Configurar o AnyConnect Flexvpn com autenticação EAP e DUO

Contents

Introdução

Este documento descreve como configurar a autenticação externa de dois fatores para a conexão IPSec do AnyConnect a um roteador Cisco IOS® XE.

Contribuição de Sadhana K S e Rishabh Aggarwal Engenheiros do Cisco TAC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Experiência com configuração de VPN RA em um roteador
- Administração do Identity Services Engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst 8000V (C8000V) executando a versão 17.10.01a
- Cisco AnyConnect Secure Mobility Client versão 4.10.04071

- Cisco ISE executando a versão 3.1.0
- Servidor proxy de autenticação Duo (Windows 10 ou qualquer PC com Linux)
- Conta da Web do Duo
- PC cliente com AnyConnect instalado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Fluxo de autenticação

O usuário do AnyConnect autentica com um nome de usuário e senha no servidor ISE. O servidor Proxy de Autenticação Duo também envia uma autenticação adicional na forma de notificação por push ao dispositivo móvel do usuário.

Diagrama de fluxo

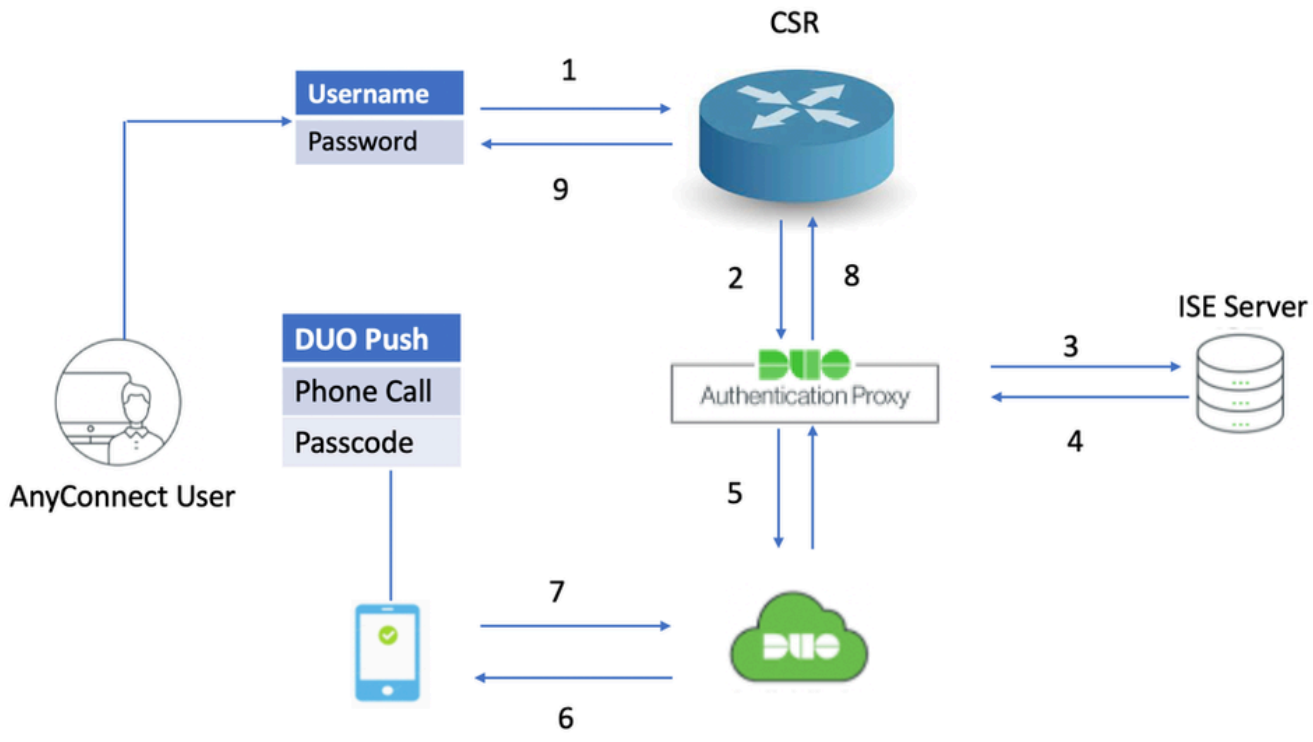


Diagrama de fluxo de autenticação

Processo de comunicação

1. O usuário inicia uma conexão RAVPN com o C8000V e fornece um nome de usuário e uma senha para a Autenticação primária.
2. O C8000V envia uma solicitação de autenticação ao Proxy de Autenticação Duo.
3. O Duo Authentication Proxy envia então a solicitação principal ao servidor Ative Diretory ou

RADIUS.
4. A resposta de autenticação é enviada de volta ao Proxy de autenticação.
5. Assim que a autenticação primária for bem-sucedida, o proxy de autenticação Duo solicitará a autenticação secundária através do servidor Duo.
6. O serviço Duo autentica então o usuário, dependendo do método de autenticação secundário (push, chamada telefônica, senha).
7. O proxy de autenticação Duo recebe a resposta de autenticação.
8. A resposta é enviada para o C8000V.
9. Se obtiver êxito, a conexão do AnyConnect será estabelecida.

Configurar

Para concluir a configuração, leve em consideração estas seções.

Etapas de configuração no C8000V (VPN Headend)

1. Configure o servidor RADIUS. O endereço IP do servidor RADIUS deve ser o IP do Proxy de Autenticação Duo.

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

2. Configure o servidor RADIUS como aaa autenticação e autorização 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. Crie um Ponto Confiável para instalar o certificado de identidade, se ainda não estiver presente para autenticação local. Você pode consultar Inscrição de certificado para uma PKI para obter mais detalhes sobre a criação do 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 uma lista de acesso padrão a ser usada para o túnel dividido. Essa lista de acesso consiste nas redes de destino que podem ser acessadas através do túnel VPN. Por padrão, todo o tráfego passa pelo túnel VPN se o túnel dividido não estiver 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. Crie um pool de endereços IPv4.

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

O pool de endereços IP criado atribui um endereço IPv4 ao cliente AnyConnect durante uma conexão bem-sucedida do AnyConnect.

6. Configure uma política de autorização.

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

O pool IP, o DNS, a lista de túneis divididos e assim por diante são especificados na política de autorização.

Note: Se a política de autorização IKEv2 personalizada não estiver configurada, a política de autorização padrão chamada 'padrão' será usada para autorização. Os atributos especificados na política de autorização IKEv2 também podem ser enviados por meio do servidor RADIUS.

---

7. Configure uma proposta e política de 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. Carregue o perfil do cliente AnyConnect para o flash de inicialização do roteador e defina o perfil conforme indicado:

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

9. Desabilite o servidor seguro HTTP.

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

10. Configure a política SSL e especifique o IP WAN do roteador como o endereço local para fazer download do perfil.

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

           port 443
```

11. Configure um Modelo virtual a partir do qual o int de acesso virtualAs interfaces são clonadas

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

O comando não numerado obtém o endereço IP da interface configurada (GigabitEthernet1).

13. Configure um perfil IKEv2 que contenha todas as conexõesad riz Informação promenorizada.

