Configurer AnyConnect Flexvpn avec authentification EAP et DUO

Table des matières

Introduction

Ce document décrit comment configurer l'authentification externe à deux facteurs pour une connexion AnyConnect IPSec à un routeur Cisco IOS® XE.

Contribution de Sadhana K S et Rishabh Aggarwal Ingénieurs du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expérience de la configuration VPN RA sur un routeur
- Administration ISE (Identity Services Engine)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Catalyst 8000V (C8000V) version 17.10.01a
- Client Cisco AnyConnect Secure Mobility version 4.10.04071
- Cisco ISE version 3.1.0
- Serveur proxy Duo Authentication (Windows 10 ou tout PC Linux)
- Compte Web Duo
- PC client avec AnyConnect installé

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Flux d'authentification

L'utilisateur AnyConnect s'authentifie avec un nom d'utilisateur et un mot de passe sur le serveur ISE. Le serveur proxy d'authentification duo envoie également une authentification supplémentaire sous la forme d'une notification de transmission à l'appareil mobile de l'utilisateur.

Diagramme De Flux

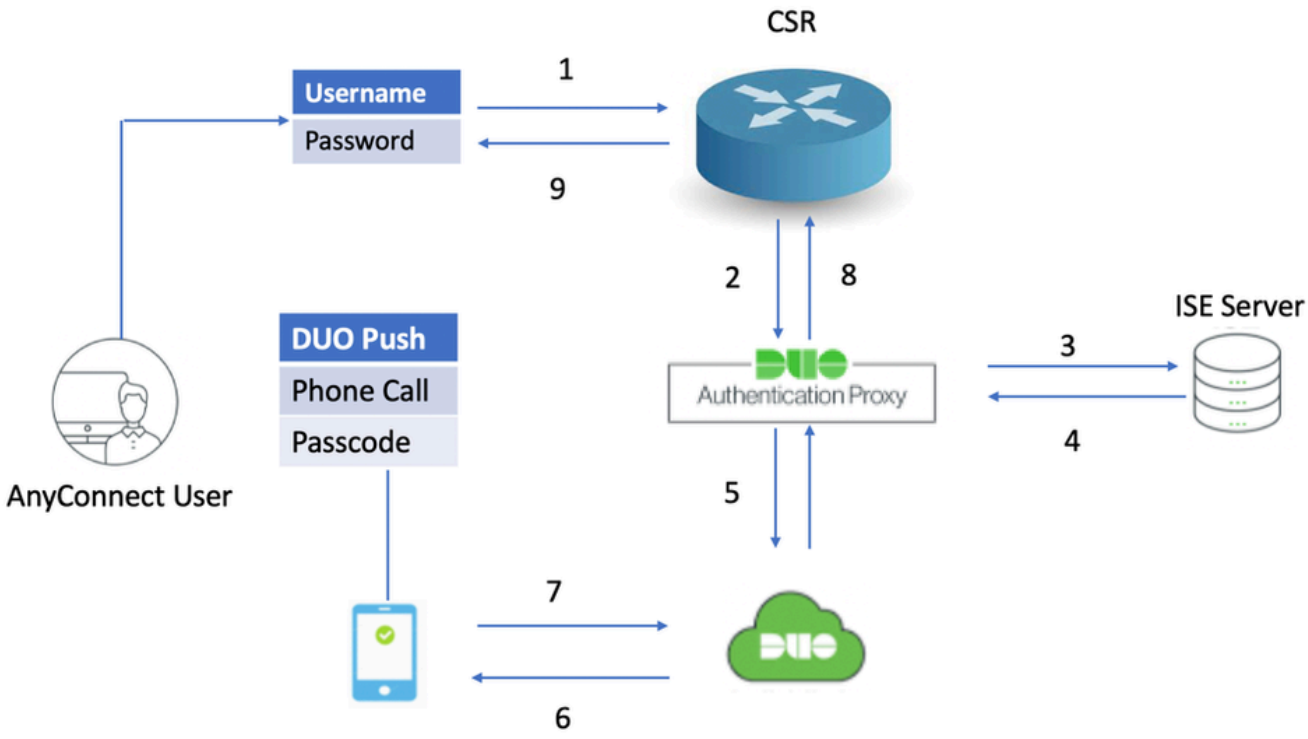


Diagramme de flux d'authentification

Processus de communication

1. L'utilisateur établit une connexion RAVPN au C8000V et fournit un nom d'utilisateur et un mot de passe pour l'authentification principale.
2. Le C8000V envoie une demande d'authentification au proxy d'authentification duo.

3. Duo Authentication Proxy envoie ensuite la requête principale au serveur Active Directory ou RADIUS.
4. La réponse d'authentification est renvoyée au proxy d'authentification.
5. Une fois l'authentification principale réussie, le proxy d'authentification Duo demande une authentification secondaire via le serveur Duo.
6. Le service Duo authentifie ensuite l'utilisateur, selon la méthode d'authentification secondaire (push, appel téléphonique, code secret).
7. Le proxy d'authentification duo reçoit la réponse d'authentification.
8. La réponse est envoyée au C800V.
9. En cas de réussite, la connexion AnyConnect est établie.

Configurer

Afin de compléter la configuration, prenez en considération ces sections.

Étapes de configuration sur C8000V (tête de réseau VPN)

1. Configurer le serveur RADIUS. L'adresse IP du serveur RADIUS doit être celle du proxy d'authentification duo.

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

2. Configurez le serveur RADIUS en tant qu' aaa authentification et l'autorisation en tant que 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. Créez un point de confiance afin d'installer le certificat d'identité, s'il n'est pas déjà présent pour l'authentification locale. Vous pouvez vous référer à Inscription de certificat pour une PKI pour plus de détails sur la création de certificat.

```
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. (Facultatif) Configurez une liste d'accès standard à utiliser pour le tunnel partagé. Cette liste d'accès comprend les réseaux de destination accessibles via le tunnel VPN. Par défaut, tout le trafic passe par le tunnel VPN si le tunnel partagé n'est pas configuré.

```
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. Créez un pool d’adresses IPv4.

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

Le pool d'adresses IP créé attribue une adresse IPv4 au client AnyConnect lors d'une connexion AnyConnect réussie.

6. Configurez une stratégie d’autorisation.

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

Le pool d'adresses IP, le DNS, la liste de split-tunnel, etc. sont spécifiés dans la stratégie d'autorisation.

Remarque : Si la stratégie d'autorisation IKEv2 personnalisée n'est pas configurée, la stratégie d'autorisation par défaut appelée « default » est utilisée pour l'autorisation. Les attributs spécifiés dans la stratégie d'autorisation IKEv2 peuvent également être transmis via le serveur RADIUS.

---

7. Configurez une proposition et une stratégie 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. Téléchargez le profil client AnyConnect sur le bootflash du routeur et définissez le profil comme indiqué :

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

9. Désactivez le serveur sécurisé HTTP.

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

10. Configurez la stratégie SSL et spécifiez l'adresse IP WAN du routeur comme adresse locale pour le téléchargement du profil.

