# Configurazione di AnyConnect Flexvpn con autenticazione EAP e DUO

## Sommario



## Introduzione

In questo documento viene descritto come configurare l'autenticazione a due fattori esterni per la connessione AnyConnect IPSec a un router Cisco IOS® XE.

Contributo dei tecnici TAC di Sadhana K.S. e Rishabh Aggarwal Cisco.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Esperienza con la configurazione di RSA VPN su un router
- Amministrazione di Identity Services Engine (ISE)

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Catalyst 8000V (C800V) con versione 17.10.01a

- Cisco AnyConnect Secure Mobility Client versione 4.10.04071
- Cisco ISE versione 3.1.0
- Duo Authentication proxy server (Windows 10 o qualsiasi PC Linux)
- Account Web Duo
- PC client con AnyConnect installato

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Flusso di autenticazione

L'utente AnyConnect esegue l'autenticazione con un nome utente e una password sul server ISE. Il server Duo Authentication Proxy invia inoltre un'ulteriore autenticazione sotto forma di notifica push al dispositivo mobile dell'utente.

## Diagramma di flusso

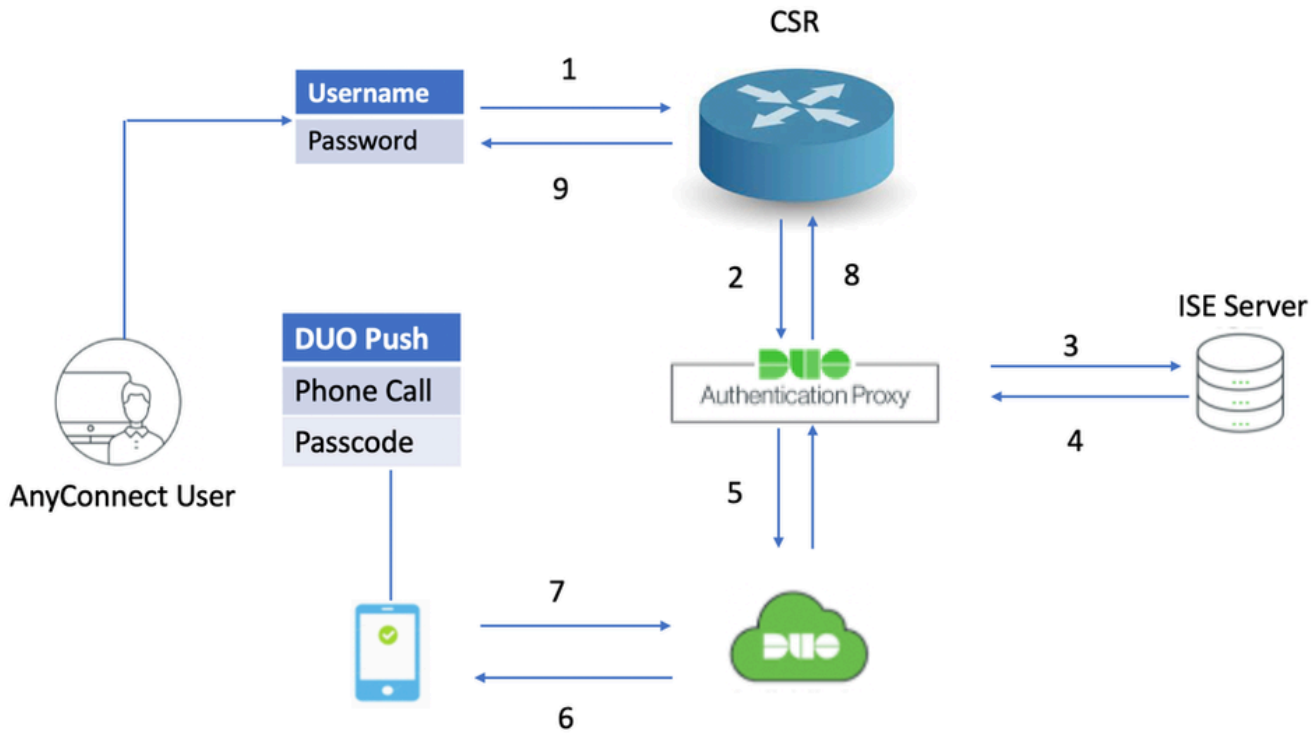



Diagramma di flusso dell'autenticazione

## Processo di comunicazione

1. L'utente avvia una connessione RAVPN al C8000V e fornisce un nome utente e una password per l'autenticazione primaria.
2. Il C800V invia una richiesta di autenticazione al proxy di autenticazione Duo.

3. Duo Authentication Proxy invia quindi la richiesta primaria al server Active Directory o RADIUS.
4. La risposta di autenticazione viene inviata di nuovo al proxy di autenticazione.
5. Una volta completata l'autenticazione primaria, il proxy di autenticazione Duo richiede l'autenticazione secondaria tramite il server Duo.
6. Il servizio Duo autentica quindi l'utente, a seconda del metodo di autenticazione secondario (push, chiamata telefonica, passcode).
7. Il proxy di autenticazione Duo riceve la risposta di autenticazione.
8. La risposta viene inviata al C800V.
9. Se il tentativo ha esito positivo, la connessione AnyConnect viene stabilita.

# Configurazione

Per completare la configurazione, prendere in considerazione le sezioni seguenti.

## Procedura di configurazione su C800V (headend VPN)

1. Configurare il server RADIUS. L'indirizzo IP del server RADIUS deve essere l'indirizzo IP del proxy di autenticazione Duo.

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

2. Configurare il server RADIUS come aaa autenticazione e autorizzazione locale.

```
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. Creare un trust point per installare il certificato di identità, se non è già presente per l'autenticazione locale. È possibile fare riferimento a Registrazione certificato per una PKI per ulteriori dettagli sulla creazione del certificato.

```
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. (Facoltativo) Configurare un elenco degli accessi standard da utilizzare per il tunnel suddiviso. Questo elenco degli accessi è composto dalle reti di destinazione a cui è possibile accedere tramite il tunnel VPN. Per impostazione predefinita, tutto il traffico passa attraverso il tunnel VPN se il tunnel suddiviso non è configurato.

```
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. Creare un pool di indirizzi IPv4.

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

Il pool di indirizzi IP creato assegna un indirizzo IPv4 al client AnyConnect durante una connessione AnyConnect riuscita.

6. Configurare un criterio di autorizzazione.

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

Il pool IP, il DNS, l'elenco di split-tunnel e così via sono specificati nei criteri di autorizzazione.

---

Nota: Se il criterio di autorizzazione IKEv2 personalizzato non è configurato, per l'autorizzazione viene utilizzato il criterio di autorizzazione predefinito denominato 'default'. Gli attributi specificati nel criterio di autorizzazione IKEv2 possono inoltre essere sottoposti a push tramite il server RADIUS.

---

7. Configurare una proposta e un criterio 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. Caricare il profilo del client AnyConnect nella memoria flash del router e definire il profilo come indicato:

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

9. Disabilitare il server protetto HTTP.

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

10. Configurare il criterio SSL e specificare l'indirizzo IP WAN del router come indirizzo locale per il download del profilo.

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

           port 443
```

11. Configurare un modello virtuale dal quale l'interfaccia di accesso virtualele interfacce vengono clonate

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

Il comando senza numero ottiene l'indirizzo IP dall'interfaccia configurata (Gigabit Ethernet1).

