

AnyConnect FlexVPN configureren met EAP- en DUO-verificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[verificatiestroom](#)

[stroonschema](#)

[communicatieproces](#)

[Configureren](#)

[Configuratiestappen op C8000V \(VPN Headend\)](#)

[Fragment van het clientprofiel \(XML-profiel\)](#)

[Configuratiestappen voor de DUO-verificatieproxy](#)

[Configuratiestappen op ISE](#)

[Configuratiestappen op het DUO-beheerportaal](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u externe twee-factorenverificatie configureert voor een AnyConnect IPSec-verbinding met een Cisco IOS® XE-router.

Bijgedragen door Sadhana KS en Rishabh Aggarwal Cisco TAC Engineers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Ervaring met RA VPN-configuratie op een router
- Beheer Identity Services Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 8000V (C8000V) met versie 17.10.01a
- Cisco AnyConnect Secure Mobility Client versie 4.10.04071

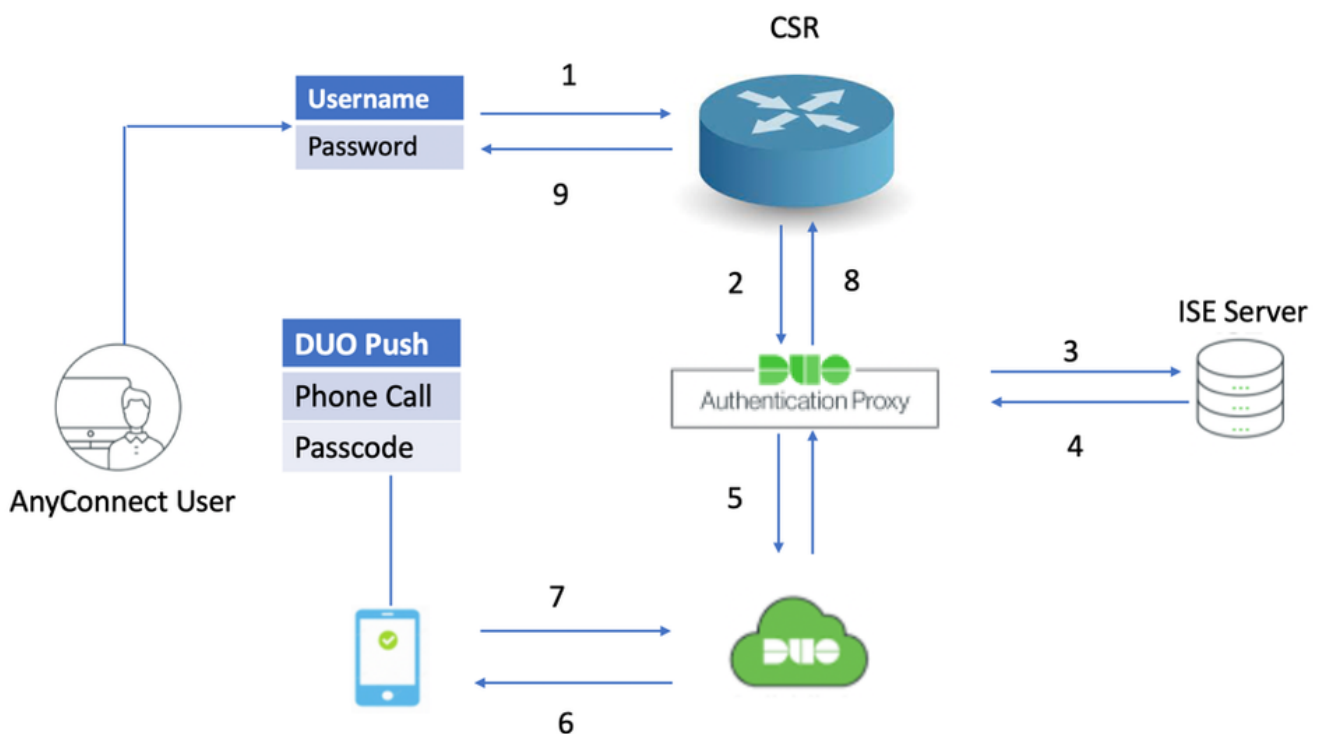
- Cisco ISE met versie 3.1.0
- Proxyserver voor Duo-verificatie (Windows 10 of elke Linux-pc)
- Duo-webaccount
- Client-pc waarop AnyConnect is geïnstalleerd

