Configuración de AnyConnect Flexvpn con autenticación EAP y DUO

Contenido

Introducción

Este documento describe cómo configurar la autenticación externa de dos factores para la conexión de AnyConnect IPSec a un router Cisco IOS® XE.

Colaboración de Sadhana K S y Rishabh Aggarwal, ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Experiencia con la configuración de VPN de RA en un router
- Administración de Identity Services Engine (ISE)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Catalyst 8000V (C8000V) que ejecuta la versión 17.10.01a

- Cisco AnyConnect Secure Mobility Client versión 4.10.04071
- Cisco ISE con la versión 3.1.0
- Servidor proxy de autenticación Duo (Windows 10 o cualquier PC Linux)
- Cuenta web Duo
- PC cliente con AnyConnect instalado

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). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Flujo de autenticación

El usuario de AnyConnect se autentica con un nombre de usuario y una contraseña en el servidor ISE. El servidor proxy de autenticación Duo también envía una autenticación adicional en forma de una notificación de inserción al dispositivo móvil del usuario.

Diagrama de flujo

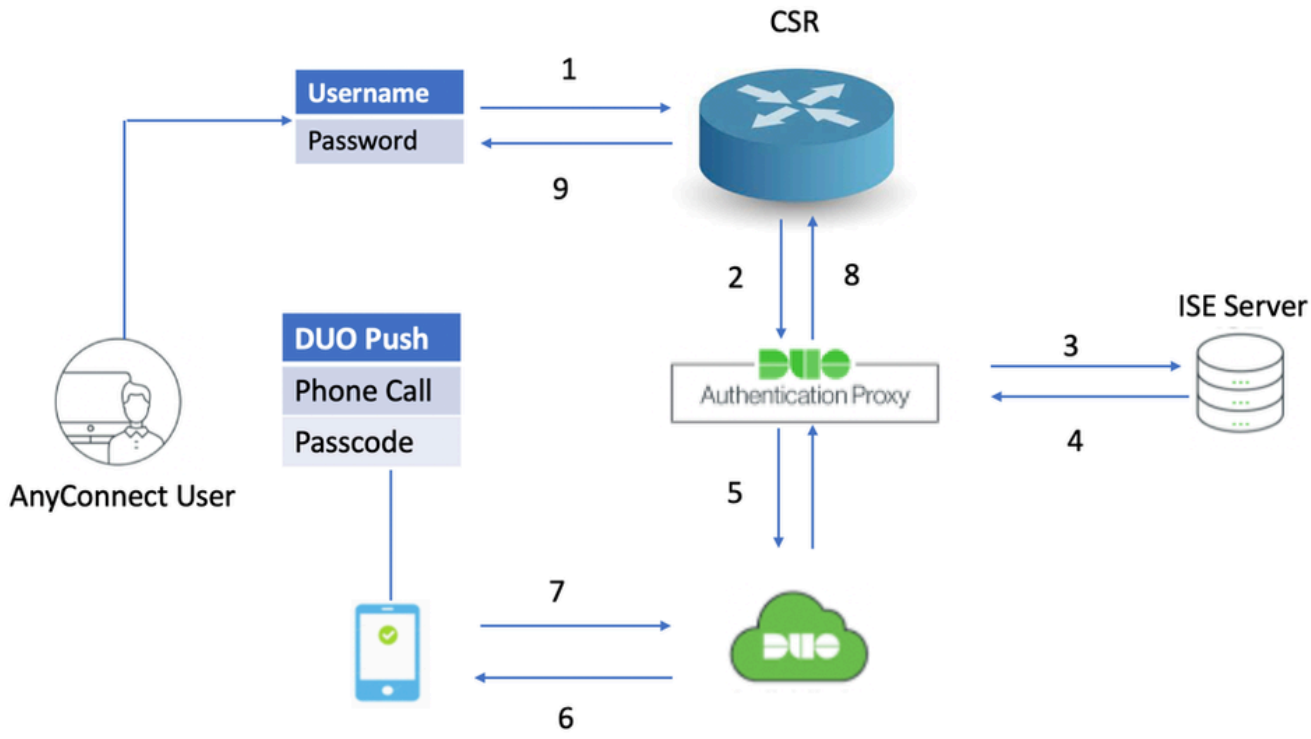


Diagrama de flujo de autenticación

Proceso de comunicación

1. El usuario inicia una conexión RAVPN al C8000V y proporciona un nombre de usuario y una contraseña para la autenticación principal.
2. El C8000V envía una solicitud de autenticación al proxy de autenticación doble.

3. A continuación, Duo Authentication Proxy envía la solicitud principal al servidor de Active Directory o RADIUS.
4. La respuesta de autenticación se devuelve al proxy de autenticación.
5. Una vez que la autenticación primaria es exitosa, el proxy de autenticación Duo solicita la autenticación secundaria a través del servidor Duo.
6. A continuación, el servicio Duo autentica al usuario, en función del método de autenticación secundario (pulsación, llamada telefónica, código de acceso).
7. El proxy de autenticación Duo recibe la respuesta de autenticación.
8. La respuesta se envía al C8000V.
9. Si se realiza correctamente, se establece la conexión de AnyConnect.

Configurar

Para completar la configuración, tenga en cuenta estas secciones.

Pasos de configuración en C8000V (cabecera de VPN)

1. Configure el servidor RADIUS. La dirección IP del servidor RADIUS debe ser la IP del proxy de autenticación doble.

```
radius server rad_server
 address ipv4 10.197.243.97 auth-port 1812 acct-port 1813
 timeout 120
 key cisco
```

2. Configure el servidor RADIUS como aaa autenticación y la autorización como local.

```
aaa new-model
aaa group server radius FlexVPN_auth_server
 server name rad_server
aaa authentication login FlexVPN_auth group FlexVPN_auth_server
aaa authorization network FlexVPN_authz local
```

3. Cree un punto de confianza para instalar el certificado de identidad, si aún no está presente para la autenticación local. Puede consultar Inscripción de Certificados para una PKI para obtener más detalles sobre la creación del certificado.

```
crypto pki trustpoint TP_AnyConnect
enrollment url http://x.x.x.x:80/certsrv/mscep/mscep.dll
```

```
usage ike
serial-number none
fqdn flexvpn-C8000V.cisco.com
ip-address none
subject-name cn=flexvpn-C8000V.cisco.com
revocation-check none
rsakeypair AnyConnect
```

4. (Opcional) Configure una lista de acceso estándar que se utilizará para el túnel dividido. Esta lista de acceso consta de las redes de destino a las que se puede acceder a través del túnel VPN. De forma predeterminada, todo el tráfico pasa a través del túnel VPN si el túnel dividido no está configurado.

```
ip access-list standard split-tunnel-acl
 10 permit 192.168.11.0 0.0.0.255
 20 permit 192.168.12.0 0.0.0.255
```

5. Cree un conjunto de direcciones IPv4.

```
ip local pool SSLVPN_POOL 192.168.13.1 192.168.13.10
```

El conjunto de direcciones IP creado asigna una dirección IPv4 al cliente AnyConnect durante una conexión AnyConnect correcta.

6. Configure una directiva de autorización.

```
crypto ikev2 authorization policy ikev2-authz-policy
 pool SSLVPN_POOL
 dns 10.106.60.12
 route set access-list split-tunnel-acl
```

El grupo de IP, DNS, la lista de túnel dividido, etc., se especifican en la directiva de autorización.

Nota: Si la directiva de autorización IKEv2 personalizada no está configurada, se utilizará la directiva de autorización predeterminada denominada 'default' para la autorización. Los atributos especificados en la directiva de autorización IKEv2 también se pueden enviar a través del servidor RADIUS.

