Konfigurieren von AnyConnect FlexVPN mit EAP- und DUO-Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der externen Zwei-Faktor-Authentifizierung für AnyConnect IPSec-Verbindungen mit einem Cisco IOS® XE-Router beschrieben.

Beitrag von Sadhana K S und Rishabh Aggarwal Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Erfahrung mit der RA VPN-Konfiguration auf einem Router
- Identity Services Engine (ISE)-Administration

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst 8000V (C8000V) mit Version 17.10.01a

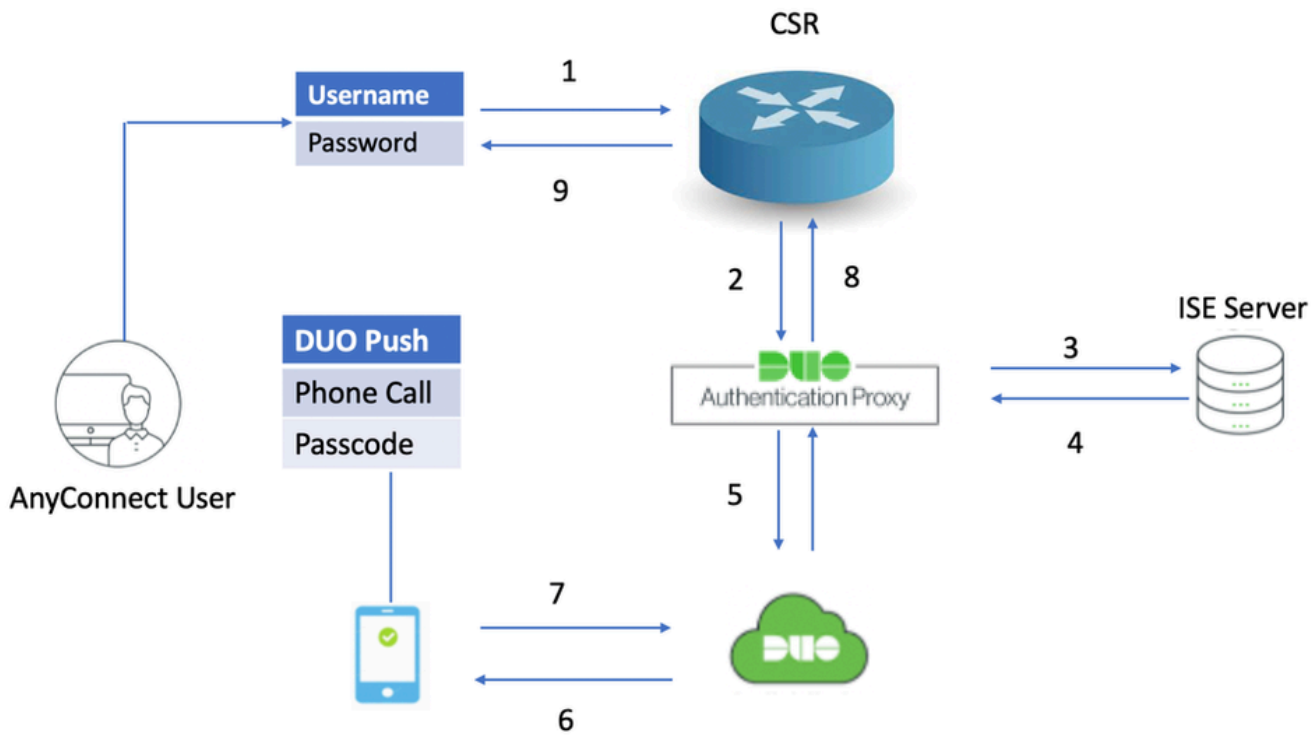
- Cisco AnyConnect Secure Mobility Client Version 4.10.04071
- Cisco ISE mit Version 3.1.0
- Duo Authentifizierungsproxyserver (Windows 10 oder ein beliebiger Linux-PC)
- Duo Webkonto
- Client-PC mit installiertem AnyConnect

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Authentifizierungsablauf

AnyConnect-Benutzer authentifiziert sich mit einem Benutzernamen und einem Kennwort auf dem ISE-Server. Der Duo Authentication Proxy-Server sendet außerdem eine zusätzliche Authentifizierung in Form einer Push-Benachrichtigung an das Mobilgerät des Benutzers.

Flussdiagramm



Authentifizierungs-Flussdiagramm

Kommunikationsprozess

1. Der Benutzer stellt eine RAVPN-Verbindung mit dem C8000V her und gibt einen Benutzernamen und ein Kennwort für die primäre Authentifizierung ein.
2. Der C8000V sendet eine Authentifizierungsanforderung an den Duo-Authentifizierungsproxy.

3. Der Duo-Authentifizierungsproxy sendet dann die primäre Anforderung an den Active Directory- oder RADIUS-Server.
4. Die Authentifizierungsantwort wird an den Authentifizierungsproxy zurückgesendet.
5. Sobald die primäre Authentifizierung erfolgreich ist, fordert der Duo Authentifizierungsproxy eine sekundäre Authentifizierung über den Duo Server an.
6. Der Duo-Dienst authentifiziert dann den Benutzer, abhängig von der sekundären Authentifizierungsmethode (Push, Telefonanruf, Passcode).
7. Der Duo-Authentifizierungsproxy empfängt die Authentifizierungsantwort.
8. Die Antwort wird an den C8000V gesendet.
9. Bei Erfolg wird die AnyConnect-Verbindung hergestellt.

Konfigurieren

Berücksichtigen Sie diese Abschnitte, um die Konfiguration abzuschließen.

Konfigurationsschritte auf dem C8000V (VPN-Headend)

1. Konfigurieren des RADIUS-Servers Die IP-Adresse des RADIUS-Servers muss die IP-Adresse des Duo-Authentifizierungsproxys sein.

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

2. Konfigurieren Sie den RADIUS-Server als aaa Authentifizierung und die Autorisierung als lokal.

```
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. Erstellen Sie einen Vertrauenspunkt, um das Identitätszertifikat zu installieren, falls es nicht bereits für die lokale Authentifizierung vorhanden ist. Weitere Informationen zur Zertifikatserstellung finden Sie unter Zertifikatregistrierung für eine PKI.

```
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. (Optional) Konfigurieren Sie eine Standard-Zugriffsliste für den Split-Tunnel. Diese Zugriffsliste besteht aus den Zielnetzwerken, auf die über den VPN-Tunnel zugegriffen werden kann. Standardmäßig durchläuft der gesamte Datenverkehr den VPN-Tunnel, wenn der Split-Tunnel nicht konfiguriert ist.

```
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. Erstellen Sie einen IPv4-Adresspool.

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

Der erstellte IP-Adresspool weist dem AnyConnect-Client während einer erfolgreichen AnyConnect-Verbindung eine IPv4-Adresse zu.

6. Konfigurieren einer Autorisierungsrichtlinie

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

Der IP-Pool, DNS, die Split-Tunnel-Liste usw. werden unter der Autorisierungsrichtlinie angegeben.

Anmerkung: Wenn die benutzerdefinierte IKEv2-Autorisierungsrichtlinie nicht konfiguriert ist, wird die Standardautorisierungsrichtlinie mit dem Namen "default" für die Autorisierung verwendet. Die in der IKEv2-Autorisierungsrichtlinie angegebenen Attribute können auch über den RADIUS-Server übertragen werden.

---

7. Konfigurieren Sie einen IKEv2-Vorschlag und eine IKEv2-Richtlinie.