```
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
```

Eles são usados no perfil IKEv2:

- match identity remote any - Se refere à identidade do cliente. Aqui 'any' é configurado para que qualquer cliente com as credenciais corretas possa se conectar
- authentication remote - Menciona que o protocolo EAP deve ser usado para autenticação do cliente
- authentication local - Menciona que os certificados devem ser usados para autenticação local
- aaa authentication eap - Durante a autenticação EAP, o servidor FlexVPN_auth RADIUS é usado
- aaa authorization group eap list - Durante a autorização, a lista de redes FlexVPN_authzé usado com a política de autorização ikev2-authz-policy
- aaa authorization user eap cached- Habilita a autorização implícita do usuário
- virtual-template 20 mode auto - Define o modelo virtual a ser clonado
- anyconnect profile Client_Profile - O perfil de cliente definido na Etapa 8. é aplicado aqui a este perfil IKEv2

14. Configure um conjunto de transformação e um 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. Adicione o perfil IPSec ao molde Virtual.

```
interface Virtual-Template20 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile Flexvpn_IPsec_Profile
```

Trecho do Perfil do Cliente (Perfil XML)

Antes do Cisco IOS XE 16.9.1, os downloads automáticos de perfil do headend não estavam disponíveis. Após 16.9.1, é possível fazer o download do perfil do headend.

<#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>
```

Etapas de Configuração no Proxy de Autenticação DUO

Note: Duo Authentication Proxy oferece suporte a MS-CHAPv2 somente com autenticação RADIUS.

Etapa 1. Baixar e instalar o servidor proxy de autenticação Duo.

Faça login na máquina Windows e instale o servidor Proxy de Autenticação Duo.

É recomendável usar um sistema com pelo menos 1 CPU, 200 MB de espaço em disco e 4 GB de RAM.

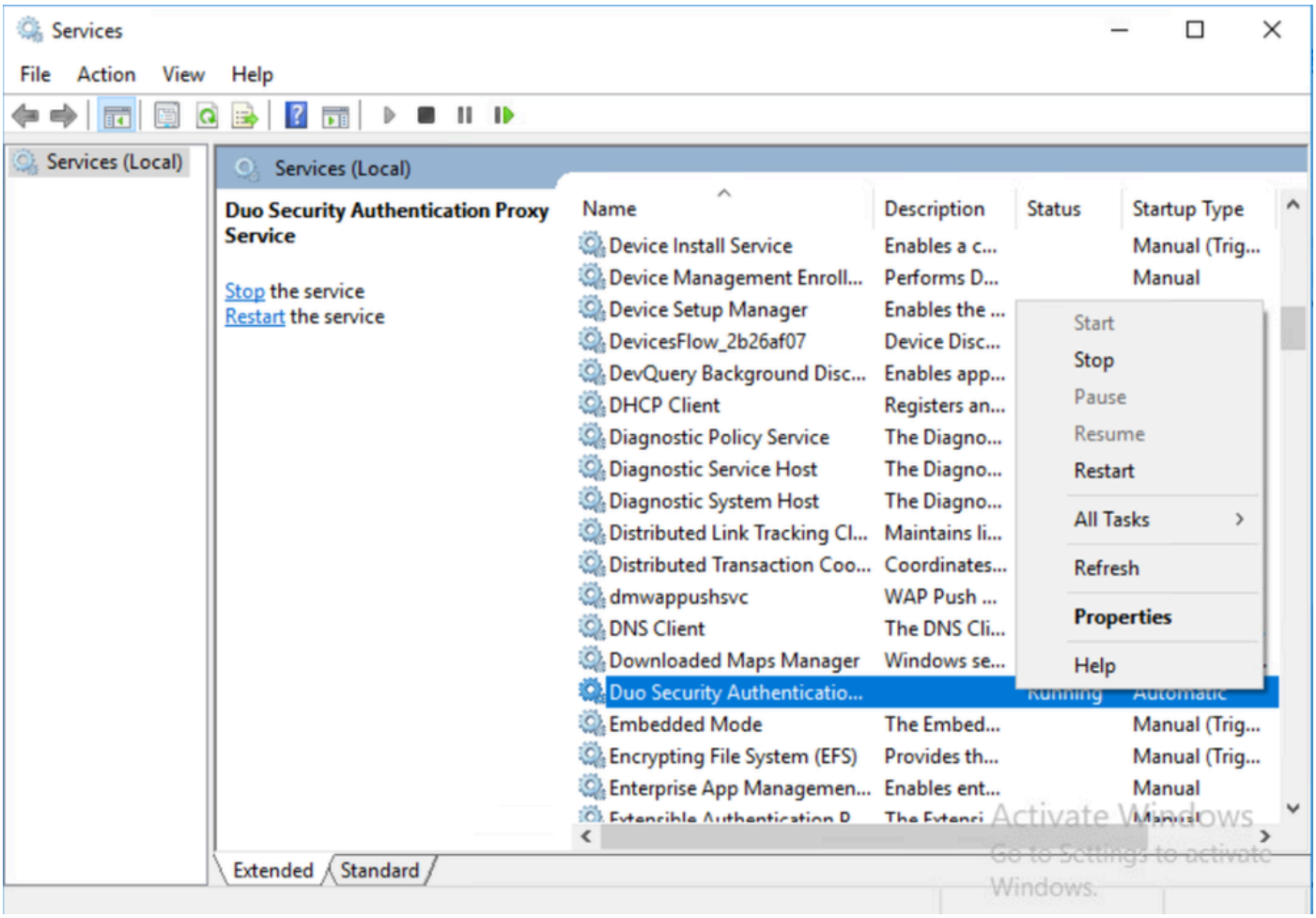
Etapa 2. Navegue até C:\Program Files\Duo Security Authentication Proxy\conf\e abra authproxy.cfg para configurar o proxy de autenticação com os detalhes apropriados.

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

Note: Aqui '10.197.243.116' é o endereço IP do servidor ISE e 'cisco' é a senha configurada para validar a autenticação primária.

Depois de fazer essas alterações, salve o arquivo.

Etapa 3. Abra o console de Serviços do Windows (services.msc). E reinicie Duo Security Authentication Proxy Service.

