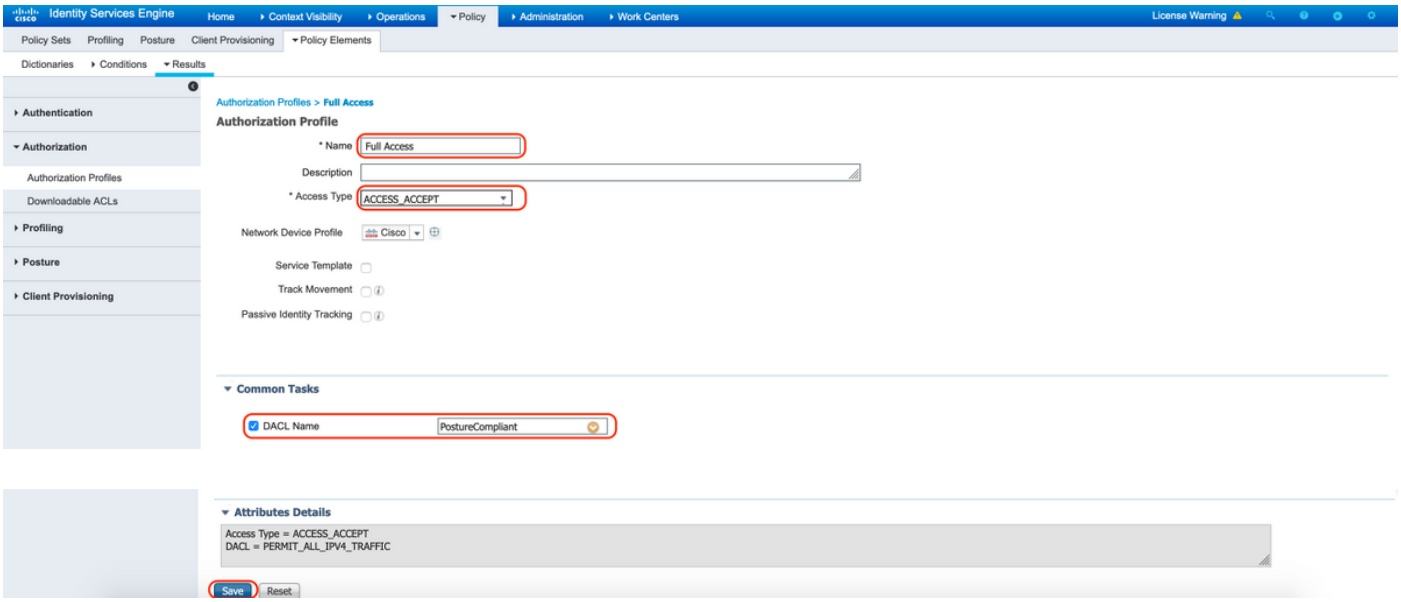

B. Perfil de autorización para postura no conforme

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




C. Perfil de autorización para el cumplimiento del estado

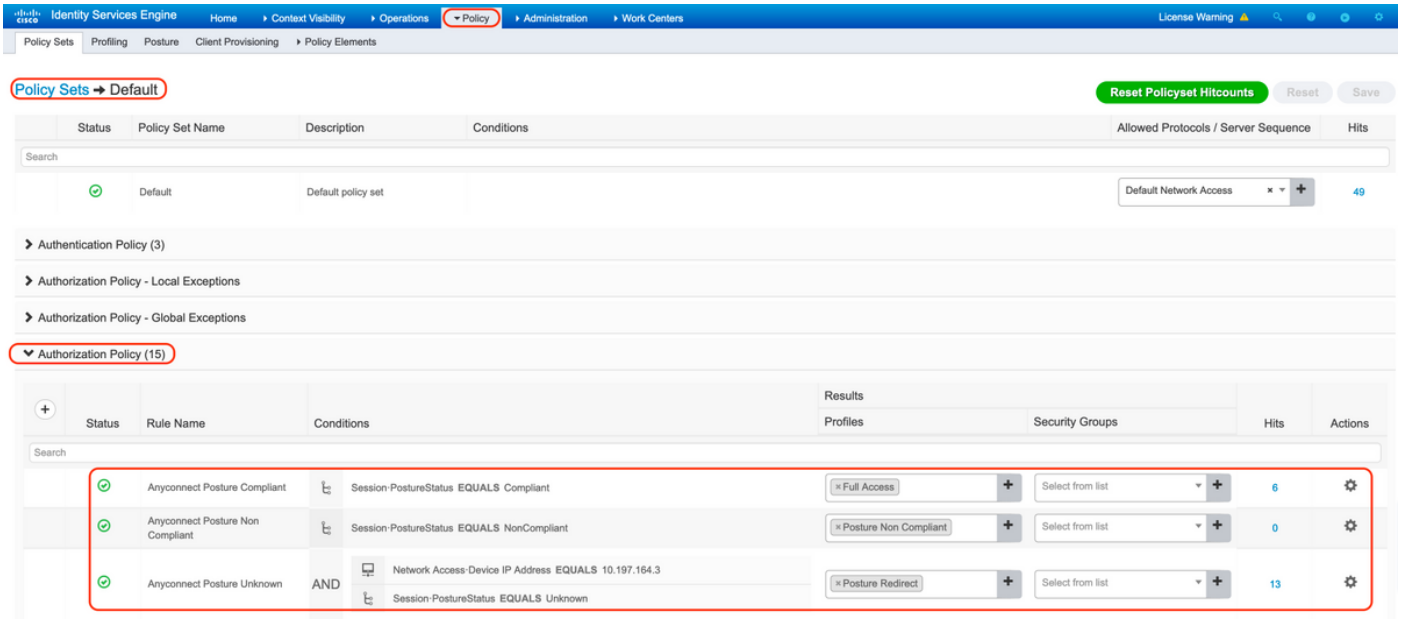
Seleccione DACL "PostureCompliant" para permitir el acceso completo a la red




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

Utilize 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&po
  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 :
```

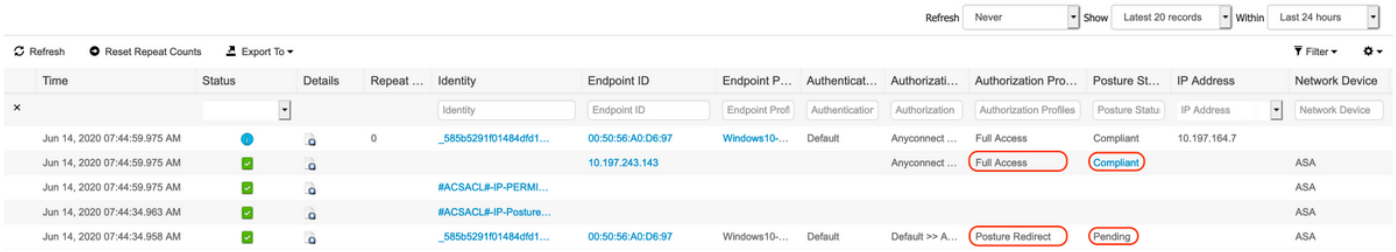
**TG_SAML**

```
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.