```
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. Laden Sie das AnyConnect-Clientprofil in den Bootflash des Routers hoch, und definieren Sie das Profil wie folgt:

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

9. Deaktivieren des sicheren HTTP-Servers.

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

10. Konfigurieren Sie die SSL-Richtlinie, und geben Sie die WAN-IP-Adresse des Routers als lokale Adresse für den Download des Profils an.

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

           port 443
```

11. Konfigurieren Sie eine virtuelle Vorlage, von der aus der virtuelle Zugriff intOberflächen werden geklont

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

Der Befehl unnumbered (nicht nummerierte) ruft die IP-Adresse von der konfigurierten Schnittstelle ab (GigabitEthernet1).

13. Konfigurieren Sie ein IKEv2-Profil, das alle verbindungsbezogenenInformationen.

```
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
```

Diese werden im IKEv2-Profil verwendet:

- match identity remote any - Bezieht sich auf die Identität des Clients. Hier ist "any" konfiguriert, sodass jeder Client mit den richtigen Anmeldeinformationen eine Verbindung herstellen kann.
- authentication remote - Gibt an, dass das EAP-Protokoll für die Client-Authentifizierung verwendet werden muss
- authentication local - Gibt an, dass Zertifikate für die lokale Authentifizierung verwendet werden müssen.
- aaa authentication eap - Bei der EAP-Authentifizierung wird der RADIUS-Server FlexVPN_auth verwendet.
- aaa authorization group eap list - Während der Autorisierung wird die Netzliste FlexVPN_authzwird zusammen mit der Autorisierungsrichtlinie verwendet ikev2-authz-policy
- aaa authorization user eap cached- Ermöglicht implizite Benutzerautorisierung
- virtual-template 20 mode auto - Definiert die zu klonende virtuelle Vorlage.
- anyconnect profile Client_Profile - Das in Schritt 8 definierte Client-Profil wird hier auf dieses IKEv2-Profil angewendet.

14. Konfigurieren eines Transformationssatzes und eines IPSec-Profils

```
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. Fügen Sie das IPSec-Profil zur virtuellen Vorlage hinzu.

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

Ausschnitt des Clientprofils (XML-Profil)

Vor Cisco IOS XE 16.9.1 ist kein automatischer Profildownload vom Headend möglich. Nach 16.9.1 kann das Profil vom Headend heruntergeladen werden.

