EAPおよびDUO認証を使用したAnyConnect Flexvpnの設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

認証フロー

- フロー図
- 通信プロセス

設定

- C8000V（VPNヘッドエンド）の設定手順
  - クライアントプロファイルのスニペット（XMLプロファイル）
- DUO認証プロキシの設定手順
- ISEでの設定手順
- DUO Administration Portalの設定手順

確認

トラブルシュート

はじめに

このドキュメントでは、Cisco IOS® XEルータへのAnyConnect IPSec接続の外部2要素認証を設定する方法について説明します。

著者：Cisco TACエンジニア、Sadhana K S、Rishabh Aggarwal

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ルータでのRA VPN設定の経験
- Identity Services Engine(ISE)の管理

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン17.10.01aを実行するCisco Catalyst 8000V(C8000V)
- Cisco AnyConnectセキュアモビリティクライアントバージョン4.10.04071

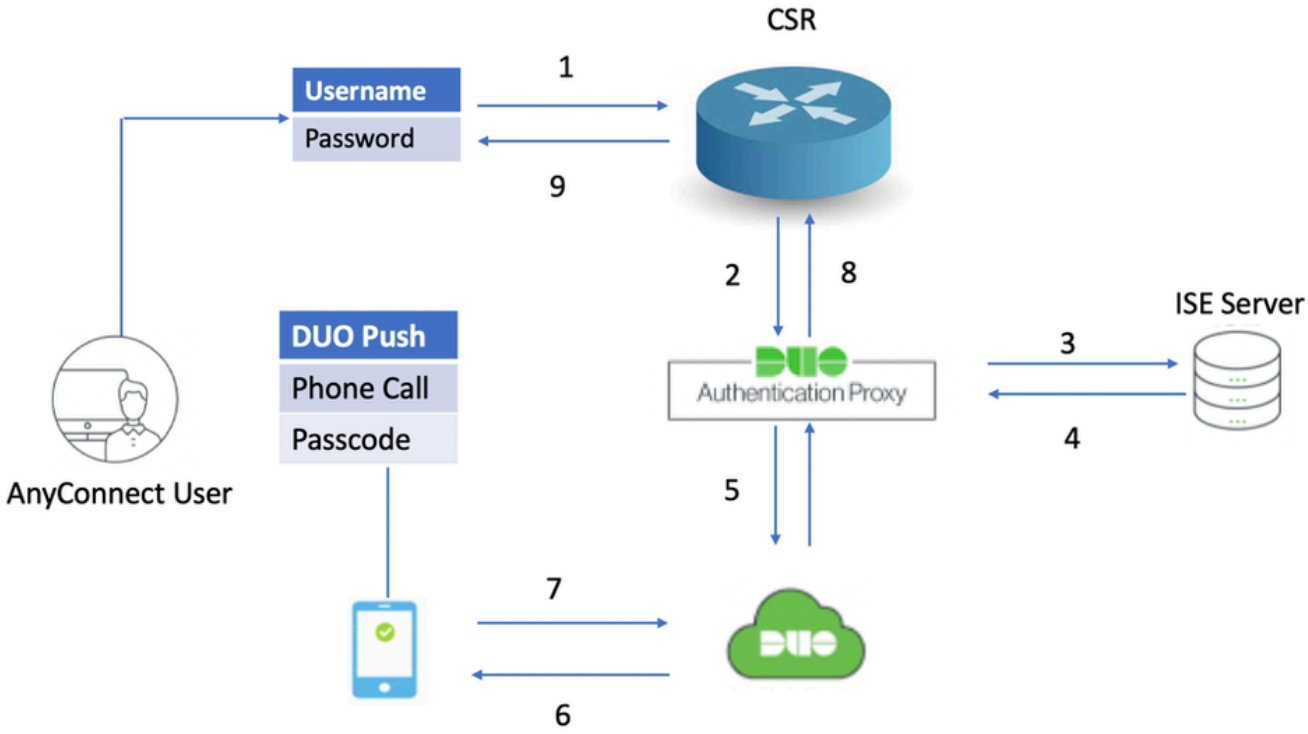
- バージョン3.1.0を実行しているCisco ISE
- Duo認証プロキシサーバ（Windows 10または任意のLinux PC）
- Duo Webアカウント
- AnyConnectがインストールされたクライアントPC

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

認証フロー

AnyConnectユーザは、ISEサーバでユーザ名とパスワードを使用して認証されます。また、Duo Authentication Proxyサーバは、ユーザのモバイルデバイスにプッシュ通知の形式で追加の認証を送信します。

フロー図



認証フロー図

通信プロセス

1. ユーザがC8000VへのRAVPN接続を開始し、プライマリ認証用のユーザ名とパスワードを入力します。
2. C8000Vは、Duo認証プロキシに認証要求を送信します。
3. 次に、Duo Authentication Proxyはプライマリ要求をActive DirectoryまたはRADIUSサーバに

送信します。
4. 認証応答が認証プロキシに返信されます。
5. プライマリ認証が成功すると、Duo認証プロキシはDuoサーバを介してセカンダリ認証を要求します。
6. 次に、Duoサービスは、セカンダリ認証方式（プッシュ、電話、パスコード）に応じてユーザを認証します。
7. Duo認証プロキシが認証応答を受信します。
8. 応答がC8000Vに送信されます。
9. 成功すると、AnyConnect接続が確立されます。

設定

設定を完了するには、次のセクションを考慮してください。

C8000V（VPNヘッドエンド）の設定手順

1. RADIUSサーバーを構成します。RADIUSサーバのIPアドレスは、Duo認証プロキシのIPである必要があります。

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

2. RADIUSサーバをaaa認証として、認可をローカルとして設定します。

```
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. ローカル認証用のID証明書がない場合は、インストールするトラストポイントを作成します。証明書の作成の詳細については、『PKIの証明書の登録』を参照してください。

```
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.（オプション）スプリットトンネルに使用する標準アクセスリストを設定します。このアクセスリストは、VPNトンネルを介してアクセス可能な宛先ネットワークで構成されます。スプリットトンネルが設定されていない場合、デフォルトでは、すべてのトラフィックはVPNトンネルを通過します。

```
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. IPv4アドレスプールを作成します。

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

作成されたIPアドレスプールは、AnyConnect接続が成功した際に、AnyConnectクライアントにIPv4アドレスを割り当てます。

6. 許可ポリシーを設定します。

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

IPプール、DNS、スプリットトンネルリストなどは、認可ポリシーで指定されます。

注：カスタムIKEv2認可ポリシーが設定されていない場合、認可には「default」と呼ばれるデフォルトの認可ポリシーが使用されます。IKEv2許可ポリシーで指定された属性は、RADIUSサーバ経由でプッシュすることもできます。

---

7. IKEv2プロポーザルとポリシーを設定します。

```
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. AnyConnectクライアントプロファイルをルータのブートフラッシュにアップロードし、次のようにプロファイルを定義します。