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

          port 443
```

11. Configurez un modèle virtuel à partir duquel l'interface d'accès virtuel intLes surfaces sont clonées

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

La commande non numérotée obtient l'adresse IP de l'interface configurée (GigabitEthernet1).

13. Configurez un profil IKEv2 qui contient tous les paramètres de connexionInformations de lecture.

```
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
```

Ils sont utilisés dans le profil IKEv2 :

- match identity remote any - Se rapporte à l'identité du client. Ici, « any » est configuré pour que tout client disposant des informations d'identification appropriées puisse se connecter
- authentication remote - Mentionne que le protocole EAP doit être utilisé pour l'authentification client
- authentication local - Indique que les certificats doivent être utilisés pour l'authentification locale
- aaa authentication eap - Lors de l'authentification EAP, le serveur RADIUS FlexVPN_auth est utilisé
- aaa authorization group eap list - Pendant l'autorisation, la liste des réseaux FlexVPN_authzest utilisé avec la stratégie d'autorisation ikev2-authz-policy
- aaa authorization user eap cached- Active l'autorisation utilisateur implicite
- virtual-template 20 mode auto - Définit le modèle virtuel à cloner
- anyconnect profile Client_Profile - Le profil client défini à l'étape 8. est appliqué ici à ce profil IKEv2

14. Configurez un jeu de transformation et un profil 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. Ajoutez le profil IPSec au modèle virtuel.

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

Extrait du profil client (profil XML)

Avant Cisco IOS XE 16.9.1, les téléchargements automatiques de profils à partir de la tête de réseau n'étaient pas disponibles. Après 16.9.1, il est possible de télécharger le profil à partir de la tête de réseau.

<#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>
```

Étapes de configuration sur le proxy d'authentification DUO

Remarque : Duo Authentication Proxy prend en charge MS-CHAPv2 uniquement avec l'authentification RADIUS.

Étape 1 : téléchargement et installation du serveur proxy d’authentification duo

Connectez-vous à l'ordinateur Windows et installez le serveur proxy d'authentification Duo.

Il est recommandé d'utiliser un système avec au moins 1 processeur, 200 Mo d'espace disque et 4 Go de RAM.

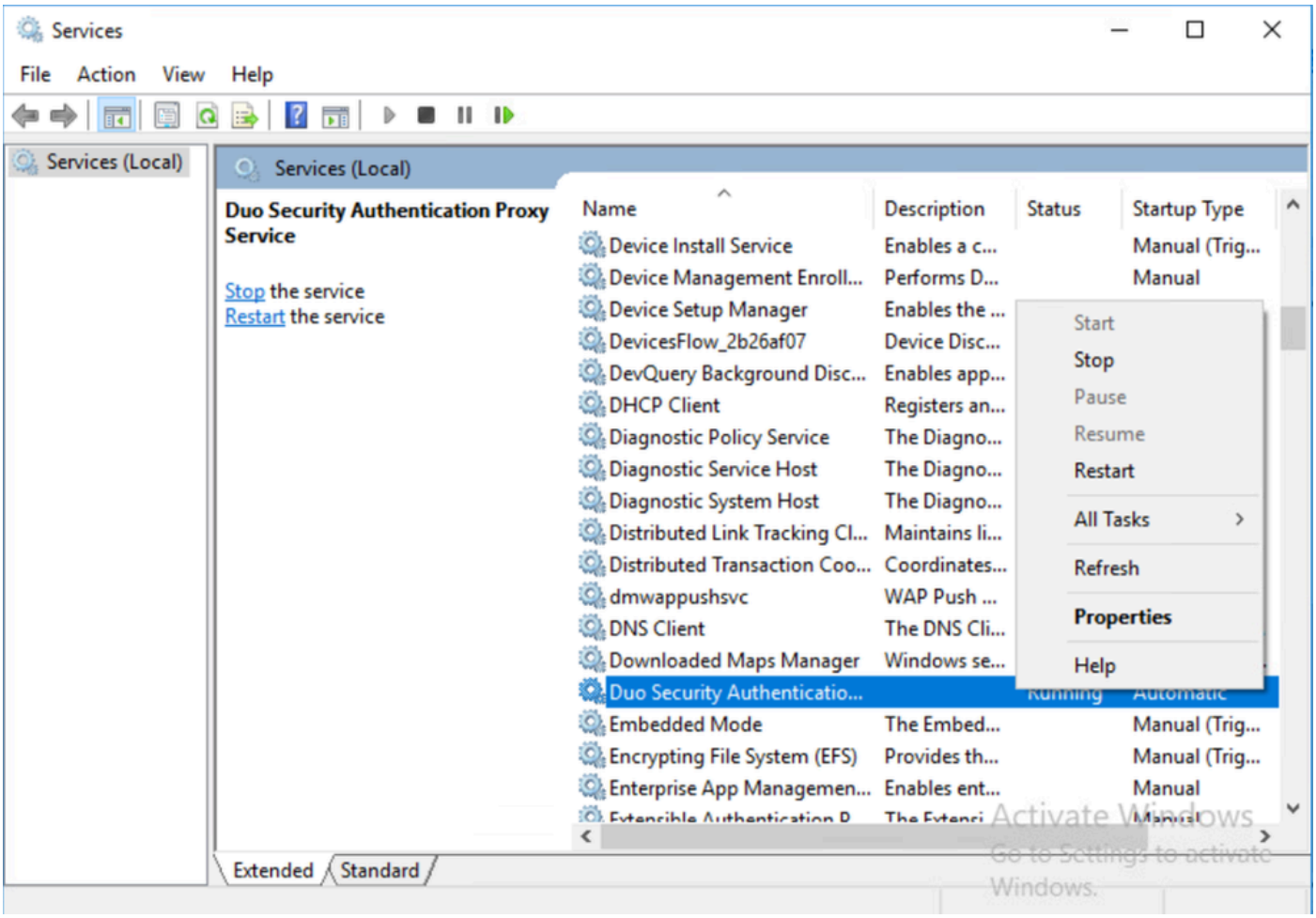
Étape 2. Accédez à et ouvrez C:\Program Files\Duo Security Authentication Proxy\conf\ authproxy.cfg afin de configurer le proxy d'authentification avec les détails appropriés.

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

Remarque : Ici, « 10.197.243.116 » est l'adresse IP du serveur ISE et « cisco » est le mot de passe configuré afin de valider l'authentification principale.

Une fois ces modifications effectuées, enregistrez le fichier.

Étape 3. Ouvrez la console (services.msc) des services Windows. Et redémarrez Duo Security Authentication Proxy Service.

