

配置採用EAP和DUO身份驗證的AnyConnect Flexvpn

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[身份驗證流程](#)

[流程圖](#)

[通訊過程](#)

[設定](#)

[C8000V \(VPN頭端\) 的配置步驟](#)

[客戶端配置檔案片段 \(XML配置檔案\)](#)

[DUO Authentication Proxy的配置步驟](#)

[ISE的配置步驟](#)

[DUO管理門戶的配置步驟](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何為到Cisco IOS® XE路由器的AnyConnect IPSec連線配置外部雙因素身份驗證。

由Sadhana K S和Rishabh Aggarwal思科TAC工程師貢獻。

必要條件

需求

思科建議您瞭解以下主題：

- 在路由器上配置RA VPN的經驗
- 身分識別服務引擎(ISE)管理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行版本17.10.01a的Cisco Catalyst 8000V(C8000V)
- Cisco AnyConnect安全行動化使用者端版本4.10.04071
- 運行版本3.1.0的Cisco ISE

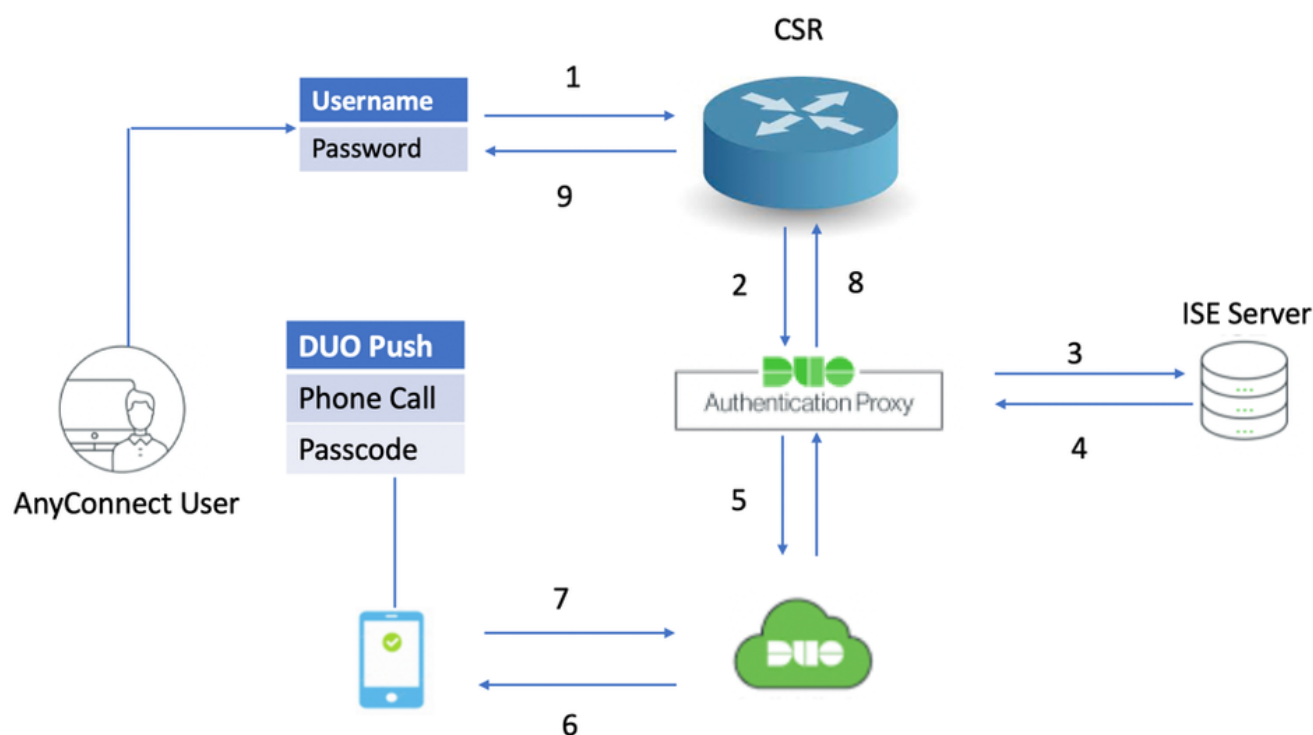
- Duo Authentication代理伺服器（windows 10或任何Linux PC）
- Duo Web帳戶
- 安裝了AnyConnect的客戶端PC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