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

9. HTTPセキュアサーバを無効にします。

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

10. SSLポリシーを設定し、プロファイルをダウンロードするためのローカルアドレスとしてルータのWAN IPを指定します。

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

           port 443
```

11. バーチャルアクセスインターフェイスの起点となるバーチャルテンプレートをクローンが作成される

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

unnumberedコマンドは、設定されたインターフェイス(GigabitEthernet1)からIPアドレスを取得します。

13. すべての接続関連情報を含むIKEv2プロファイルを設定します。ed情報。

```
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
```

これらはIKEv2プロファイルで使用されます。

- match identity remote any：クライアントのIDを参照します。適切なクレデンシャルを持つすべてのクライアントが接続できるように、「any」を設定します
- authentication remote：クライアント認証にEAPプロトコルを使用する必要があることを示します
- authentication local：ローカル認証に証明書を使用する必要があることを示します
- aaa authentication eap:EAP認証中に、RADIUSサーバFlexVPN_authが使用されます
- aaa authorization group eap list：認可中、ネットワークリストはFlexVPN_authzは、認可ポリシーikev2-authz-policy
- aaa authorization user eap cached:暗黙的なユーザ認証を有効にします。
- virtual-template 20 mode auto：クローニングする仮想テンプレートを定義します
- anyconnect profile Client_Profile：ステップ8で定義したクライアントプロファイルが、このIKEv2プロファイルに適用されます

14 . トランスフォームセットとIPSecプロファイルを設定します。

```
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. IPSecプロファイルを仮想テンプレートに追加します。

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

クライアントプロファイルのスニペット（XMLプロファイル）

Cisco IOS XE 16.9.1より前のリリースでは、ヘッドエンドからのプロファイルの自動ダウンロードは使用できません。16.9.1以降では、ヘッドエンドからプロファイルをダウンロードできます。