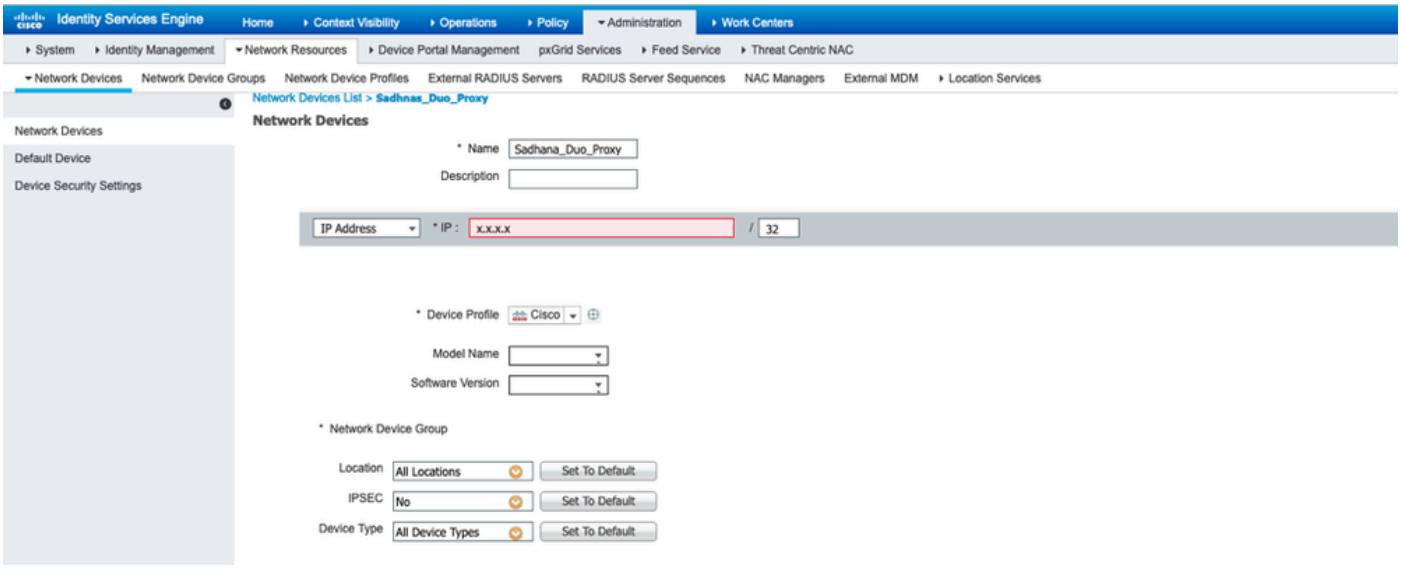


Service proxy d'authentification Duo Security

Étapes de configuration sur ISE

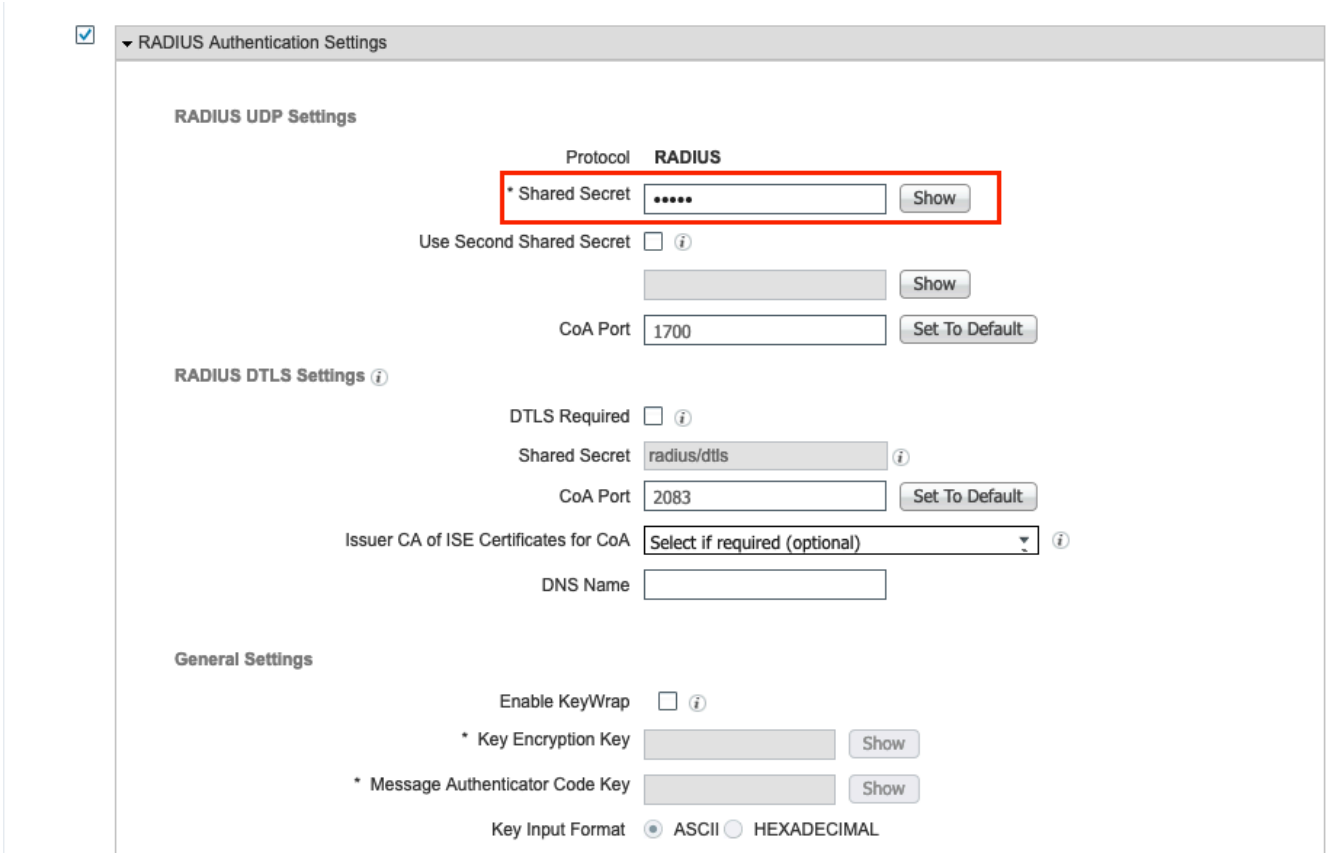
Étape 1 : accédez à **Administration** > **Network Devices**, puis cliquezAddsur afin de configurer le périphérique réseau.

Remarque : Remplacez x.x.x.x par l'adresse IP de votre serveur proxy d'authentification duo.