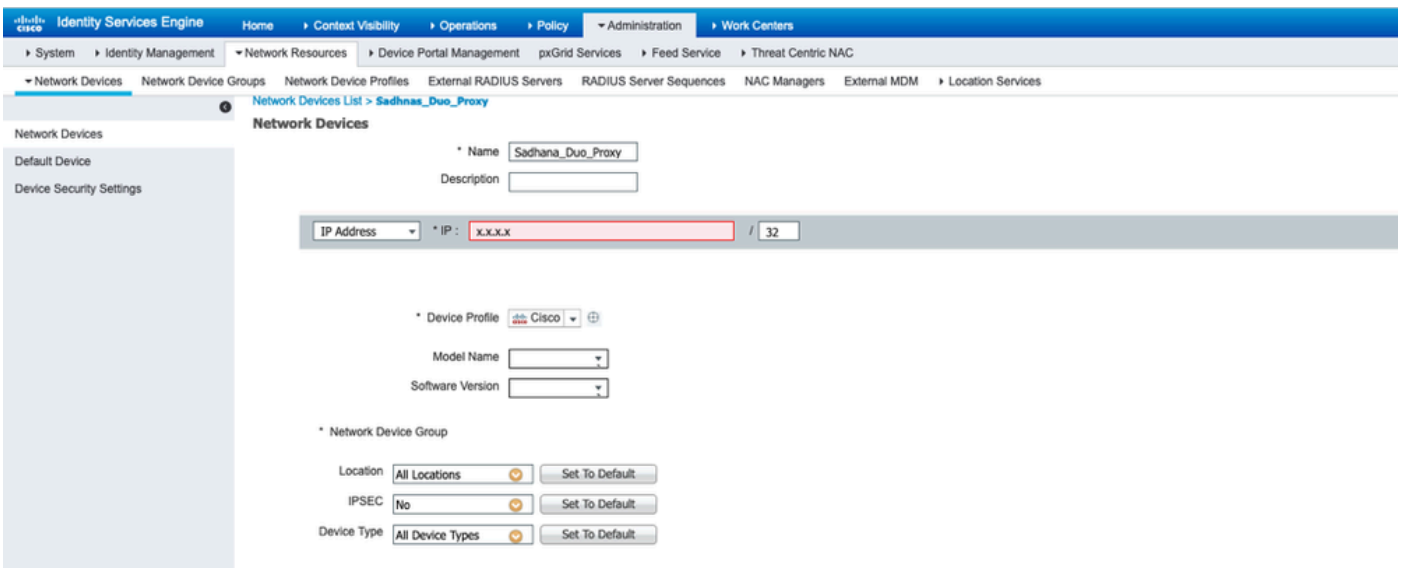


Serviço de Proxy de Autenticação de Segurança Duo

Etapas de configuração no ISE

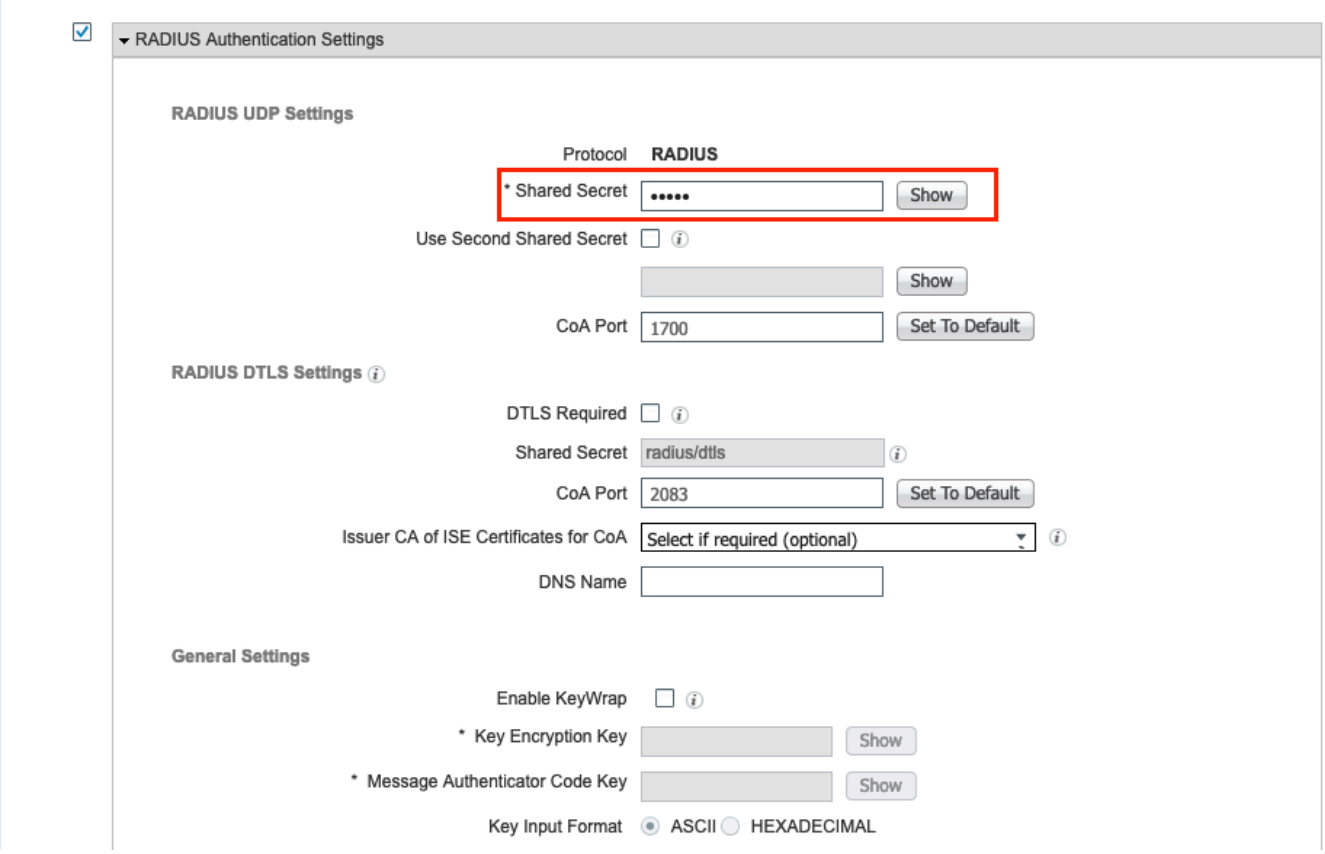
Etapa 1. Navegue até **Administration** > **Network Devices**e cliqueAddpara configurar o dispositivo de rede.

Note: Substituir x.x.x.x pelo endereço IP do servidor Proxy de Autenticação Duo.