<#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>
```

DUO認証プロキシの設定手順

注:Duo Authentication Proxyは、RADIUS認証でのみMS-CHAPv2をサポートします。

ステップ 1：Duo Authentication Proxy Serverをダウンロードしてインストールします。

Windowsマシンにログインし、Duo Authentication Proxyサーバをインストールします。

1つ以上のCPU、200 MBのディスク領域、および4 GBのRAMを搭載したシステムを使用することをお勧めします。

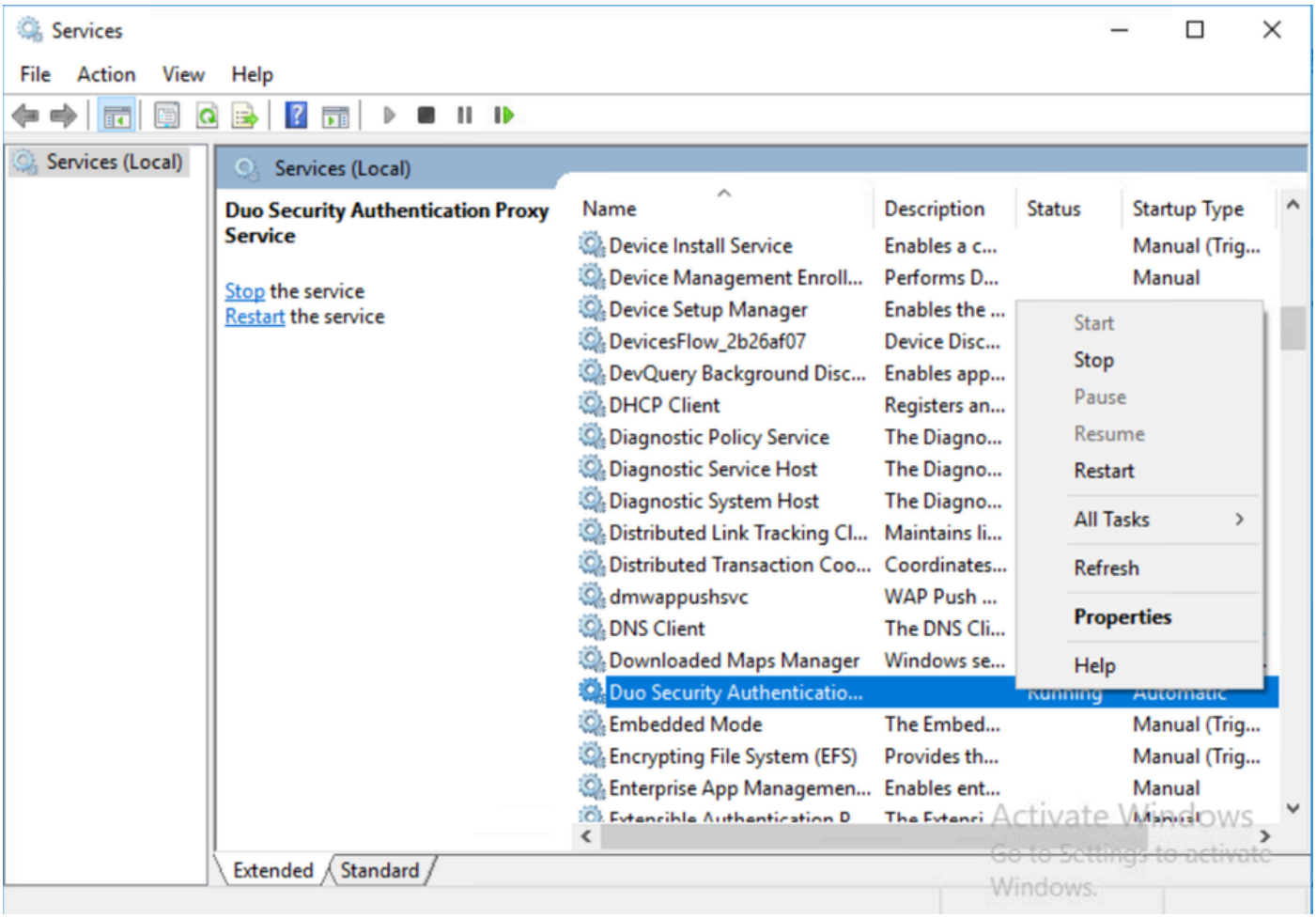
ステップ 2：C:\Program Files\Duo Security Authentication Proxy\conf\に移動し、authproxy.cfgを開いて、認証プロキシに適切な詳細情報を設定します。

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

注：ここで、「10.197.243.116」はISEサーバのIPアドレスで、「cisco」はプライマリ認証を検証するために設定されたパスワードです。

これらの変更を行ったら、ファイルを保存します。