身份驗證流程

AnyConnect使用者在ISE伺服器上使用使用者名稱和密碼進行身份驗證。Duo Authentication Proxy伺服器還以推送通知的形式向使用者的流動裝置傳送附加身份驗證。

流程圖



驗證流程圖

通訊過程

1. 使用者啟動到C8000V的RAVPN連線，並提供用於主身份驗證的使用者名稱和密碼。
2. C8000V向Duo Authentication Proxy傳送驗證要求。
3. 然後，Duo Authentication Proxy將主請求傳送到Active Directory或RADIUS伺服器。
4. 驗證回應會傳送回驗證代理。
5. 主要身份驗證成功後，Duo身份驗證代理會通過Duo伺服器請求次要身份驗證。
6. 然後，Duo服務根據輔助身份驗證方法（推送、電話呼叫、密碼）對使用者進行身份驗證。
7. Duo authentication proxy接收身份驗證響應。
8. 響應將傳送到C8000V。

9. 如果成功，則建立AnyConnect連線。

設定

要完成配置，請考慮以下各節。

C8000V (VPN頭端) 的配置步驟

1.配置RADIUS伺服器。RADIUS伺服器的IP地址必須是Duo Authentication Proxy的IP。

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

2.將RADIUS伺服器配置為本地身份驗證^{aaa}，並將授權配置為本地身份驗證。

```
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.建立信任點以安裝身份證書 (如果本地身份驗證尚未提供)。有關證書建立的詳細資訊，請參閱[PKI的證書註冊](#)。

```
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. (可選) 配置要用於拆分隧道的標準訪問清單。此訪問清單包括可通過VPN隧道訪問的目標網路。預設情況下，如果沒有配置拆分隧道，則所有流量都會通過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.建立IPv4地址池。

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

在成功的AnyConnect連線過程中，建立的IP地址池為AnyConnect客戶端分配一個IPv4地址。

6.配置授權策略。

```
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、拆分通道清單等在授權策略下指定。



附註：如果未配置自定義IKEv2授權策略，則使用名為「default」的預設授權策略進行授權。也可以通過RADIUS伺服器推送在IKEv2授權策略中指定的屬性。

7.配置IKEv2建議和策略。

```
crypto ikev2 proposal FlexVPN_IKEv2_Proposal
 encryption aes-cbc-128
 integrity sha384
 group 19

crypto ikev2 policy FlexVPN_IKEv2_Policy
 match fvrfl any
 proposal FlexVPN_IKEv2_Proposal
```

8.將AnyConnect客戶端配置檔案上傳到路由器的bootflash中，並按給定的定義配置檔案：

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

9.禁用HTTP安全伺服器。

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

10.配置SSL策略並將路由器的WAN IP指定為下載配置檔案的本地地址。

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

      port 443
```

11.配置一個虛擬模板，虛擬訪問可以從該模板中克隆介面

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

unnumbered命令從配置的介面(GigabitEthernet1)獲取IP地址。

13.配置包含所有連線關係的IKEv2配置檔案ed資訊。

```
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
```

這些在IKEv2配置檔案中使用：

- match identity remote any — 表示客戶端的標識。此處配置了「any」，以便具有正確憑證的任何客戶端都可以連線
- authentication remote — 提及EAP協定必須用於客戶端身份驗證
- authentication local — 提及證書必須用於本地身份驗證
- aaa authentication eap — 在EAP身份驗證期間，使用RADIUSFlexVPN_auth伺服器
- aaa authorization group eap list — 在授權過程中，網路清單 FlexVPN_authz與授權策略一起使用 ikev2-authz-policy
- aaa authorization user eap cached-啟用隱式使用者授權
- virtual-template 20 mode auto — 定義要克隆的虛擬模板
- anyconnect profile Client_Profile — 在此將步驟8中定義的客戶端配置檔案應用到此IKEv2配置檔案