13. Configurare un profilo IKEv2 che contenga tutte le informazioni relative alla connessioneinformazioni finali.

```
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
```

Questi elementi vengono utilizzati nel profilo IKEv2:

- match identity remote any - Si riferisce all'identità del client. Qui 'any' è configurato in modo che qualsiasi client con le credenziali corrette possa connettersi
- authentication remote - Indica che il protocollo EAP deve essere utilizzato per l'autenticazione client
- authentication local - Indica che i certificati devono essere utilizzati per l'autenticazione locale
- aaa authentication eap - Durante l'autenticazione EAP viene utilizzato il server FlexVPN_auth RADIUS
- aaa authorization group eap list - Durante l'autorizzazione, l'elenco delle reti FlexVPN_authzviene utilizzato con i criteri di autorizzazione ikev2-authz-policy
- aaa authorization user eap cached- Abilita l'autorizzazione utente implicita
- virtual-template 20 mode auto - Definisce il modello virtuale da clonare
- anyconnect profile Client_Profile - Il profilo client definito nel passaggio 8. viene applicato a questo profilo IKEv2

14. Configurare un set di trasformazioni e un profilo 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. Aggiungere il profilo IPSec al modello virtuale.

```
interface Virtual-Template20 type tunnel
 tunnel mode ipsec ipv4
```

```
 tunnel protection ipsec profile Flexvpn_IPsec_Profile
```

Frammento del profilo client (profilo XML)