ステップ 3：Windowsサービスコンソール(services.msc)を開きます。 Duo Security Authentication Proxy Serviceを再起動します。

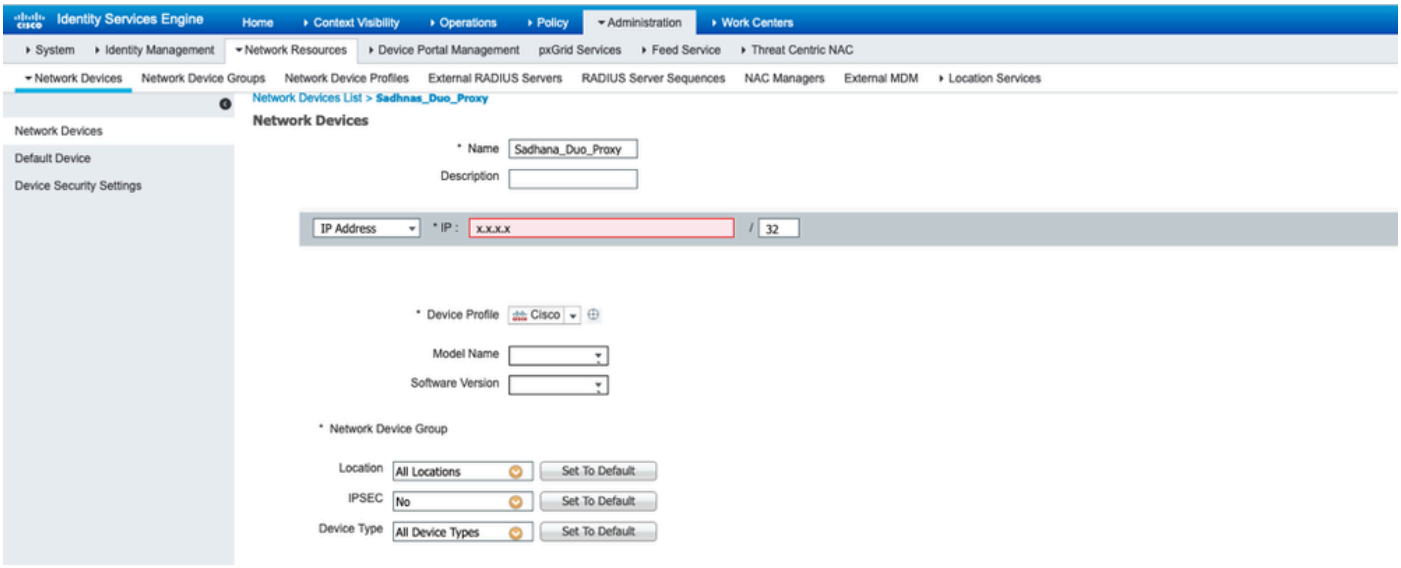


Duoセキュリティ認証プロキシサービス

ISEでの設定手順

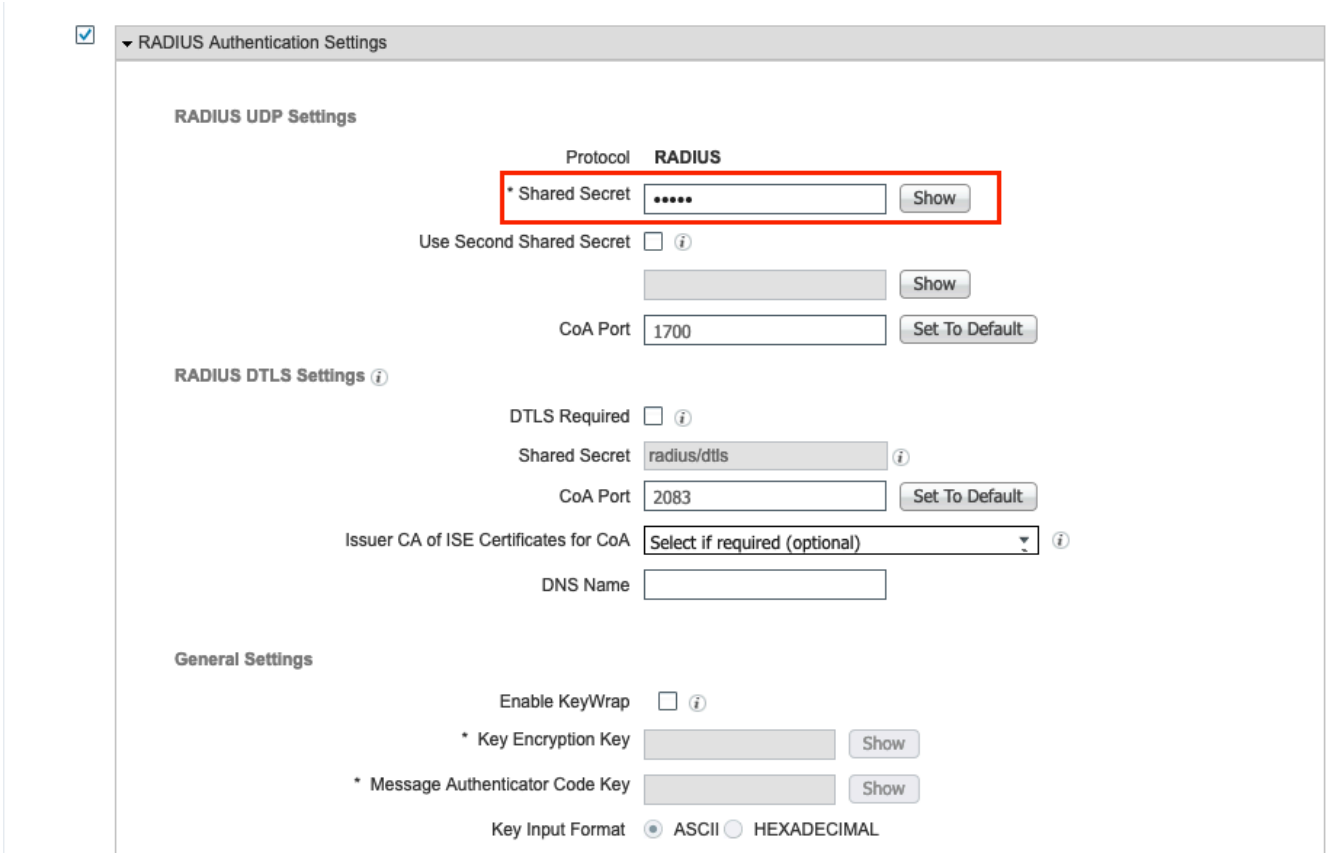
ステップ 1：ネットワークデバイスを設定するには、**Administration** > **Network Devices**に移動し、Addをクリックします。

注:x.x.x.xの部分は、使用しているDuo認証プロキシサーバのIPアドレスに置き換えてください。



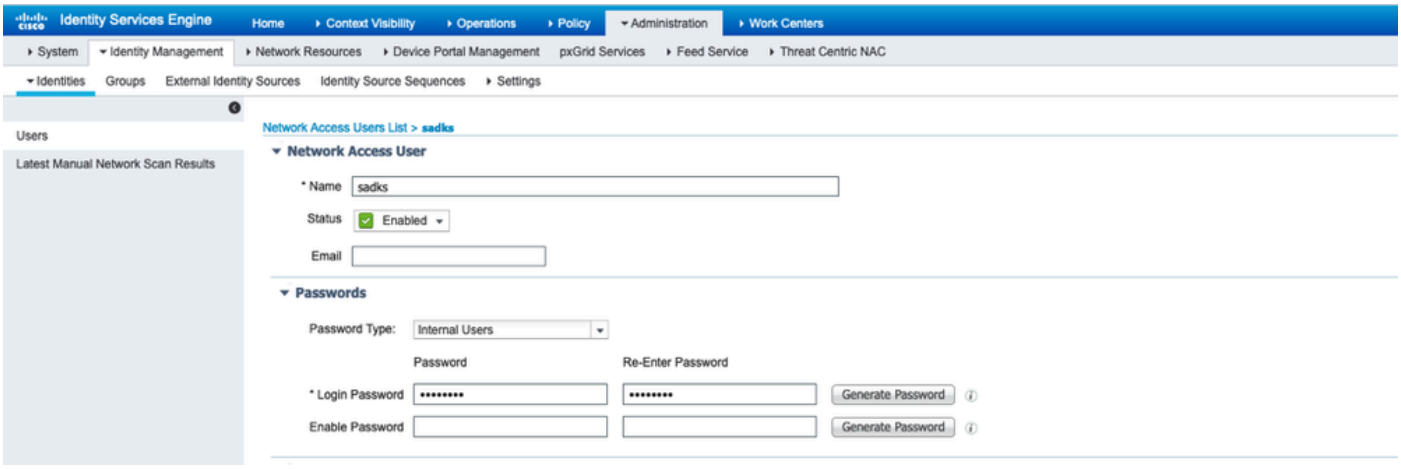
ISE:Network Devices（ネットワークデバイス）

ステップ 2：authproxy.cfgの「secret」で説明されているように、共有秘密を設定します。



ISE:Shared Secret（共有秘密）

ステップ 3：Administration > Identities > Usersの順に移動します。Addを選択して、AnyConnectプライマリ認証用のIDユーザを設定します。

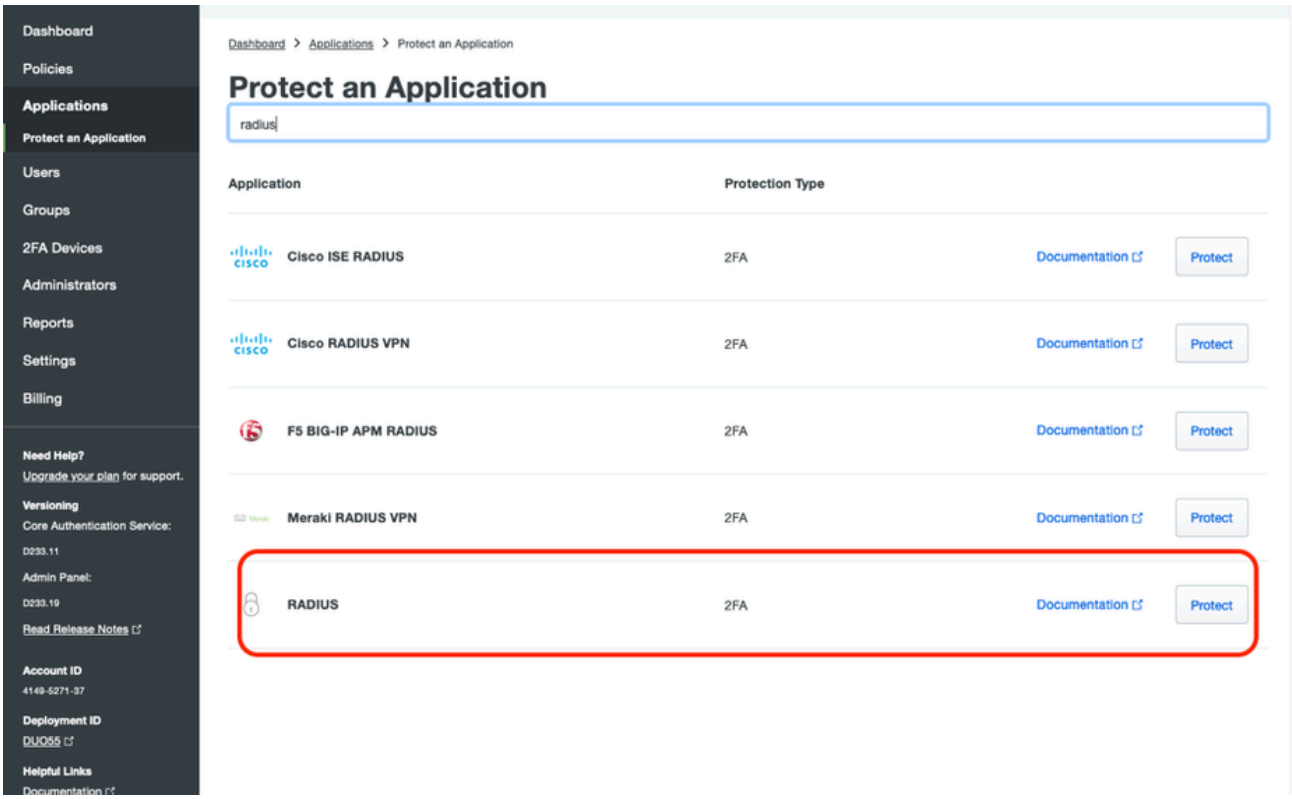


ISE – ユーザ

DUO Administration Portalの設定手順

ステップ 1：Duoアカウントにログインします。