---

7. Configure una propuesta y una política IKEv2.

```
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-128
 integrity sha384
 group 19

crypto ikev2 policy FlexVPN_IKEv2_Policy
match fvrf any
proposal FlexVPN_IKEv2_Proposal
```

8. Cargue el perfil de cliente de AnyConnect en la memoria de inicialización del router y defina el perfil como se indica a continuación:

```
crypto vpn anyconnect profile Client_Profile bootflash:/Client_Profile.xml
```

9. Desactive el servidor HTTP seguro.

```
no ip http secure-server
```

10. Configure la política SSL y especifique la IP de WAN del router como la dirección local para descargar el perfil.

```
crypto ssl policy ssl-server
  pki trustpoint TP_AnyConnect sign
  ip address local

          port 443
```

11. Configure una plantilla virtual a partir de la cual el int de acceso virtualLas interfaces se clonan

```
interface Virtual-Template20 type tunnel
 ip unnumbered GigabitEthernet1
```

El comando no numerado obtiene la dirección IP de la interfaz configurada (GigabitEthernet1).

13. Configure un perfil IKEv2 que contenga todos los elementos relacionados con la conexióna lad información.

```
crypto ikev2 profile Flexvpn_ikev2_Profile
 match identity remote any
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint TP_AnyConnect
 dpd 60 2 on-demand
 aaa authentication eap FlexVPN_auth
 aaa authorization group eap list FlexVPN_authz ikev2-authz-policy
 aaa authorization user eap cached
 virtual-template 20 mode auto
 anyconnect profile Client_Profile
```

Se utilizan en el perfil IKEv2:

- match identity remote any - Se refiere a la identidad del cliente. Aquí 'any' está configurado para que cualquier cliente con las credenciales correctas pueda conectarse
- authentication remote - Indica que se debe utilizar el protocolo EAP para la autenticación de clientes
- authentication local - Menciona que los certificados deben utilizarse para la autenticación local
- aaa authentication eap - Durante la autenticación EAP, se utiliza el servidor FlexVPN_auth RADIUS
- aaa authorization group eap list - Durante la autorización, la lista de redes FlexVPN_authzse utiliza con la directiva de autorización ikev2-authz-policy
- aaa authorization user eap cached- Habilita la autorización de usuario implícita
- virtual-template 20 mode auto - Define la plantilla virtual que se va a clonar
- anyconnect profile Client_Profile - El perfil de cliente definido en el paso 8 se aplica aquí a este perfil IKEv2

14. Configure un conjunto de transformación y un perfil IPSec.

```
crypto ipsec transform-set TS esp-gcm 256
 mode tunnel

crypto ipsec profile Flexvpn_IPsec_Profile
 set transform-set TS
 set ikev2-profile Flexvpn_ikev2_Profile
```

15. Agregue el perfil IPSec a la plantilla virtual.

```
interface Virtual-Template20 type tunnel
```

```
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flexvpn_IPsec_Profile
```

Fragmento del perfil del cliente (perfil XML)

Antes de Cisco IOS XE 16.9.1, las descargas de perfiles automáticas desde la cabecera no estaban disponibles. Post 16.9.1, es posible descargar el perfil de la cabecera.

<#root>

```
!
!
```

```
        false
```

```
        true
```

```
        false
```

All

All

false

Native

false

```
30

false

true

false
```

false

true

IPv4,IPv6

true

ReconnectAfterResume

false

true

Automatic

SingleLocalLogon

SingleLocalLogon

AllowRemoteUsers

LocalUsersOnly

false

Automatic

```
false
```

```
false
```

```
 20
```

```
 4
```

false

false

true

<ServerList>
<HostEntry>
<HostName>FlexVPN</HostName>
<HostAddress>

flexvpn-csr.cisco.com

</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>

EAP

-

MD5

```
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

Pasos de configuración en el proxy de autenticación DUO

Nota: El proxy de autenticación doble sólo admite MS-CHAPv2 con autenticación RADIUS.

Paso 1. Descargue e instale el servidor proxy de autenticación Duo.

Inicie sesión en el equipo Windows e instale el servidor proxy de autenticación Duo.

Se recomienda utilizar un sistema con al menos 1 CPU, 200 MB de espacio en disco y 4 GB de RAM.

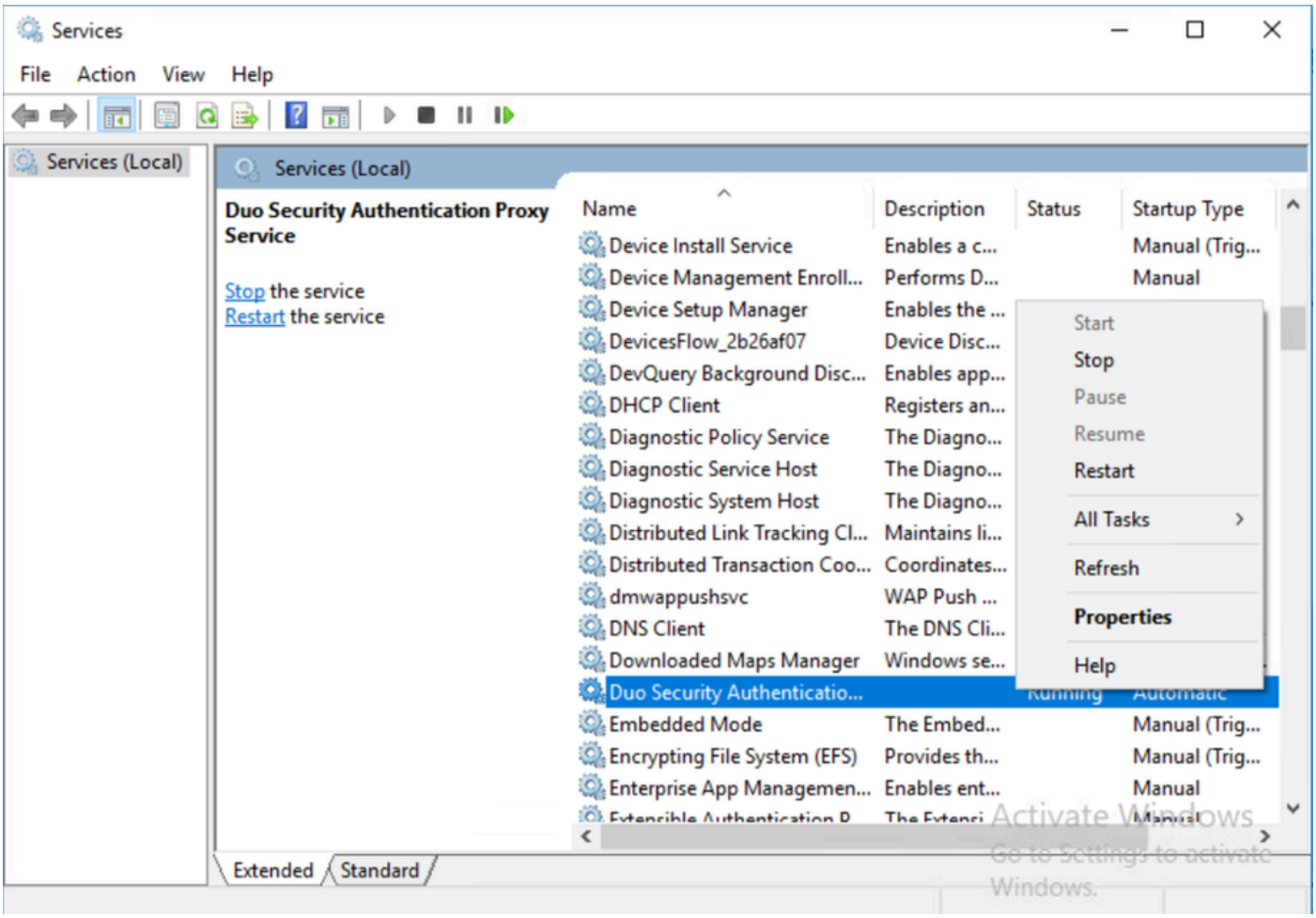
Paso 2. Navegue hasta C:\Program Files\Duo Security Authentication Proxy\conf\y abra authproxy.cfg para configurar el proxy de autenticación con los detalles adecuados.