Nelle versioni precedenti a Cisco IOS XE 16.9.1, il download automatico del profilo dall'headend non è disponibile. Dopo 16.9.1, è possibile scaricare il profilo dall'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>
```

## Procedura di configurazione sul proxy di autenticazione DUO

---

Nota: Duo Authentication Proxy supporta MS-CHAPv2 solo con autenticazione RADIUS.

---

Passaggio 1. Scaricare e installare Duo Authentication Proxy Server.

Accedere al computer Windows e installare il server Duo Authentication Proxy.

Si consiglia di utilizzare un sistema con almeno 1 CPU, 200 MB di spazio su disco e 4 GB di RAM.

Passaggio 2. Passare C:\Program Files\Duo Security Authentication Proxy\conf\a e aprire authproxy.cfg per configurare il proxy di autenticazione con i dettagli appropriati.

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

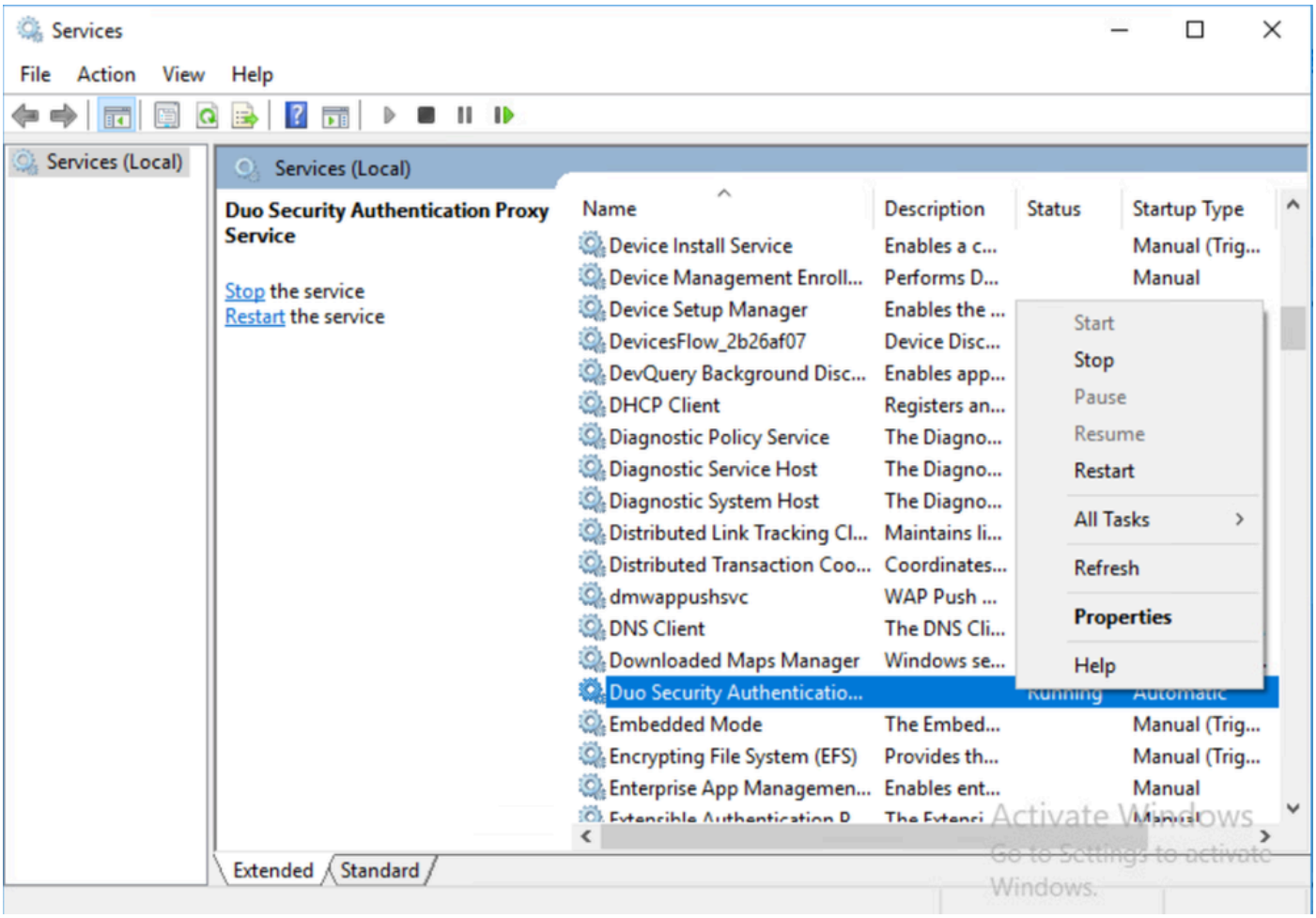
---

Nota: Qui '10.197.243.116' è l'indirizzo IP del server ISE e 'cisco' è la password configurata per convalidare l'autenticazione primaria.

---

Dopo aver apportato le modifiche, salvare il file.

Passaggio 3. Aprire Windows Services Console (services.msc). E riavvia Duo Security Authentication Proxy Service.




Duo Security Authentication Proxy Service

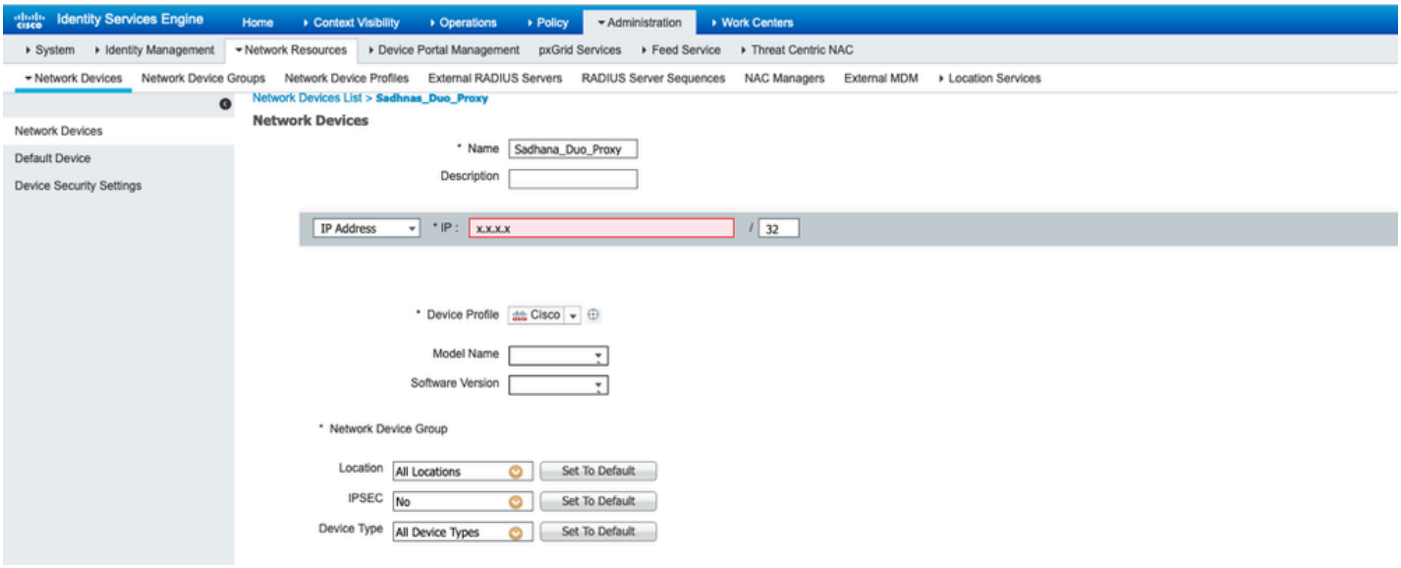
## Procedura di configurazione su ISE

Passaggio 1. Passare a **Administration** > **Network Devices**e fareAddclic su per configurare il dispositivo di rete.