14. 配置轉換集和IPSec配置檔案。

```
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.將IPSec配置檔案新增到虛擬模板。

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

客戶端配置檔案片段 (XML配置檔案)

在Cisco IOS XE 16.9.1之前的版本中，無法從頭端自動下載配置檔案。16.9.1之後，可以從頭端下載配置檔案。

```
<#root>
```

```
!
!
```

false

true

false

A11

A11

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 Authentication Proxy的配置步驟



附註：Duo Authentication Proxy僅支援具有RADIUS身份驗證的MS-CHAPv2。

步驟1. [下載](#)並安裝Duo Authentication Proxy Server。

登入到Windows機器並安裝Duo Authentication Proxy伺服器。

建議使用至少具有1個CPU、200 MB磁碟空間和4 GB RAM的系統。

步驟2. 導覽至C:\Program Files\Duo Security Authentication Proxy\conf\，然後開啟authproxy.cfg，以便使用適當的詳細資訊設定驗證代理。

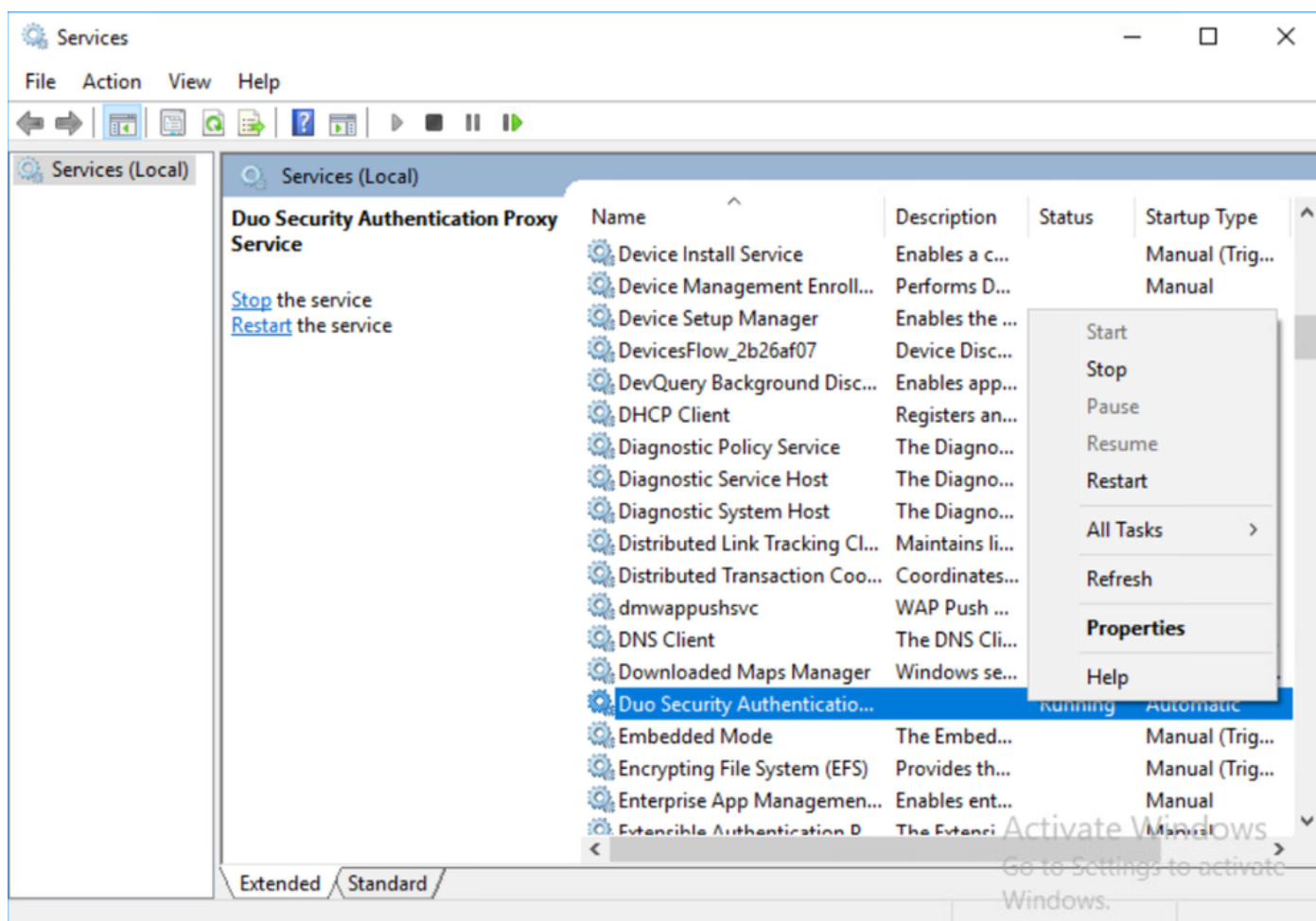
```
[radius_client]
host=10.197.243.116
secret=cisco
```



附註：其中「10.197.243.116」是ISE伺服器的IP地址，而「cisco」是為驗證主要身份驗證而配置的密碼。

完成這些更改後，請儲存檔案。

步驟3. 開啟Windows服務主控台(services.msc)。然後重啟Duo Security Authentication Proxy Service。



Duo Security Authentication Proxy Service

ISE的配置步驟

步驟1. 導覽至Administration > Network Devices,然後按一下Add以便設定網路裝置。



附註：將x.x.x.x替換為Duo Authentication Proxy伺服器的IP地址。

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequences > NAC Managers > External MDM > Location Services

Network Devices List > **Sadhana_Duo_Proxy**

Network Devices

* Name:

Description:

IP Address: /

* Device Profile:

Model Name:

Software Version:

* Network Device Group

Location:

IPSEC:

Device Type:

ISE — 網路裝置

步驟2. 配置 Shared Secret，如中 authproxy.cfg 所述 secret:

☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol: **RADIUS**

* Shared Secret:

Use Second Shared Secret: ☐

CoA Port:

RADIUS DTLS Settings

DTLS Required: ☐

Shared Secret:

CoA Port:

Issuer CA of ISE Certificates for CoA:

DNS Name:

General Settings

Enable KeyWrap: ☐

* Key Encryption Key:

* Message Authenticator Code Key:

Key Input Format: ☒ ASCII ☐ HEXADECIMAL

ISE — 共用金鑰