```
[radius_client]
host=10.197.243.116
secret=cisco
```

Nota: Aquí '10.197.243.116' es la dirección IP del servidor ISE y 'cisco' es la contraseña configurada para validar la autenticación principal.

Una vez realizados estos cambios, guarde el archivo.

Paso 3. Abra la consola de Servicios de Windows (services.msc). Y reinicie Duo Security Authentication Proxy Service.

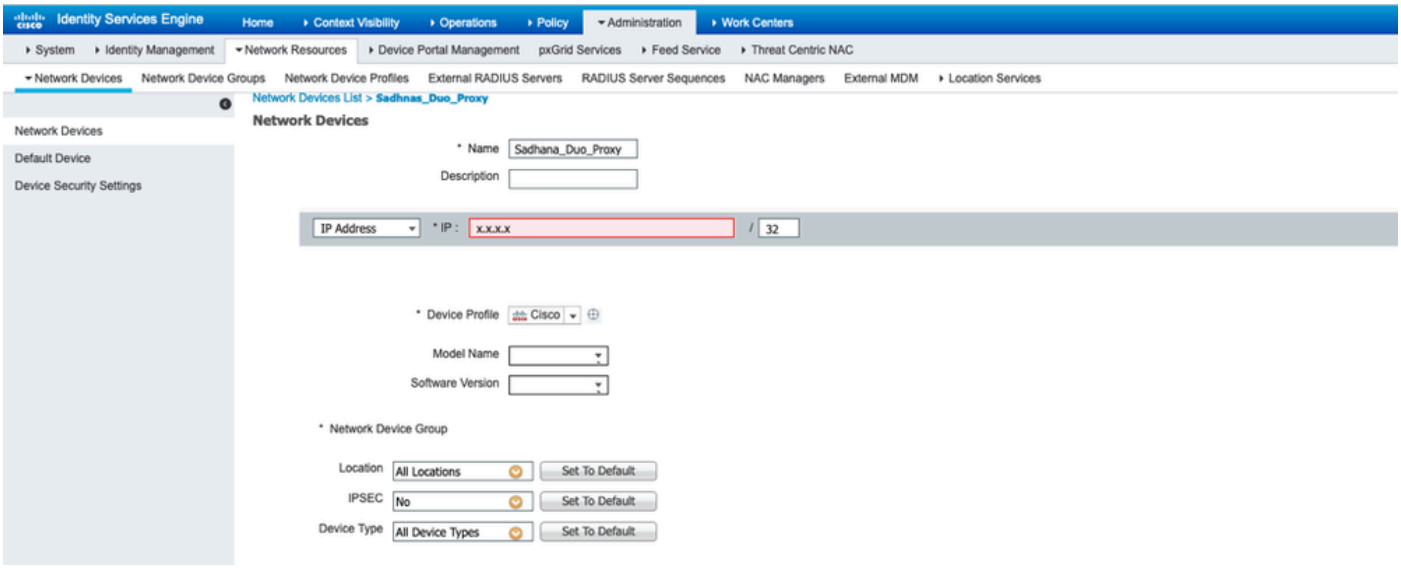


Servicio Duo Security Authentication Proxy

Pasos de configuración en ISE

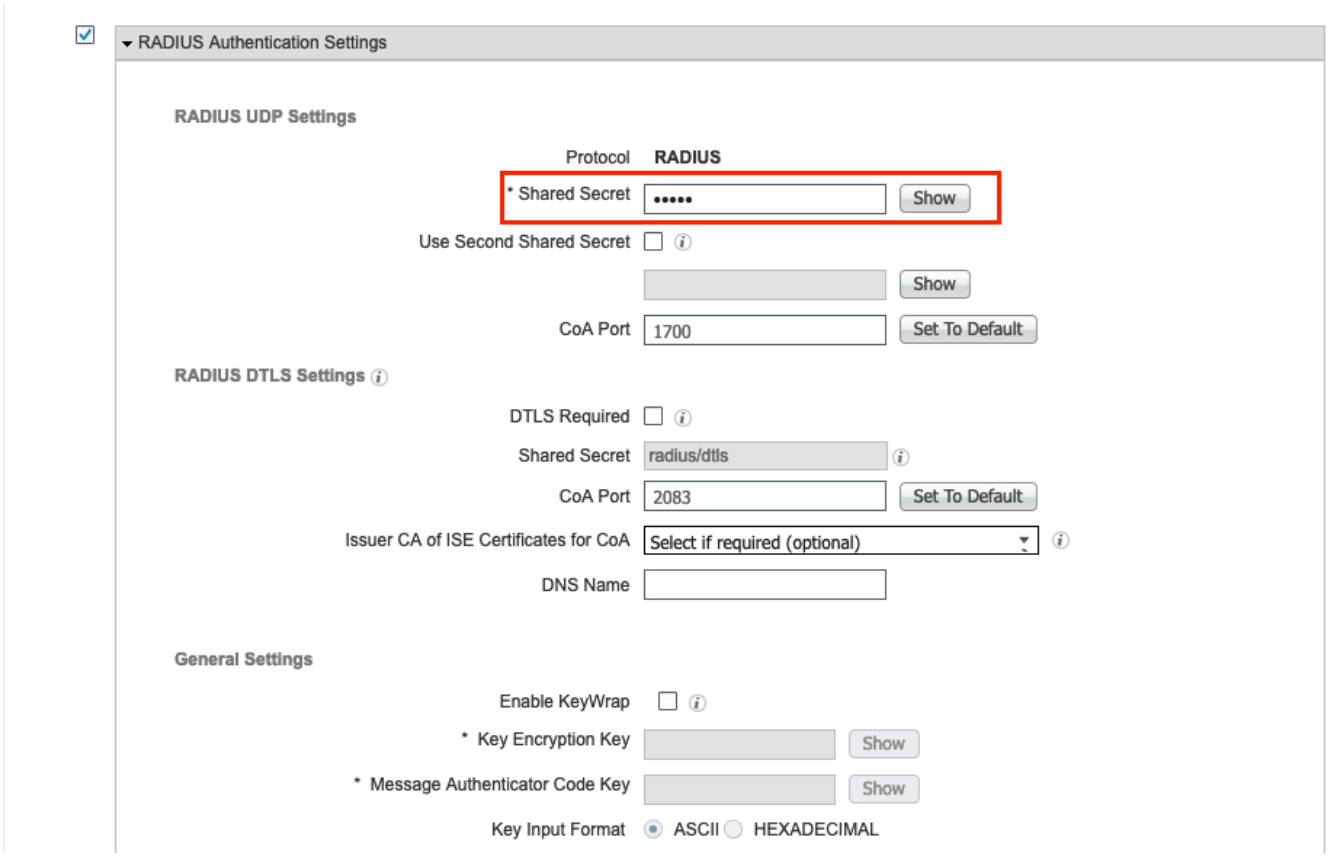
Paso 1. Navegue hasta **Administration** > **Network Devices**, y haga clicAddpara configurar el dispositivo de red.

Nota: Reemplazar x.x.x.x por la dirección IP del servidor proxy de autenticación Duo.



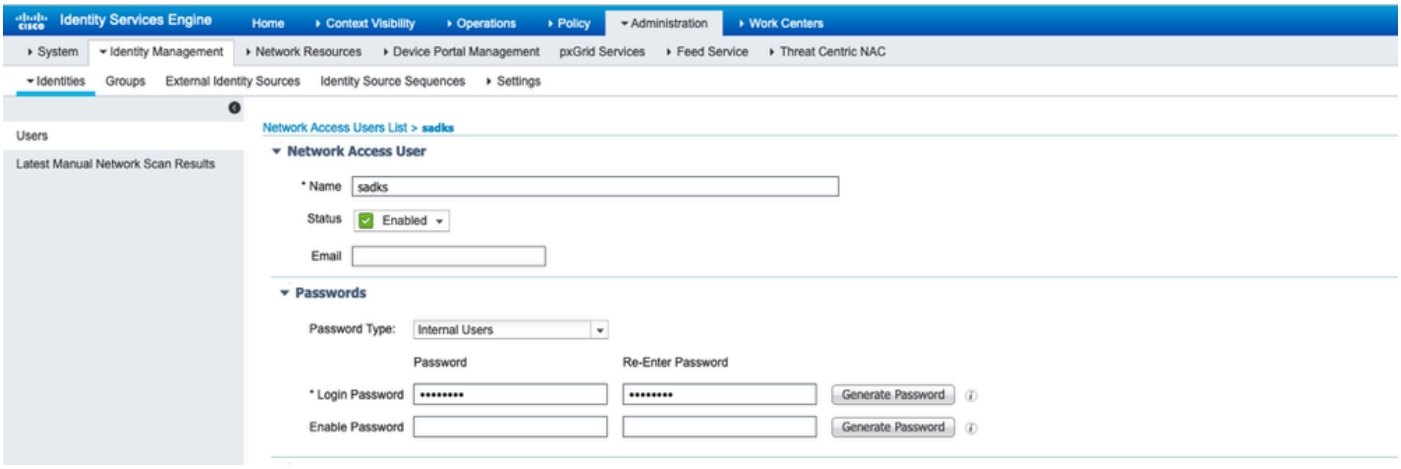
ISE - Dispositivos de red

Paso 2. Configure el Shared Secretcomo se menciona en la authproxy.cfgen secret:



ISE - Secreto compartido