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

verificatiestroom

AnyConnect-gebruiker verifieert met een gebruikersnaam en wachtwoord op de ISE-server. De Duo Authentication Proxy-server verzendt ook een extra verificatie in de vorm van een pushmelding naar het mobiele apparaat van de gebruiker.

stroomschema



Authentication Flow Diagram

communicatieproces

1. De gebruiker initieert een RAVPN-verbinding met de C8000V en geeft een gebruikersnaam en wachtwoord voor primaire verificatie.
2. De C8000V verzendt een verificatieverzoek naar de Duo-verificatieproxy.
3. De Duo Authentication Proxy stuurt het primaire verzoek vervolgens naar de Active

Directory- of RADIUS-server.

4. Het verificatierespons wordt teruggestuurd naar de verificatieproxy.
5. Zodra de primaire verificatie is geslaagd, vraagt de Duo-verificatieproxy secundaire verificatie aan via de Duo-server.
6. De Duo-service verifieert vervolgens de gebruiker, afhankelijk van de secundaire verificatiemethode (push, telefoongesprek, toegangscode).
7. Duo-verificatieproxy ontvangt het verificatierespons.
8. Het antwoord wordt verzonden naar de C8000V.
9. Als dit lukt, wordt de AnyConnect-verbinding tot stand gebracht.

Configureren

Om de configuratie te voltooien, moet u rekening houden met deze secties.

Configuratiestappen op C8000V (VPN Headend)

1. De RADIUS-server configureren. Het IP-adres van de RADIUS-server moet het IP-adres van de Duo Authentication Proxy zijn.

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

2. Configureer de RADIUS-server als `aaa` lokale verificatie en autorisatie.

```
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. Maak een Trustpoint aan om het identiteitscertificaat te installeren, indien dit nog niet aanwezig is voor lokale verificatie. U kunt naar [Certificaatregistratie](#) verwijzen [voor een PKI](#) voor meer informatie over het maken van certificaten.

```
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. (Optioneel) Configureer een standaardtoegangslijst voor de gesplitste tunnel. Deze toegangslijst bestaat uit de bestemmingsnetwerken die toegankelijk zijn via de VPN-tunnel. Standaard gaat al het verkeer door de VPN-tunnel als de gesplitste tunnel niet is geconfigureerd.

```
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. Maak een IPv4-adresgroep.

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

De gemaakte IP-adresgroep wijst een IPv4-adres toe aan de AnyConnect-client tijdens een geslaagde AnyConnect-verbinding.

6. Configureer een machtigingsbeleid.

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

De IP-pool, DNS, split-tunnel lijst, enzovoort, worden gespecificeerd onder het autorisatiebeleid.



Opmerking: Als het aangepaste IKEv2-autorisatiebeleid niet is geconfigureerd, wordt het standaardautorisatiebeleid met de naam 'standaard' gebruikt voor autorisatie. De attributen die zijn opgegeven in het IKEv2-autorisatiebeleid kunnen ook worden gepusht via de RADIUS-server.

7. Configureer een IKEv2-voorstel en -beleid.

```
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. Upload het AnyConnect-clientprofiel naar de bootflash van de router en definieer het profiel als volgt:

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

9. HTTP-beveiligde server uitschakelen.

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

10. Configureer het SSL-beleid en geef het WAN-IP van de router op als het lokale adres voor het downloaden van het profiel.

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

      port 443
```

11. Configureer een virtuele sjabloon van waaruit de virtuele toegangspunt intOppervlakken worden gekloond

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

Met de opdracht Ongenummerd wordt het IP-adres van de geconfigureerde interface (Gigabit Ethernet1) opgehaald.

13. Configureer een IKEv2-profiel met alle verbindingsrelatiesED informatie.