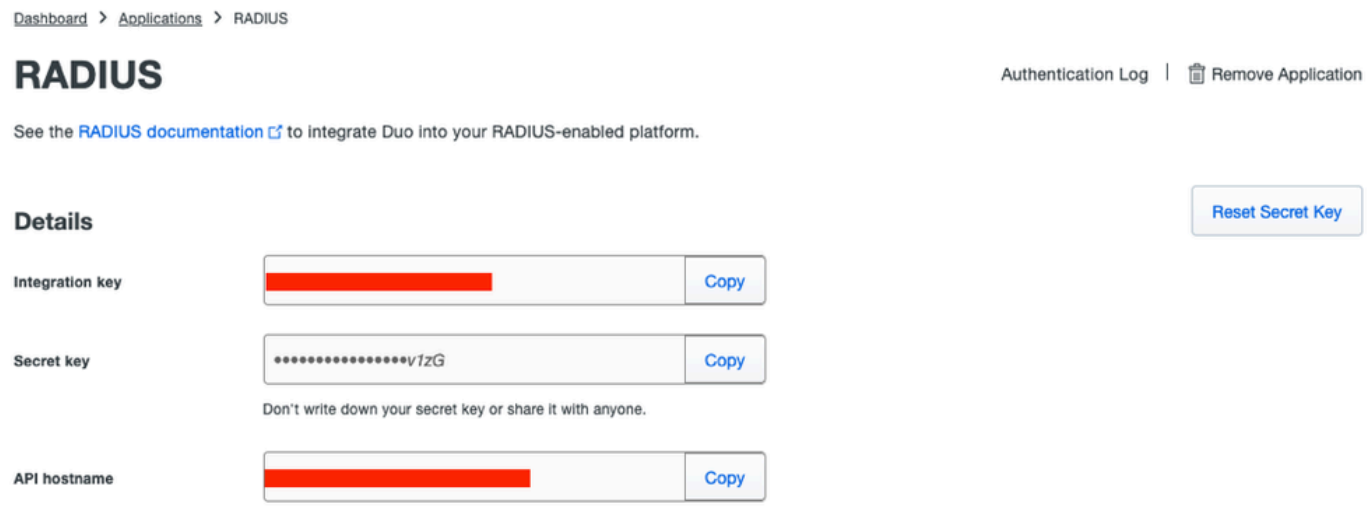
Applications > Protect an Applicationの順に移動します。使用するアプリケーションのProtectをクリックします。（この場合は半径）



DUO – アプリケーション

ステップ 2：使用するアプリケーションのProtectをクリックします。（この場合は半径）

統合キー、秘密キー、およびAPIホスト名をコピーして、Duo認証プロキシのauthproxy.cfgofに貼り付けます。



DUO – 半径

これらの値をコピーして、DUO認証プロキシに戻り、 authproxy.cfg (認証プロファイル) をクリックし、次に示すように値を貼り付けます。

統合キー= ikey

秘密鍵= skey

APIホスト名= 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：サーバを設定する際には、ikey、skey、api_hostをDuoサーバからコピーする必要があります。「10.106.54.143」はC8000Vルータの IPアドレスで、「cisco」はRADIUSサーバ設定でルータに設定されているキーです。

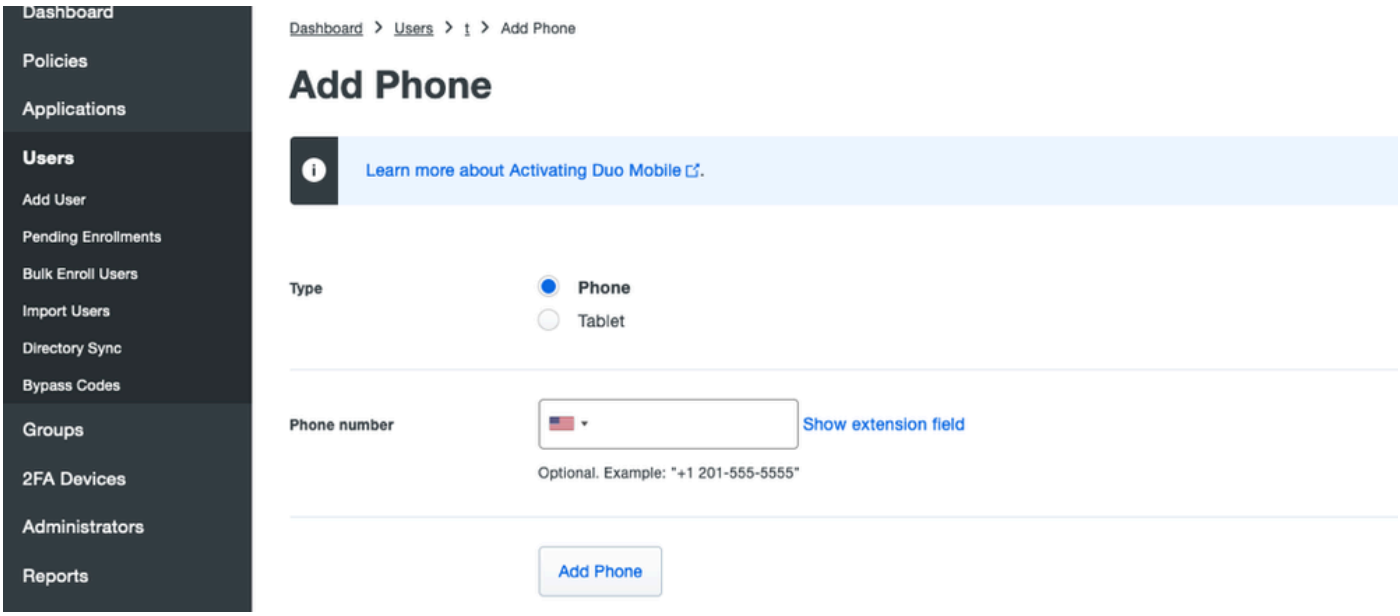
これらの変更を行ったら、ファイルを再度保存し、Duo Security Authentication Proxy Service(services.msc)を再起動します。