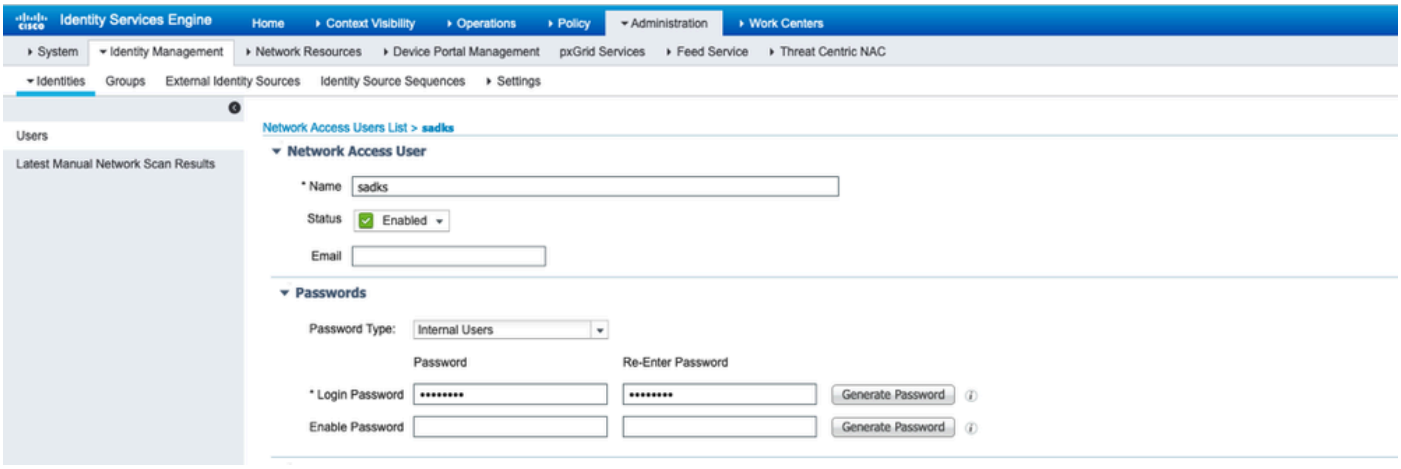
ISE - Périphériques réseau

Étape 2. Configurez le Shared Secretcomme indiqué dans la authproxy.cfgde la section secret:



ISE - Secret partagé

Étape 3. Accédez à Administration > Identities > Users.Choisissez Addafin de configurer l'utilisateur Identity pour l'authentification principale AnyConnect :

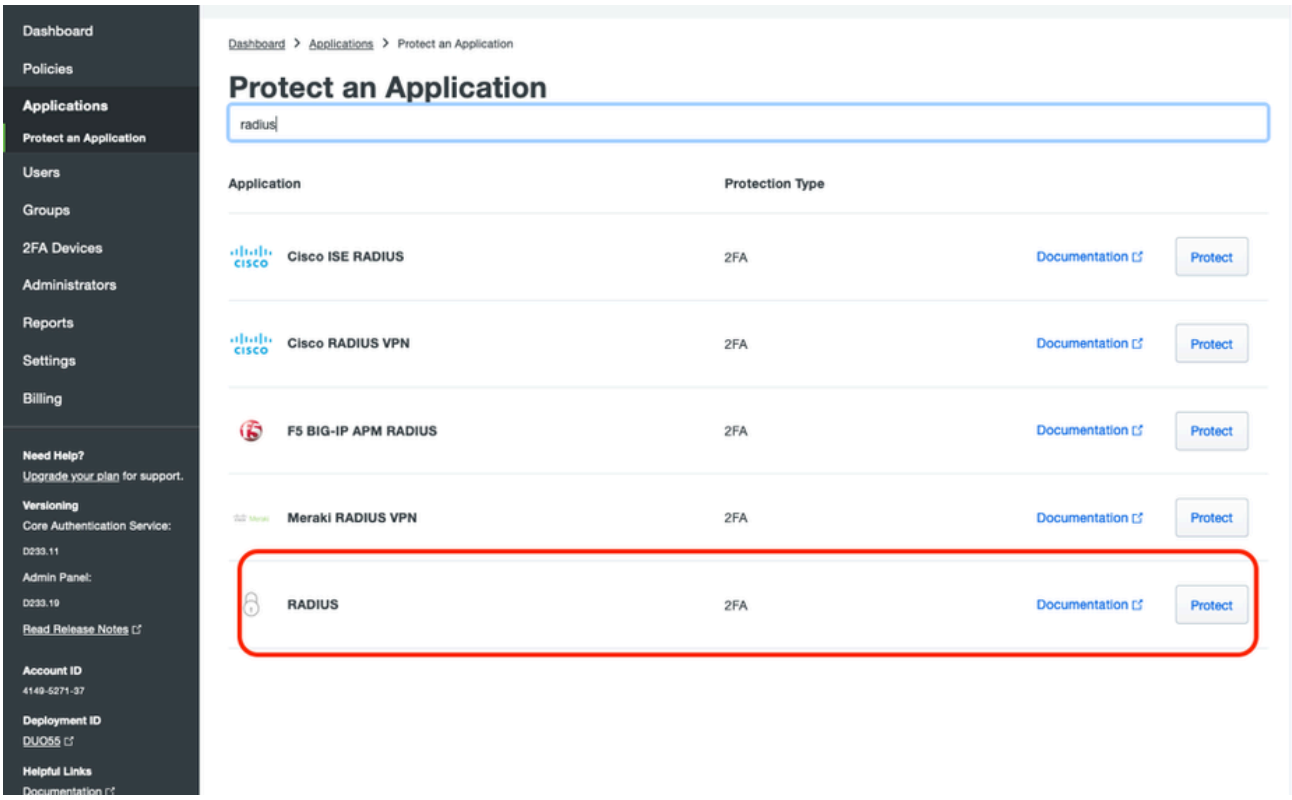


ISE - Utilisateurs

Étapes de configuration sur le portail DUO Administration

Étape 1. Connectez-vous à votre compte Duo.

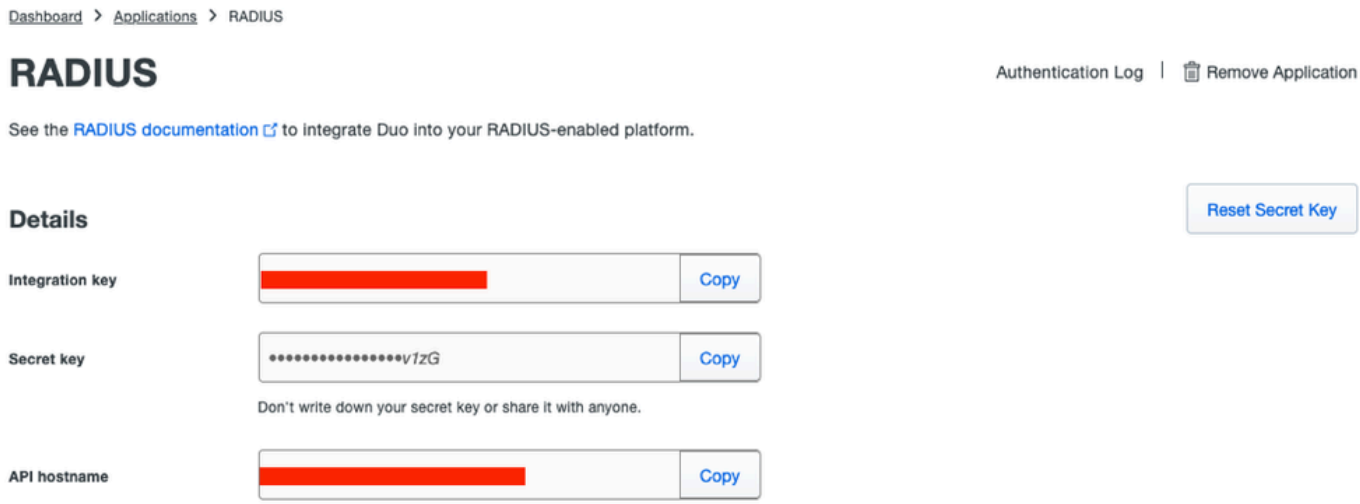
Accédez àApplications > Protect an Application. Cliquez sur Protect l'application que vous souhaitez utiliser. (RADIUS dans ce cas)



DUO - Application

Étape 2. Cliquez sur Protect pour l'application que vous souhaitez utiliser. (RADIUS dans ce cas)

Copiez la clé d'intégration, la clé secrète et le nom d'hôte de l'API et collez-les sur le authproxy.cfgserveur proxy Duo Authentication.