```
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
```

Deze worden gebruikt in het IKEv2-profiel:

- match identity remote any - Verwijst naar de identiteit van de klant. Hier is 'any' geconfigureerd zodat elke client met de juiste referenties verbinding kan maken
- authentication remote - Vermeld dat het EAP-protocol moet worden gebruikt voor clientverificatie
- authentication local - Vermeld dat certificaten moeten worden gebruikt voor lokale authenticatie
- aaa authentication eap - Tijdens EAP-verificatie wordt de RADIUS-server FlexVPN_auth gebruikt
- aaa authorization group eap list - Tijdens de autorisatie wordt de netwerklIJst FlexVPN_authzwordt gebruikt in het kader van het toelatingsbeleid ikev2-authz-policy
- aaa authorization user eap cached- Maakt impliciete gebruikersautorisatie mogelijk
- virtual-template 20 mode auto - Bepaalt welke virtuele sjabloon moet worden gekloond
- anyconnect profile Client_Profile - Het clientprofiel gedefinieerd in stap 8. wordt hier toegepast op dit IKEv2-profiel

14. Een transformatieset en een IPSec-profiel configureren.

```
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. Voeg het IPSec-profiel toe aan de virtuele sjabloon.

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

Fragment van het clientprofiel (XML-profiel)

Voorafgaand aan Cisco IOS XE 16.9.1, automatische profiel downloads van de kop is niet beschikbaar. Na 16.9.1 is het mogelijk om het profiel van de kop te downloaden.