ステップ 3：セカンダリ認証用のユーザをDUOで作成します。

Users > Add Userの順に移動し、ユーザ名を入力します。

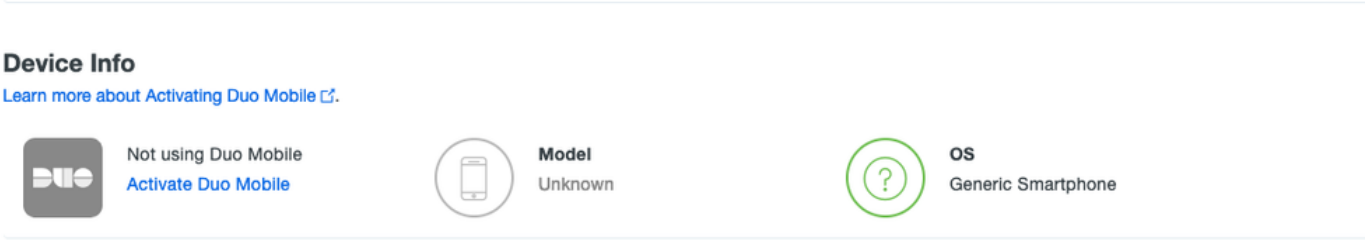
注：ユーザ名はプライマリ認証のユーザ名と一致している必要があります。

Add Userをクリックします。作成したら、Phonesの下で、Add Phoneをクリックし、電話番号を入力して、Add Phoneをクリックします。



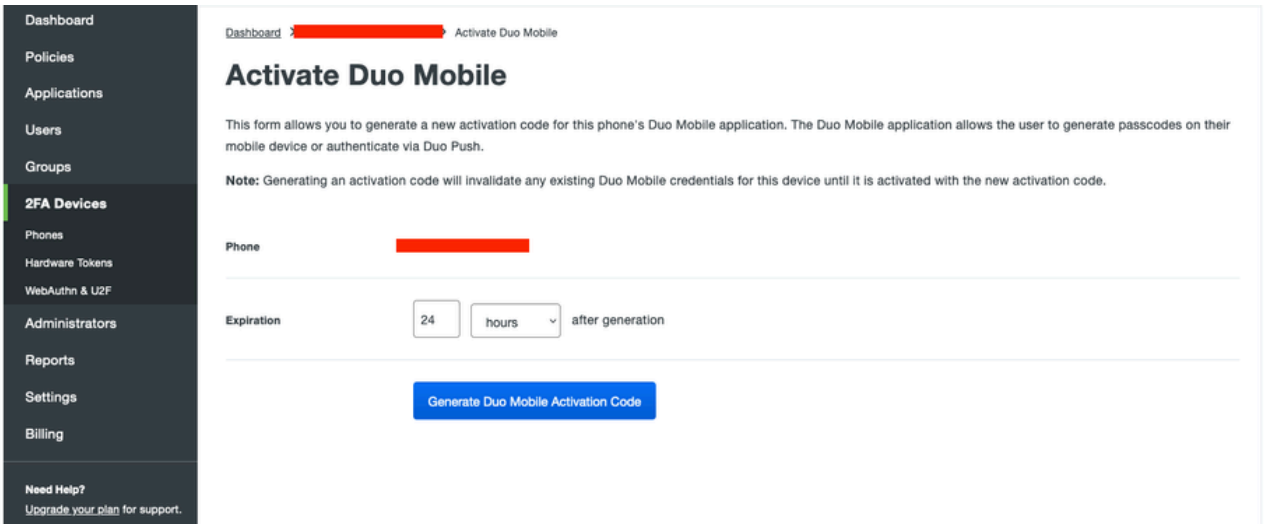
DUO – 電話の追加

認証のタイプを選択します。



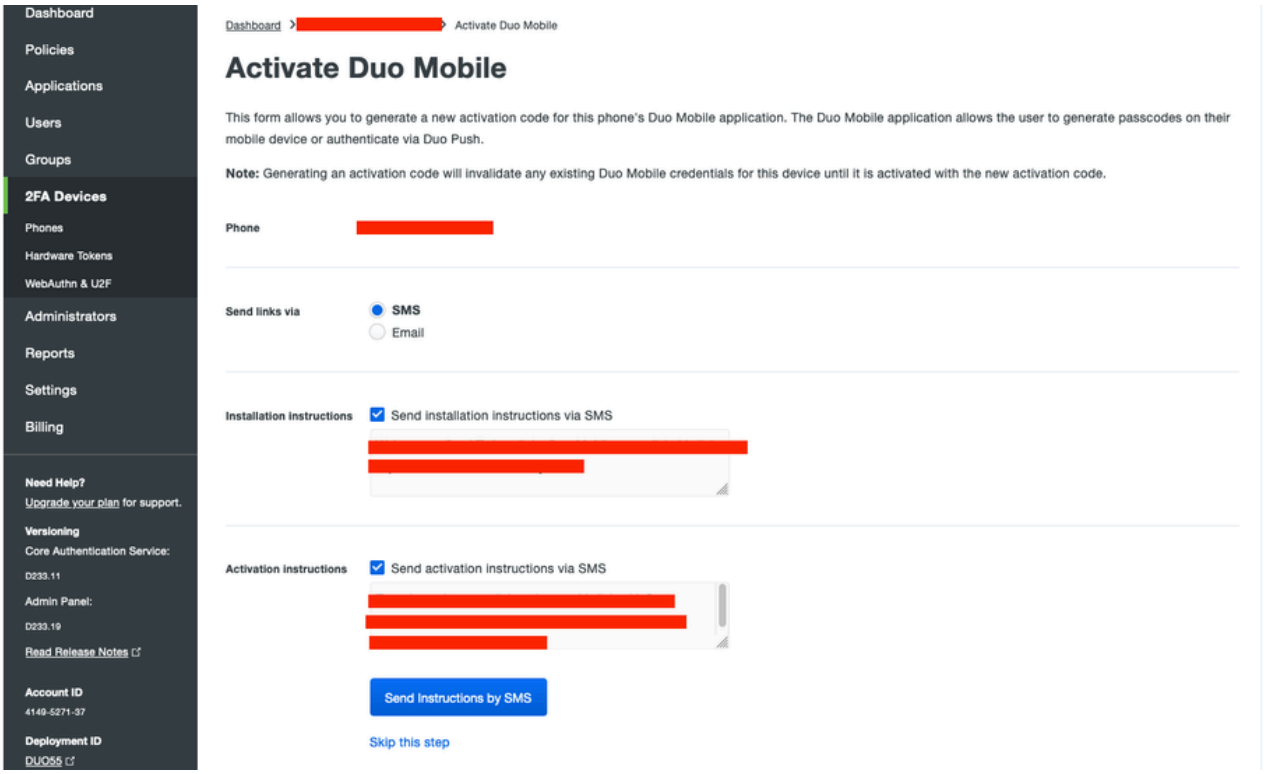
DUO – デバイス情報

Generate Duo Mobile Activation Codeを選択します。



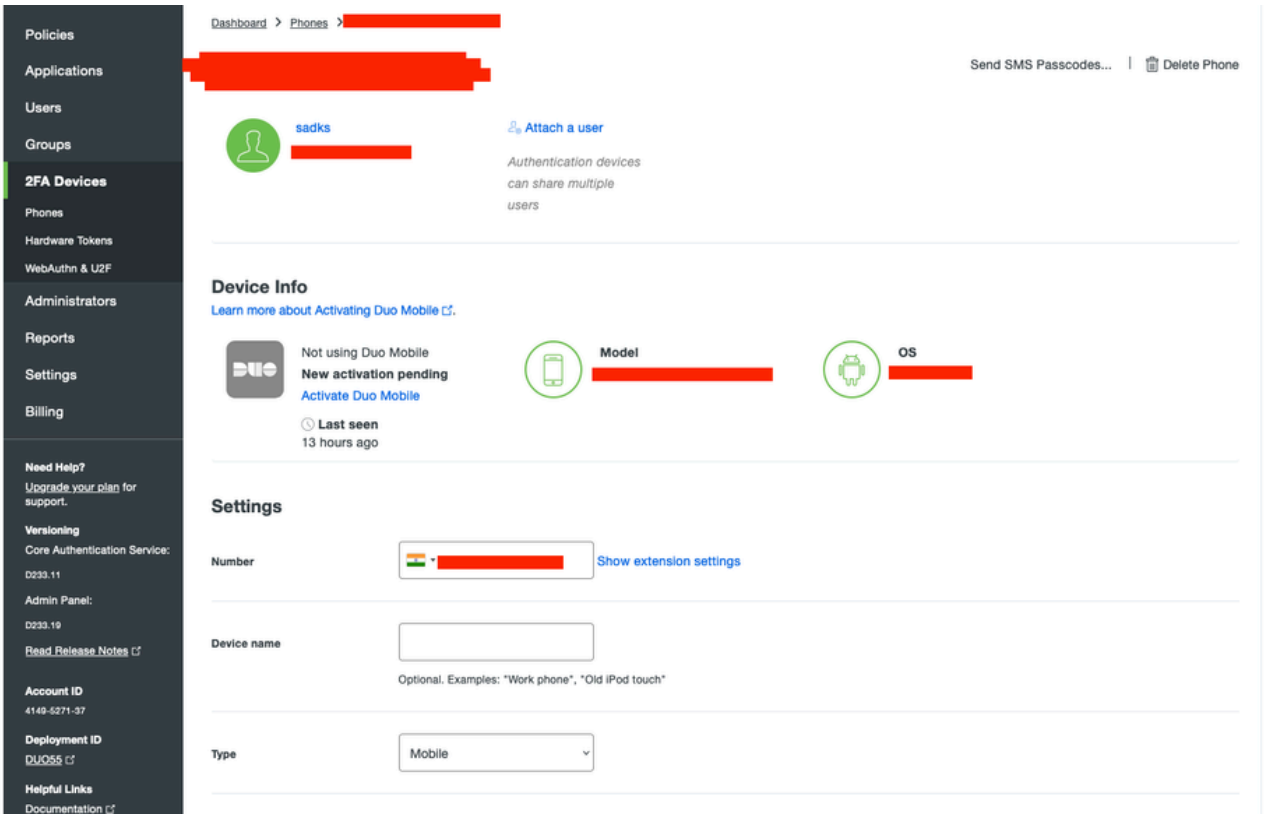
DUO – 電話の有効化

Send Instructions by SMSを選択します。



DUO - SMSの送信

電話機に送信されたリンクをクリックすると、次の図に示すように、DUOアプリが「デバイス情報」セクションのユーザアカウントにリンクされます。

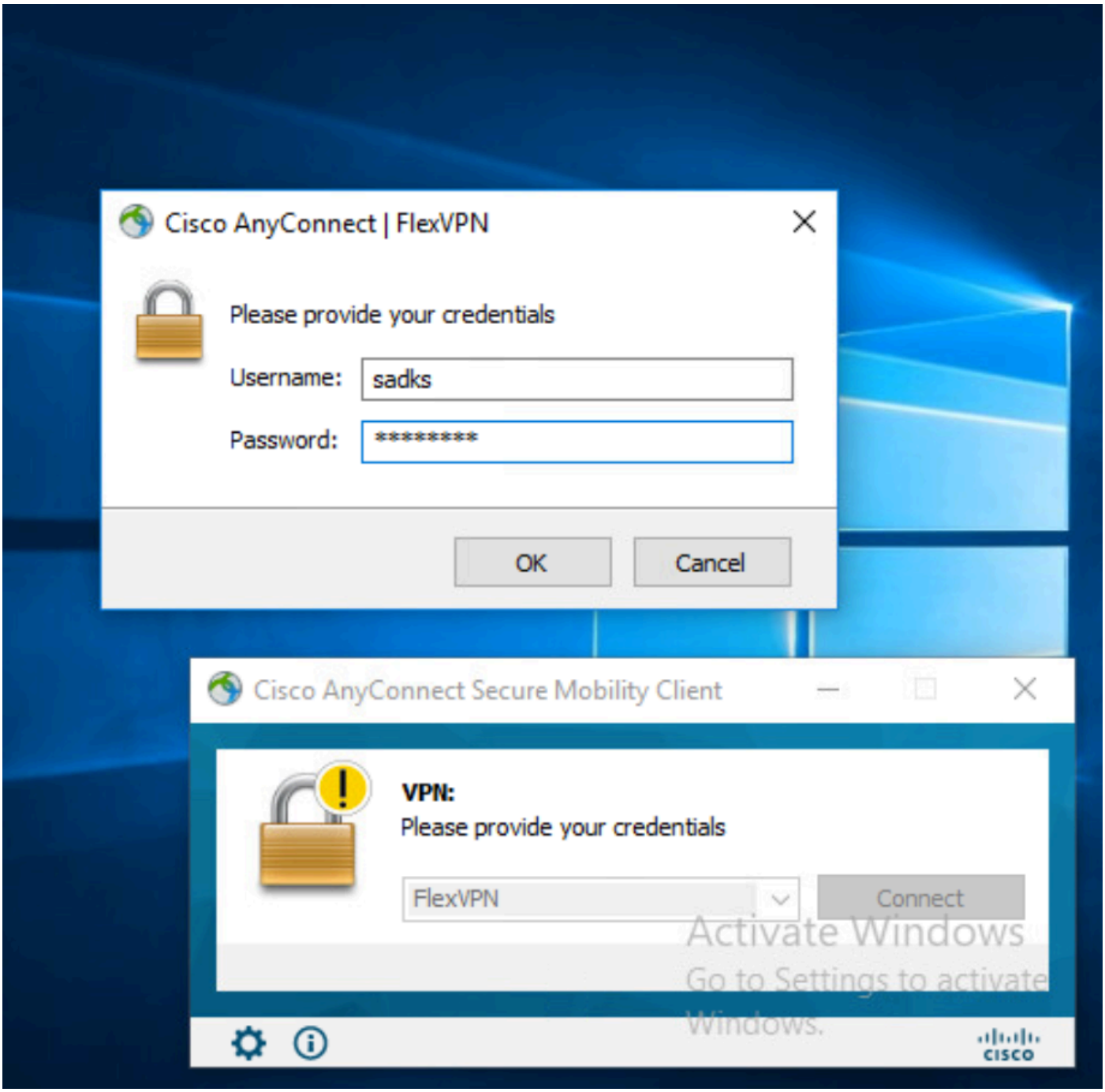


DUO – デバイスリンク

確認