步驟3. 導航至 Administration > Identities > Users。選擇 Add 以配置 AnyConnect 主身份驗證的身份使用者:

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows the navigation menu with 'Users' selected. The main content area is titled 'Network Access Users List > sads'. Under the 'Network Access User' section, the 'Name' field is 'sads', 'Status' is 'Enabled', and 'Email' is empty. The 'Passwords' section shows 'Password Type' as 'Internal Users'. There are fields for 'Login Password' and 'Enable Password', each with a 'Generate Password' button. The 'Re-Enter Password' field is also present.

ISE — 使用者

DUO管理門戶的配置步驟

步驟1.登入您的Duo帳戶。

導航至Applications > Protect an Application。按一下Protect，選擇您要使用的應用程式。（此案例中的RADIUS）

The screenshot shows the Duo 'Protect an Application' page. The breadcrumb trail is: Dashboard > Applications > Protect an Application. The page title is 'Protect an Application'. A search bar contains the text 'radius'. Below the search bar is a table with columns 'Application' and 'Protection Type'. The table lists several applications, with the last one, 'RADIUS', highlighted by a red rectangle. The 'RADIUS' application has a lock icon, the name 'RADIUS', and a 'Protection Type' of '2FA'. To the right of the application name are links for 'Documentation' and a 'Protect' button.

Application	Protection Type
Cisco ISE RADIUS	2FA
Cisco RADIUS VPN	2FA
F5 BIG-IP APM RADIUS	2FA
Meraki RADIUS VPN	2FA
RADIUS	2FA

DUO — 應用程式

步驟2.按一下Protect，選擇您要使用的應用程式。（此案例中的RADIUS）

複製整合金鑰、金鑰和API主機名，並將其貼上到authproxy.cfgDuo Authentication Proxy上。

RADIUS

Authentication Log |  Remove Application

See the [RADIUS documentation](#) to integrate Duo into your RADIUS-enabled platform.

Details

[Reset Secret Key](#)

Integration key

Copy

Secret key

*****v1zG

Copy

Don't write down your secret key or share it with anyone.

API hostname

Copy

DUO - RADIUS

複製這些值並導航回到DUO驗證代理，然後開啟 `authproxy.cfg` 並貼上值，如下所示：

整合金鑰= ikey

secret key = skey

API主機名= api_host