<#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>
```

Konfigurationsschritte auf dem DUO-Authentifizierungsproxy

Anmerkung: Der Duo Authentifizierungsproxy unterstützt MS-CHAPv2 nur mit RADIUS-Authentifizierung.

Schritt 1. Laden Sie den Duo Authentication Proxy Server herunter, und installieren Sie ihn.

Melden Sie sich beim Windows-Computer an, und installieren Sie den Duo Authentication Proxy-Server.

Es wird empfohlen, ein System mit mindestens 1 CPU, 200 MB Festplattenspeicher und 4 GB RAM zu verwenden.

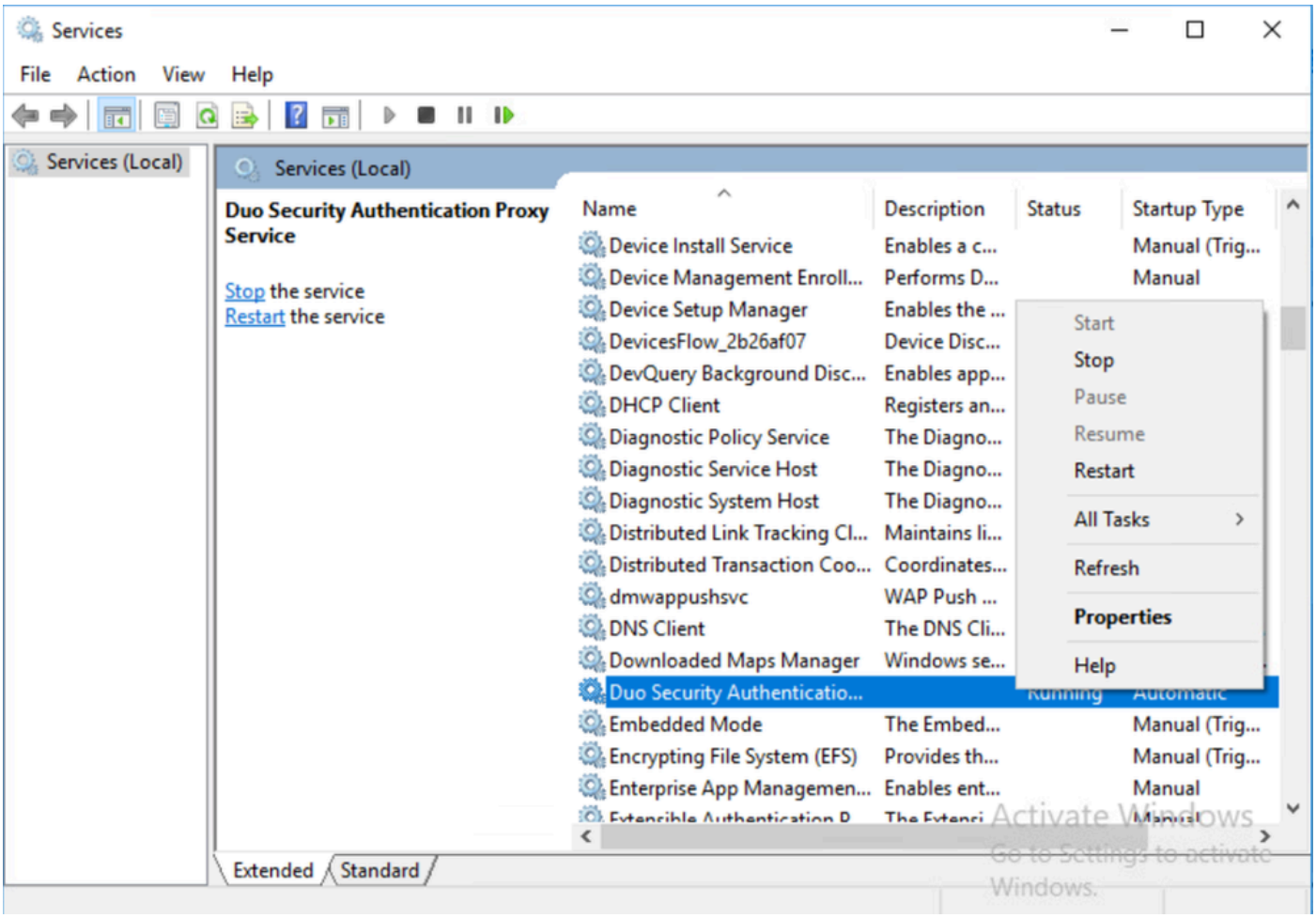
Schritt 2: Navigieren Sie zu C:\Program Files\Duo Security Authentication Proxy\conf\, und öffnen Sie authproxy.cfg , um den Authentifizierungsproxy mit den entsprechenden Details zu konfigurieren.

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

Anmerkung: Hier ist "10.197.243.116" die IP-Adresse des ISE-Servers, und "cisco" ist das Kennwort, das zur Validierung der primären Authentifizierung konfiguriert wurde.

Speichern Sie die Datei, nachdem Sie diese Änderungen vorgenommen haben.

Schritt 3: Öffnen Sie die Windows-Konsole (services.msc). und starten Sie neu Duo Security Authentication Proxy Service.

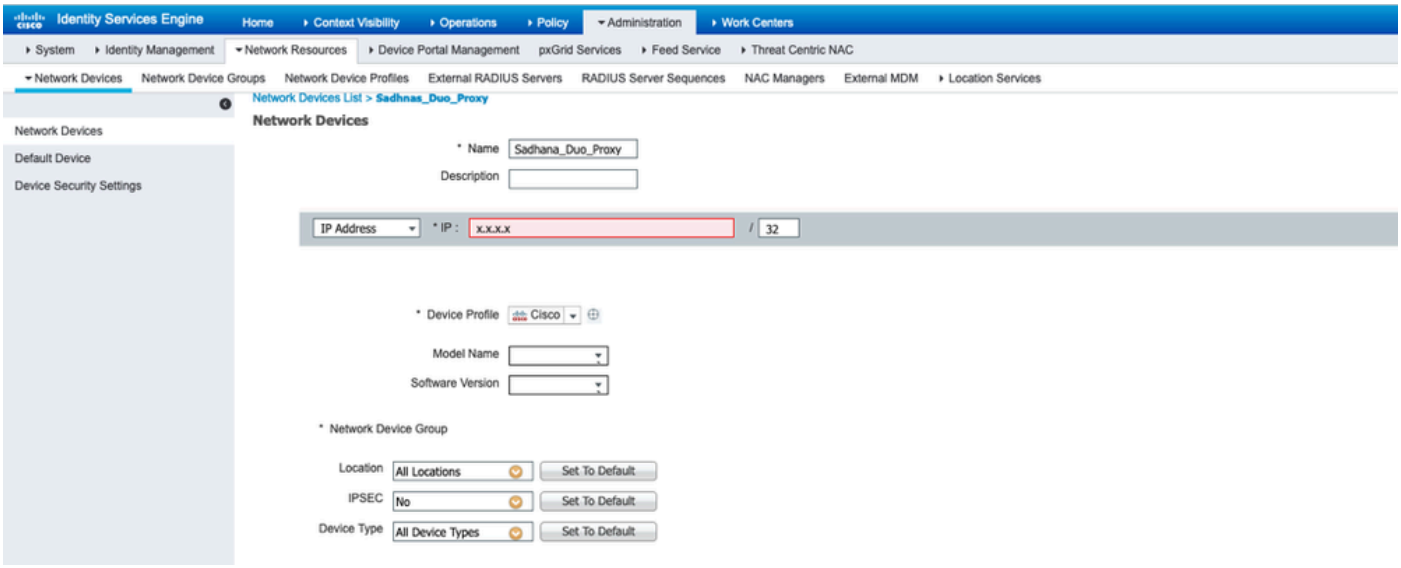


Duo Sicherheitsauthentifizierungsproxydienst

Konfigurationsschritte auf der ISE

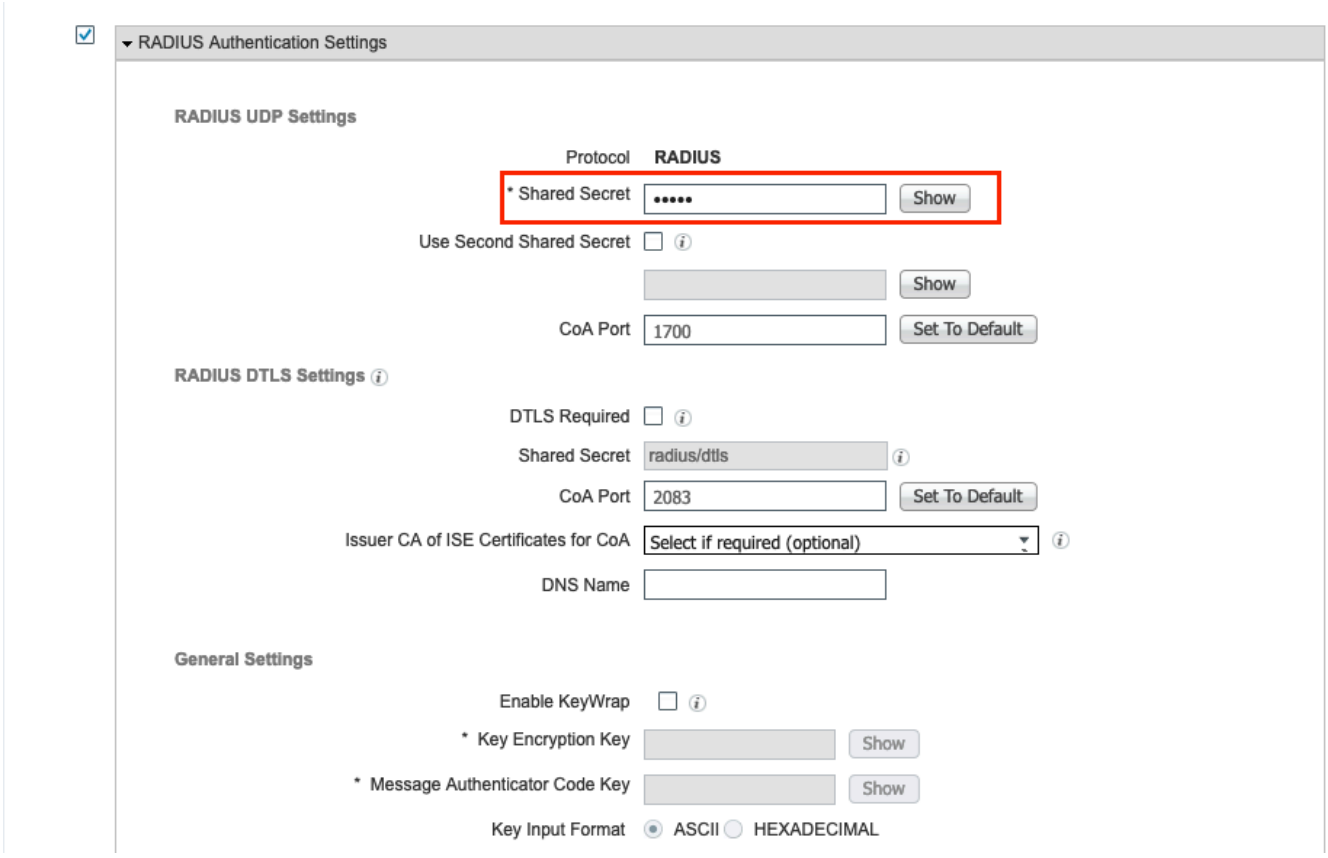
Schritt 1: Navigieren Sie zu **Administration** > **Network Devices**, und klicken SieAddauf, um das Netzwerkgerät zu konfigurieren.

