配置采用EAP和DUO身份验证的AnyConnect Flexvpn

目录

简介

本文档介绍如何为与Cisco IOS® XE路由器的AnyConnect IPSec连接配置外部双因素身份验证。

作者：Sadhana K S和Rishabh Aggarwal Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 在路由器上配置RA VPN的经验
- 身份服务引擎(ISE)管理

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本17.10.01a的Cisco Catalyst 8000V(C8000V)
- Cisco AnyConnect安全移动客户端版本4.10.04071
- 运行版本3.1.0的Cisco ISE

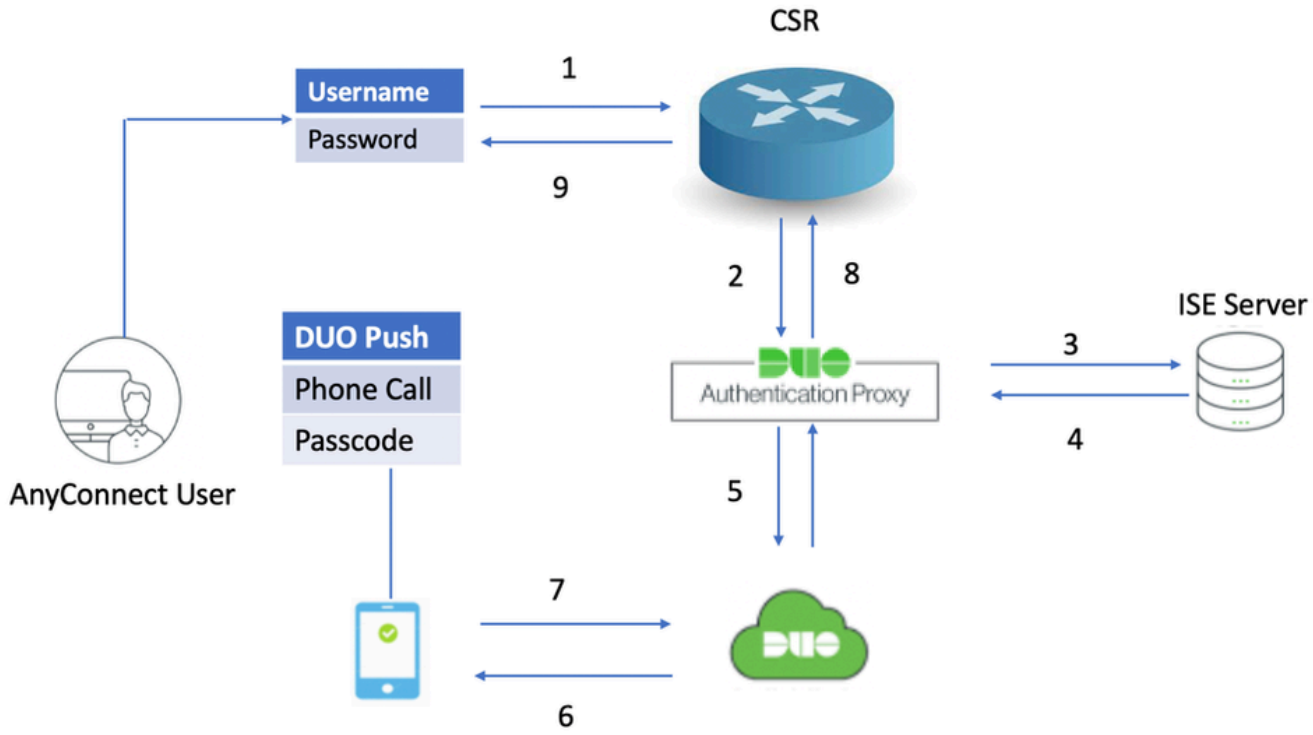
- Duo身份验证代理服务器（windows 10或任何Linux PC）
- Duo Web帐户
- 安装了AnyConnect的客户端PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

身份验证流程

AnyConnect用户使用ISE服务器上的用户名和密码进行身份验证。Duo认证代理服务器还以推送通知的形式向用户的移动设备发送附加认证。

流程图



身份验证流程图

通信过程

1. 用户发起到C8000V的RAVPN连接，并为主要身份验证提供用户名和密码。
2. C8000V向双身份验证代理发送身份验证请求。
3. 然后，Duo Authentication Proxy将主请求发送到Active Directory或RADIUS服务器。
4. 身份验证响应将发送回身份验证代理。
5. 主身份验证成功后，Duo身份验证代理会通过Duo服务器请求辅助身份验证。
6. 然后，Duo服务根据辅助身份验证方法（推送、电话呼叫、密码）对用户进行身份验证。
7. Duo身份验证代理收到身份验证响应。
8. 响应将发送到C8000V。

9. 如果成功，则建立AnyConnect连接。

配置

要完成配置，请考虑以下部分。

C8000V（VPN前端）的配置步骤

1.配置RADIUS服务器。RADIUS服务器的IP地址必须是双身份验证代理的IP。

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

2.将RADIUS服务器配置为本地身份aaa，将授权配置为本地身份。

```
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.创建信任点以安装身份证书（如果本地身份验证中不存在身份证书）。有关证书创建的详细信息，请参阅PKI的证书注册。

```
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.（可选）配置用于拆分隧道的标准访问列表。此访问列表包括可通过VPN隧道访问的目标网络。默认情况下，如果未配置拆分隧道，则所有流量都会通过VPN隧道。

```
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.创建IPv4地址池。

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

在AnyConnect连接成功期间，创建的IP地址池会为AnyConnect客户端分配IPv4地址。

6.配置授权策略。

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

IP池、DNS、拆分隧道列表等在授权策略下指定。

注意：如果未配置自定义IKEv2授权策略，则使用名为“default”的默认授权策略进行授权。在IKEv2授权策略下指定的属性也可以通过RADIUS服务器推送。

7.配置IKEv2建议和策略。

```
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.将AnyConnect客户端配置文件上传到路由器的bootflash并定义配置文件，如下所示：

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

9.禁用HTTP安全服务器。

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

10.配置SSL策略并将路由器的WAN IP指定为下载配置文件的本地地址。

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

           port 443
```

11.配置一个虚拟模板，虚拟访问int克隆接口

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

unnumbered命令从配置的接口(GigabitEthernet1)获取IP地址。

13.配置包含所有连接关系的IKEv2配置文件ed信息。