```
[radius_server_auto]
ikey=xxxxxxx
skey=xxxxxxv1zG
api_host=xxxxxxx
radius_ip_1=10.106.54.143
radius_secret_1=cisco
failmode=safe
client=radius_client
port=1812
```



附註：配置伺服器時，必須從Duo伺服器複製ikey、skey和api_host，並且「10.106.54.143」是C8000V路由器的IP地址，而「cisco」是在radius伺服器配置下在路由器上配置的金鑰。

進行這些更改後，再次儲存該檔案，然後重新啟動Duo Security Authentication Proxy Service(在 `services.msc`)。

步驟3. 在DUO上建立使用者以進行輔助身份驗證。

導覽至 `Users > Add User` 並輸入使用者名稱。



附註：使用者名稱必須與主身份驗證使用者名稱匹配。

按一下 Add User。建立後，在 Phones 下，按一下 Add Phone，輸入電話號碼，然後按一下 Add Phone。

Dashboard

Policies

Applications

Users

Add User

Pending Enrollments

Bulk Enroll Users

Import Users

Directory Sync

Bypass Codes

Groups

2FA Devices

Administrators

Reports

Dashboard > Users > **t** > Add Phone

Add Phone

Learn more about Activating Duo Mobile [↗](#).

Type

☒ Phone

☐ Tablet

Phone number



Show extension field

Optional. Example: "+1 201-555-5555"

Add Phone

DUO — 新增電話

選擇身份驗證型別。

Device Info

[Learn more about Activating Duo Mobile \[↗\]\(#\).](#)



Not using Duo Mobile
[Activate Duo Mobile](#)



Model
Unknown



OS
Generic Smartphone

DUO — 裝置資訊

選擇 .Generate Duo Mobile Activation Code

Dashboard

Policies

Applications

Users

Groups

2FA Devices

Phones

Hardware Tokens

WebAuthn & U2F

Administrators

Reports

Settings

Billing

Need Help?
Upgrade your plan for support.

Dashboard > **XXXXXXXXXX** > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone

XXXXXXXXXX

Expiration

24

hours

▼

after generation

Generate Duo Mobile Activation Code

選擇 Send Instructions by SMS.

Dashboard

Policies

Applications

Users

Groups

2FA Devices

Phones

Hardware Tokens

WebAuthn & U2F

Administrators

Reports

Settings

Billing

Need Help?
Upgrade your plan for support.

Versioning

Core Authentication Service:
0233.11

Admin Panel:
0233.19

Read Release Notes

Account ID
4149-5271-37

Deployment ID
DUO55

Helpful Links
Documentation

Dashboard > > Activate Duo Mobile