Anmerkung: x.x.x.x Ersetzen Sie dies durch die IP-Adresse Ihres Duo-Authentifizierungsproxy-Servers.



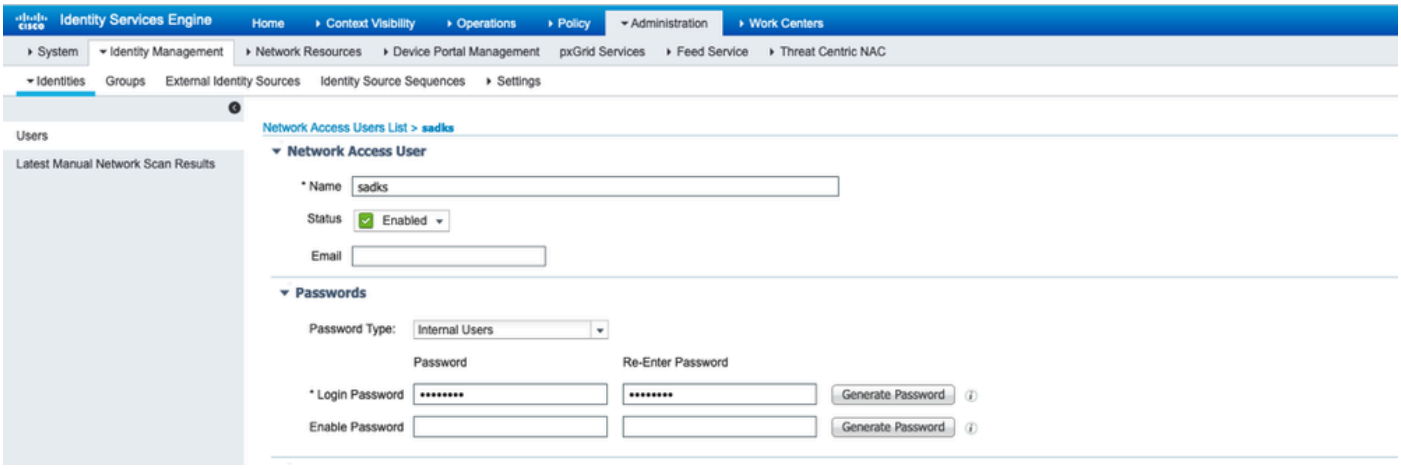
ISE - Netzwerkgeräte

Schritt 2: Konfigurieren Sie die Shared Secretwie in der authproxy.cfgsecretbeschrieben:



ISE - Gemeinsamer geheimer Schlüssel

Schritt 3: Navigieren Sie zu Administration > Identities > Users.Wählen Sie diese Option, Addum den Identity-Benutzer für die primäre AnyConnect-Authentifizierung zu konfigurieren:

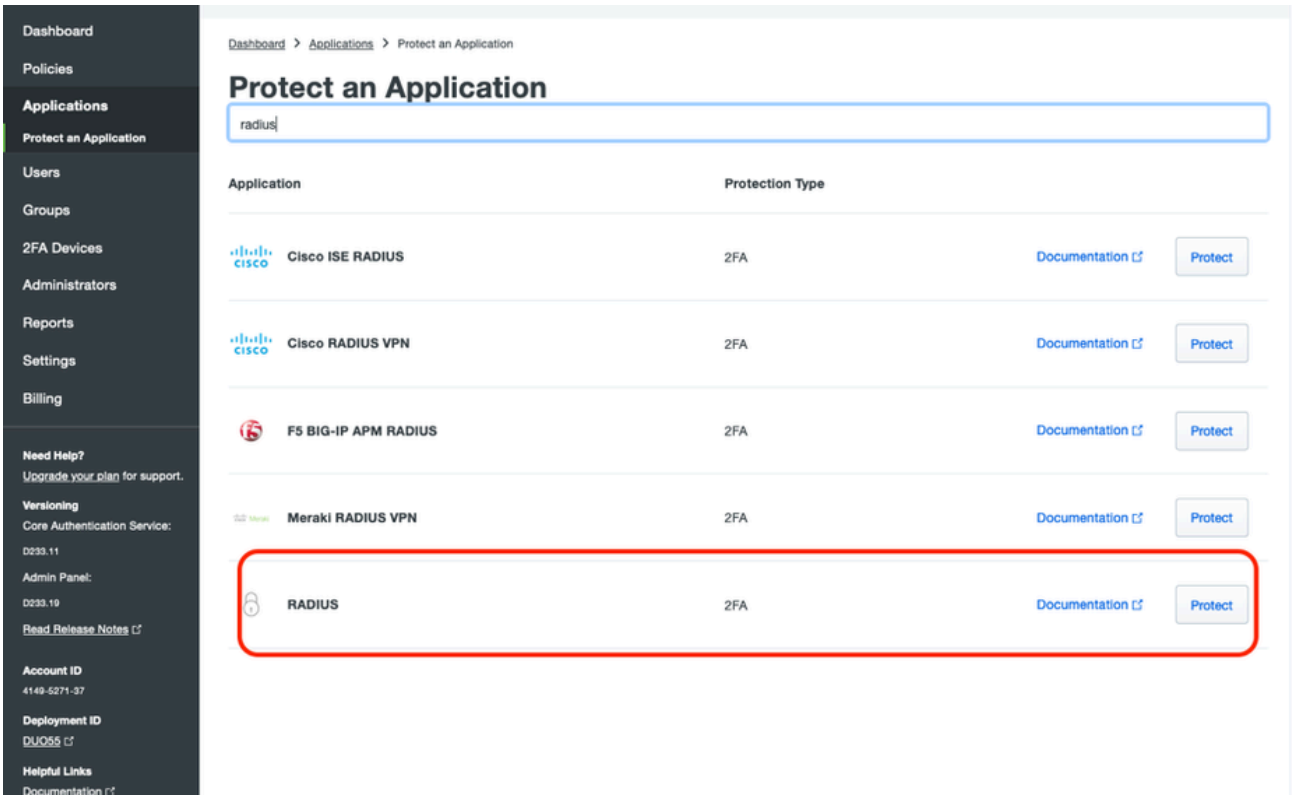


ISE - Benutzer

Konfigurationsschritte im DUO-Administrationsportal

Schritt 1: Melden Sie sich bei Ihrem Duo-Konto an.

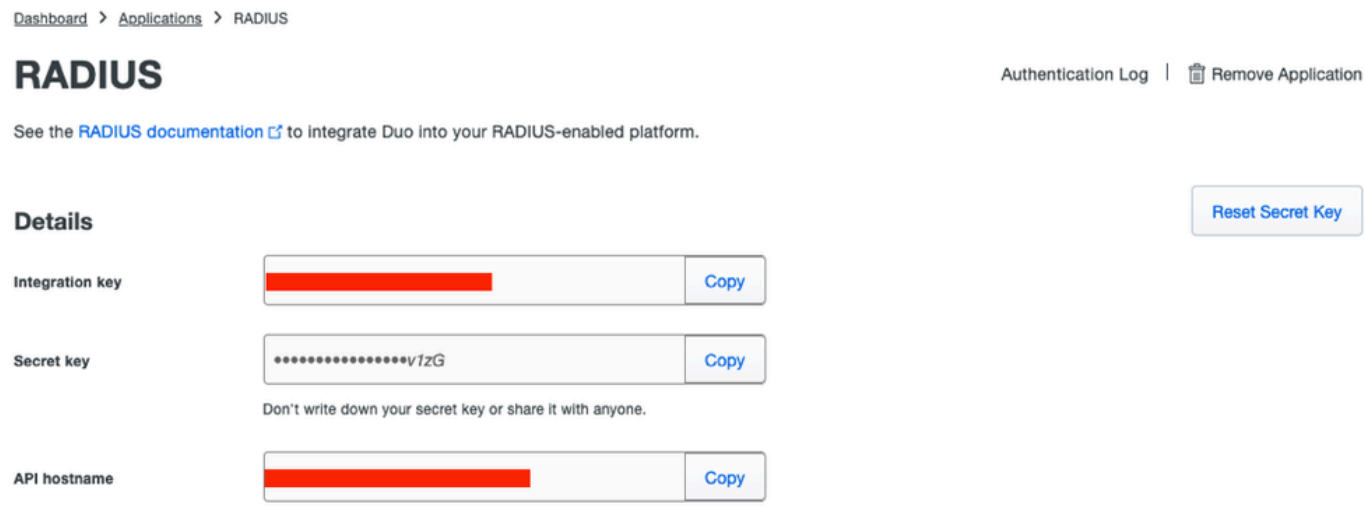
Navigieren Sie zuApplications > Protect an Application. Klicken Sie Protect auf die gewünschte Anwendung. (in diesem Fall RADIUS)



DUO - Anwendung

Protect Schritt 2. Klicken Sie für die Anwendung, die Sie verwenden möchten. (in diesem Fall RADIUS)

Kopieren Sie den Integrationsschlüssel, den geheimen Schlüssel und den API-Hostnamen, und fügen Sie ihn in authproxy.cfgden Duo Authentication-Proxy ein.



DUO - RADIUS

Kopieren Sie diese Werte, navigieren Sie zurück zum DUO-Authentifizierungsproxy, und öffnen Sie die authproxy.cfgund fügen Sie die Werte wie dargestellt ein:

Integrationsschlüssel = Schlüssel

Geheimschlüssel = 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
```