```
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
```

以下内容用于IKEv2配置文件中：

- match identity remote any — 表示客户端的标识。此处配置了“any”，以便具有正确凭证的任何客户端都可以连接
- authentication remote — 提及EAP协议必须用于客户端身份验证
- authentication local — 提及证书必须用于本地身份验证
- aaa authentication eap — 在EAP身份验证期间，使用RADIUSFlexVPN_auth服务器
- aaa authorization group eap list — 在授权过程中，网络列表 FlexVPN_authz与授权策略一起使用 ikev2-authz-policy
- aaa authorization user eap cached — 启用隐式用户授权
- virtual-template 20 mode auto — 定义要克隆的虚拟模板
- anyconnect profile Client_Profile — 第8步中定义的客户端配置文件应用于此IKEv2配置文件。

14. 配置转换集和IPSec配置文件。

```
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.将IPSec配置文件添加到虚拟模板。

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

客户端配置文件片段（XML配置文件）

在Cisco IOS XE 16.9.1版本之前，不能从头端自动下载配置文件。在16.9.1之后，可以从头端下载配置文件。

<#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

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>
```

DUO身份验证代理的配置步骤

注意：Duo身份验证代理仅支持使用RADIUS身份验证的MS-CHAPv2。

步骤1.下载并安装Duo Authentication Proxy Server。

登录到Windows计算机并安装Duo身份验证代理服务器。

建议使用至少具有1个CPU、200 MB磁盘空间和4 GB RAM的系统。

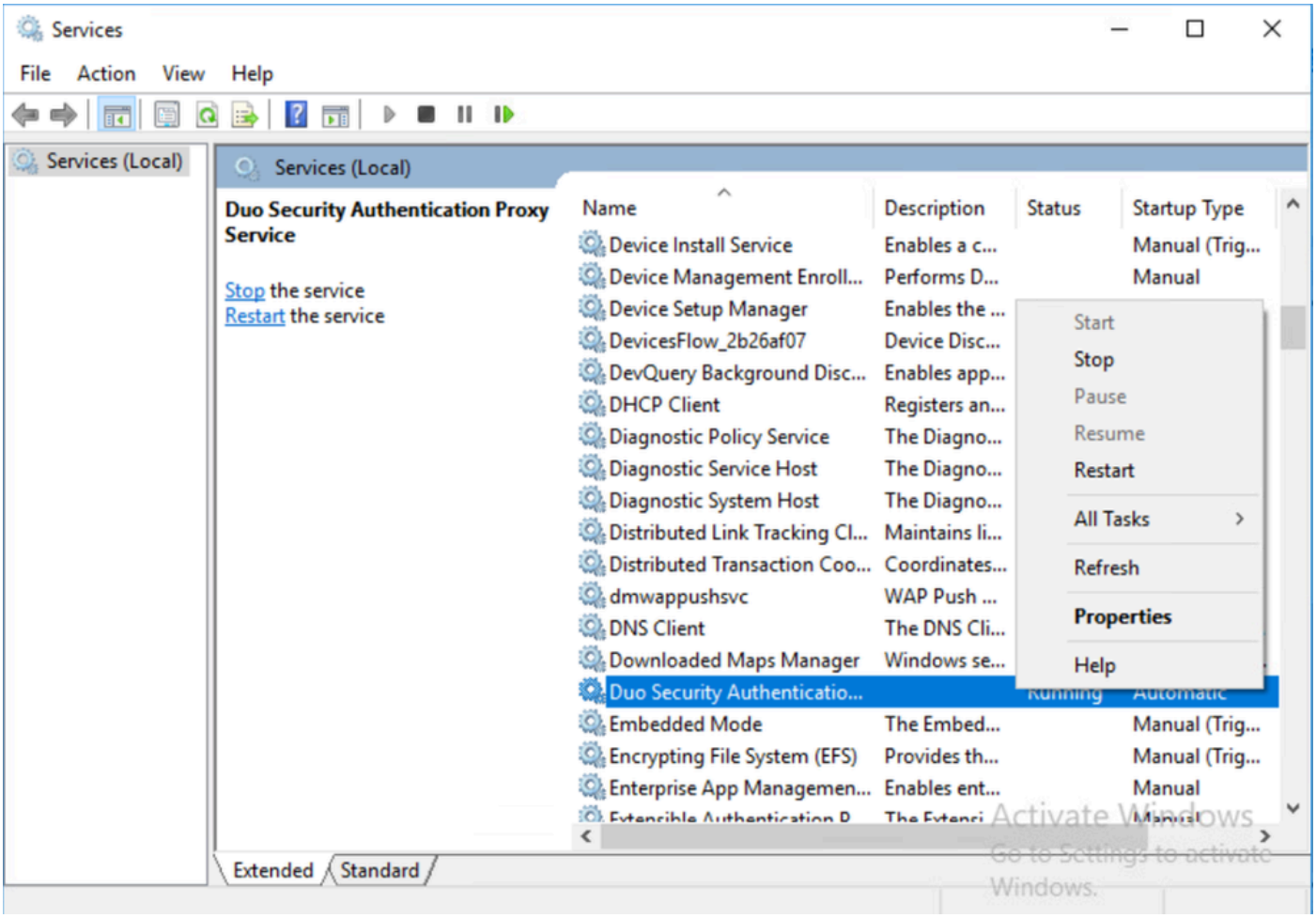
步骤2.导航至C:\Program Files\Duo Security Authentication Proxy\conf\，打开authproxy.cfg，以便使用适当的详细信息配置身份验证代理。

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

注意：此处的“10.197.243.116”是ISE服务器的IP地址，“cisco”是配置的密码以验证主要身份验证。

完成这些更改后，请保存文件。

步骤3.打开Windows服务控制台(services.msc)。 然后重启Duo Security Authentication Proxy Service。

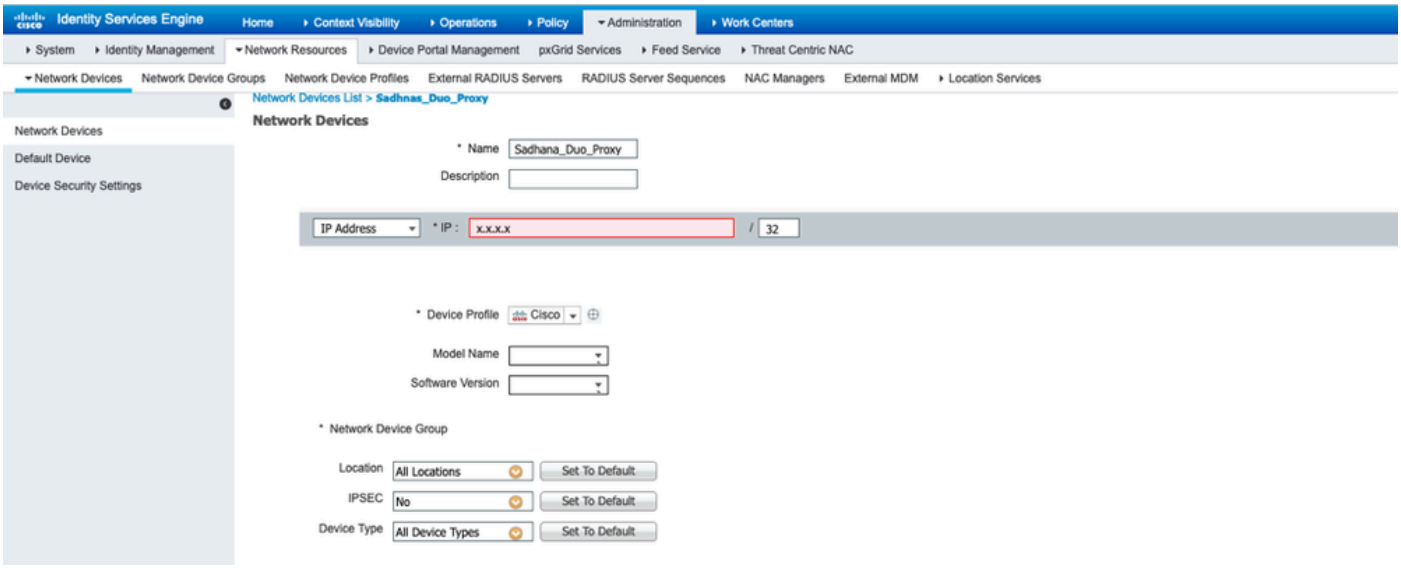


Duo安全身份验证代理服务

ISE的配置步骤

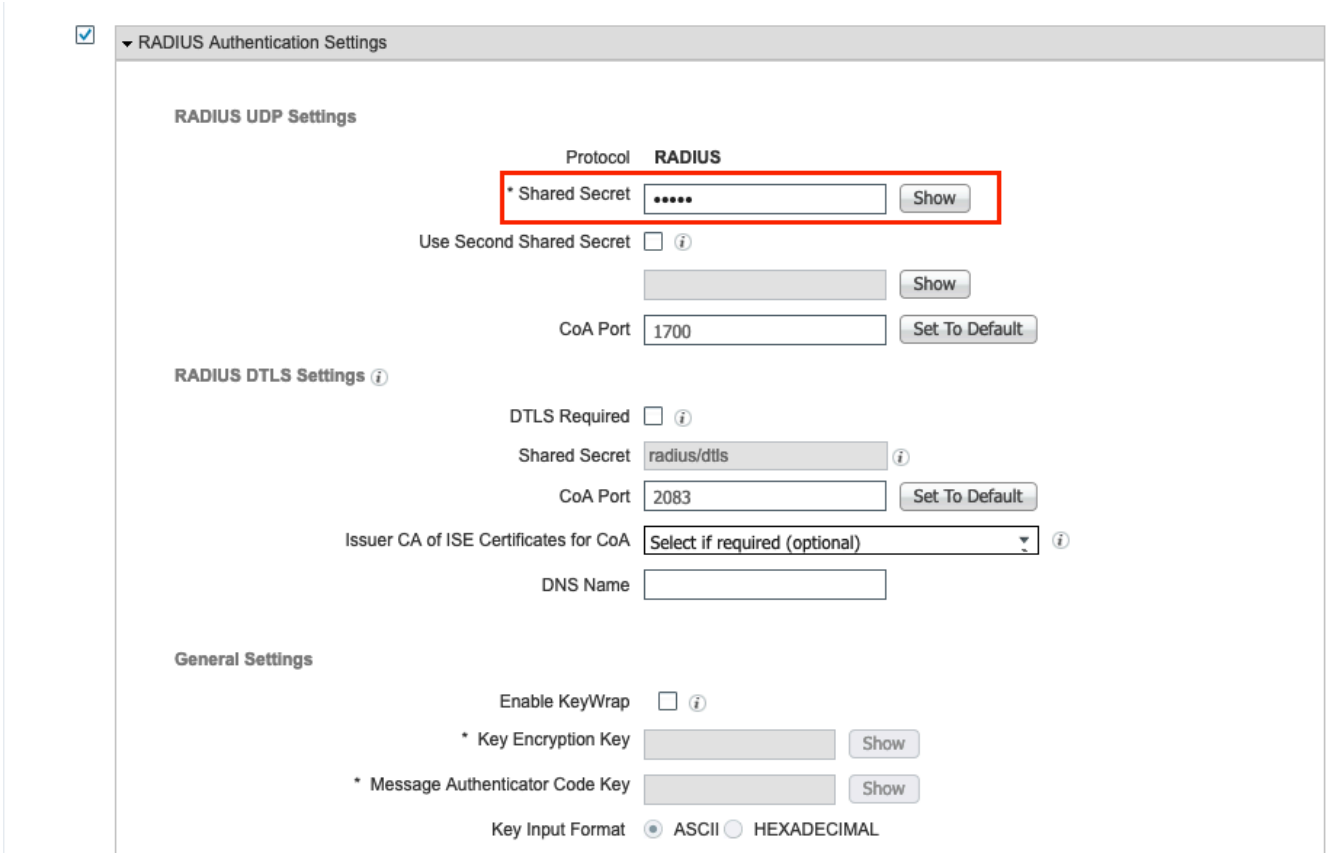