Paso 3. Vaya a Administration > Identities > Users.Elija Addpara configurar el usuario de identidad para la autenticación principal de AnyConnect:

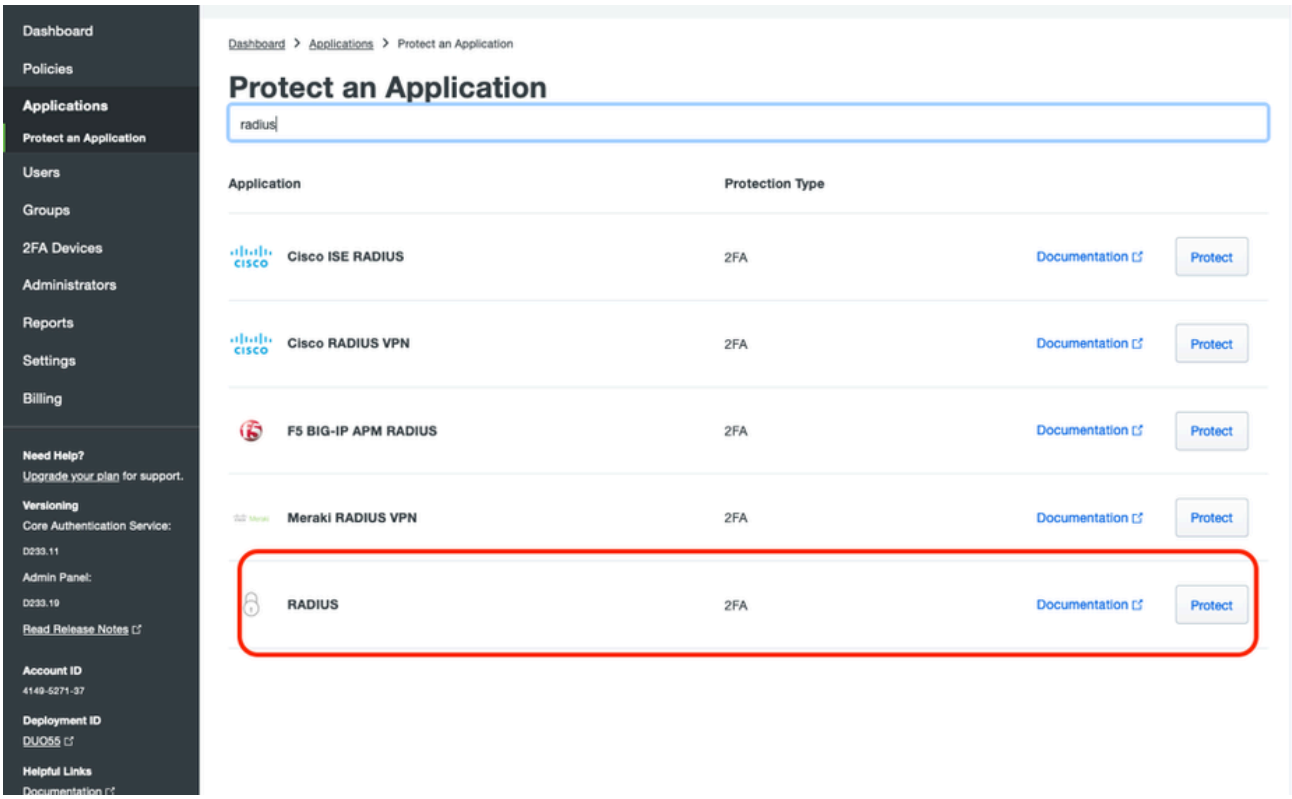


ISE - Usuarios

Pasos de configuración en el portal de administración DUO

Paso 1. Inicie sesión en su cuenta Duo.

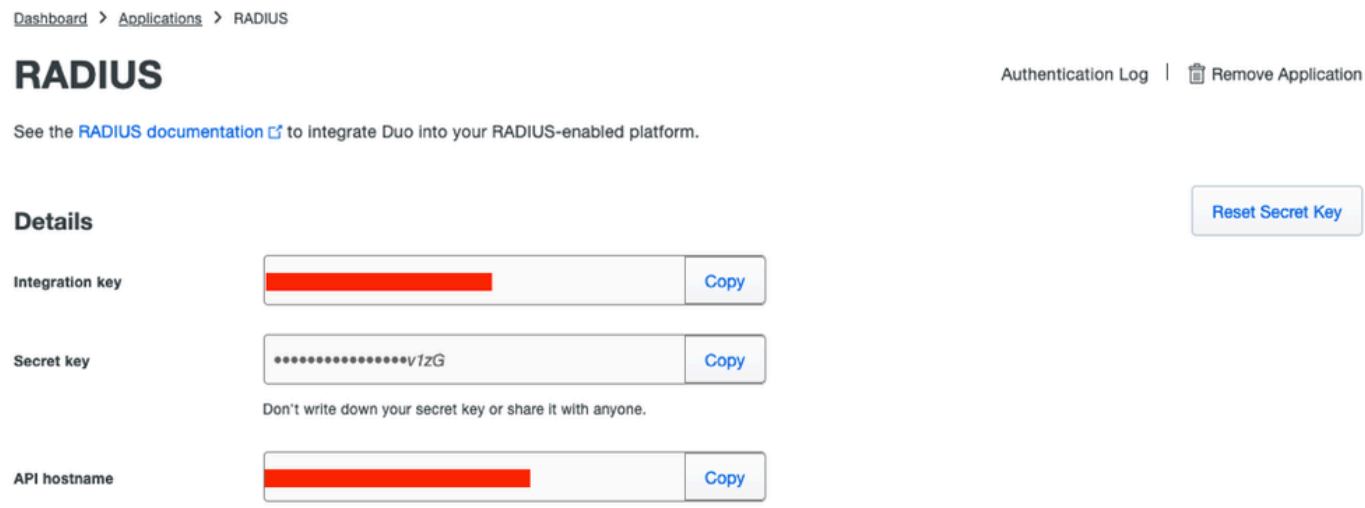
Desplácese hasta Applications > Protect an Application. Haga clic Protect en la aplicación que desee utilizar. (RADIUS en este caso)



DUO - Aplicación

Paso 2. Haga clic Protect en la aplicación que desea utilizar. (RADIUS en este caso)

Copie la clave de integración, la clave secreta y el nombre de host de la API y péguelo en el authproxy.cfgdel proxy de autenticación doble.



DUO - RADIUS

Copie estos valores y navegue de nuevo al proxy de autenticación DUO y abra el authproxy.cfgy pegue los valores como se indica:

Clave de integración = ikey

clave secreta = skey

API hostname = api_host