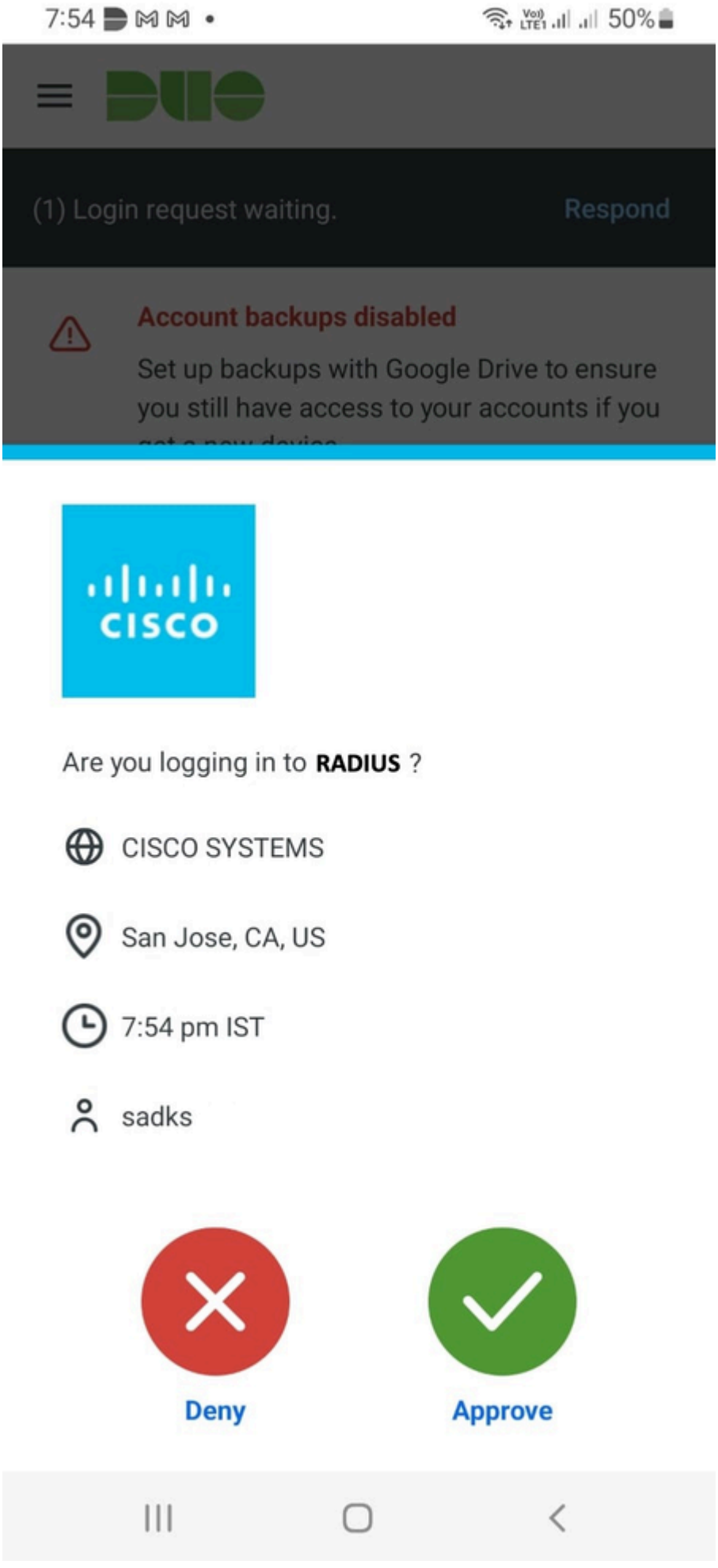
認証をテストするには、ユーザのPCからAnyConnectを介してC8000Vに接続します。

プライマリ認証のユーザ名とパスワードを入力します。



AnyConnect接続

次に、モバイル上のDUOプッシュを受け入れます。



DUOプッシュ

接続が確立されます

<#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. VPNセッションの暗号化セッションの詳細

<#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

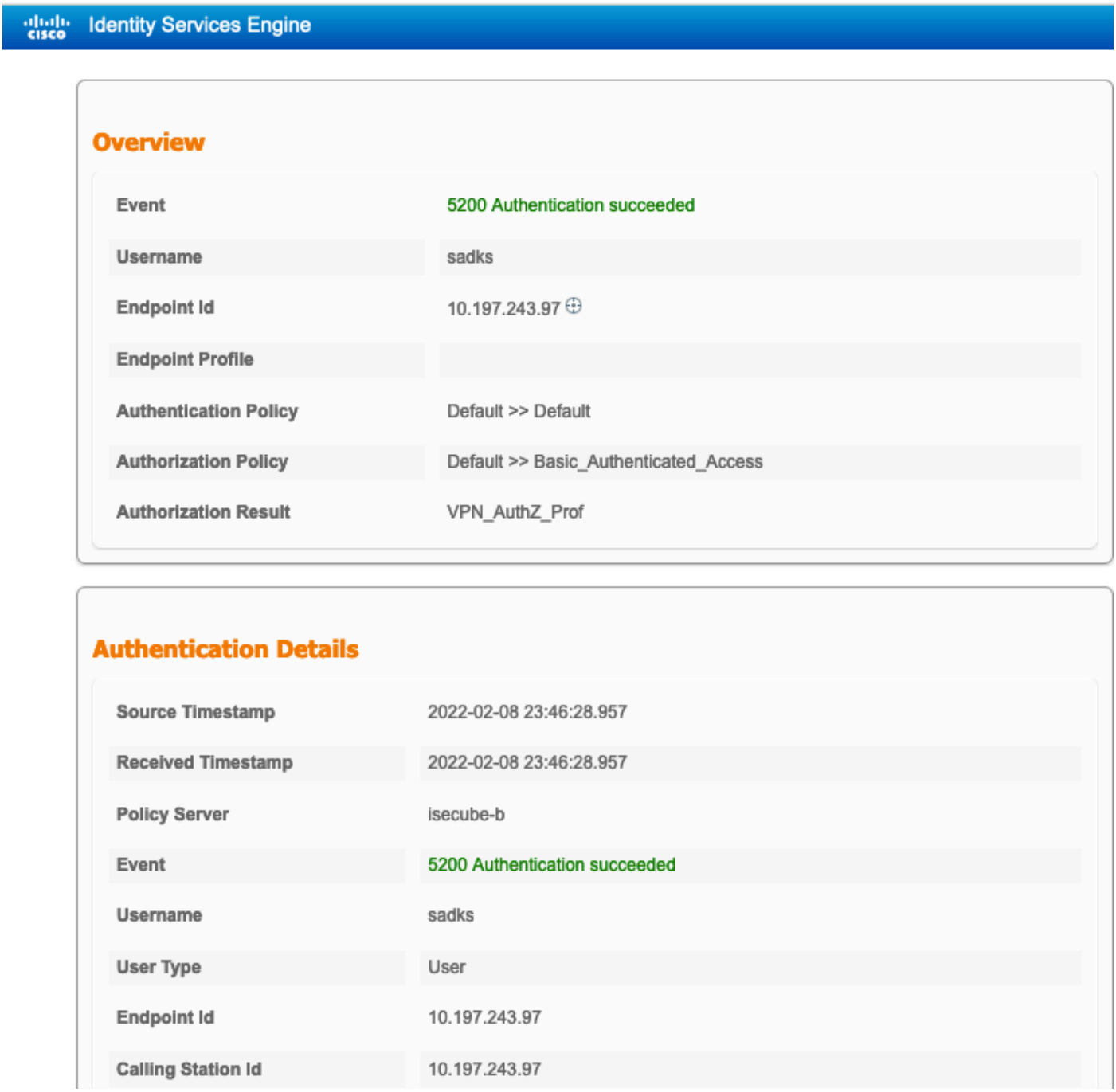
```
Session status: UP-ACTIVE
Peer: 10.197.243.97 port 54198 fvrf: (none) ivrf: (none)
      Phase1_id: cisco.com
      Desc: (none)
  Session ID: 114
  IKEv2 SA: local 10.106.54.143/4500 remote 10.197.243.98/54198 Active
          Capabilities:DN connid:1 lifetime:23:58:53
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0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

ISEで、Operations > Live Logsの順に移動します。プライマリ認証の認証レポートを表示できます。



ISE：ライブログ

4. DUO認証プロキシの検証

DUO Authentication Proxyで次のファイルに移動します。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
```

トラブルシュート

1. C8000Vのデバッグ

IKEv2の場合：

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

IPSecの場合

- debug crypto ipsec
- debug crypto ipsec error

2. DUO認証プロキシに関しては、ログファイルのプロキシ関連のログを確認します。(C:\Program Files\Duo Security Authentication Proxy\log)

ISEがプライマリ認証を拒否するエラーログのスニペットを次に示します。

<#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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。