步骤1.导航到**Administration > Network Devices**，然后单击Add以配置网络设备。

注意：用x.x.x.xDuo身份验证代理服务器的IP地址替换。



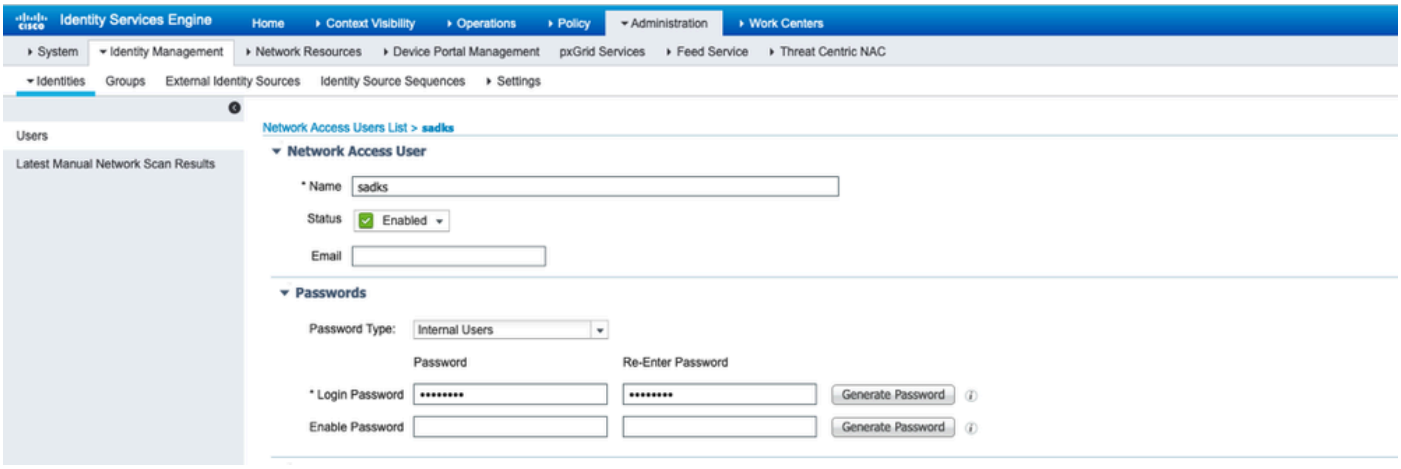
ISE — 网络设备

步骤2.按照中Shared Secret所述配置authproxy.cfgsecret：



ISE — 共享密钥

步骤3.导航至Administration > Identities > Users。选择Add以配置AnyConnect主身份验证的身份用户：

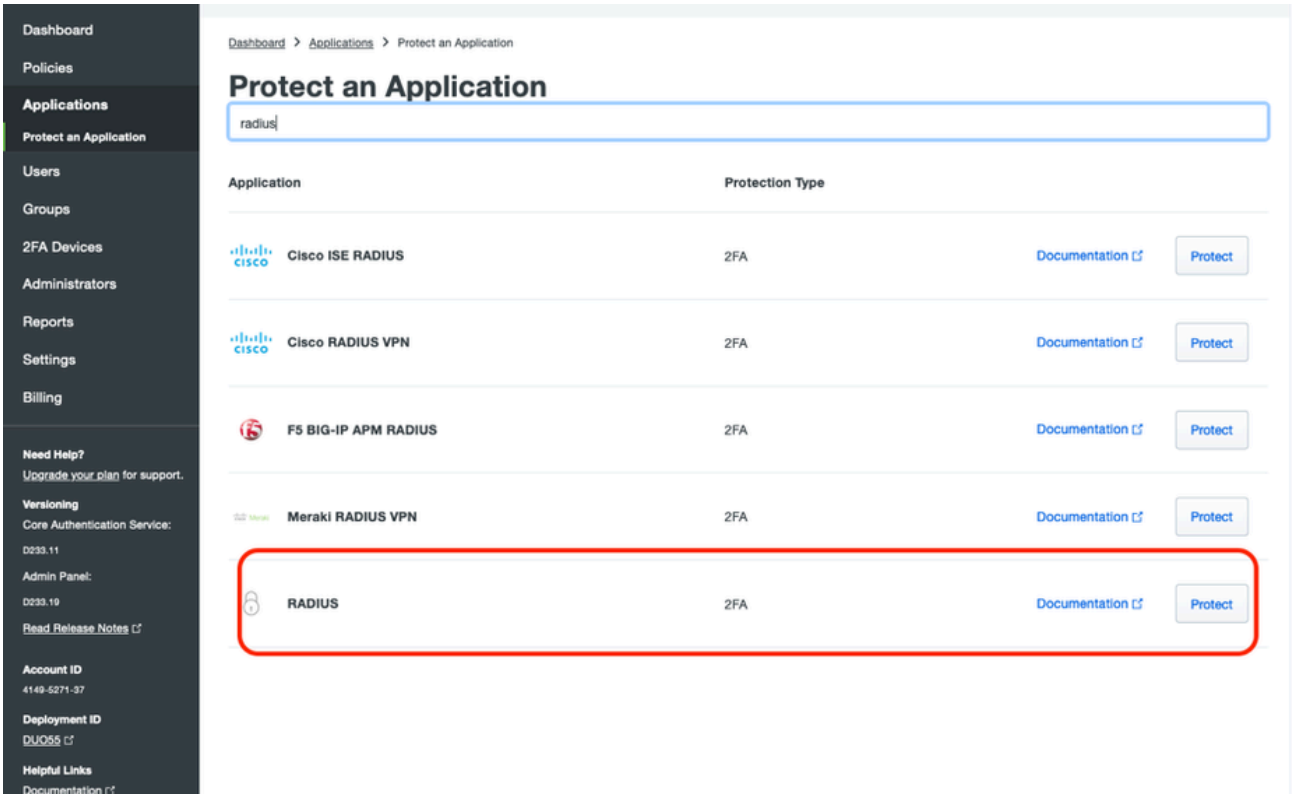


ISE — 用户

DUO管理门户的配置步骤

步骤1.登录您的Duo帐户。

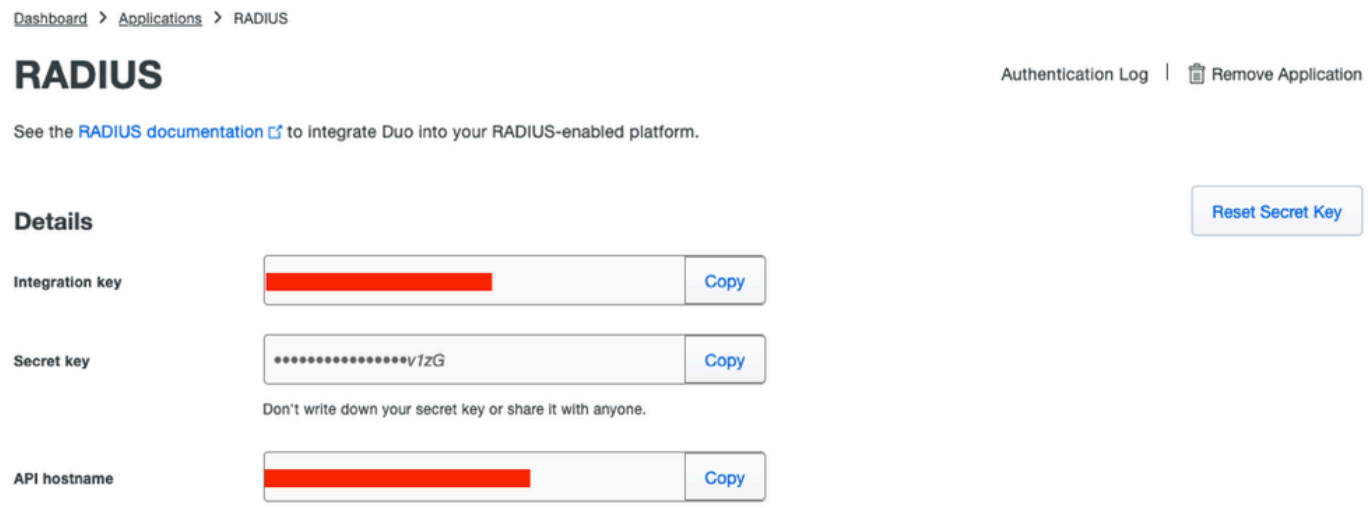
导航至Applications > Protect an Application。单击Protect，查看要使用的应用程序。（本例中为RADIUS）



DUO — 应用程序

步骤2.点击Protect，查找要使用的应用程序。（本例中为RADIUS）

复制集成密钥、密钥和API主机名，并将其粘贴到Duoauthproxy.cfg身份验证代理上。



双核 — RADIUS

复制这些值并导航回DUO身份验证代理，然后打开 authproxy.cfg并粘贴值，如下所示：

集成密钥= ikey

secret key = skey

API主机名= 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
```