Anmerkung: Der Schlüssel, der Schlüssel und der api_host müssen bei der Konfiguration des Servers vom Duo-Server kopiert werden, und "10.106.54.143" ist die IP-Adresse des C8000V-Routers, und "cisco" ist der Schlüssel, der auf dem Router in der Radius-Server-Konfiguration konfiguriert wurde.

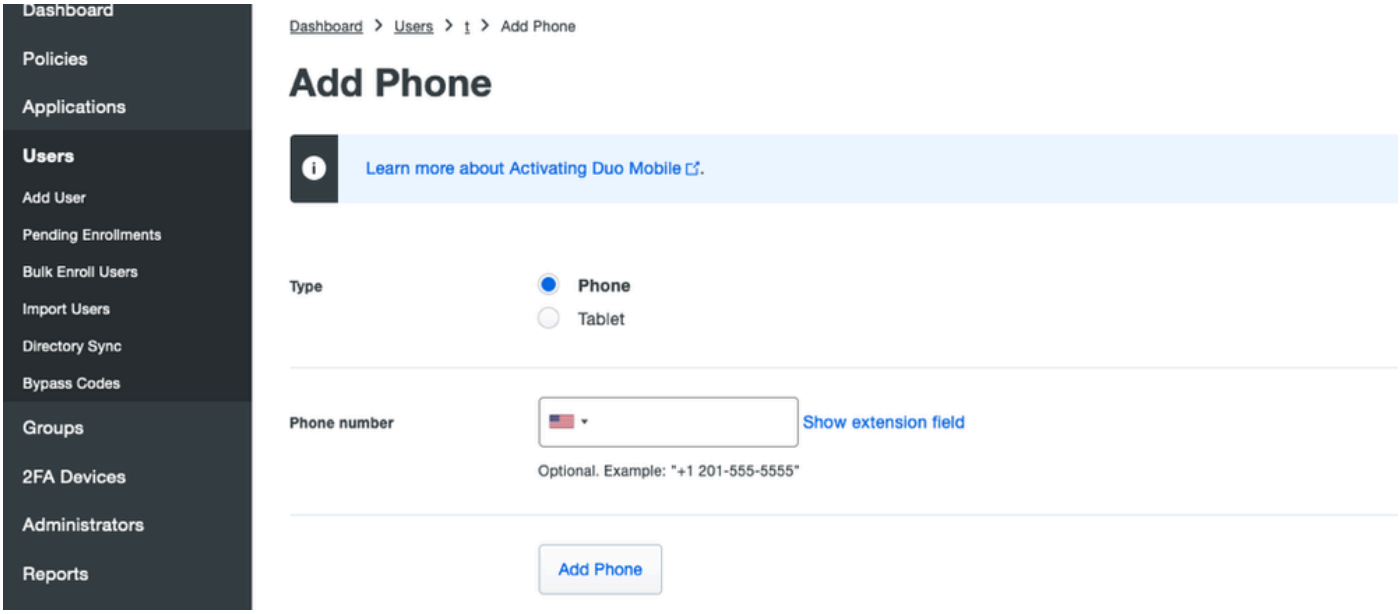
Wenn Sie diese Änderungen vorgenommen haben, speichern Sie die Datei erneut, und starten Sie den Duo Security Authentication Proxy Service (in services.msc) neu.

Schritt 3: Erstellen Sie Benutzer für die sekundäre Authentifizierung auf DUO.

Navigieren Sie zu,Users > Add Userund geben Sie den Benutzernamen ein.

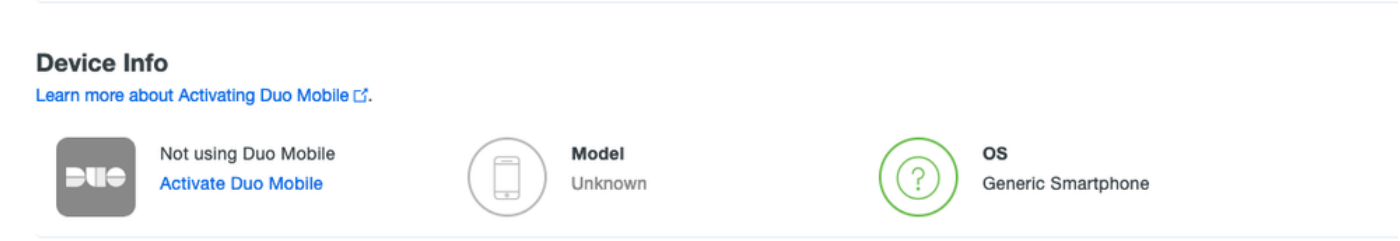
Anmerkung: Der Benutzername muss mit dem Benutzernamen für die primäre Authentifizierung übereinstimmen.

Klicken Sie auf .Add User Nach der Erstellung klicken Sie unter Phonesauf Add Phone, geben Sie die Telefonnummer ein, und klicken Sie auf Add Phone.