---

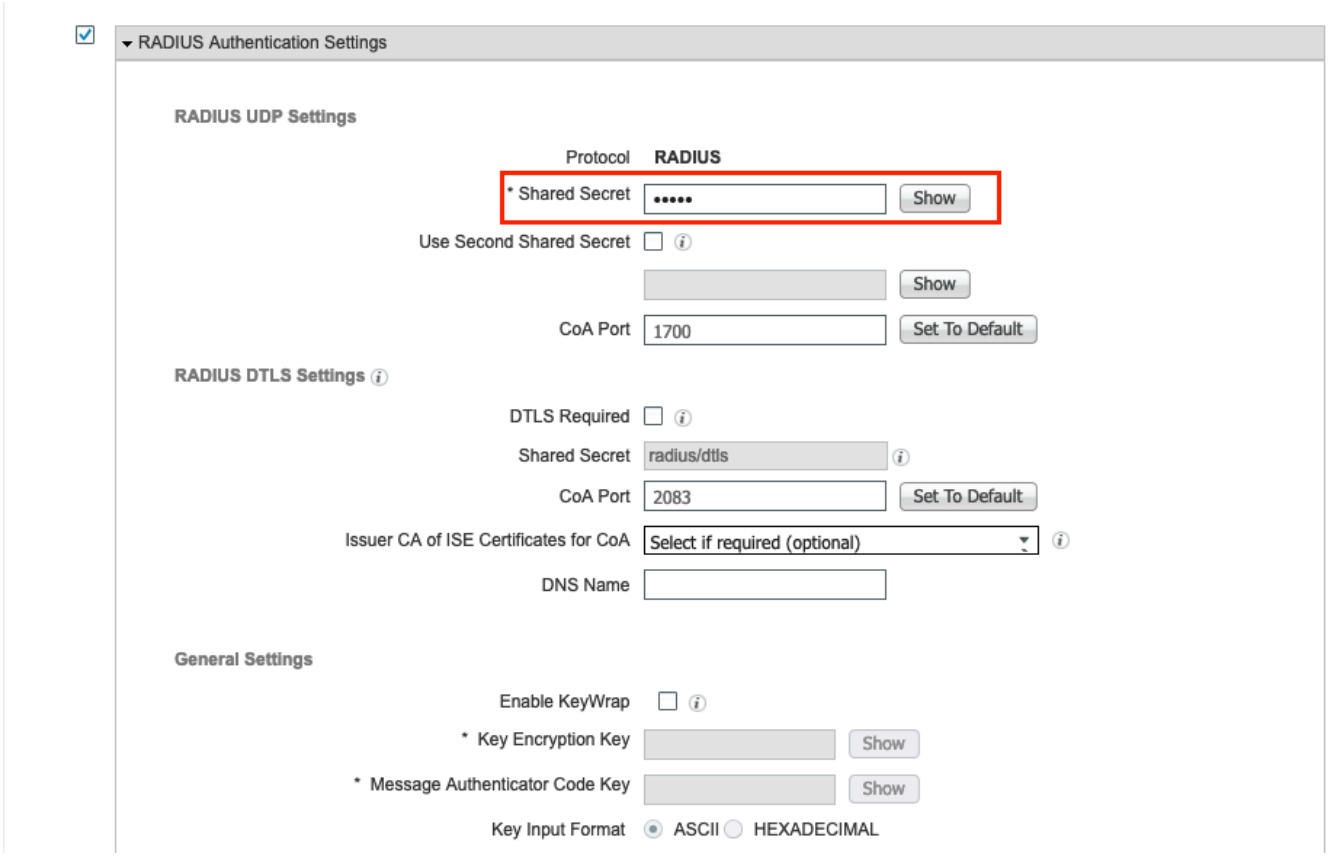
Nota: Sostituire con x.x.x.x l'indirizzo IP del server proxy di autenticazione Duo.

---



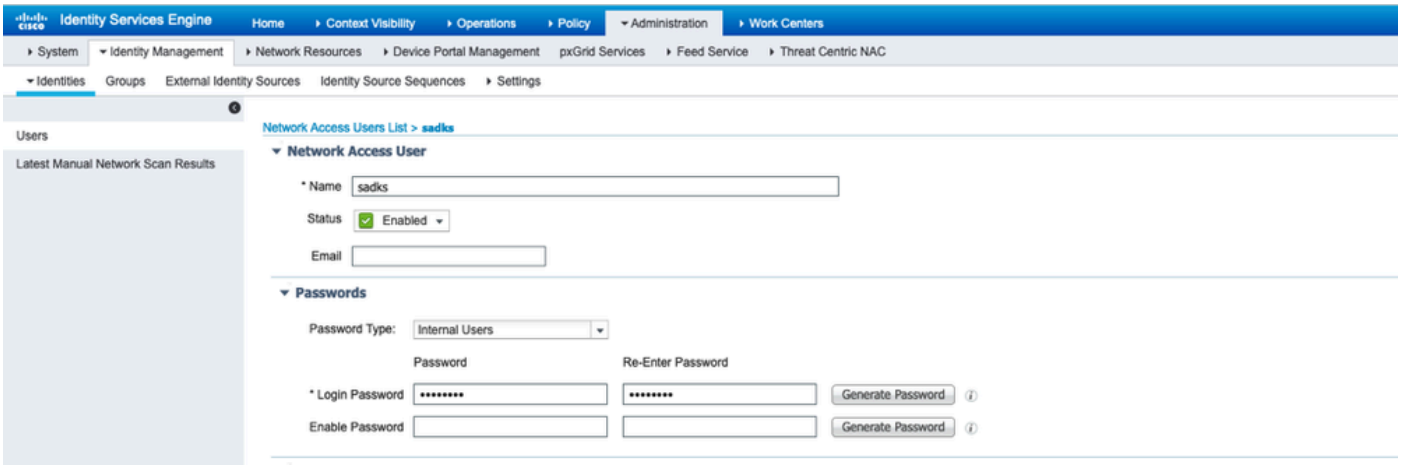

ISE - Dispositivi di rete

Passaggio 2. Configurare il Shared Secretcome indicato nella authproxy.cfgin secret:




ISE - Shared Secret

Passaggio 3. Passare a Administration > Identities > Users.Per Addconfigurare l'utente Identity per l'autenticazione primaria AnyConnect, scegliere:

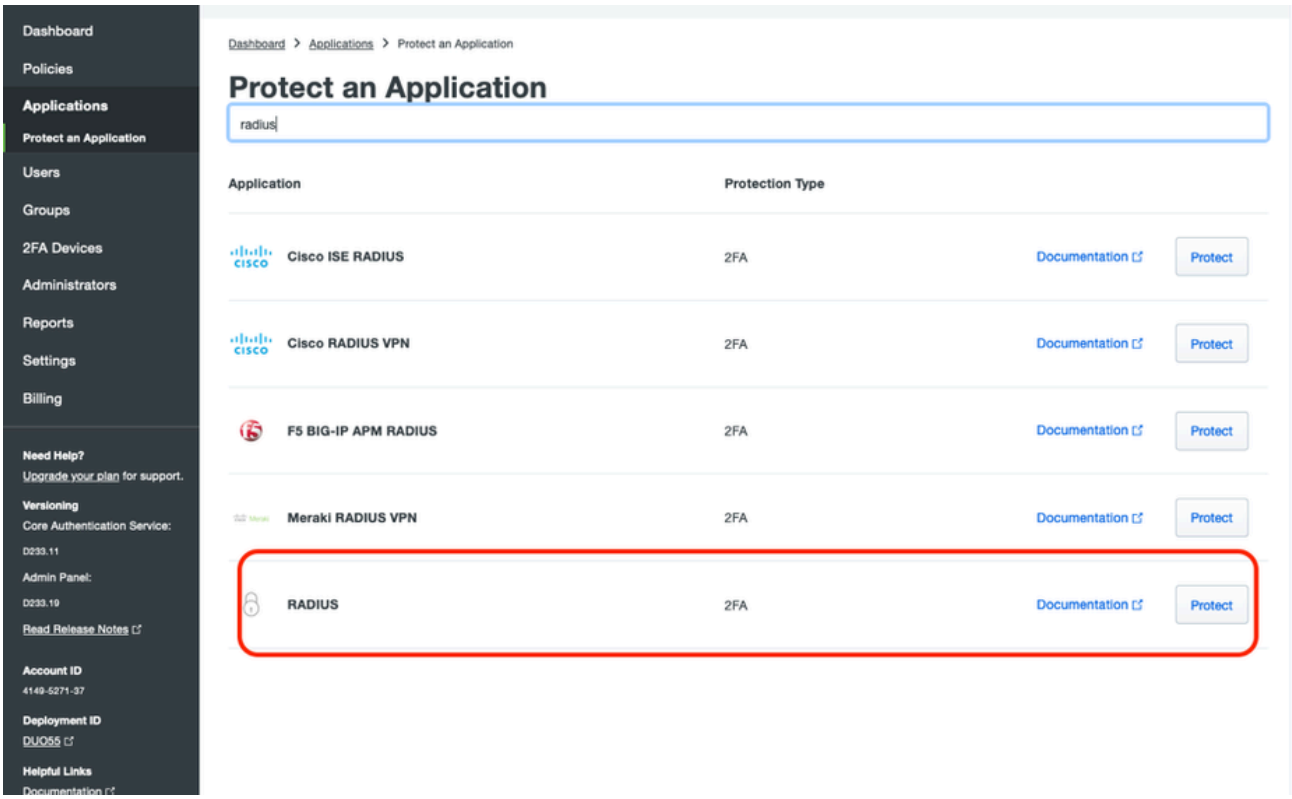



ISE - Utenti

## Procedura di configurazione sul portale di amministrazione DUO

### Passaggio 1. Accedere all'account Duo.

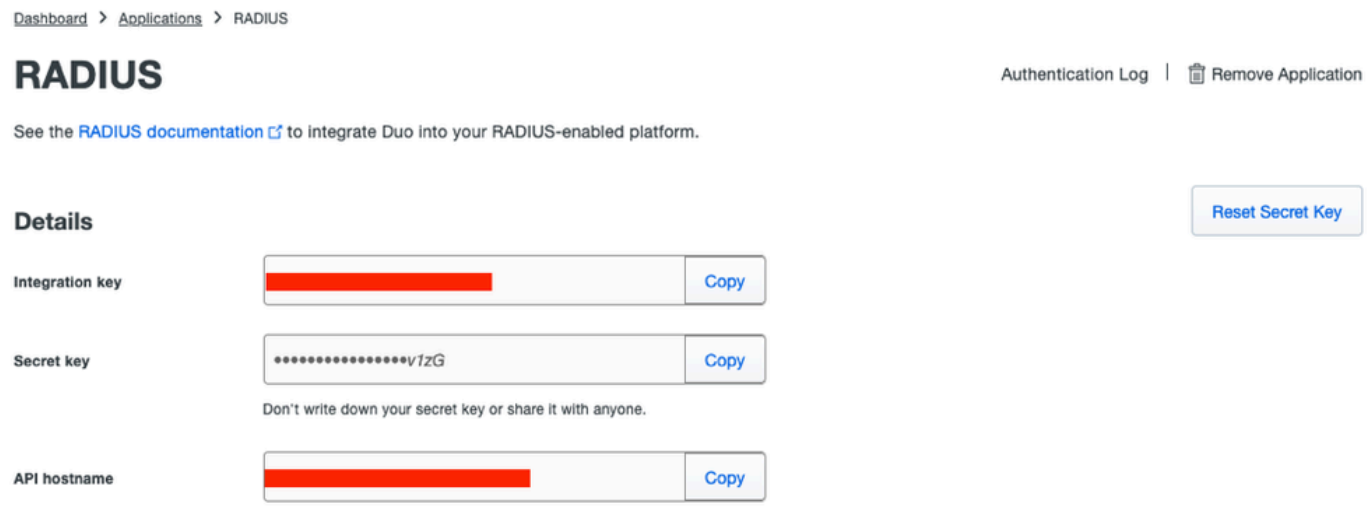
Passare aApplications > Protect an Application. Fare clic su Protect per l'applicazione che si desidera utilizzare. (in questo caso, RADIUS)




DUO - Applicazione

### Passaggio 2. Fare clic su Protect per l'applicazione che si desidera utilizzare. (in questo caso, RADIUS)

Copiare la chiave di integrazione, la chiave segreta e il nome host dell'API e incollarli sul authproxy.cfgnome del proxy di autenticazione Duo.




DUO - RADIUS

Copiare questi valori, tornare al proxy di autenticazione DUO e aprire authproxy.cfge incollare i valori come mostrato:

Chiave di integrazione = ikey

chiave segreta = chiave

Nome host 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
```