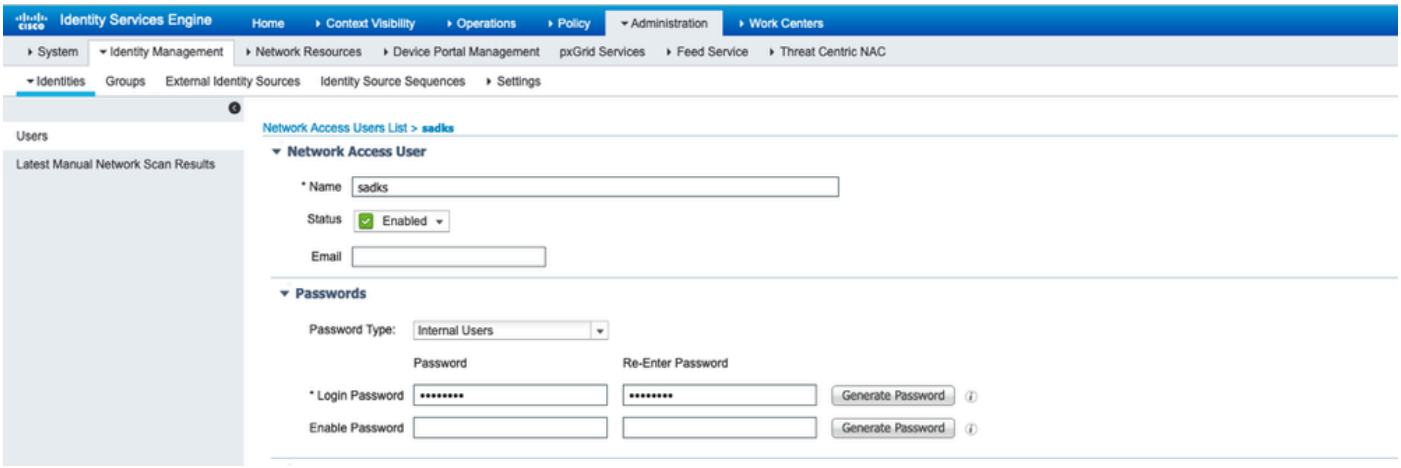
ISE - Dispositivos de rede

Etapa 2. Configure o Shared Secretconforme mencionado na authproxy.cfgem secret:



ISE - Segredo compartilhado

Etapa 3. Navegue até Administration > Identities > Users.Escolha Addna ordem para configurar o usuário de identidade para a autenticação primária do AnyConnect:



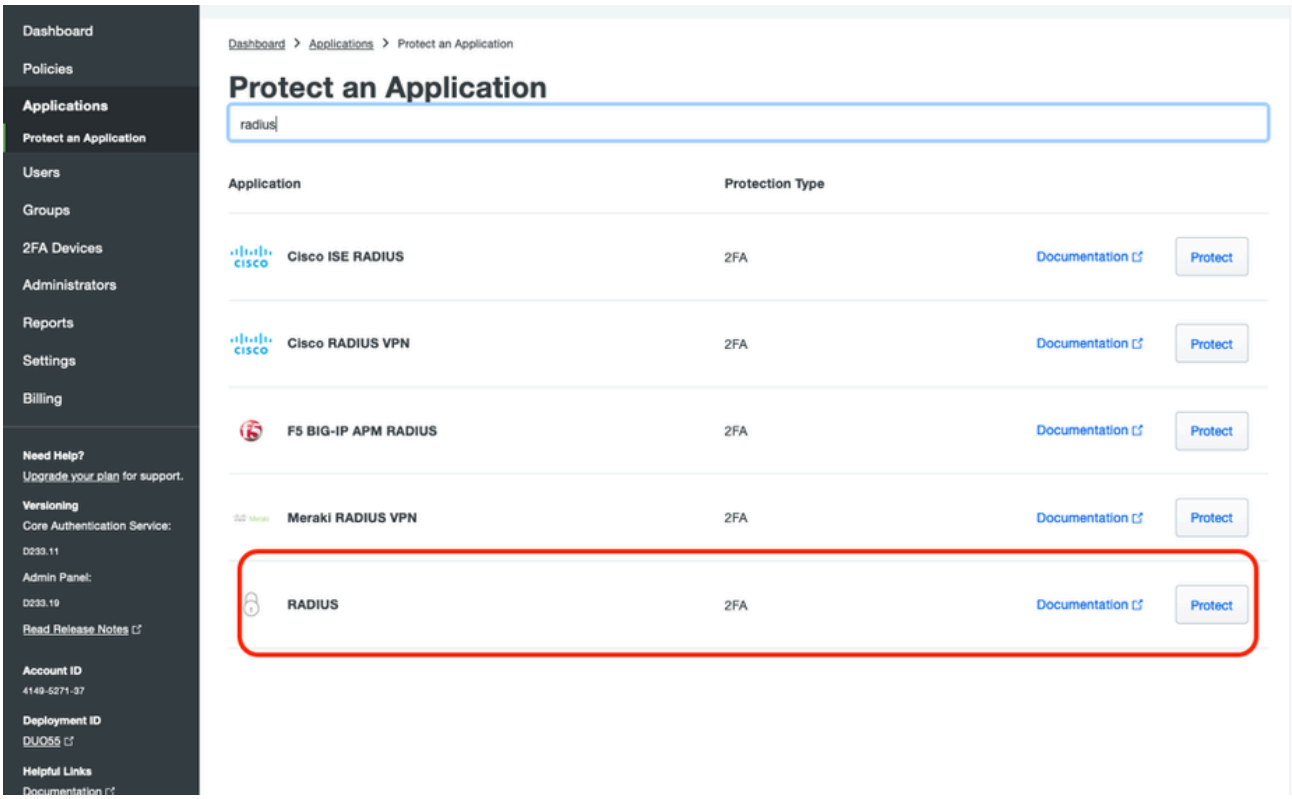
ISE - Usuários

Etapas de Configuração no Portal de Administração do DUO

Etapa 1. Efetue login na sua conta Duo.

Navegue atéApplications > Protect an Application. Clique Protect no aplicativo que deseja usar. (RADIUS

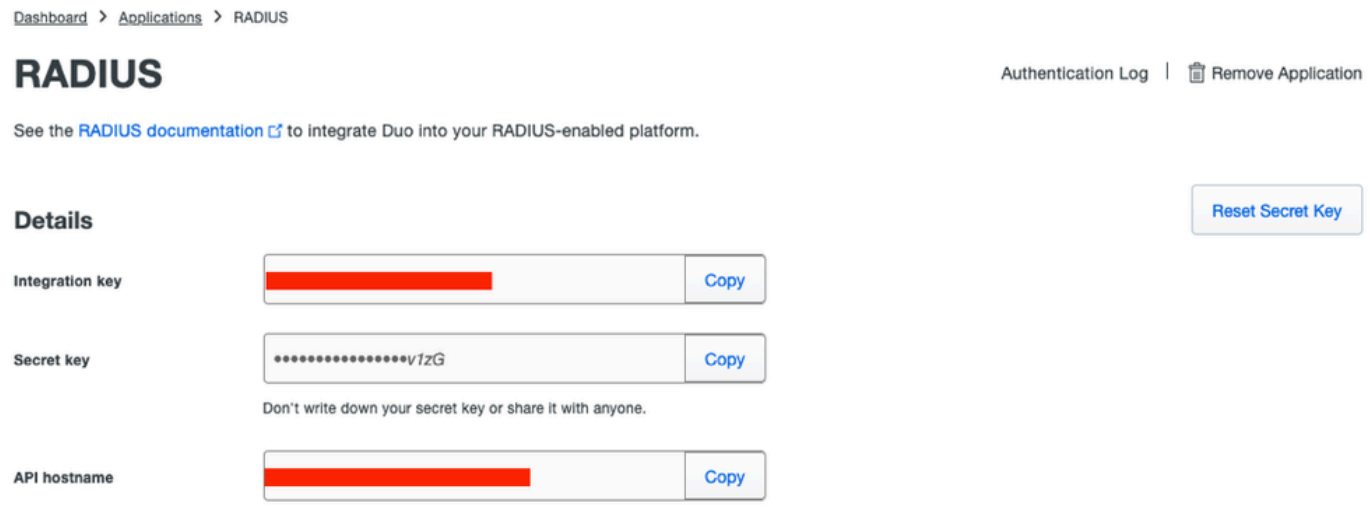
neste caso)