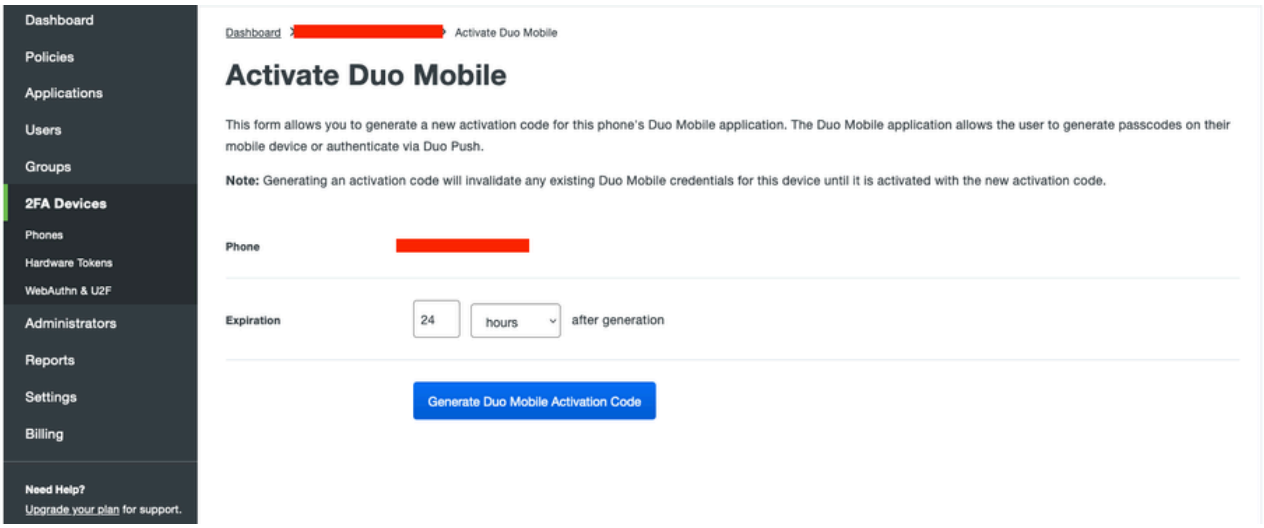
DUO - Telefon hinzufügen

Wählen Sie den Authentifizierungstyp aus.



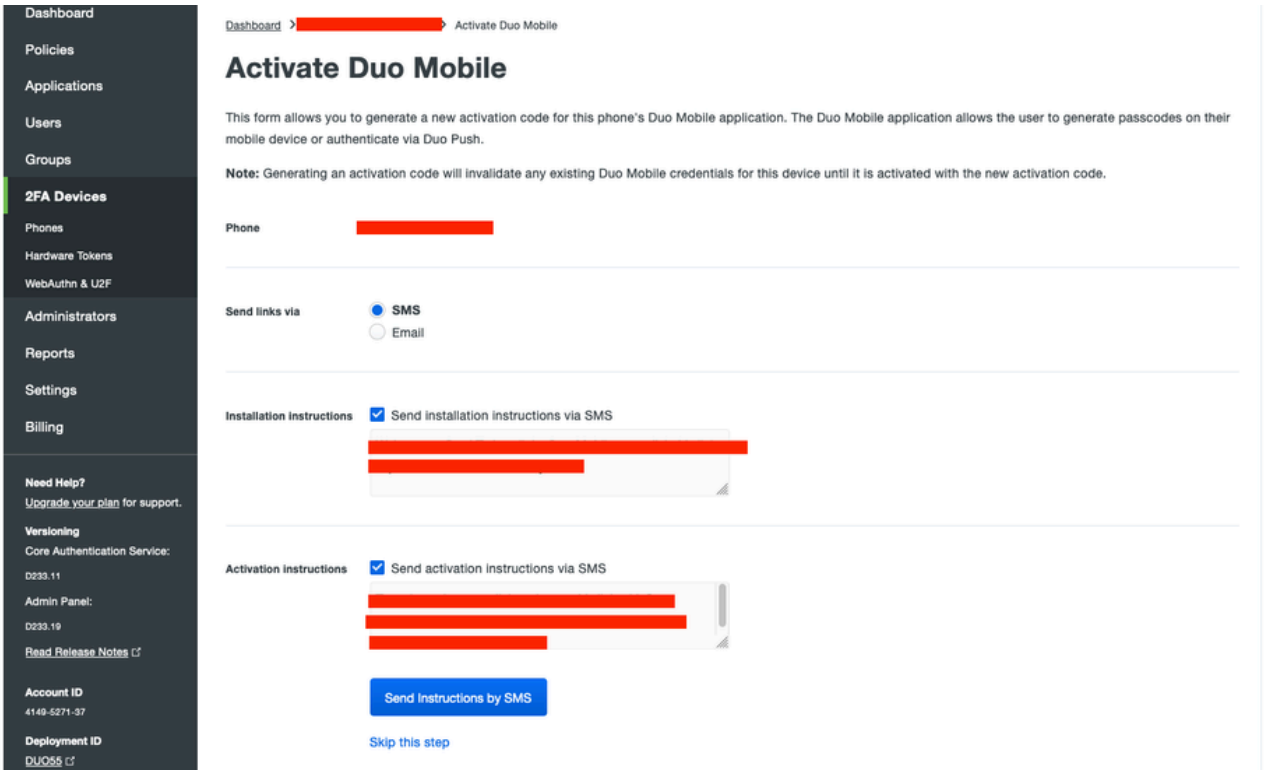
DUO - Geräteinformationen

Wählen Sie Generate Duo Mobile Activation Code.