注意：配置服务器时，必须从Duo服务器复制ikey、skey和api_host，并且“10.106.54.143”是C8000V路由器的IP地址，而“cisco”是在radius服务器配置下在路由器上配置的密钥。

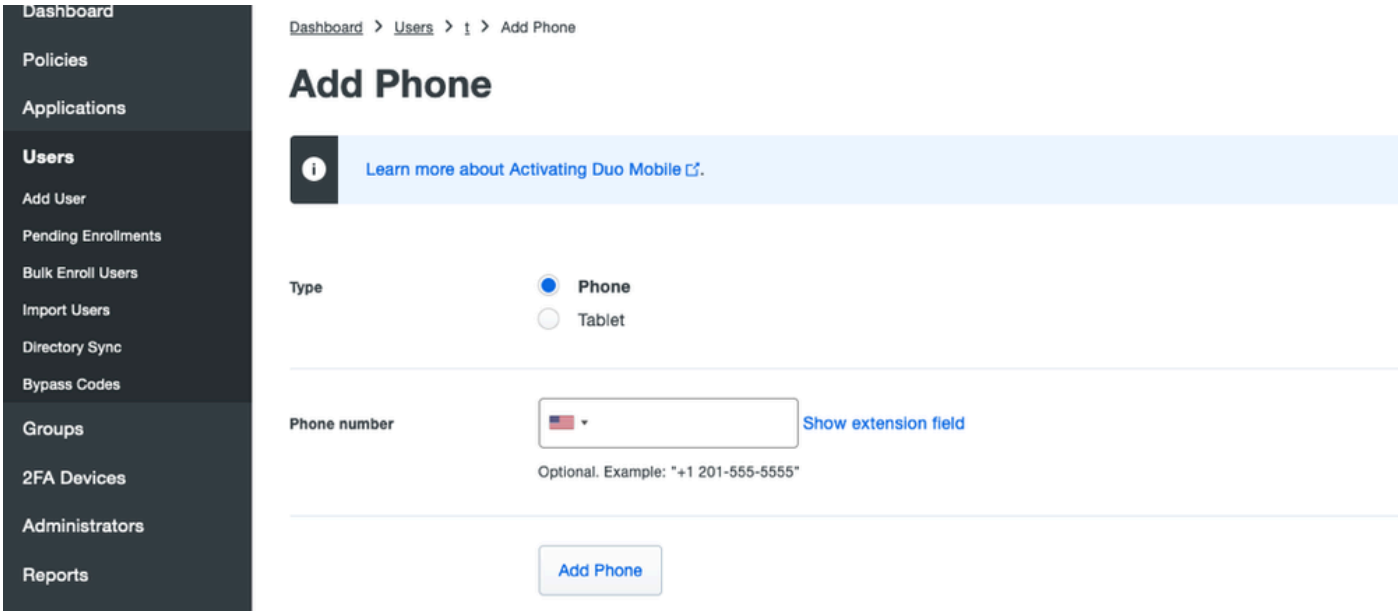
完成这些更改后，请再次保存文件并重新启动Duo Security Authentication Proxy Service(inservices.msc)。