DUO - Aplicativo

Etapa 2. Clique Protect no aplicativo que deseja usar. (RADIUS neste caso)

Copie a chave de integração, a chave secreta e o nome de host da API e cole-os no authproxy.cfgdo proxy de autenticação Duo.



DUO - RADIUS

Copie esses valores e navegue de volta para o proxy de autenticação DUO e abra a authproxy.cfge cole os valores como mostrado:

Chave de integração = ikey

chave secreta = chave

nome de host da API = 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
```

Note: O ikey, a chave e o api_host devem ser copiados do servidor Duo quando você configurar o servidor, e '10.106.54.143' é o endereço IP do roteador C8000V, e 'cisco' é a chave configurada no roteador sob a configuração do servidor radius.

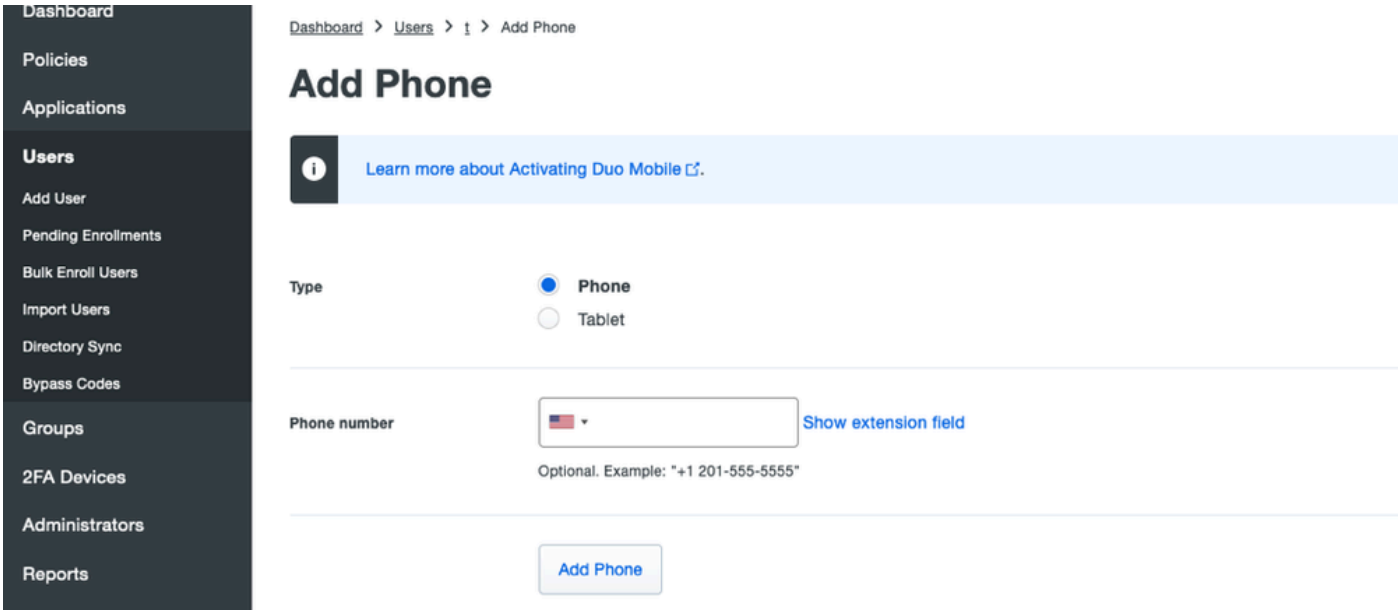