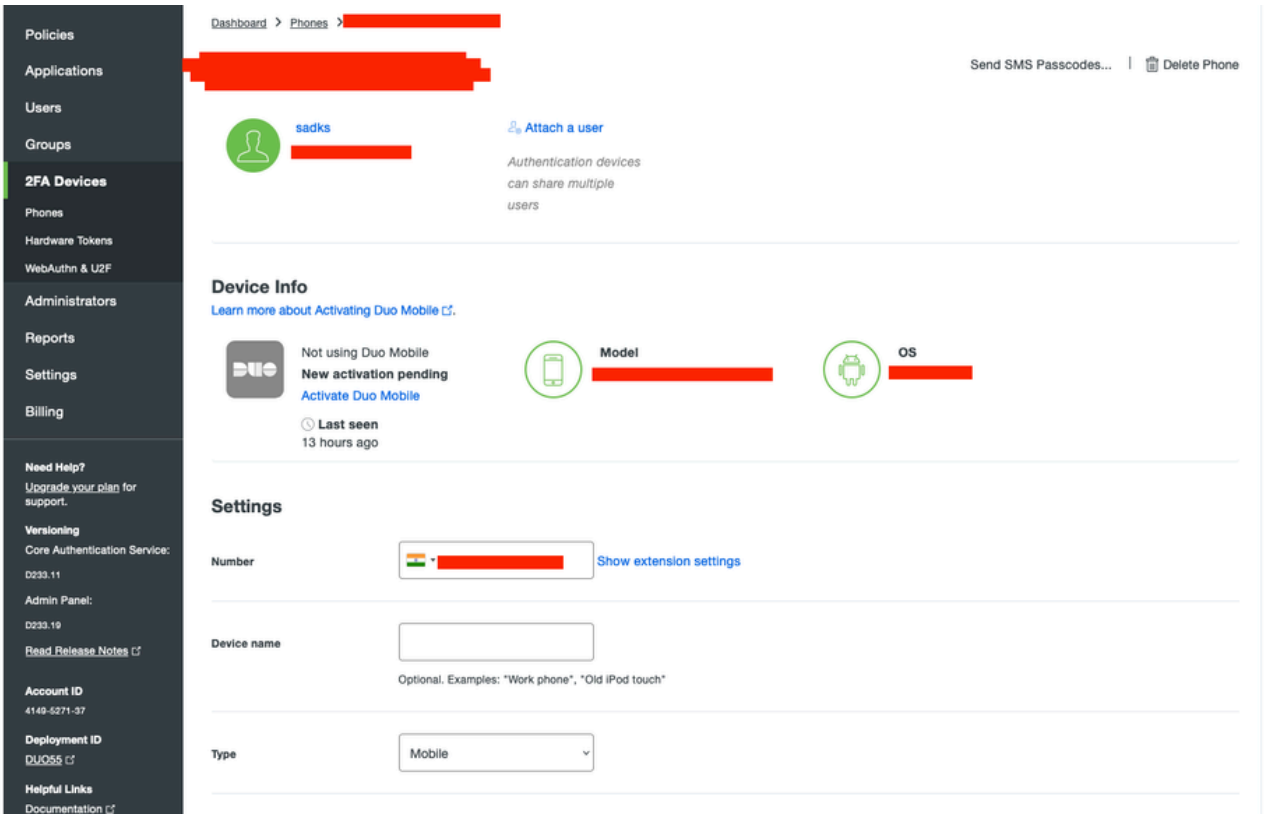
DUO - Telefonaktivierung

Auswählen Send Instructions by SMS.



DUO - SMS senden

Klicken Sie auf den Link, der an das Telefon gesendet wird, und die DUO-App wird mit dem Benutzerkonto im Device InfoAbschnitt verknüpft, wie im Bild gezeigt:

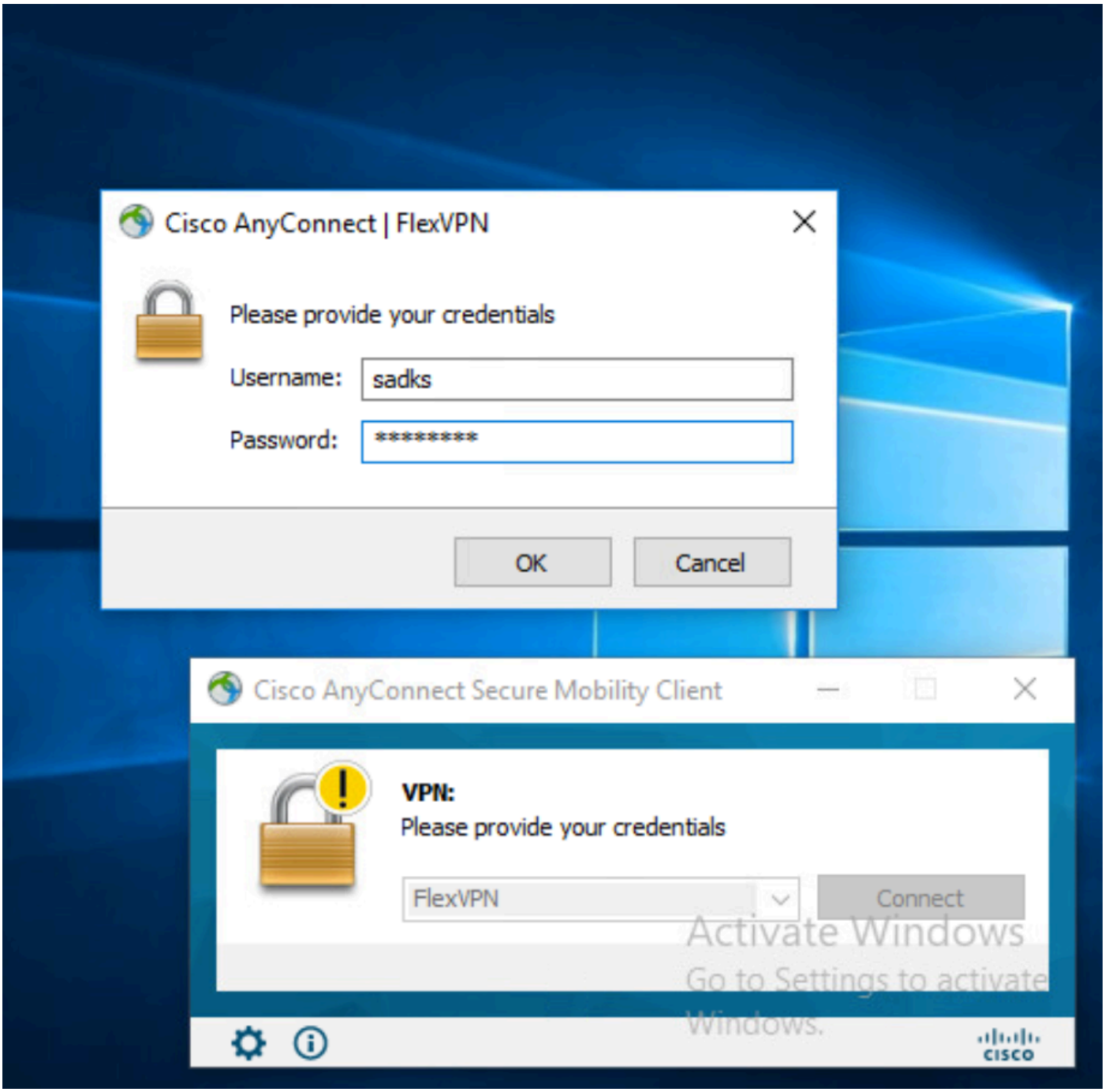


DUO = Device Linked

Überprüfung

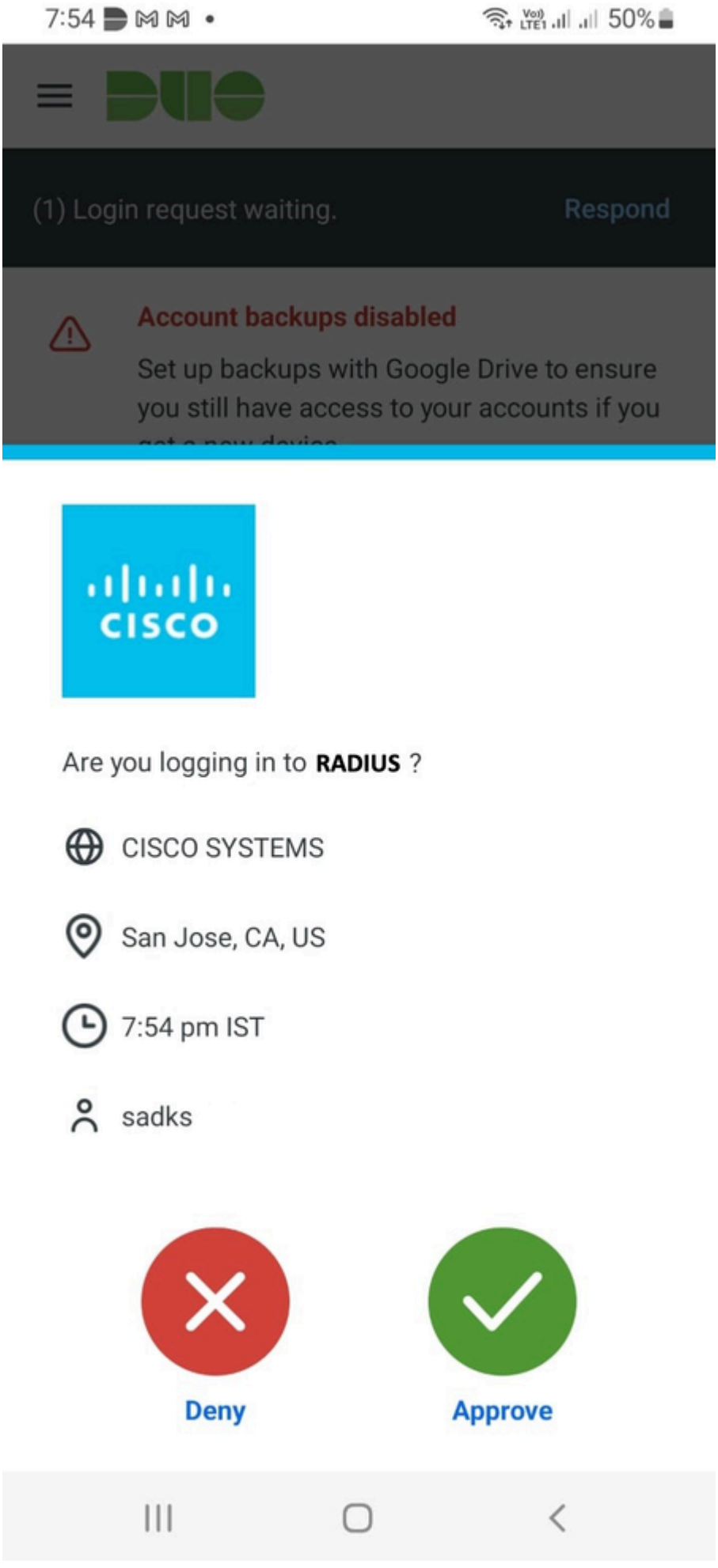
Um die Authentifizierung zu testen, stellen Sie vom PC des Benutzers über AnyConnect eine Verbindung mit dem C8000V her.

Geben Sie den Benutzernamen und das Kennwort für die primäre Authentifizierung ein.



AnyConnect-Verbindung

Dann akzeptieren die DUO schiebt auf dem Handy.



DUO-Push

Die Verbindung wird hergestellt

<#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

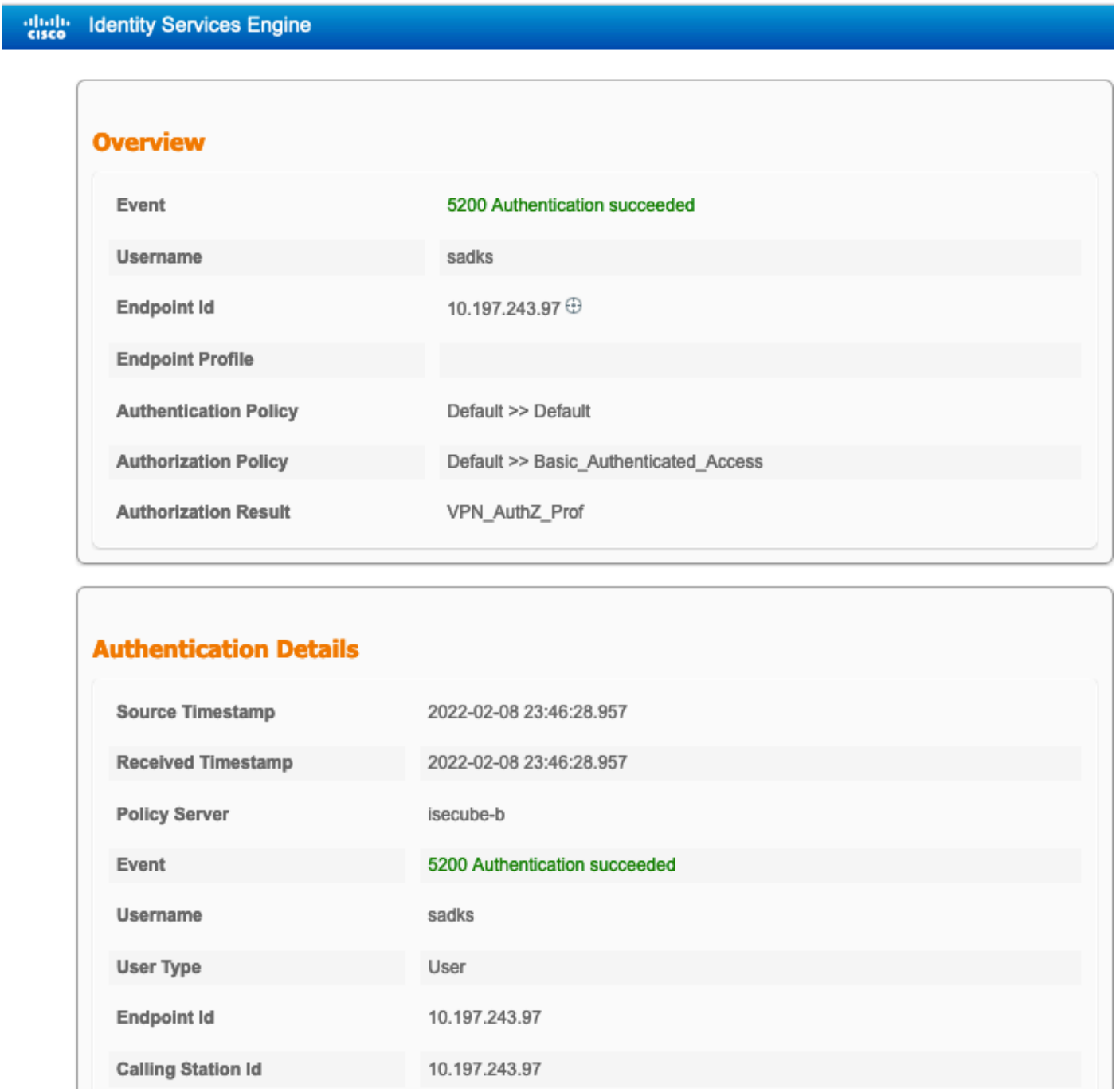
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0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

Navigieren Sie in der ISE zuOperations > Live Logs. Sie können den Authentifizierungsbericht für die primäre Authentifizierung anzeigen.



ISE - Live-Protokolle

4. Verification on DUO authentication proxy

Navigieren Sie zu dieser Datei auf DUO Authentication Proxy. 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
```

Fehlerbehebung

1. Debuggt auf C8000V.

Für IKEv2:

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

Für IPSec:

- debug crypto ipsec
- debug crypto ipsec error

2. Für den DUO-Authentifizierungsproxy überprüfen Sie die Protokolldatei mit Proxy-Protokollen. ()C:\Program Files\Duo Security Authentication Proxy\log

Der Ausschnitt für ein Fehlerprotokoll, bei dem die ISE die primäre Authentifizierung ablehnt, wird angezeigt:

<#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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.