Activate Duo Mobile

This form allows you to generate a new activation code for this phone's Duo Mobile application. The Duo Mobile application allows the user to generate passcodes on their mobile device or authenticate via Duo Push.

Note: Generating an activation code will invalidate any existing Duo Mobile credentials for this device until it is activated with the new activation code.

Phone

Send links via

SMS

Email

Installation instructions

Send installation instructions via SMS

Activation instructions

Send activation instructions via SMS

Send Instructions by SMS

Skip this step

按一下傳送至電話的連結，DUO應用將連結至Device Info「section（部分）」中的使用者帳戶，如下圖所示：

Policies

Applications

Users

Groups

2FA Devices

Phones

Hardware Tokens

WebAuthn & U2F

Administrators

Reports

Settings

Billing

Need Help?
Upgrade your plan for support.

Versioning

Core Authentication Service:
0233.11

Admin Panel:
0233.19

Read Release Notes

Account ID
4149-5271-37

Deployment ID
DUO55

Helpful Links
Documentation

Dashboard > Phones > >

Send SMS Passcodes...

Delete Phone

sadks

Attach a user

Authentication devices can share multiple users

Device Info

Learn more about Activating Duo Mobile

Not using Duo Mobile

New activation pending

Activate Duo Mobile

Last seen
13 hours ago

Model

OS

Settings

Number

Show extension settings

Device name

Optional. Examples: "Work phone", "Old iPod touch"

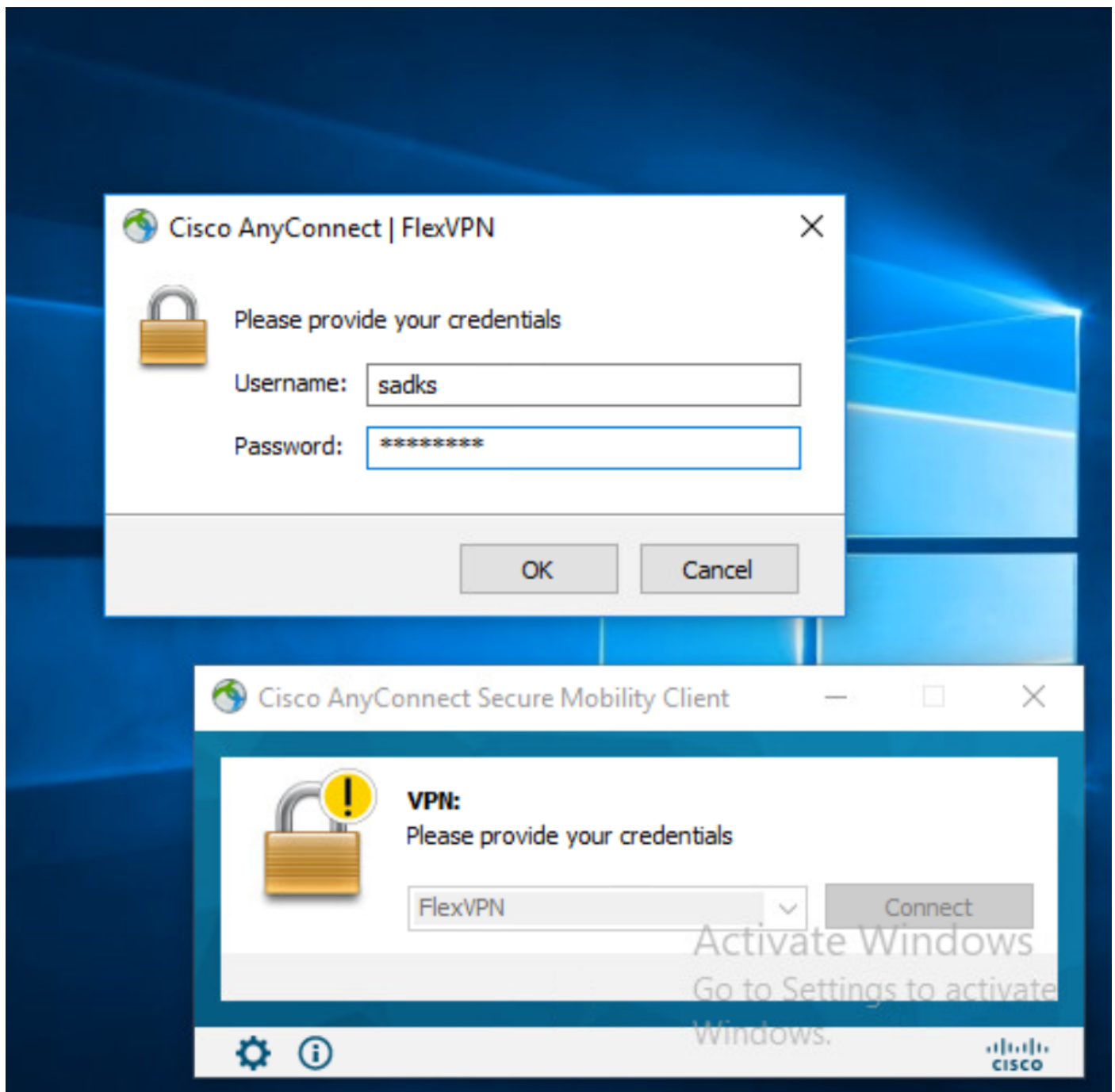
Type

Mobile

驗證

為了測試身份驗證，請通過AnyConnect從使用者PC連線到C8000V。

鍵入用於主要身份驗證的使用者名稱和密碼。



AnyConnect連線

然後，接受DUO按行動電話。



(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 get a new device.



Are you logging in to **RADIUS** ?



CISCO SYSTEMS



San Jose, CA, US



7:54 pm IST



sadks



Deny



Approve



<#root>

R1#sh crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/f/ivr/f	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: FL