Depois de fazer essas alterações, salve o arquivo novamente e reinicie o Serviço de Proxy de Autenticação de Segurança Duo (em services.msc).

Etapa 3. Criar usuários no DUO para autenticação secundária.

Navegue atéUsers > Add Usere digite o nome de usuário.

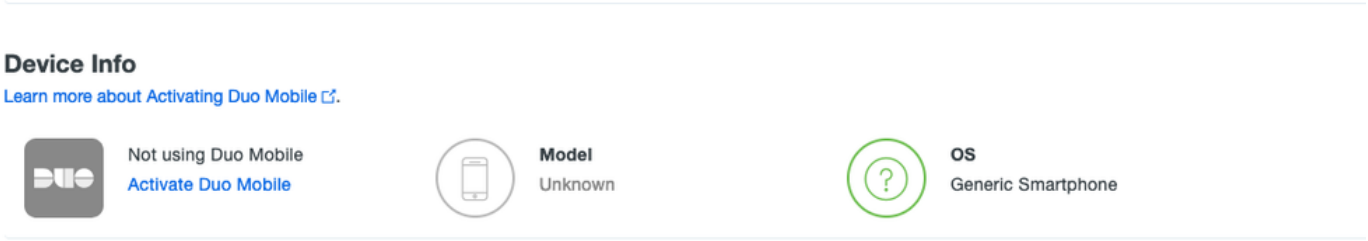
Note: O nome de usuário deve corresponder ao nome de usuário de autenticação principal.

Clique em .Add User Depois de criado, em Phones, clique em Add Phone, digite o número de telefone e clique em Add Phone.



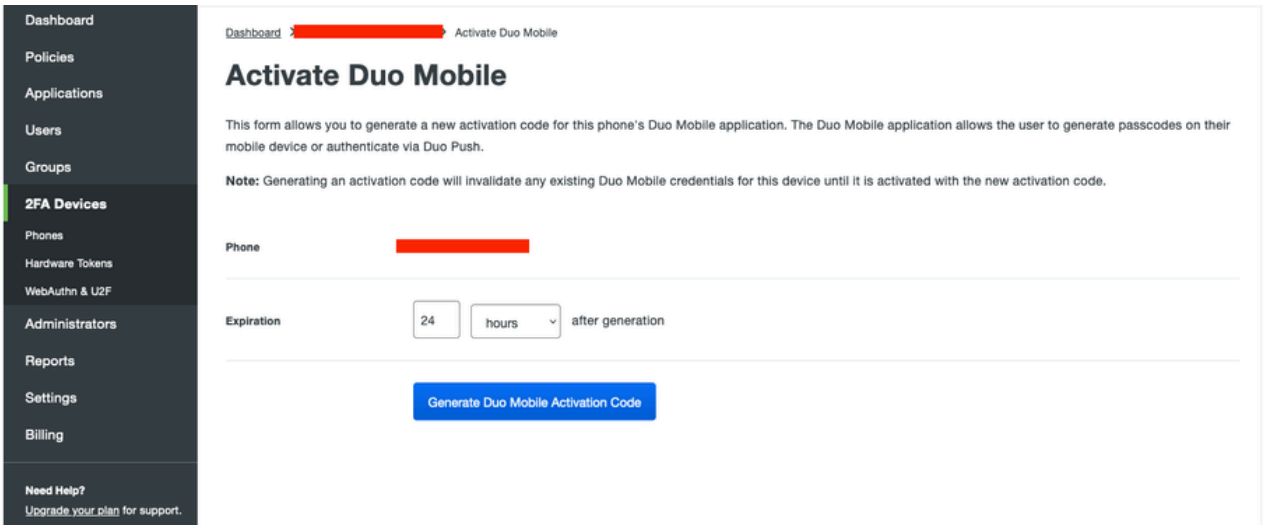
DUO - Adicionar Telefone

Escolha o Tipo de autenticação.



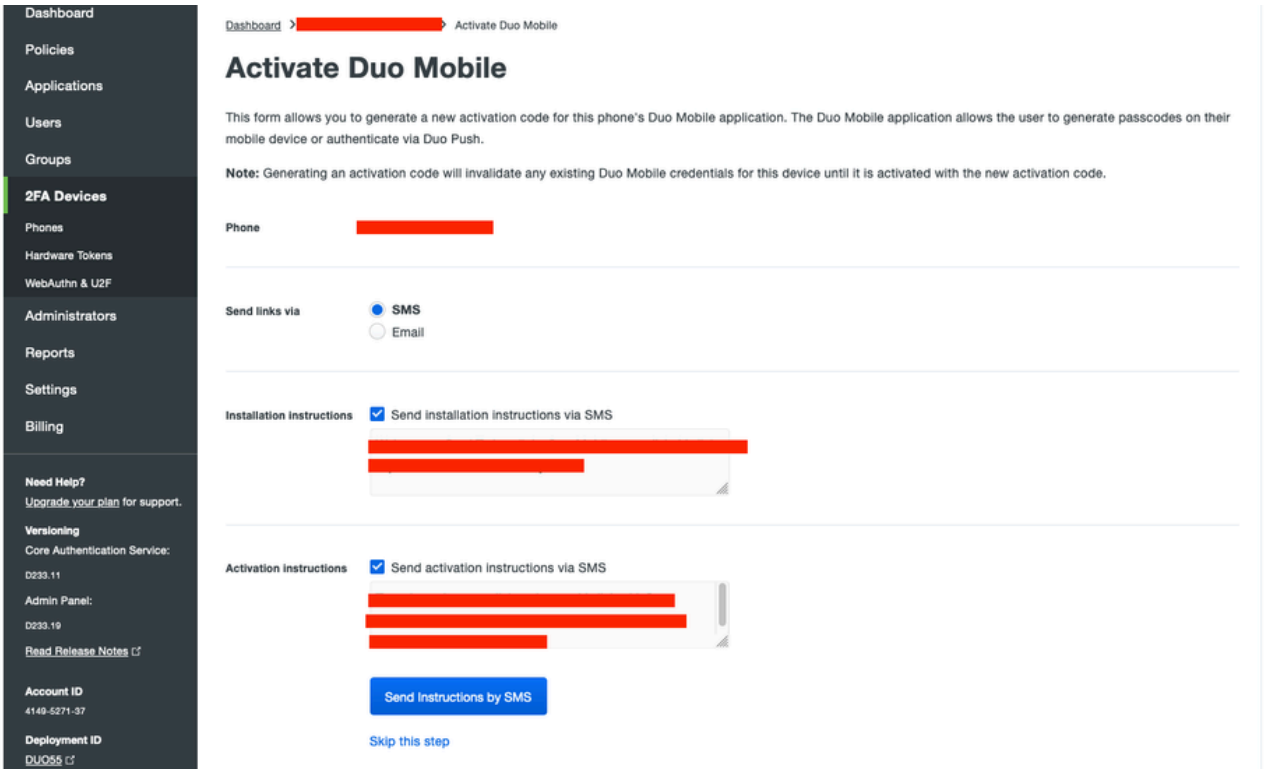
DUO - Informações do Dispositivo

Escolha .Generate Duo Mobile Activation Code



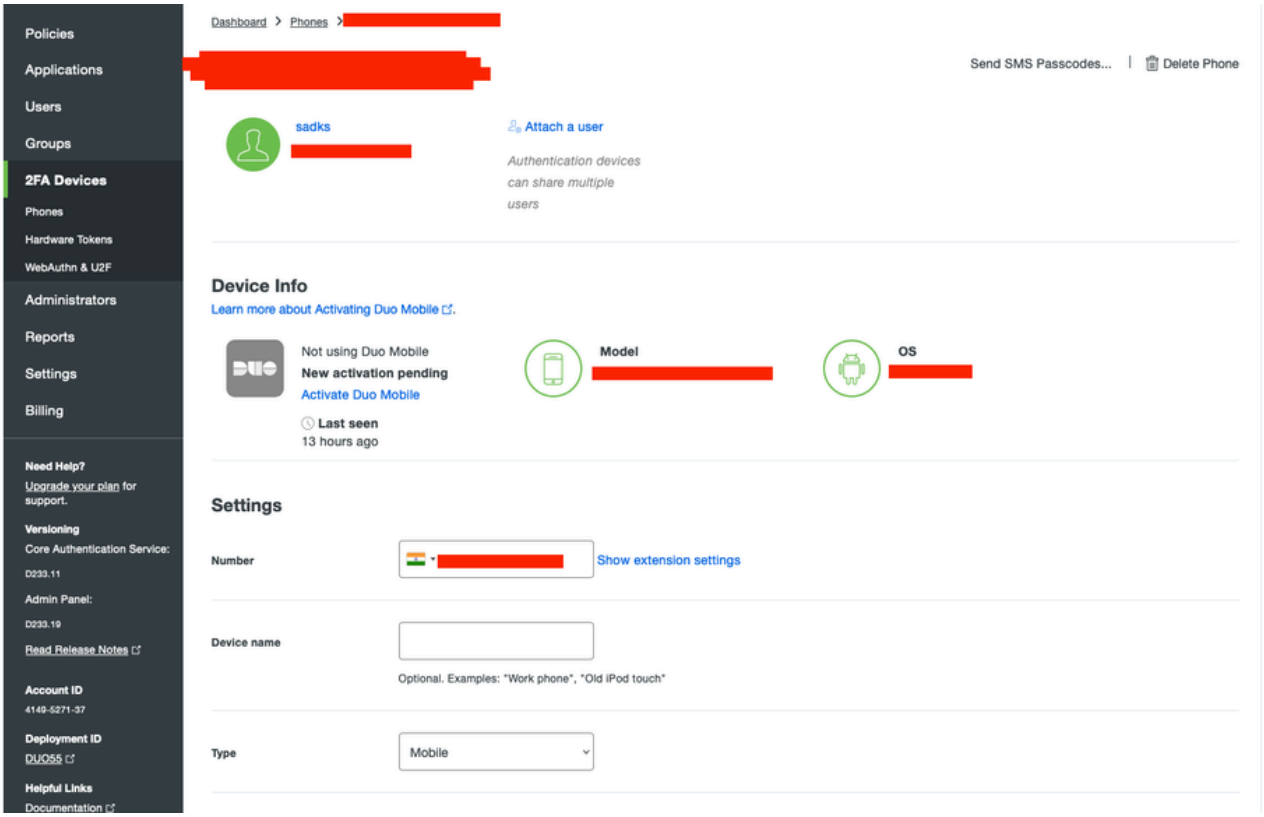