Nota: La chiave ikey, skey e api_host deve essere copiata dal server Duo quando si configura il server e '10.106.54.143' è l'indirizzo IP del router C8000V e 'cisco' è la chiave configurata sul router nella configurazione del server radius.

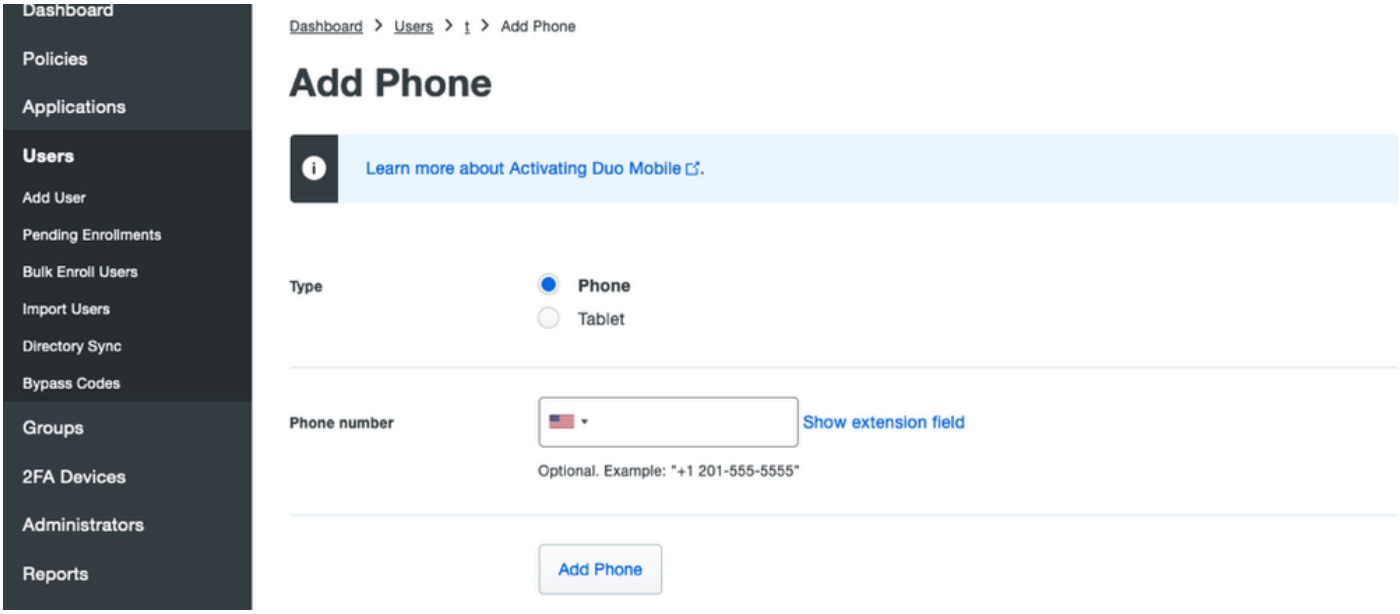
Dopo aver apportato le modifiche, salvare di nuovo il file e riavviare il servizio Duo Security Authentication Proxy (in services.msc).

Passaggio 3. Creazione di utenti su DUO per l'autenticazione secondaria.

IndividuareUsers > Add Usere digitare il nome utente.

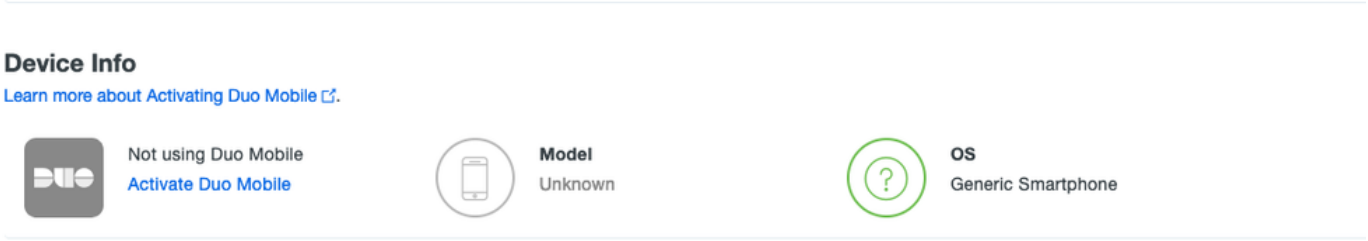
Nota: Il nome utente deve corrispondere al nome utente dell'autenticazione primaria.

Fare clic su .Add User Una volta creato, in Phones, fare clic su Add Phone, immettere il numero di telefono e fare clic su Add Phone.