DUO - RADIUS

Copiez ces valeurs et revenez au proxy d'authentification DUO et ouvrez le authproxy.cfget collez les valeurs comme indiqué :

Clé d'intégration = ikey

clé secrète = skey

Nom d'hôte 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
```

Remarque : ikey, skey et api_host doivent être copiés à partir du serveur Duo lorsque vous configurez le serveur, et « 10.106.54.143 » est l'adresse IP du routeur C8000V, et « cisco » est la clé configurée sur le routeur sous la configuration du serveur RADIUS.

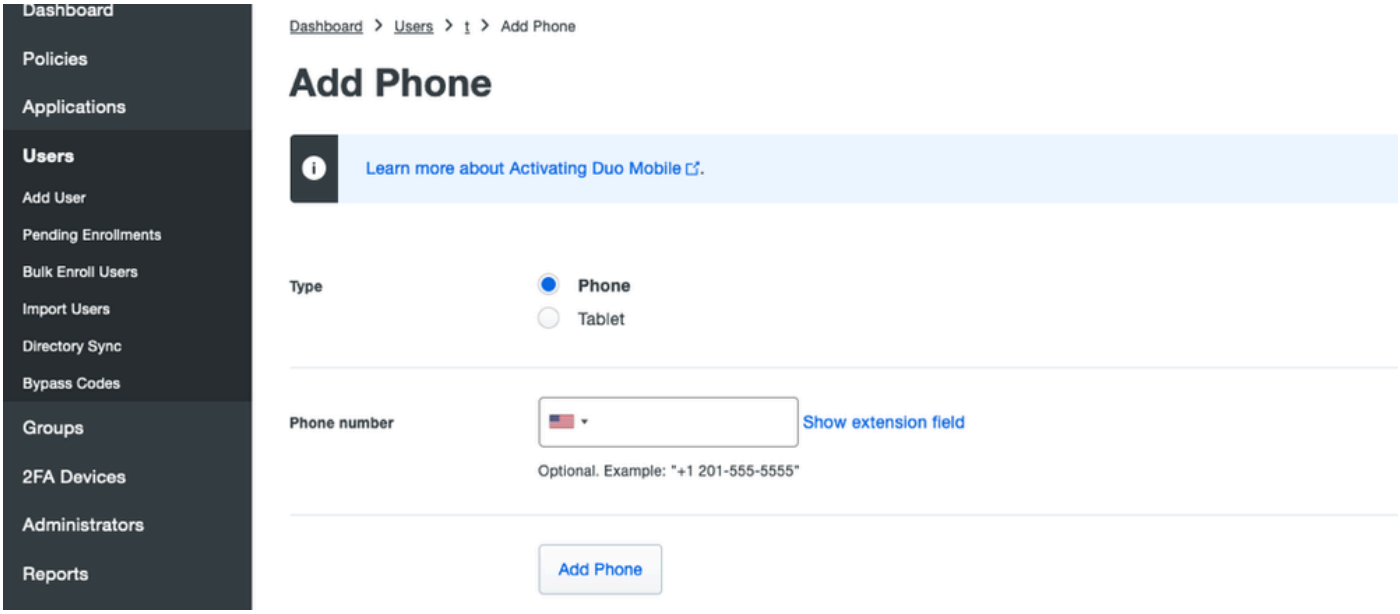
Une fois ces modifications effectuées, enregistrez à nouveau le fichier et redémarrez le service proxy d'authentification de sécurité duo (dans services.msc).

Étape 3 : création d'utilisateurs sur DUO pour l'authentification secondaire

Accédez au nom d'utilisateurUsers > Add Useret saisissez-le.

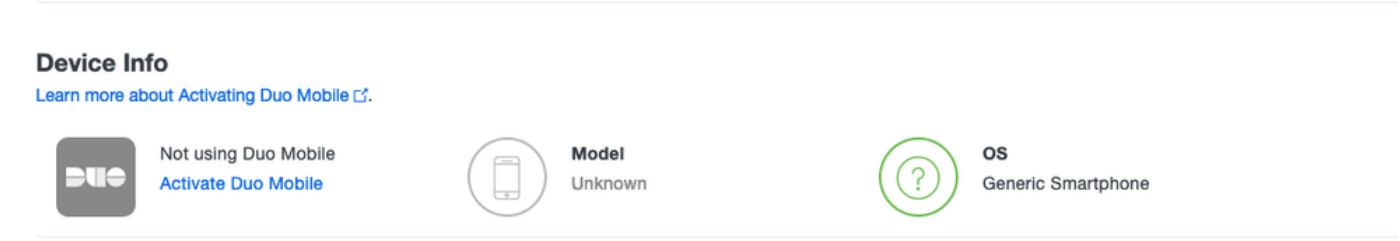