```
[radius_server_auto]
ikey=xxxxxxxx
skey=xxxxxxxv1zG
api_host=xxxxxxxx
radius_ip_1=10.106.54.143
radius_secret_1=cisco
failmode=safe
client=radius_client
port=1812
```

Nota: El ikey, skey y api_host deben copiarse del servidor Duo cuando configure el servidor, y '10.106.54.143' es la dirección IP del router C8000V, y 'cisco' es la clave configurada en el router bajo la configuración del servidor RADIUS.

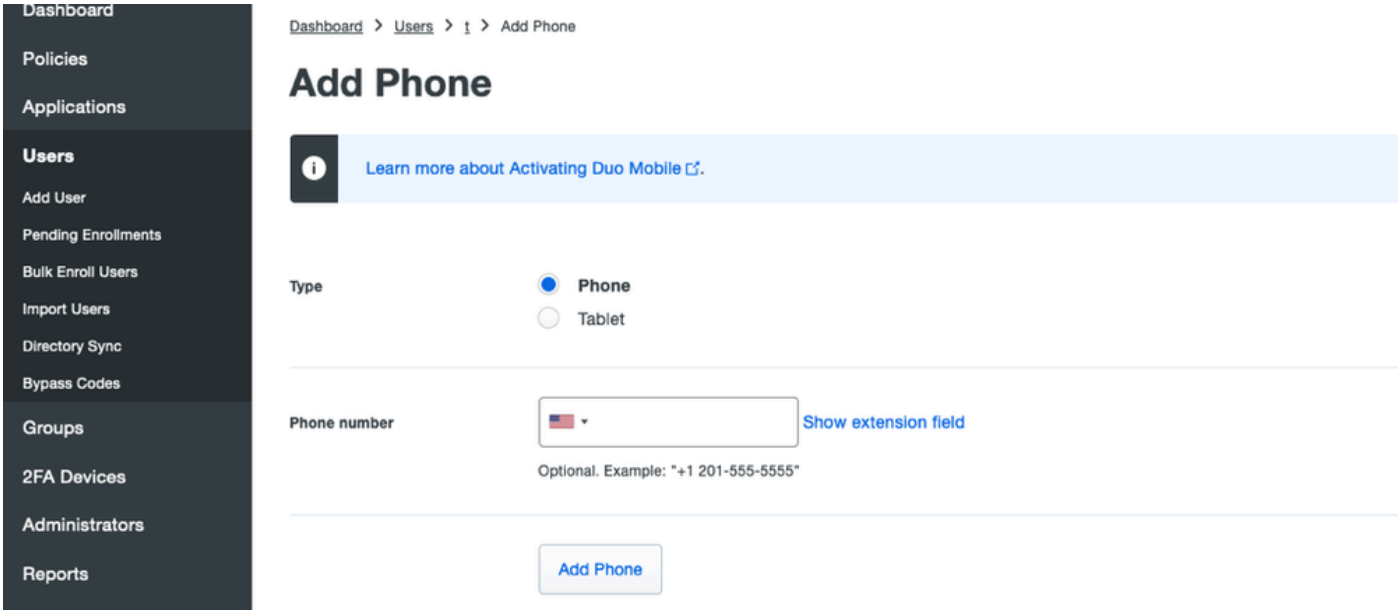
Una vez que haya realizado estos cambios, guarde el archivo de nuevo y reinicie Duo Security Authentication Proxy Service (en services.msc).

Paso 3. Crear usuarios en DUO para la autenticación secundaria.