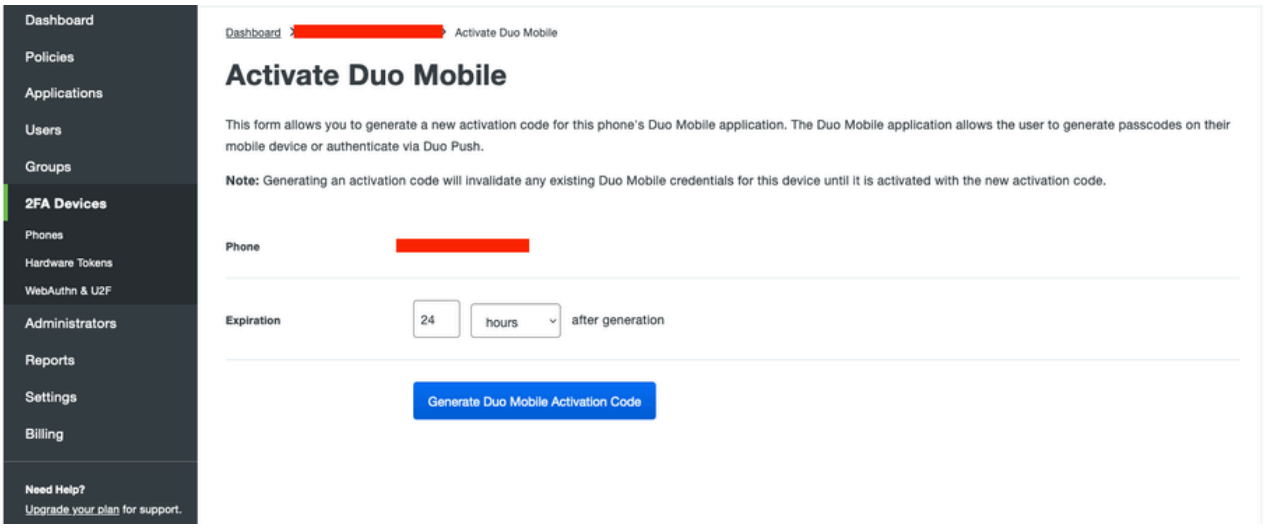

DUO - Aggiungi telefono

Scegliere il tipo di autenticazione.



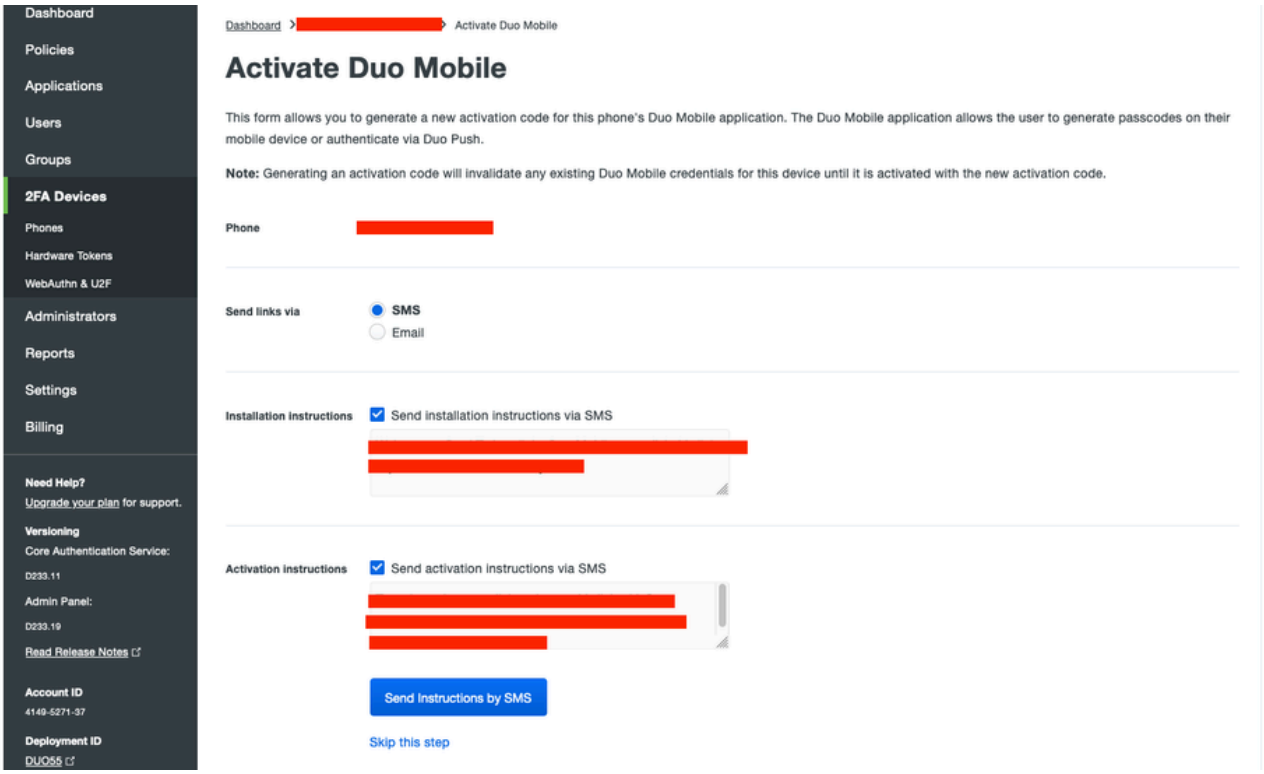

DUO - Informazioni dispositivo

Scegliere Generate Duo Mobile Activation Code.