步骤3.在DUO上创建用户以进行辅助身份验证。

导航到Users > Add User并键入用户名。

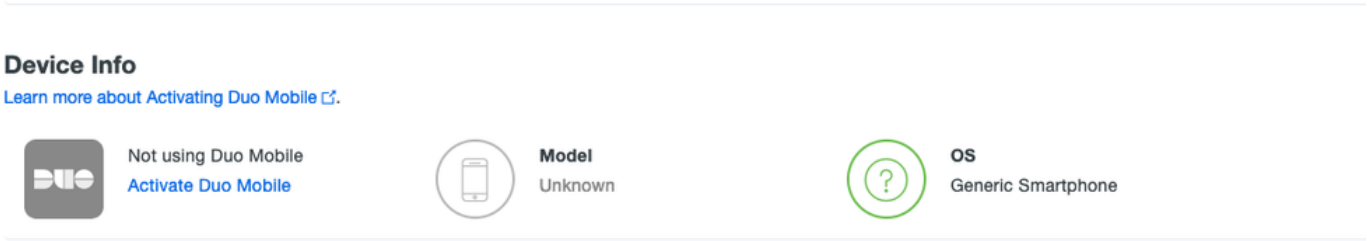
注意：用户名必须与主要身份验证用户名匹配。

单击。Add User创建后，在Phones下，单击Add Phone，输入电话号码，然后单击Add Phone。



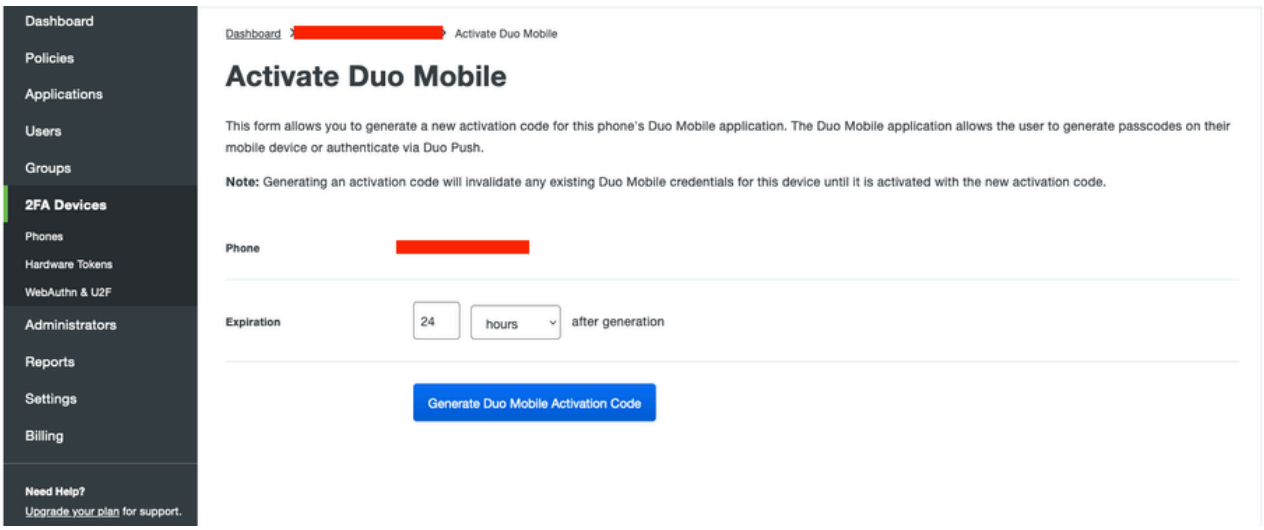
DUO — 添加电话

选择身份验证类型。



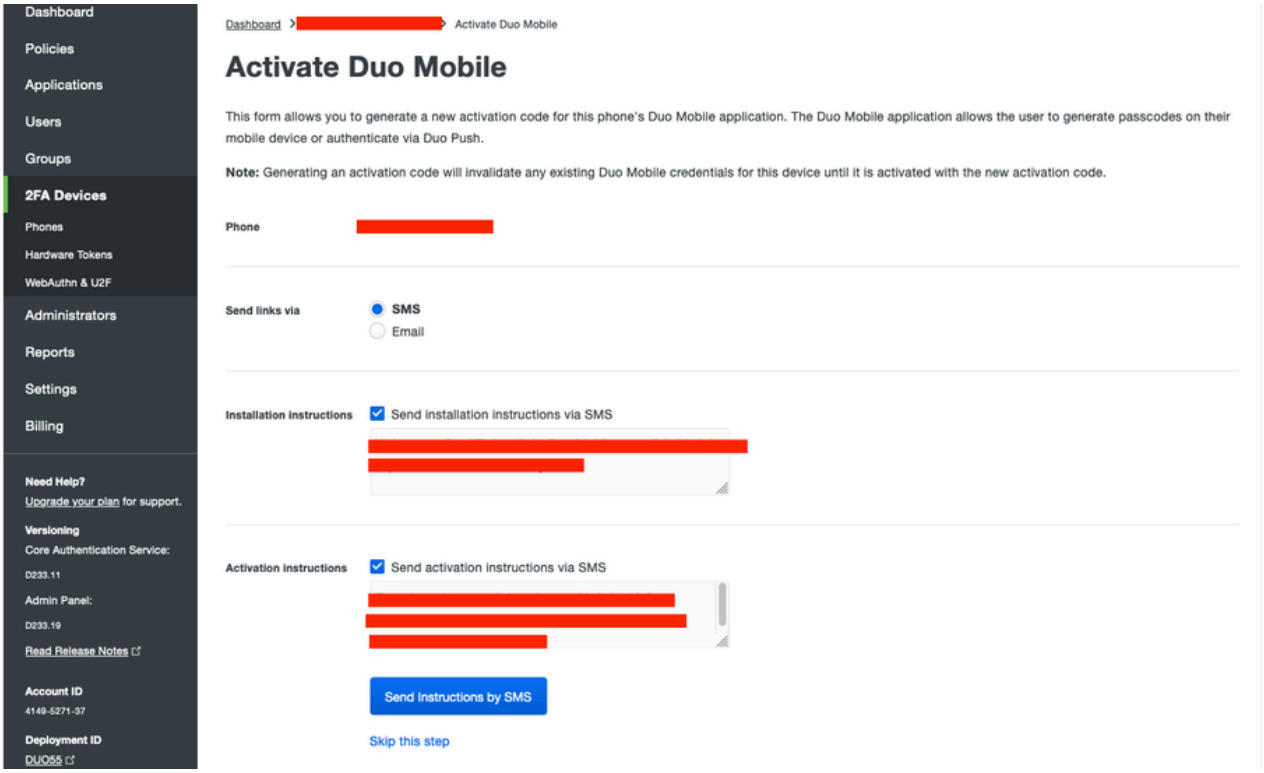
DUO — 设备信息

选择 。Generate Duo Mobile Activation Code



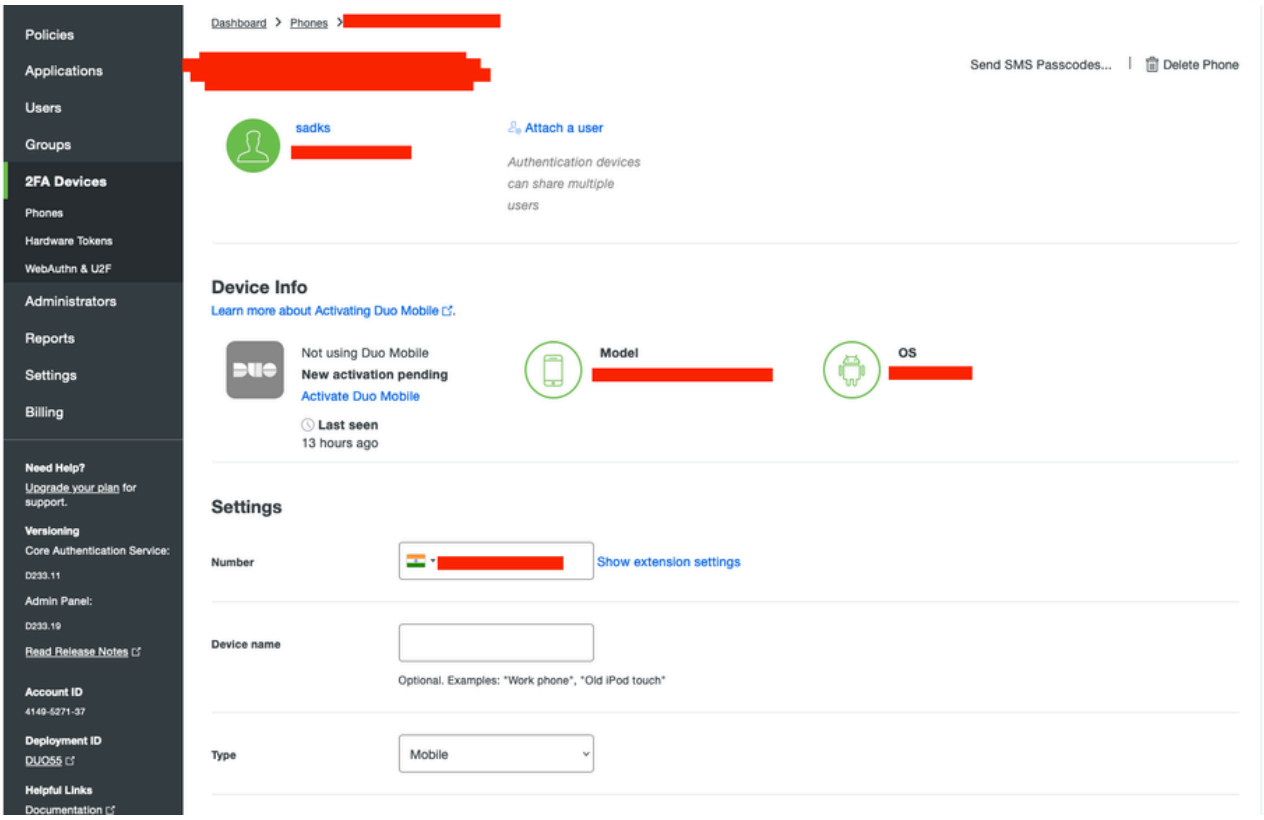
DUO — 电话激活

选择 Send Instructions by SMS.