Desplácese hastaUsers > Add Usery escriba el nombre de usuario.

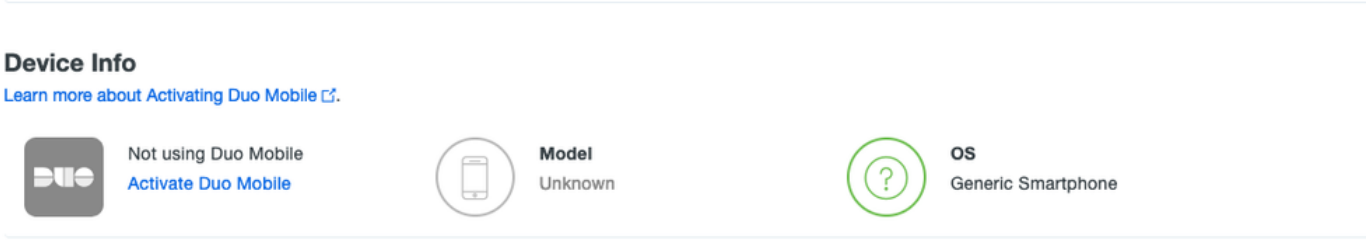
Nota: El nombre de usuario debe coincidir con el nombre de usuario de autenticación principal.

Haga clic en Add User. Una vez creado, en Phones, haga clic en Add Phone, introduzca el número de teléfono y haga clic en Add Phone.



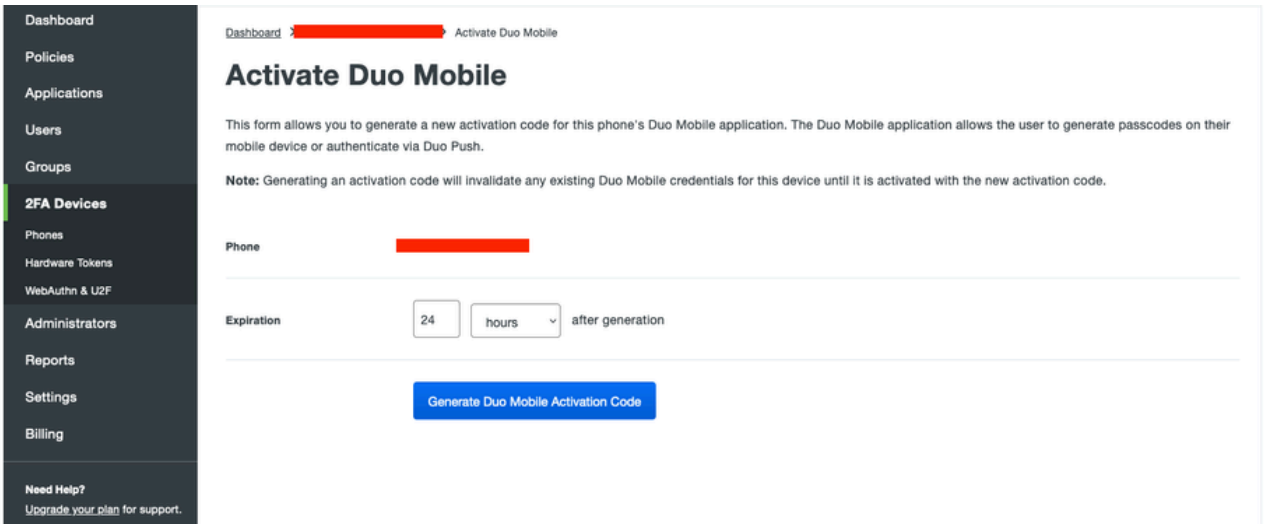
DUO - Agregar teléfono

Elija el tipo de autenticación.



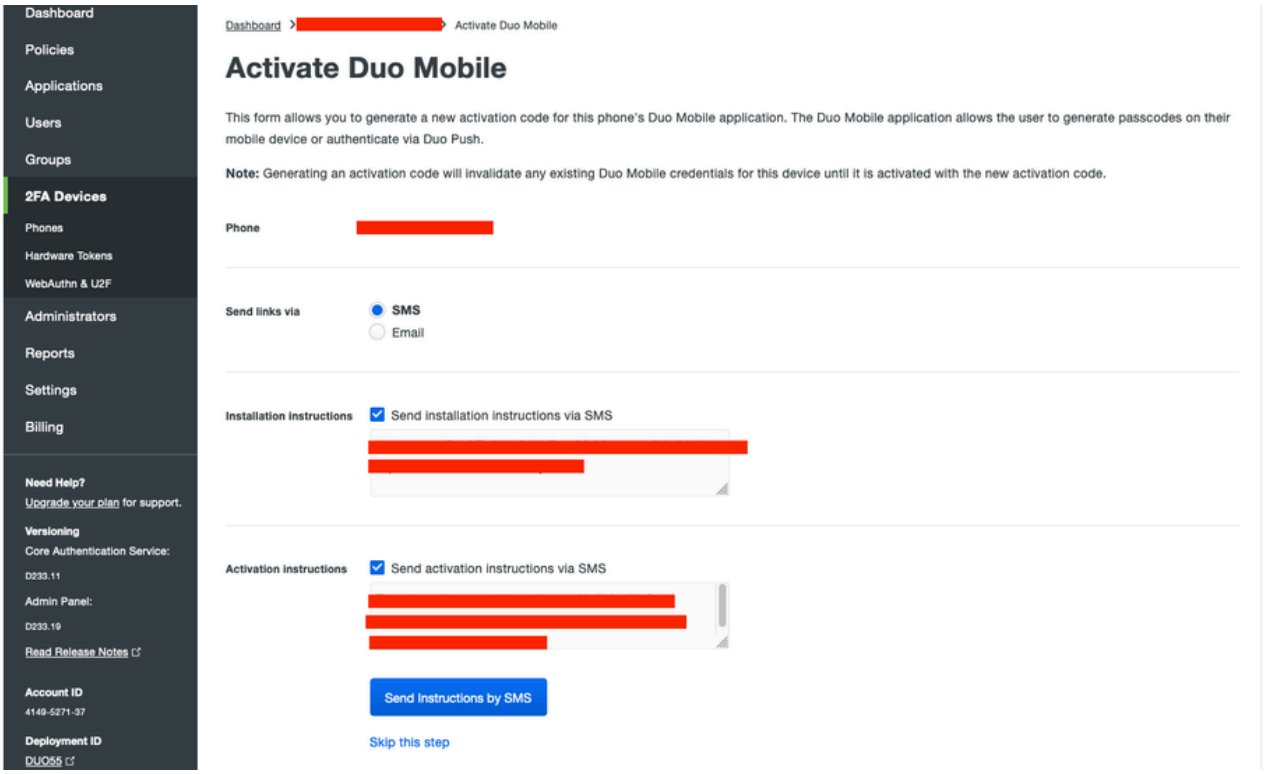
DUO: información del dispositivo

Elija Generate Duo Mobile Activation Code.



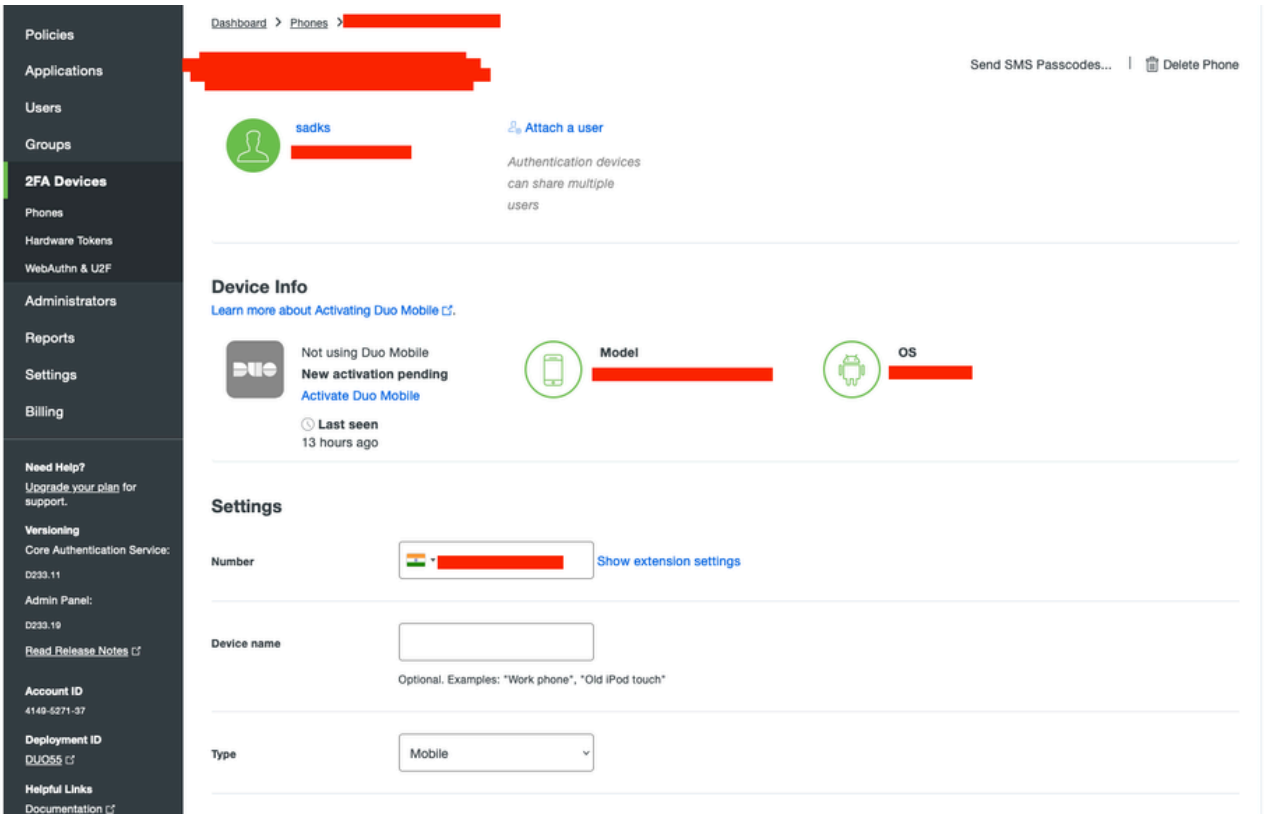
DUO: activación de teléfono