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'd 3 drop 0 life (KB/Sec) 4607998/3532

Outbound: #pkts enc'd 0 drop 0 life (KB/Sec) 4608000/3532

3.Verification on ISE live logs

在ISE中導航到Operations > Live Logs。您可以檢視主要身份驗證的身份驗證報告。

Overview

Event	5200 Authentication succeeded
Username	sadks
Endpoint Id	10.197.243.97 ⓘ
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	VPN_AuthZ_Prof

Authentication Details

Source Timestamp	2022-02-08 23:46:28.957
Received Timestamp	2022-02-08 23:46:28.957
Policy Server	isecube-b
Event	5200 Authentication succeeded
Username	sadks
User Type	User
Endpoint Id	10.197.243.97
Calling Station Id	10.197.243.97

ISE — 即時日誌

4. Verification on DUO authentication proxy

在DUO Authentication Proxy上導航到此檔案； 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 ('10.106.54.143', 1645), sadks, 163):
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 to

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 <DuoHTTPClientFactory>
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.log#info] ((('10.106.54.143', 1645), sadks, 163): Got response for id 191 from ('10.197.243.116', 1812); code 2
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 <DuoHTTPClientFactory>
2022-02-08T23:24:51.753590+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <DuoHTTPClientFactory>
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): Sending response to ('10.106.54.143', 1645), sadks, 163):
2022-02-08T23:24:59.357413+0530 [duoauthproxy.lib.http._DuoHTTPClientFactory#info] Stopping factory <DuoHTTPClientFactory>

```

疑難排解

1. C8000V上的調試

對於IKEv2:

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

對於IPSec:

- debug crypto ipsec
- debug crypto ipsec error

2.對於DUO Authentication Proxy，請檢查日誌文件代理相關日誌。(C:\Program Files\Duo Security Authentication Proxy\log)

顯示ISE拒絕主要身份驗證的錯誤日誌代碼段：

<#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): Return

AccessReject

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。