Remarque : Le nom d'utilisateur doit correspondre au nom d'utilisateur de l'authentification principale.

Cliquez sur Add User. Une fois créé, sous Phones, cliquez sur Add Phone, entrez le numéro de téléphone, puis cliquez sur Add Phone.



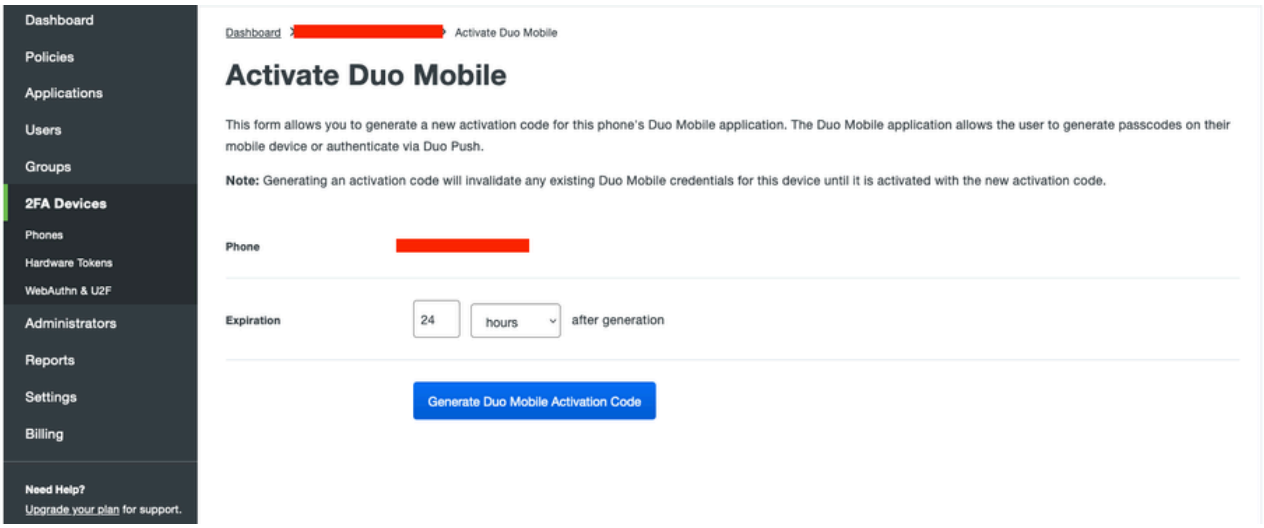
DUO - Ajouter un téléphone

Sélectionnez le type d'authentification.



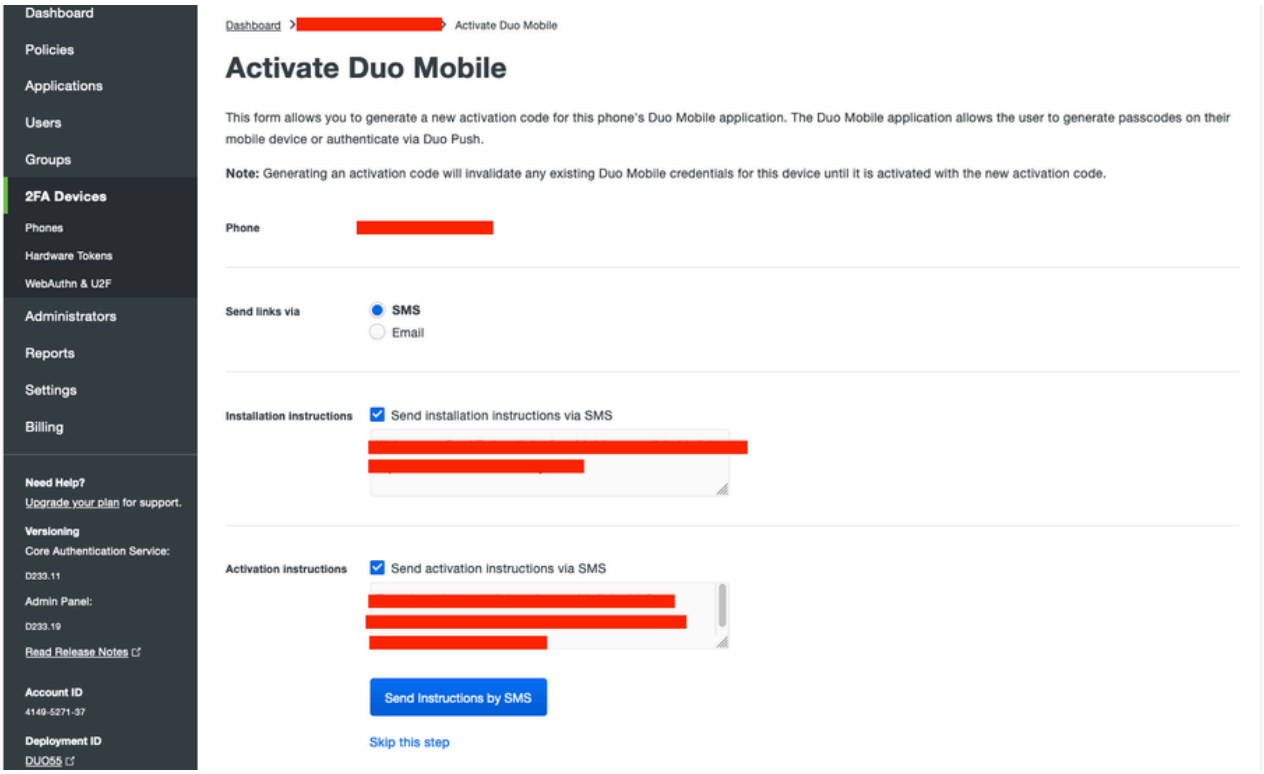
DUO - Informations sur le périphérique

Choisissez Generate Duo Mobile Activation Code.



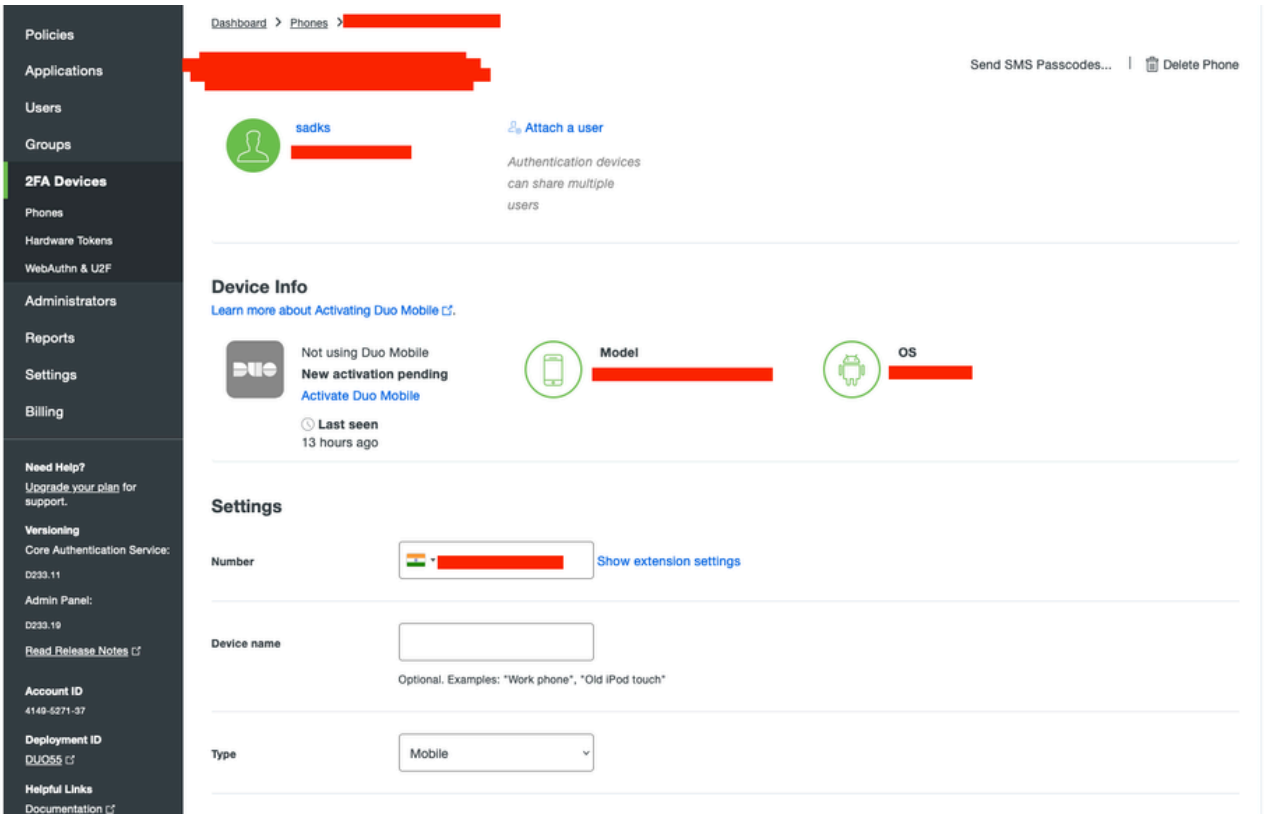
DUO - Activation du téléphone

Choisir Send Instructions by SMS.



DUO - Envoyer des SMS

Cliquez sur le lien envoyé au téléphone et l'application DUO est liée au compte d'utilisateur dans la section, Device Infocomme le montre l'image :

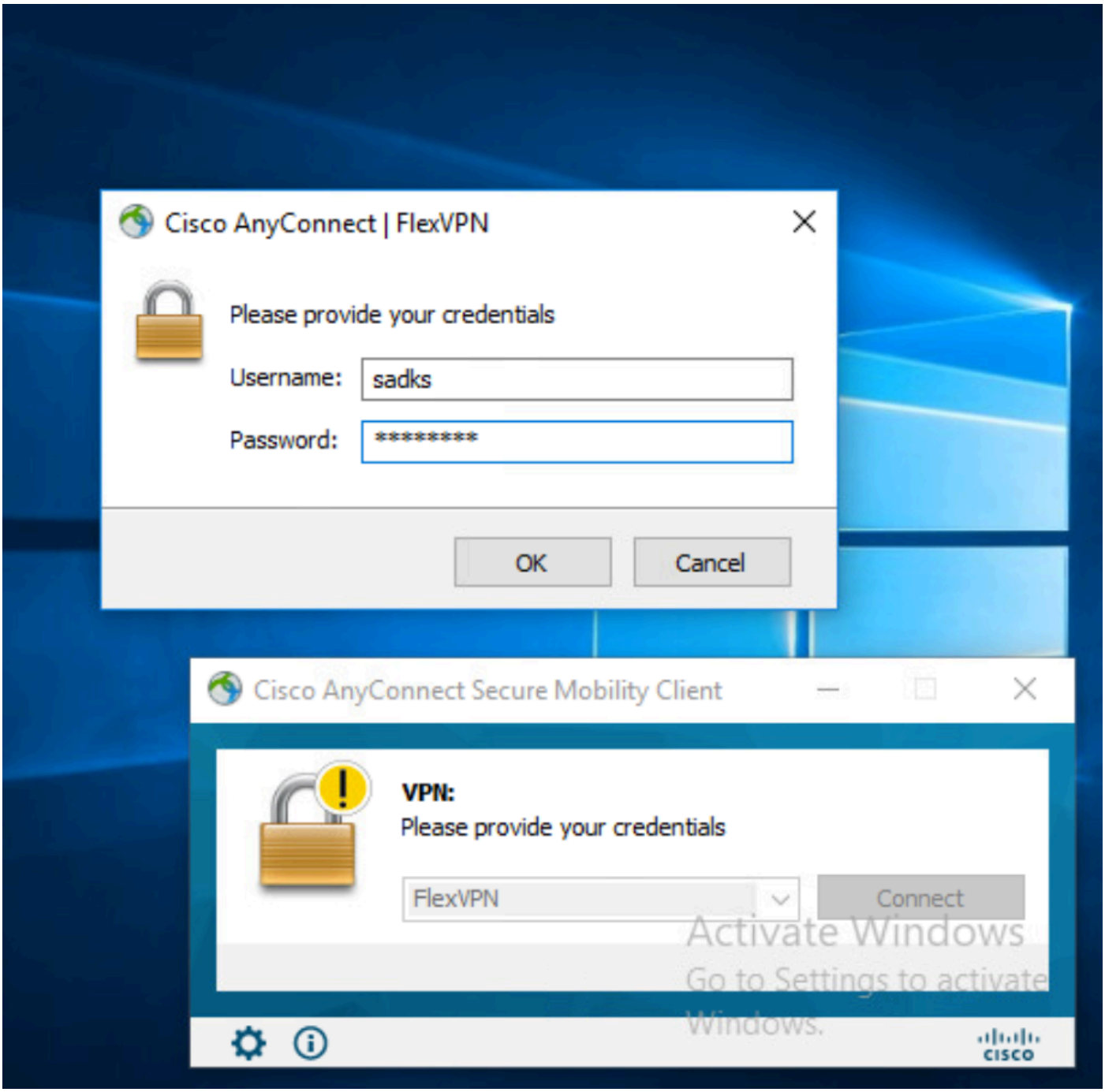


DUO - Périphérique lié

Vérifier

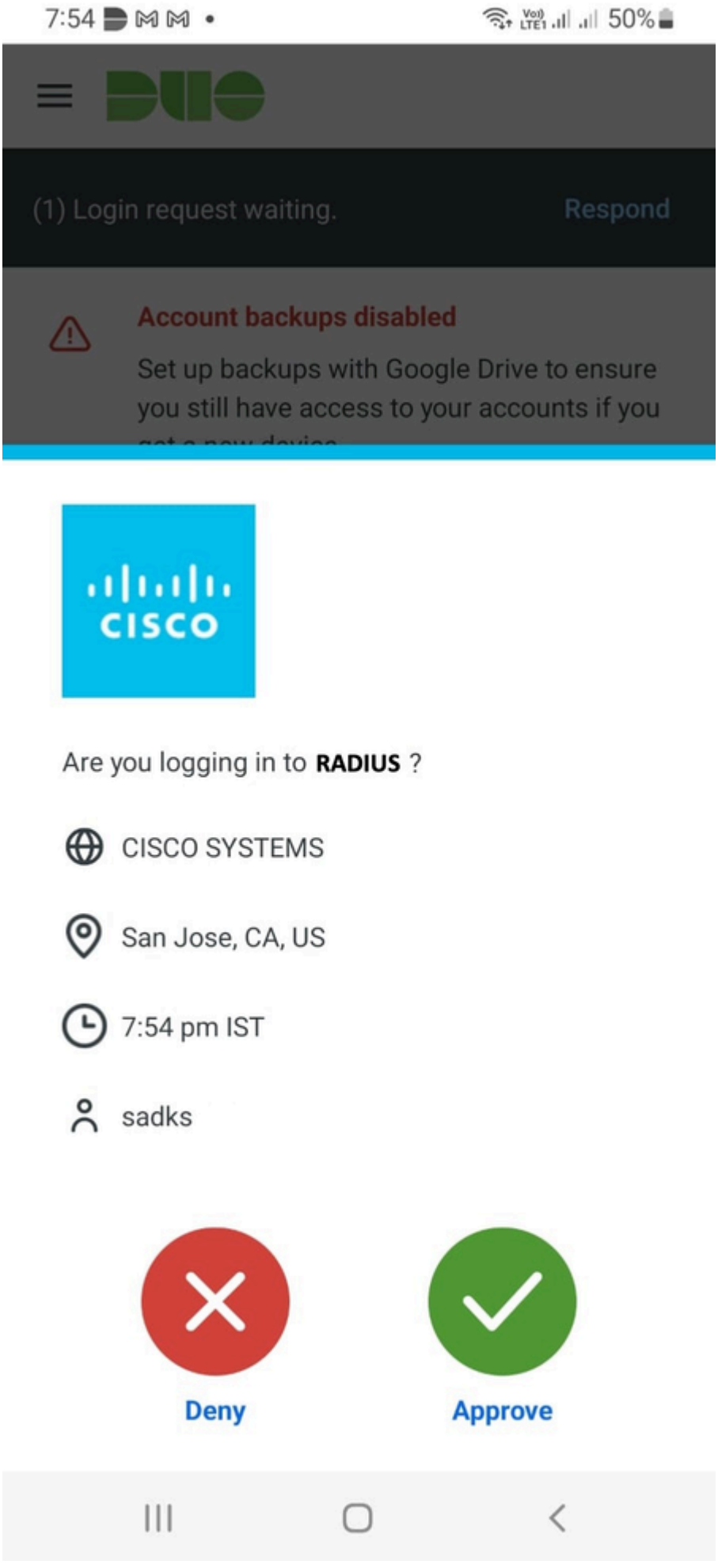