Elegir Send Instructions by SMS.



DUO - Enviar SMS

Haga clic en el enlace enviado al teléfono y la aplicación DUO se vincula a la cuenta de usuario en la Device Infosección, como se muestra en la imagen:

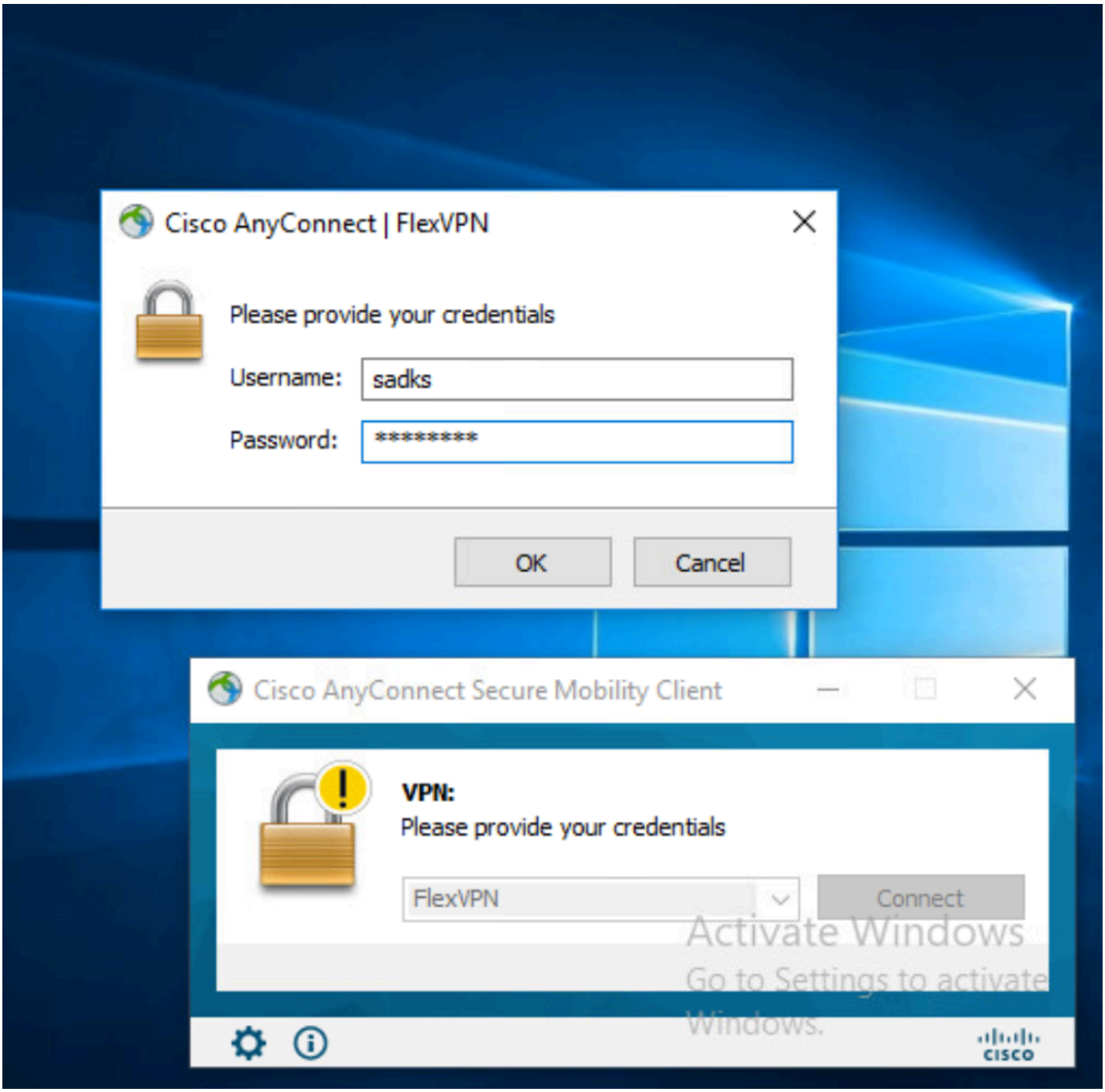


DUO: dispositivo vinculado

Verificación

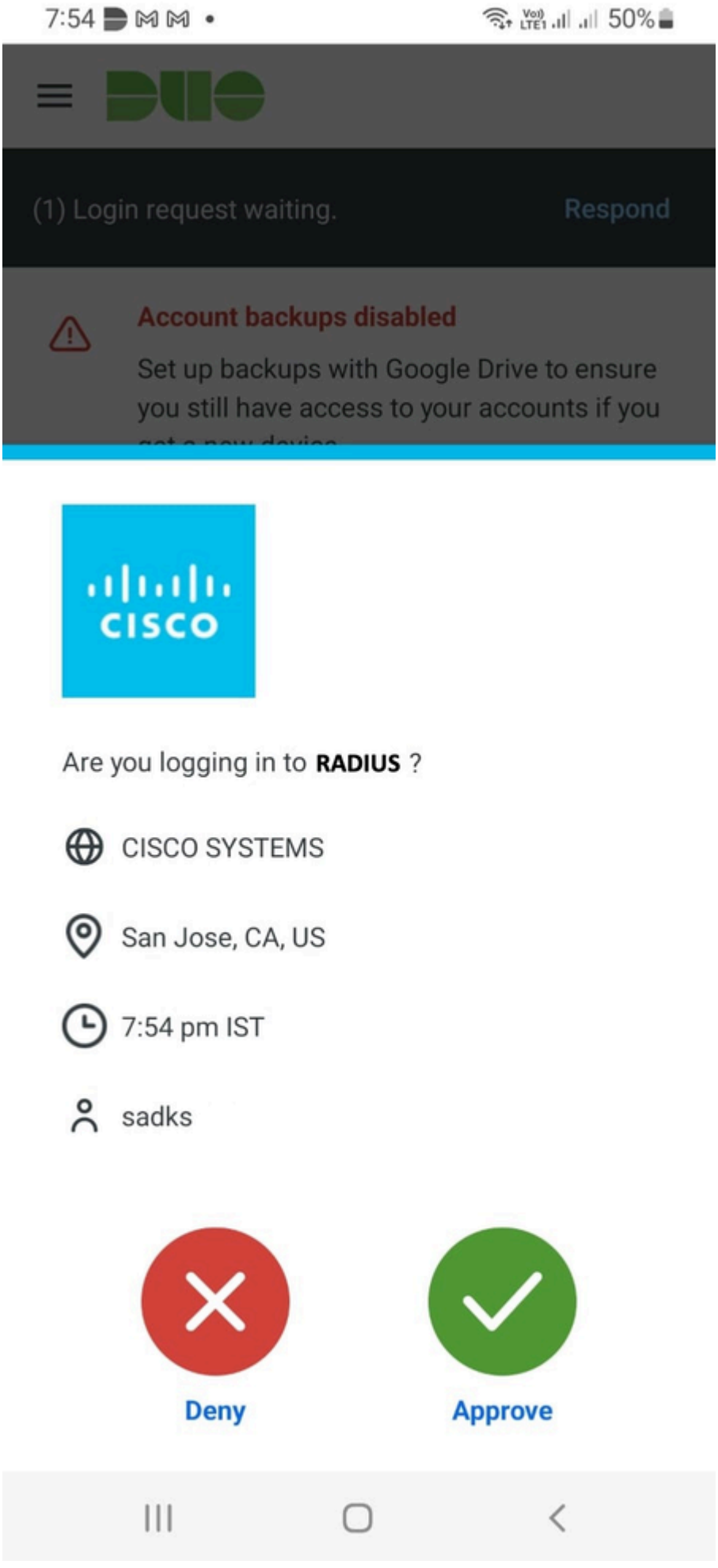
Para probar la autenticación, conéctese al C8000V desde el PC del usuario a través de AnyConnect.

Escriba el nombre de usuario y la contraseña para la autenticación principal.



Conexión AnyConnect

Entonces, acepte los empujes DUO en el móvil.



Inserción DUO

Se establece la conexión

<#root>