DUO - Ativação por Telefone

Escolha Send Instructions by SMS.



DUO - Enviar SMS

Clique no link enviado para o telefone e o aplicativo DUO será vinculado à conta de usuário na Device Infoseção, como mostrado na imagem:

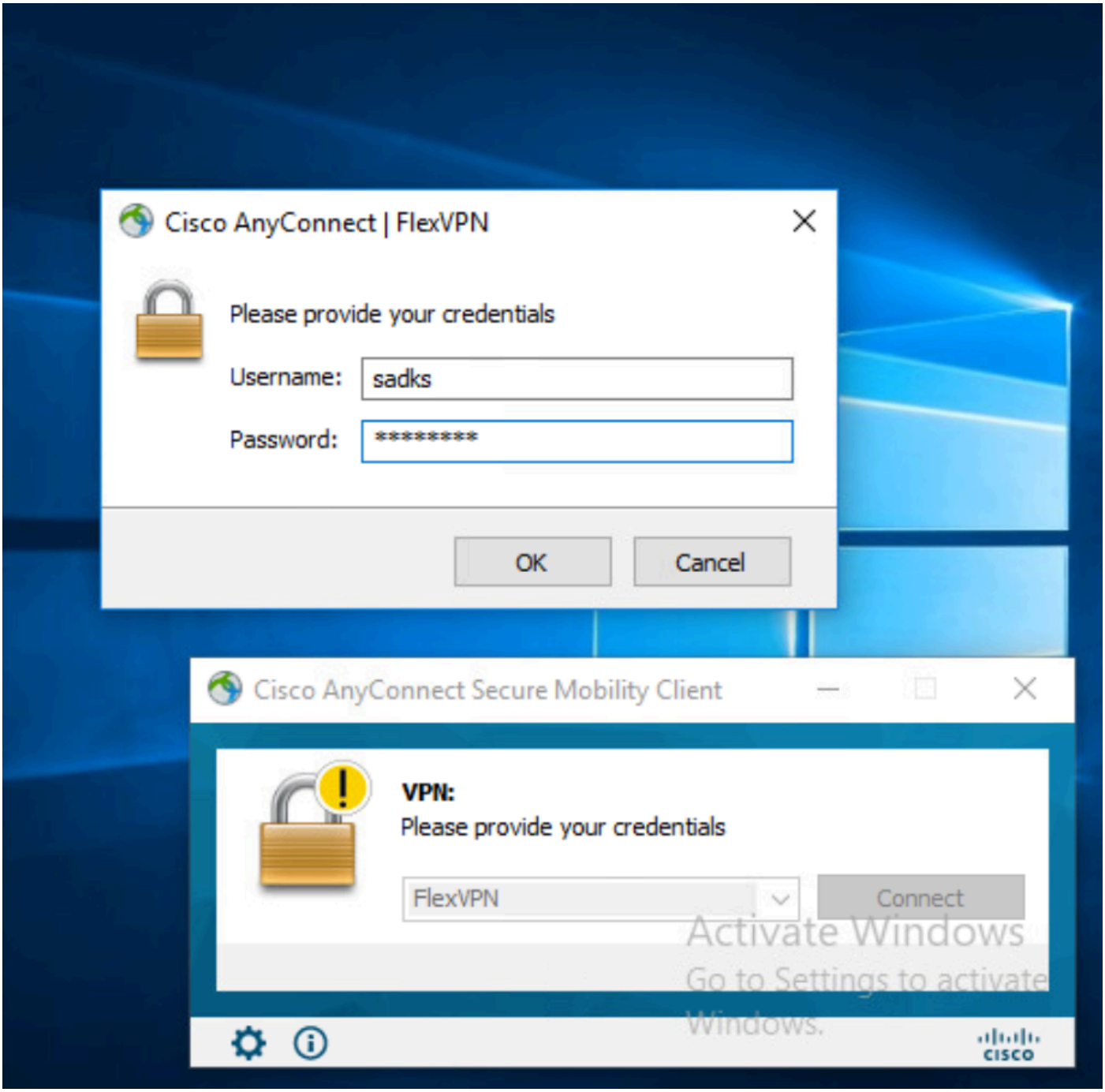


DUO - Vinculado a Dispositivo

Verificar

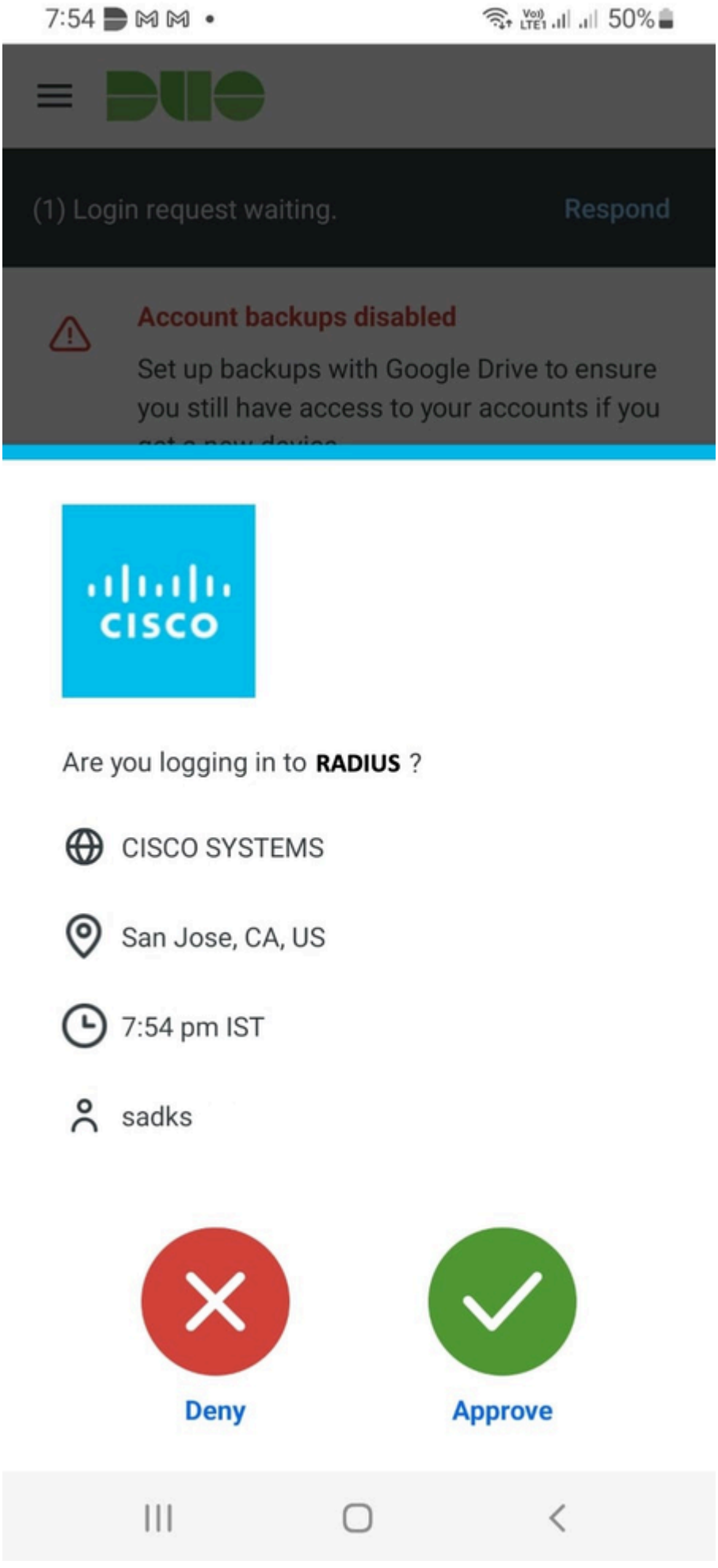
Para testar a autenticação, conecte-se ao C8000V a partir do PC do usuário através do AnyConnect.

Digite o nome de usuário e a senha para a autenticação primária.



Conexão do AnyConnect

Em seguida, aceite os envios DUO no celular.



Push DUO

A conexão é estabelecida

<#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

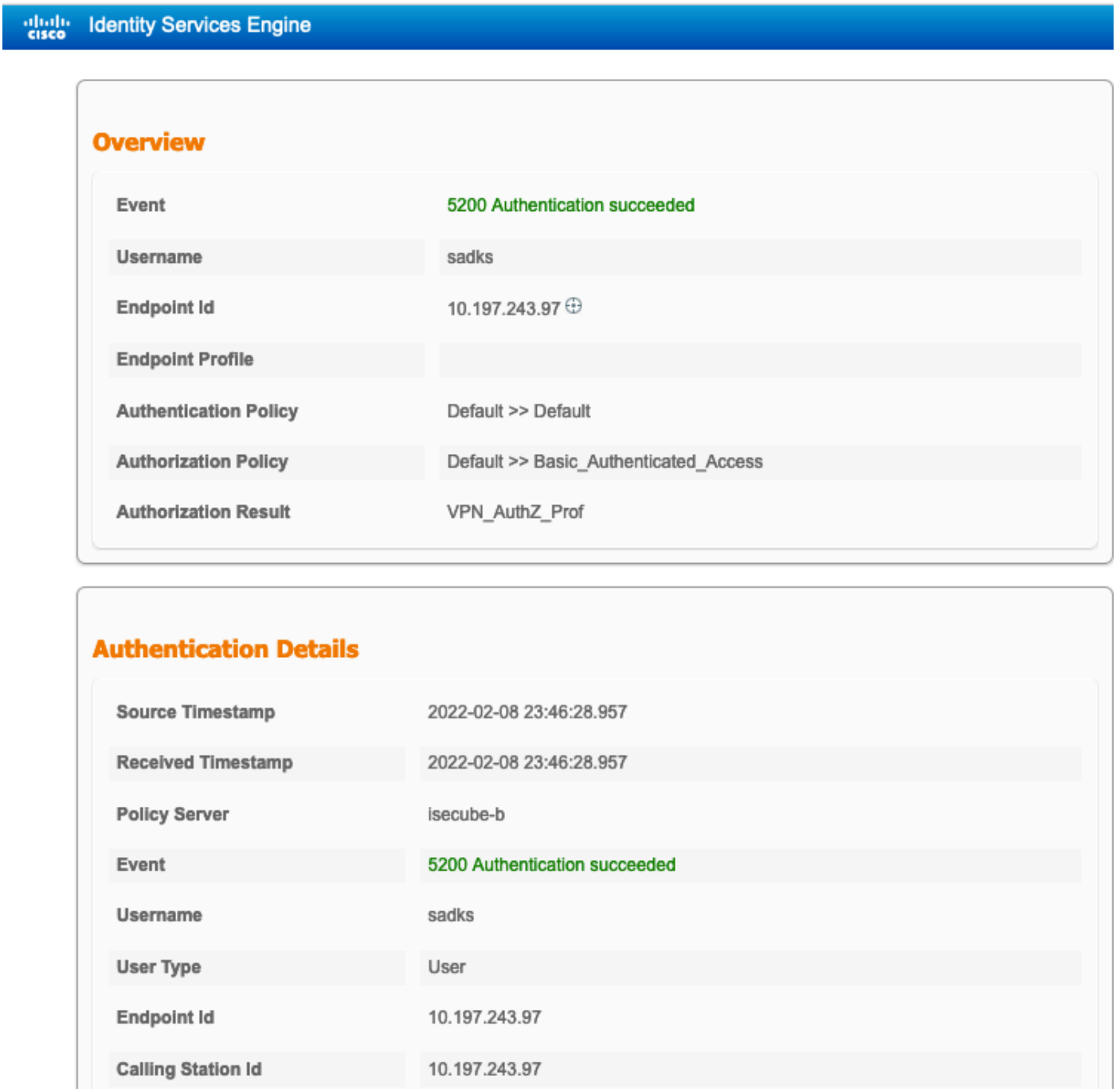
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0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

Navegue atéOperations > Live Logsno ISE. Você pode exibir o relatório de autenticação da autenticação primária.



ISE - Registros ao vivo

4. Verification on DUO authentication proxy

Navegue para este arquivo no Proxy de Autenticação 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
```

Troubleshooting

1. Depurações no 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 o Proxy de Autenticação DUO, verifique os logs relacionados ao proxy do arquivo de log. ()C:\Program Files\Duo Security Authentication Proxy\log

O trecho para um log de erros em que o ISE está rejeitando a autenticação primária é mostrado:

<#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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.