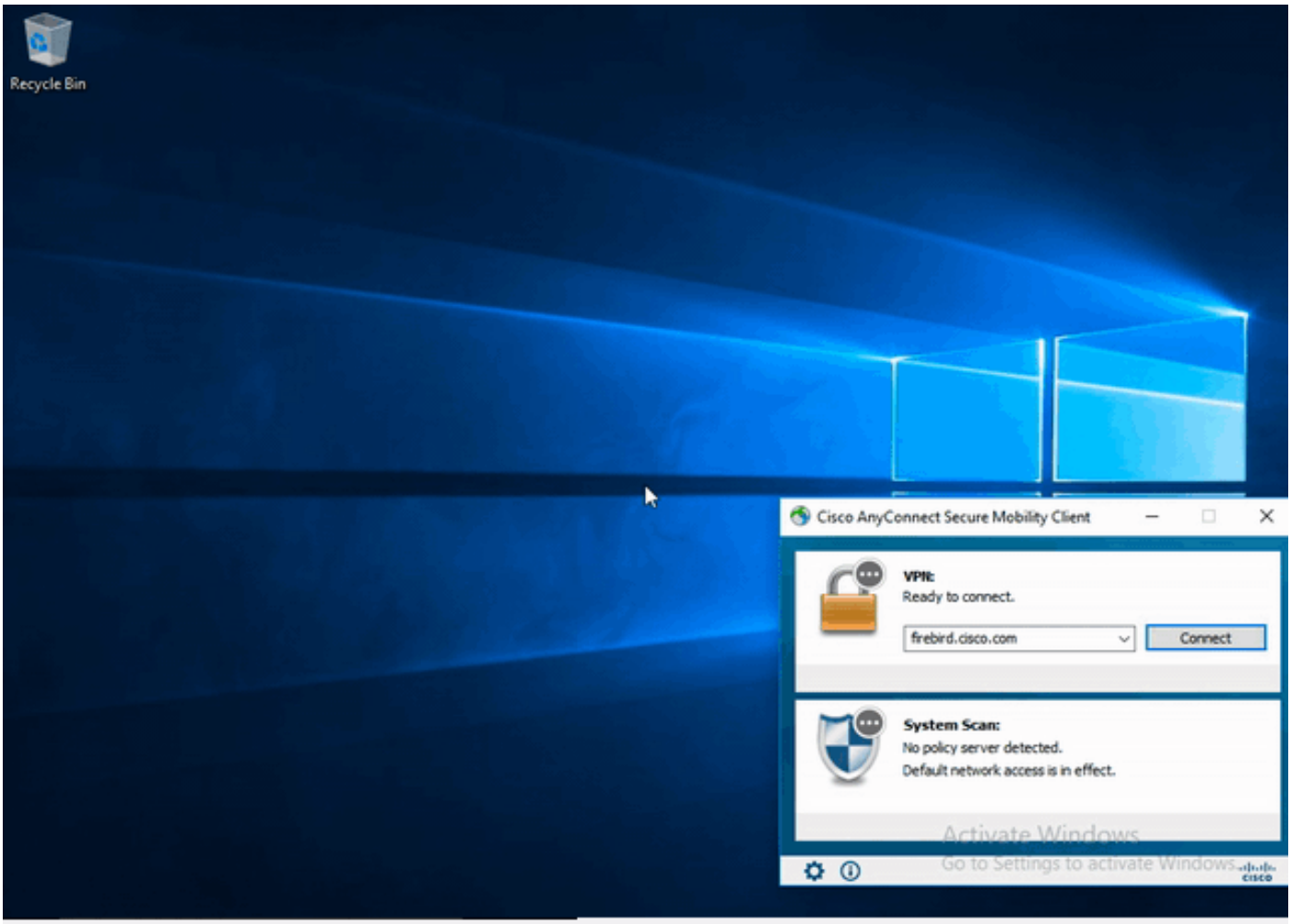
| Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authenticat... | Authorizati... | Authorization Pro... | Posture St... | IP Address | Network Device |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Jun 14, 2020 07:44:59.975 AM | | | 0 | _585b5291f01484dfd1... | 00:50:56:A0:D6:97 | Windows10-... | Default | Anyconnect ... | Full Access | Compliant | 10.197.164.7 | |
| Jun 14, 2020 07:44:59.975 AM | | | | | 10.197.243.143 | | | Anyconnect ... | Full Access | Compliant | | ASA |
| Jun 14, 2020 07:44:59.975 AM | | | | #ACSACL#-IP-PERMI... | | | | | | | | ASA |
| Jun 14, 2020 07:44:34.963 AM | | | | #ACSACL#-IP-Posture... | | | | | | | | 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

## 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

---

# 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-acces.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).