```
R1#sh crypto ikev2 sa detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.106.54.143/4500    10.197.243.98/54198   none/none
```

READY

```
      Encr: AES-CBC, keysize: 256, PRF: SHA384, Hash: SHA384, DH Grp:19, Auth sign: RSA, Auth verify: Fle
      Life/Active Time: 86400/147 sec
      CE id: 1108, Session-id: 15
      Status Description: Negotiation done
      Local spi: 81094D322A295C92       Remote spi: 802F3CC9E1C33C2F
      Local id: 10.106.54.143
      Remote id: cisco.com
      Remote EAP id:
```

sadks

//

AnyConnect username

```
      Local req msg id:  0              Remote req msg id:  10
      Local next msg id: 0              Remote next msg id: 10
      Local req queued:  0              Remote req queued:  10
      Local window:      5              Remote window:      1
      DPD configured for 60 seconds, retry 2
      Fragmentation not  configured.
      Dynamic Route Update: disabled
      Extended Authentication not configured.
      NAT-T is detected  outside
      Cisco Trust Security SGT is disabled
```

Assigned host addr: 192.168.13.5

//Assigned IP address from t

```
      Initiator of SA : No
```

2. Crypto session detail for the vpn session

<#root>

```
R1#sh crypto session  detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
```

```
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Virtual-Access2
Profile:
```

FlexVPN

-

ikev2_Profile

Uptime: 00:01:07

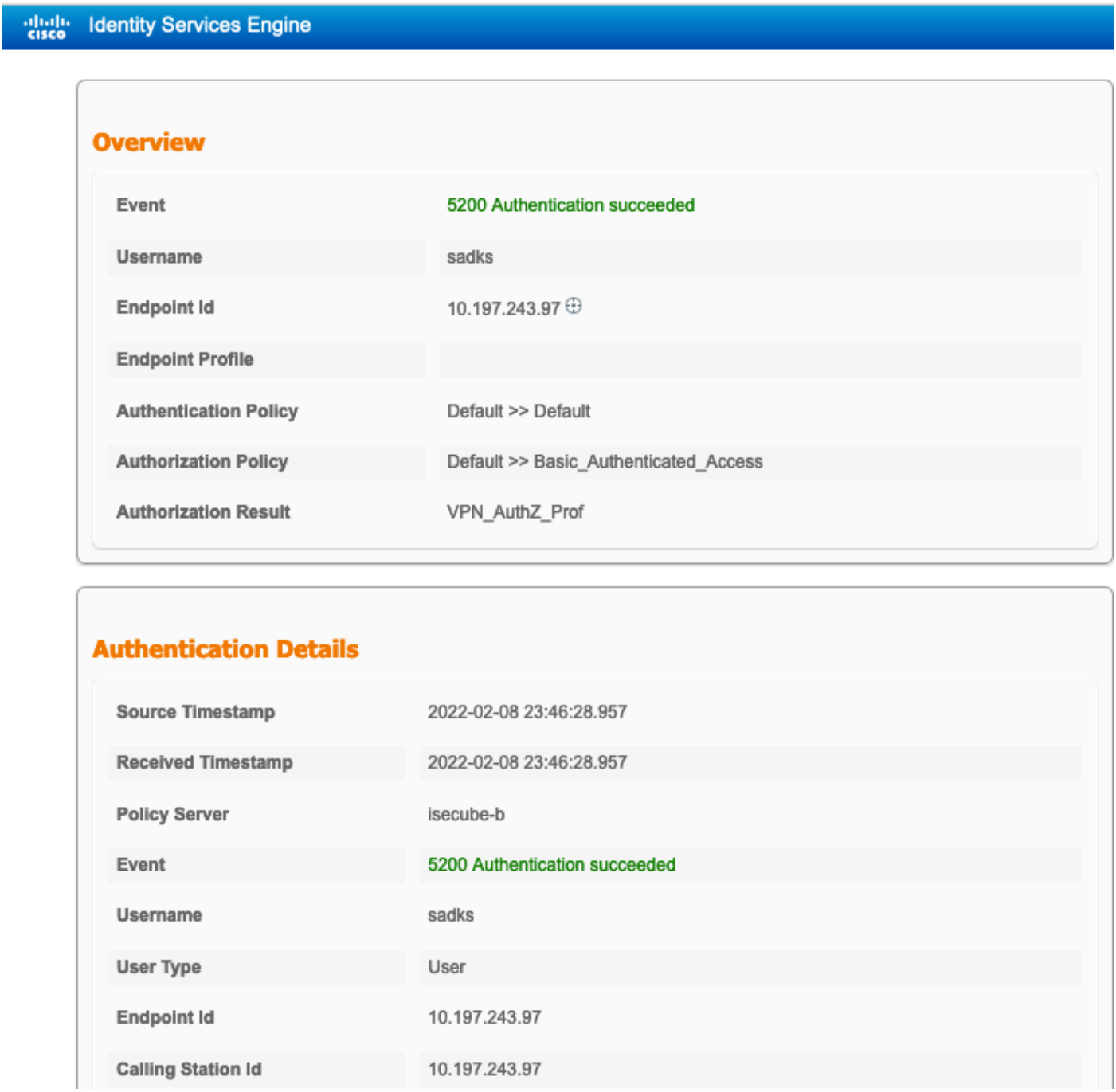
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host
```

192.168.13.5

```
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 3 drop 0 life (KB/Sec) 4607998/3532
        Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4608000/3532
```

3.Verification on ISE live logs

Vaya aOperations > Live Logsen ISE. Puede ver el informe de autenticación de la autenticación principal.



ISE - Live Logs

4. Verification on DUO authentication proxy

Navegue hasta este archivo en el proxy de autenticación DUO; C:\Program Files\Duo Security Authentication Proxy\log

<#root>

```
2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info]
 Sending request from 10.106.54.143
 to radius_server_auto
                                                                    //10.106.5
```

```
2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info] Received new request id 163 from ('10.106.54
2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163):
login attempt for username 'sadks'

2022-02-08T23:24:50.080854+0530 [duoauthproxy.lib.log#info]
Sending request for user 'sadks' to ('10.197.243.116', 1812)

with id 191                                                                    //Primary auth sent t

2022-02-08T23:24:50.174606+0530 [duoauthproxy.lib.log#info]
Got response for id 191 from ('10.197.243.116', 1812); code 2

2022-02-08T23:24:50.174606+0530 [duoauthproxy.lib.log#info] http POST to
https://api
-
xxxx[.]duosecurity[.]com:443/rest/v1/preauth

2022-02-08T23:24:50.174606+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_Du
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163): Got
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.log#info]
http POST to
https://api
-
xxxx[.]duosecurity[.]com:443/rest/v1/auth

2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Starting factory <_Du
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_Du
2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163):
Duo authentication returned 'allow': 'Success. Logging you in...'

2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163):
Returning response code 2: AccessAccept

2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 163): Send
2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_Du
```

Troubleshoot

1. Depuración en C8000V.

Para IKEv2:

- debug crypto ikev2
- debug crypto ikev2 client flexvpn
- debug crypto ikev2 internal
- debug crypto ikev2 packet
- debug crypto ikev2 error

Para IPSec:

- debug crypto ipsec
- debug crypto ipsec error

2. Para el proxy de autenticación DUO, verifique los registros relacionados con el proxy del archivo de registro. ()C:\Program Files\Duo Security Authentication Proxy\log

Se muestra el fragmento de código de un registro de errores donde ISE rechaza la autenticación principal:

<#root>

```
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info]
```

Sending proxied request

```
 for id 26 to ('10.197.243.116', 1812) with id 18
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info]
```

Got response

```
 for id 18 from ('10.197.243.116', 1812); code 3
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 26):
```

Primary credentials rejected - No reply message in packet

```
2022-02-07T13:01:39.589679+0530 [duoauthproxy.lib.log#info] (('10.106.54.143', 1645), sadks, 26): Retur
```

AccessReject

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).