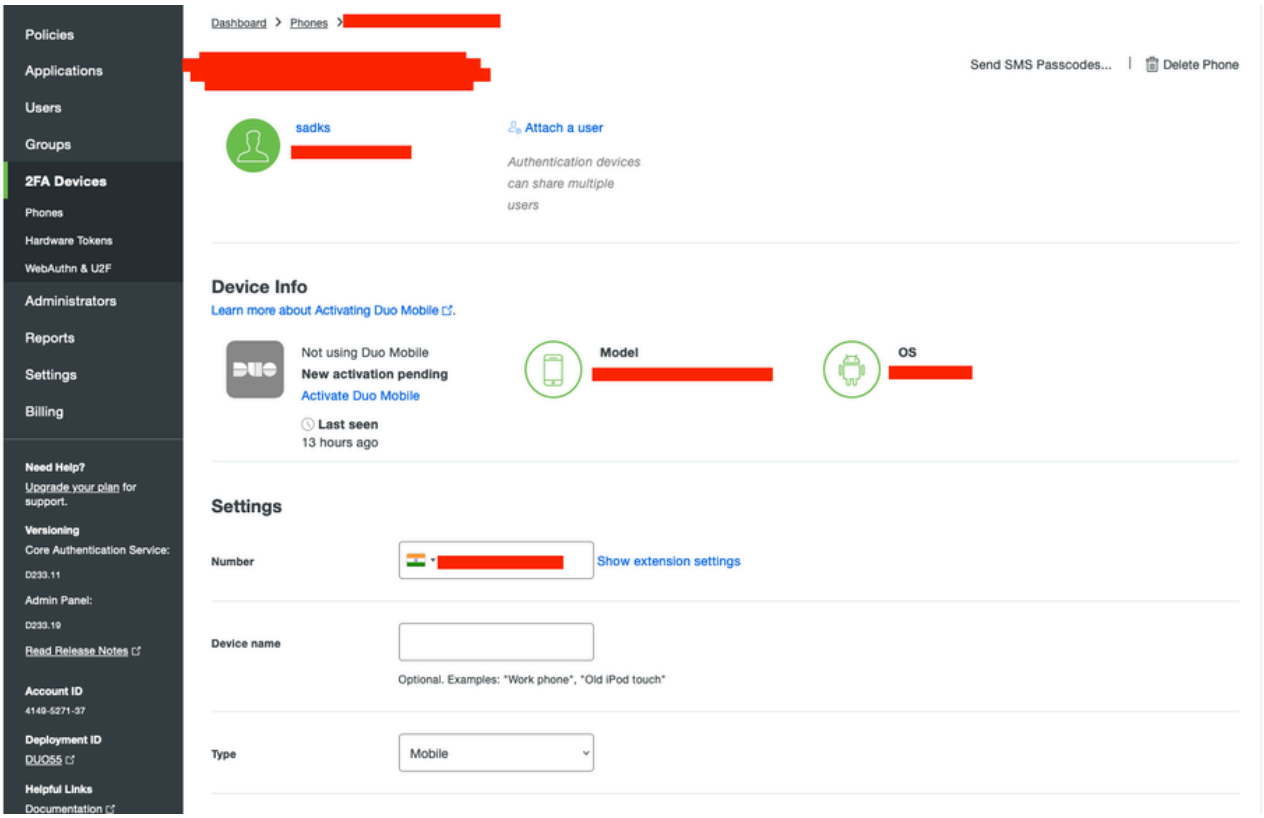

DUO - Attivazione tramite telefono

Scegli Send Instructions by SMS.




DUO - Invia SMS

Fare clic sul collegamento inviato al telefono e l'app DUO viene collegata all'account utente nella Device Infosezione, come mostrato nell'immagine:

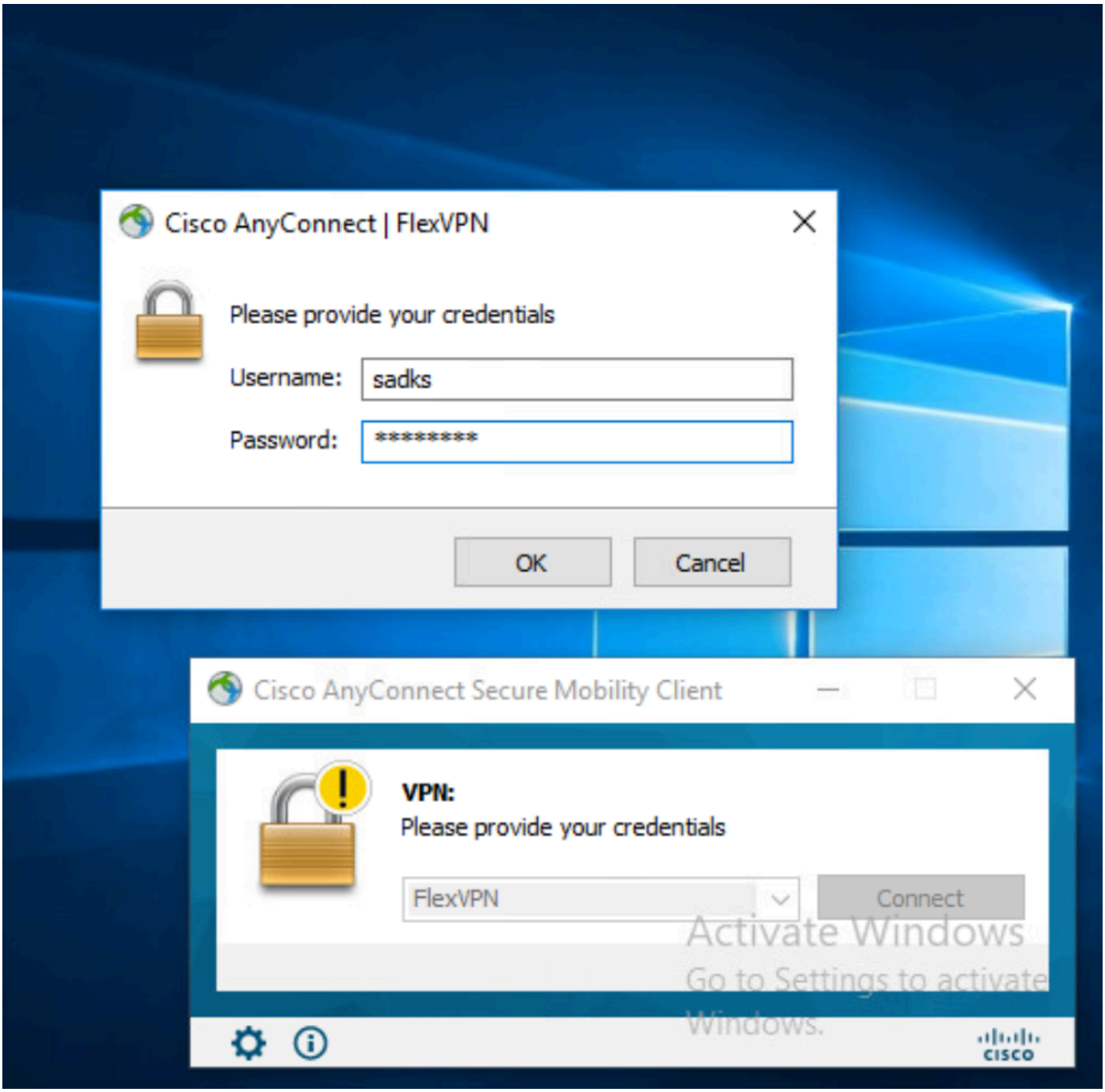



DUO - Dispositivo collegato

# Verifica

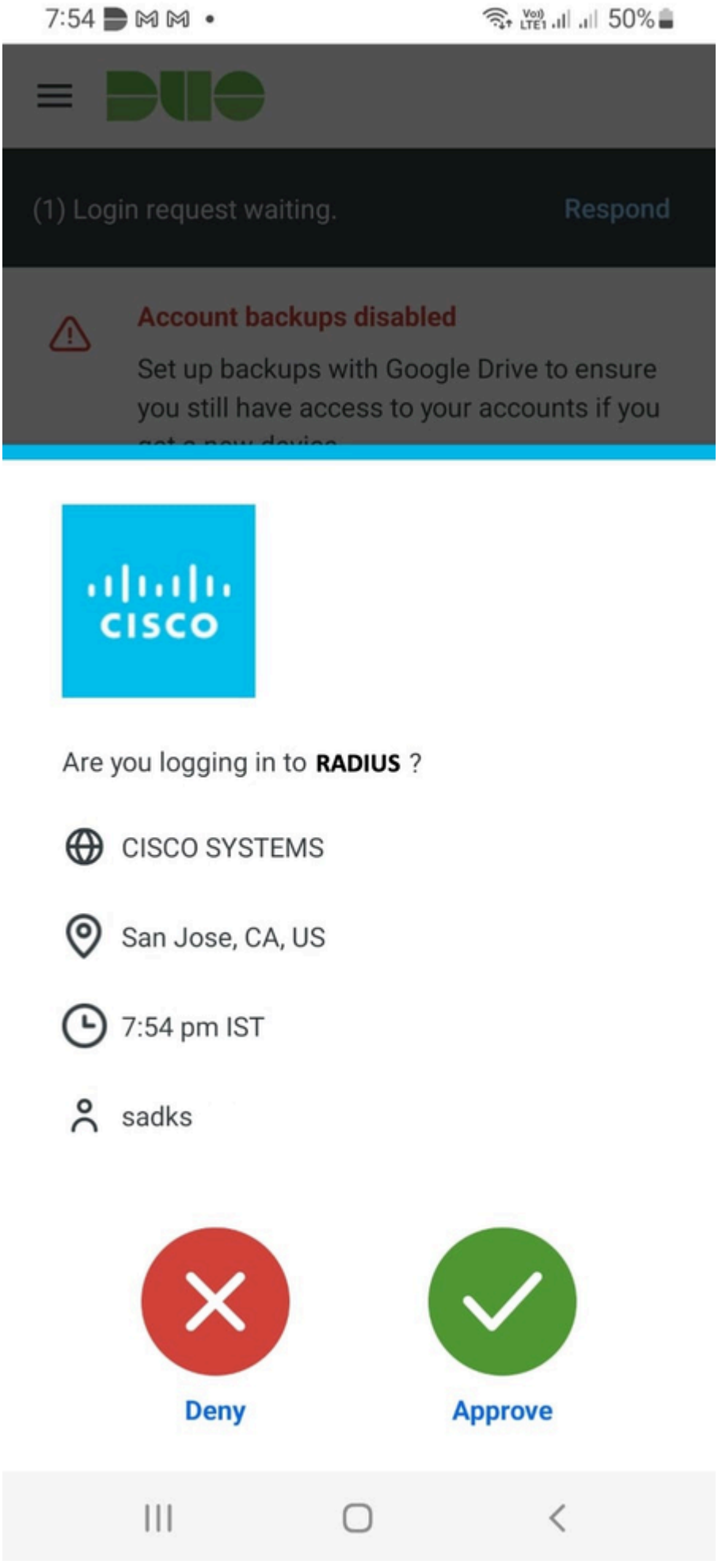
Per verificare l'autenticazione, collegarsi al C8000V dal PC dell'utente tramite AnyConnect.

Digitare il nome utente e la password per l'autenticazione primaria.




Connessione AnyConnect

Accettare quindi le spinte DUO sul cellulare.




Push DUO

Connessione stabilita

<#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**

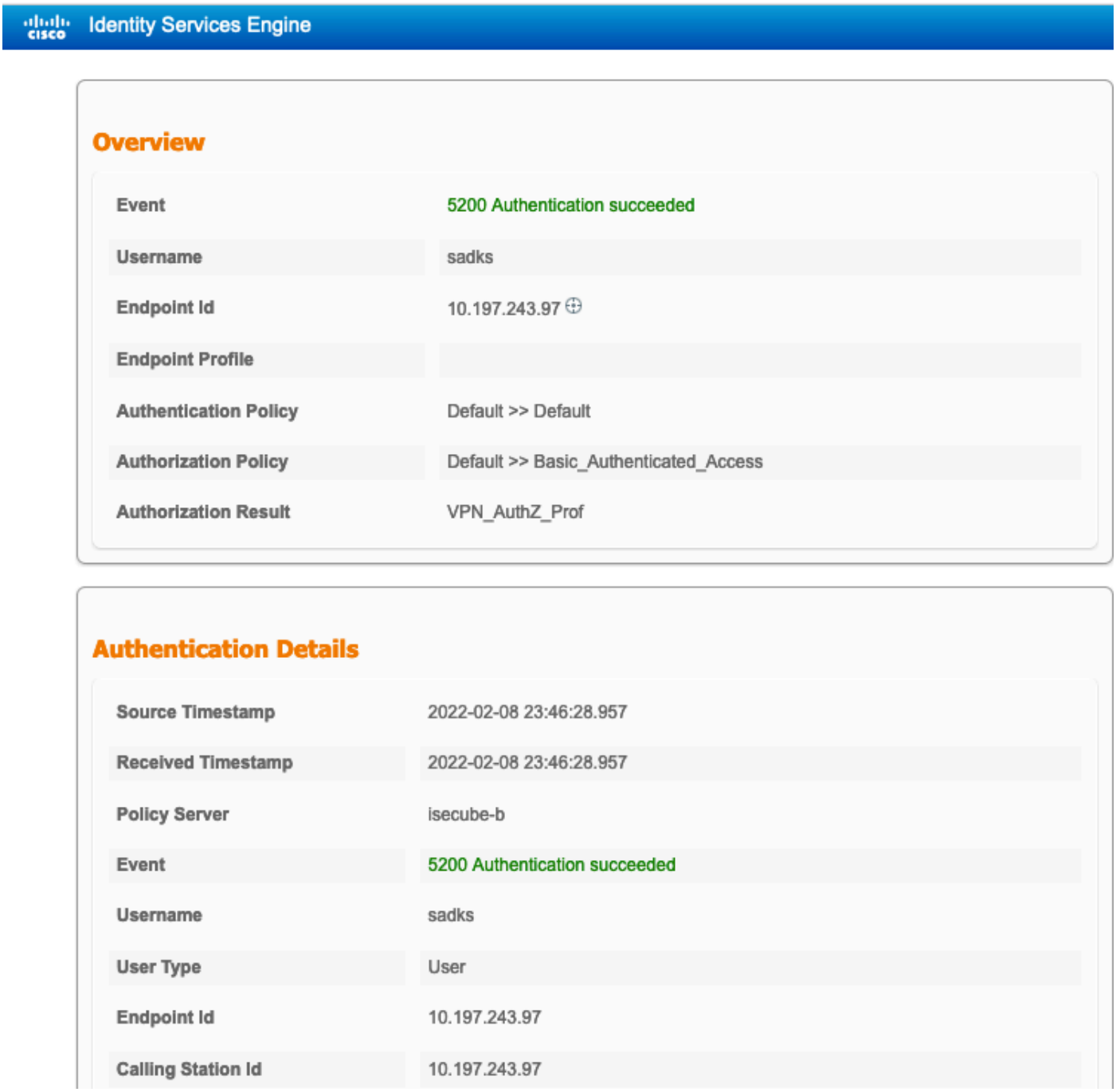
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0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

NavigareOperations > Live Logsfino ad ISE. È possibile visualizzare il report di autenticazione per l'autenticazione primaria.




ISE - Live Log

4. Verification on DUO authentication proxy

Passare a questo file con il proxy di autenticazione 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
```

# Risoluzione dei problemi

1. Debug su C800V.

Per IKEv2:

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

Per IPSec:

- debug crypto ipsec
- debug crypto ipsec error

2. Per il proxy di autenticazione DUO, controllare i registri relativi al proxy del file di registro. (C:\Program Files\Duo Security Authentication Proxy\log)

Viene mostrato lo snippet di codice di un log degli errori nel quale ISE rifiuta l'autenticazione primaria:

<#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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).