Afin de tester l'authentification, connectez-vous au C8000V à partir du PC de l'utilisateur via AnyConnect.

Saisissez le nom d'utilisateur et le mot de passe de l'authentification principale.



Connexion AnyConnect

Ensuite, acceptez les poussées DUO sur le mobile.


7:54
50%
(1) Login request waiting.
Respond
Account backups disabled
Set up backups with Google Drive to ensure you still have access to your accounts if you
CISCO
Are you logging in to RADIUS ?
CISCO SYSTEMS
San Jose, CA, US
7:54 pm IST
sadks
Deny
Approve

Push DUO

<#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

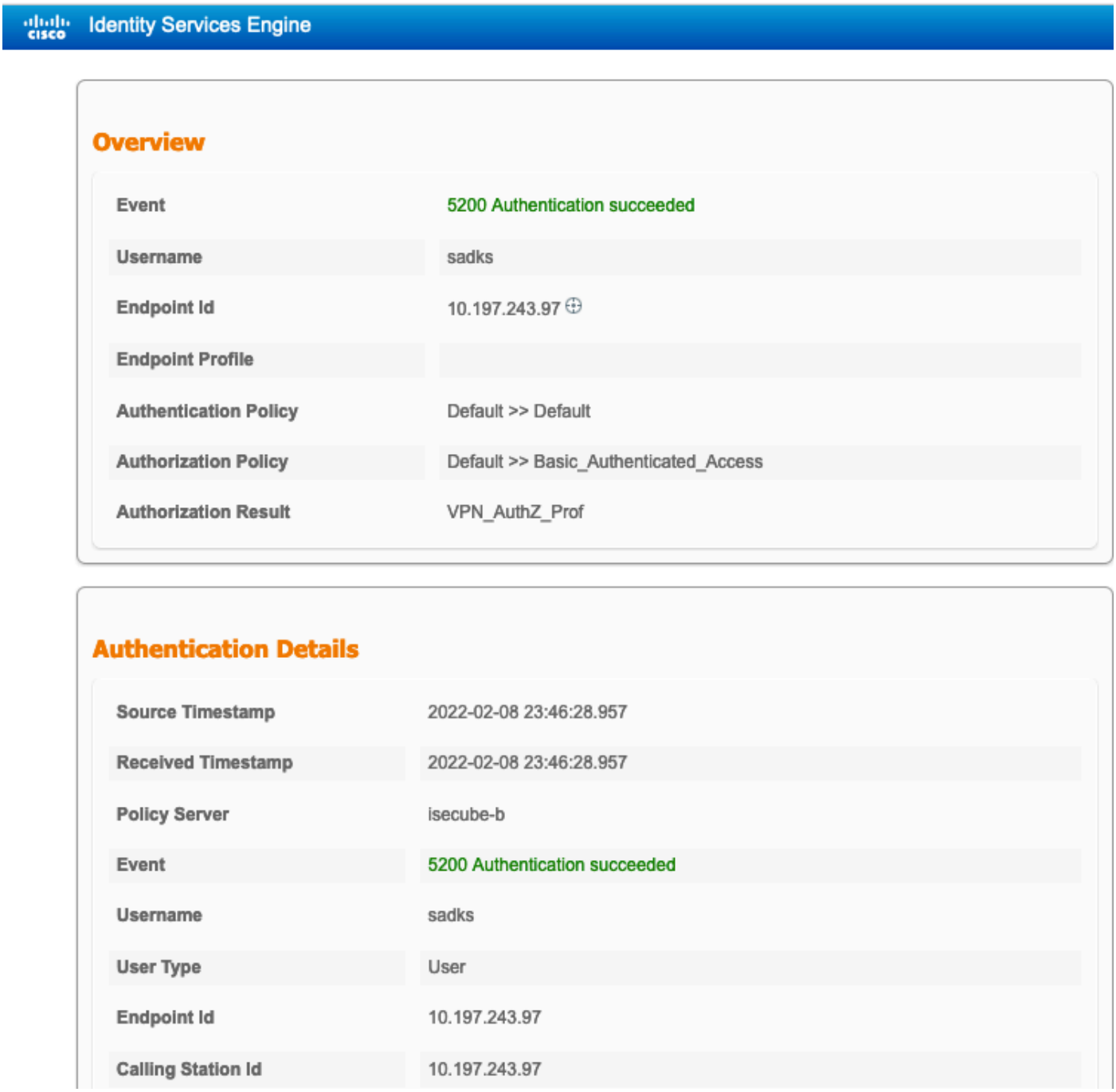
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0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

Accédez à dansOperations > Live LogsISE. Vous pouvez afficher le rapport d'authentification pour l'authentification principale.



ISE - Journaux en direct

4. Verification on DUO authentication proxy

Accédez à ce fichier sur le proxy d'authentification 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 ('10.106.5
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 <_D
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 <_D
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <_D
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 <_D
```

Dépannage

1. Débogages sur C8000V.

Pour IKEv2 :

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

Pour IPSec :

- debug crypto ipsec
- debug crypto ipsec error

2. Pour le proxy d'authentification DUO, vérifiez le fichier journal relatif au proxy. ()C:\Program Files\Duo Security Authentication Proxy\log

L'extrait de journal d'erreurs où ISE rejette l'authentification principale s'affiche :

<#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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.