DUO — 发送SMS

单击发送到电话的链接，DUO应用将链接到部分中的用户帐户Device Info，如图所示：

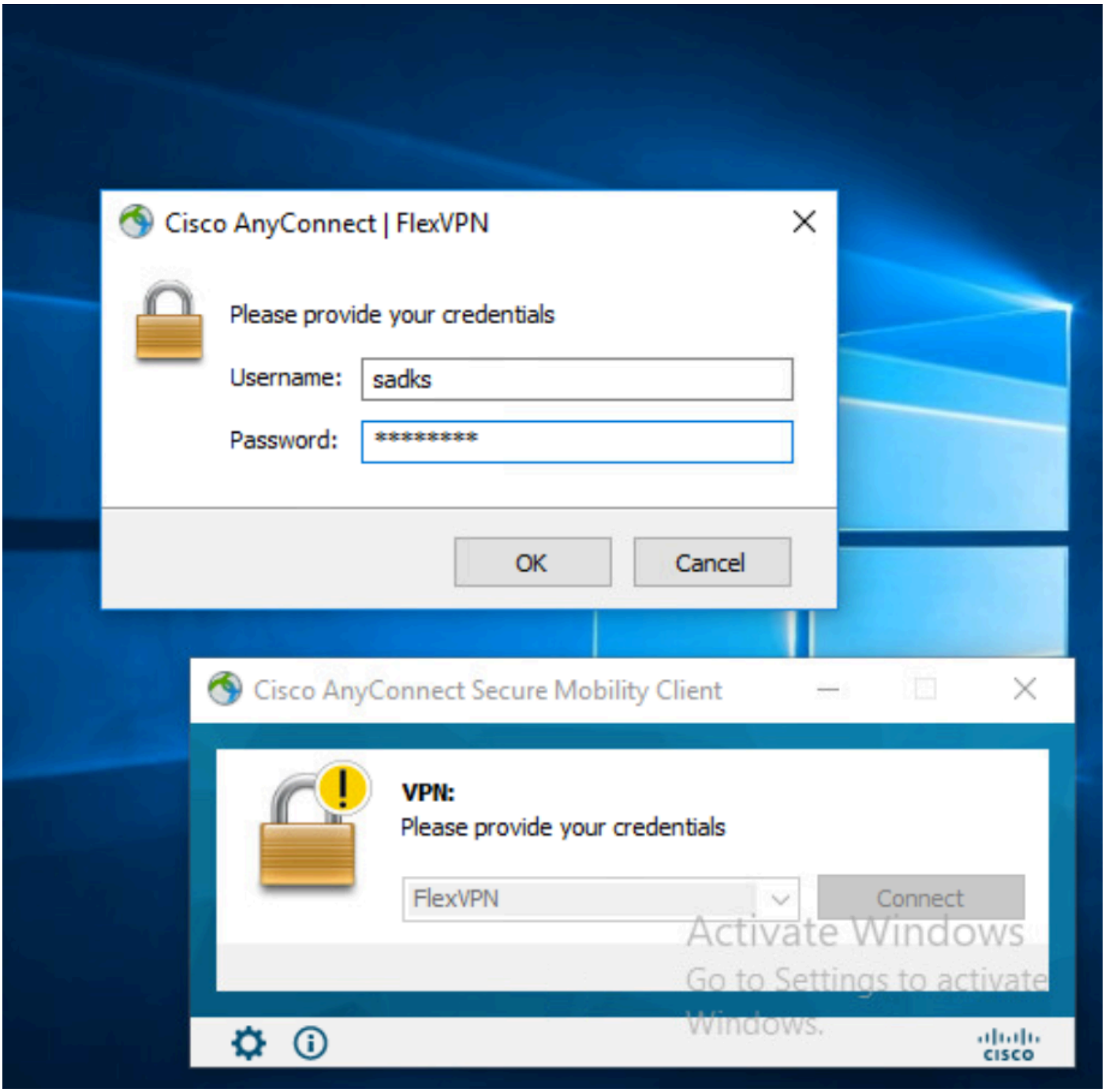


DUO — 设备已链接

验证

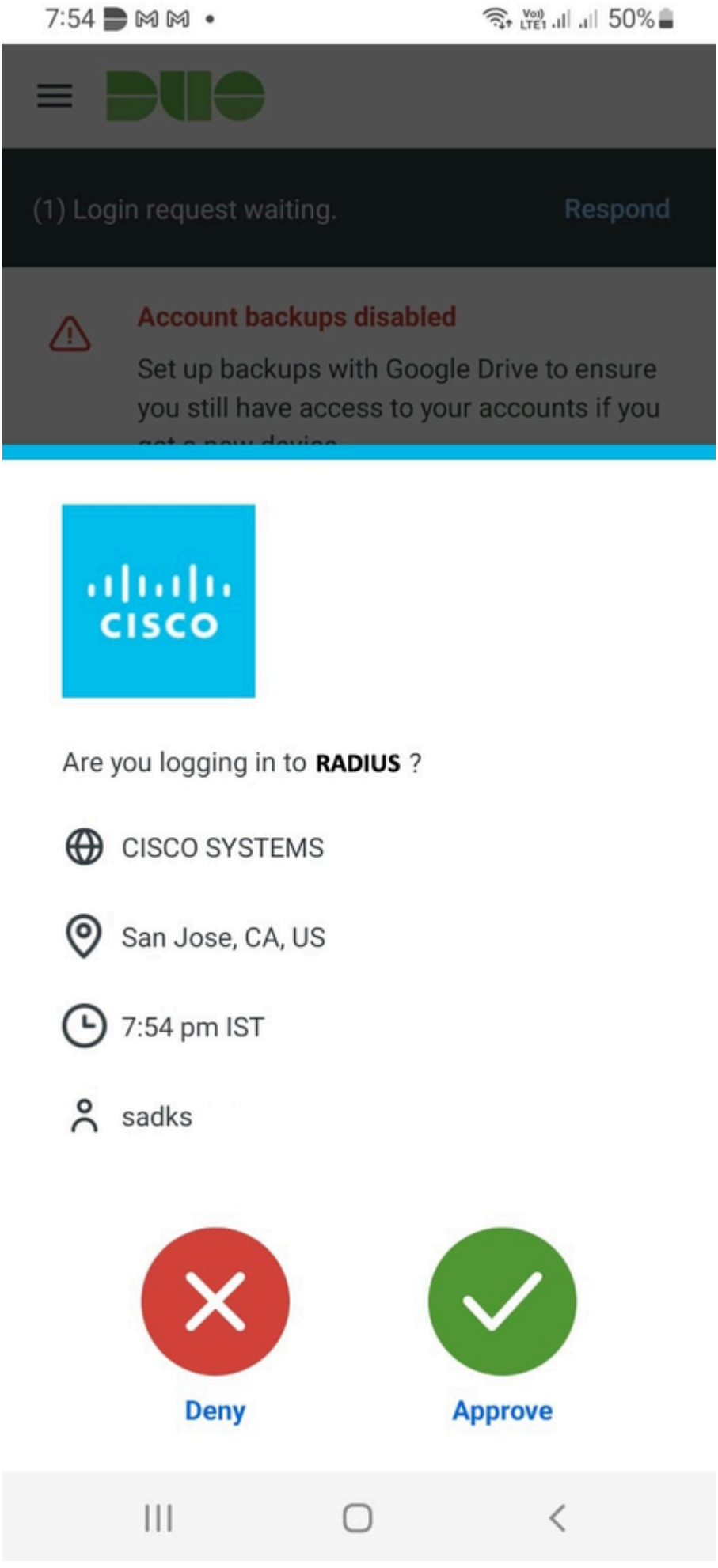
为了测试身份验证，请通过AnyConnect从用户的PC连接到C8000V。

键入用于主要身份验证的用户名和密码。



AnyConnect连接

然后，接受DUO按移动电话。



DUO Push

连接已建立

<#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

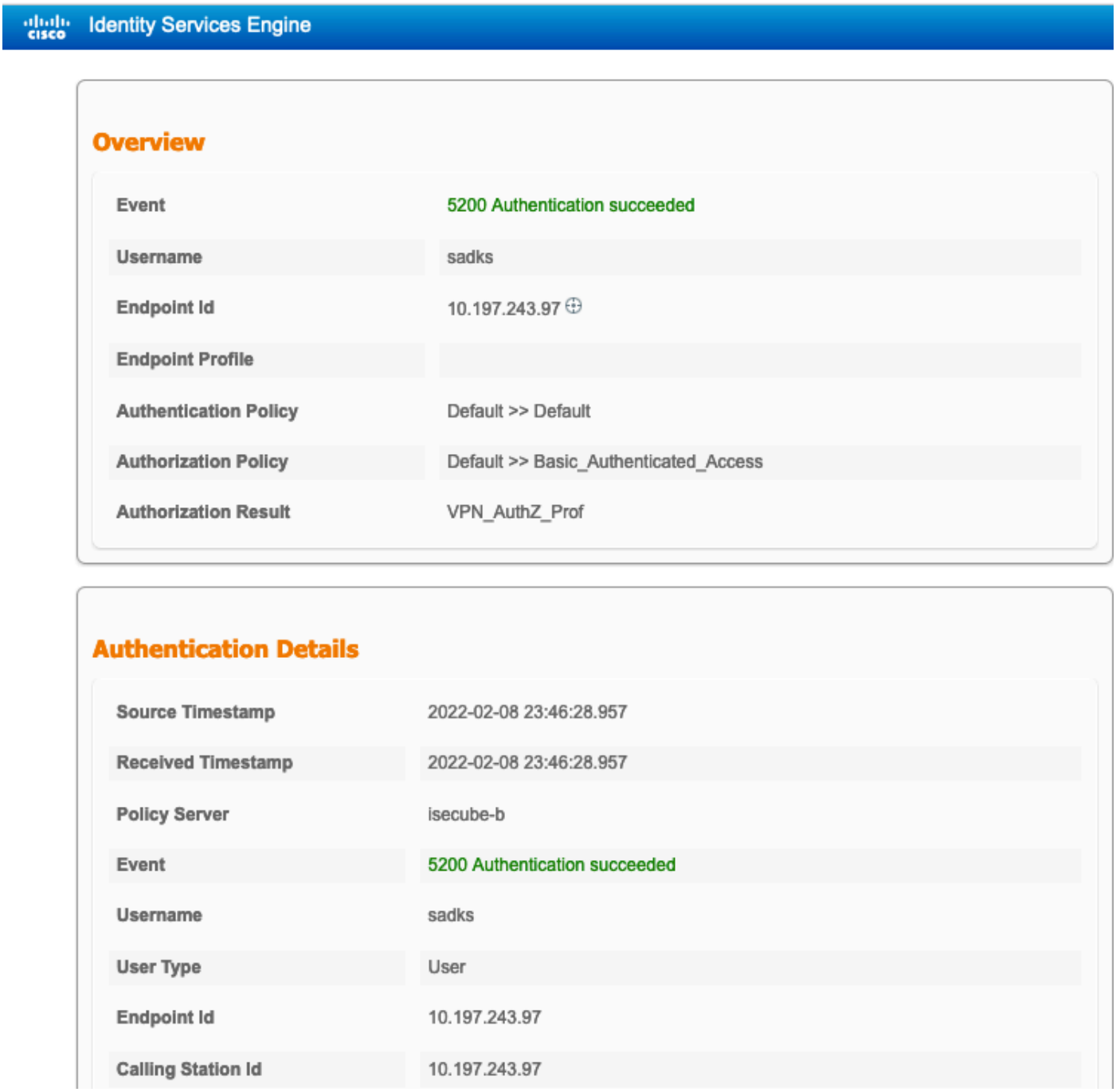
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0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

在ISE中导航至Operations > Live Logs。您可以查看主要身份验证的身份验证报告。



ISE — 实时日志

4. Verification on DUO authentication proxy

导航至DUO Authentication Proxy上的此文件； 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
```

故障排除

1. C8000V上的调试。

对于IKEv2:

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

对于IPSec:

- debug crypto ipsec
- debug crypto ipsec error

2.对于DUO身份验证代理，请检查与代理相关的日志文件。() ()C:\Program Files\Duo Security Authentication Proxy\log

显示ISE拒绝主要身份验证的错误日志代码段：

<#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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。