<#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>
```

Configuratiestappen voor de DUO-verificatieproxy



Opmerking: Duo Authentication Proxy ondersteunt MS-CHAPv2 alleen met RADIUS-verificatie.

Stap 1. [Download](#) en installeer de Duo Authentication Proxy Server.

Meld u aan bij het Windows-systeem en installeer de Duo Authentication Proxy-server.

Het wordt aanbevolen om een systeem te gebruiken met ten minste 1 CPU, 200 MB schijfruimte en 4 GB RAM.

Stap 2. Navigeer naar `C:\Program Files\Duo Security Authentication Proxy\conf\` en open `authproxy.cfg` om de verificatieproxy met de juiste details te configureren.

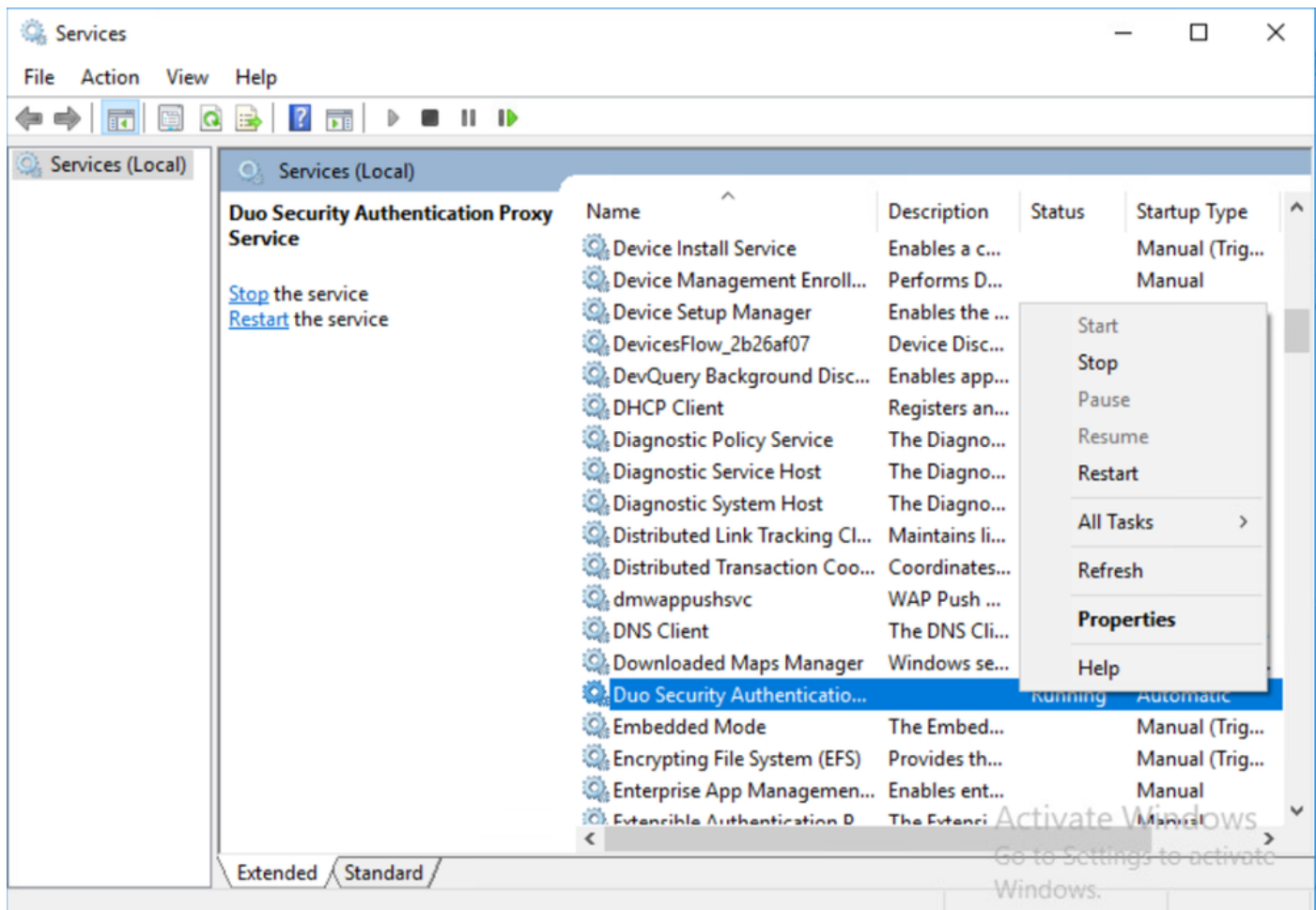
```
[radius_client]
host=10.197.243.116
secret=cisco
```



Opmerking: hier is '10.197.243.116' het IP-adres van de ISE-server en 'cisco' is het wachtwoord dat is geconfigureerd om de primaire verificatie te valideren.

Nadat u deze wijzigingen hebt aangebracht, slaat u het bestand op.

Stap 3. Open de Windows Services-console (`services.msc`). En opnieuw Duo Security Authentication Proxy Service opstarten.



Duo Security Authentication Proxy Service

Configuratiestappen op ISE

Stap 1. Navigeer naar **Administration > Network Devices** en klik **Add** op om het netwerkapparaat te configureren.



Opmerking: Vervang **x.x.x.x** het IP-adres van uw Duo Authentication Proxy-server.

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 - Netwerkkaparameten

Stap 2. Configureer de Shared Secretinstellingen zoals vermeld in de tabel authproxy.cfgin 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 - Gedeeld geheim

Stap 3. Navigeer naar Administration > Identities > UsersEuropa.Kies deze optie Addom de identiteitsgebruiker te configureren voor primaire AnyConnect-verificatie:

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > sads

Network Access User

* Name: sads

Status: ☒ Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password

* Login Password: ***** Generate Password

Enable Password: Generate Password

ISE - Gebruikers

Configuratiestappen op het DUO-beheerportaal

Stap 1. Meld u aan bij uw Duo-account.

Navigeer naar Applications > Protect an Application Europa. Klik Protect op de toepassing die u wilt gebruiken. (RADIUS in dit geval)

Dashboard Policies Applications Protect an Application Users Groups 2FA Devices 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 4149-6271-37 Deployment ID DUO55 Helpful Links Documentation

Dashboard > Applications > Protect an Application

Protect an Application

radius

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

DUO - Toepassing

Stap 2. Klik Protect op de toepassing die u wilt gebruiken. (RADIUS in dit geval)

Kopieer de integratiesleutel, geheime sleutel en API-hostnaam en plak deze op de authproxy.cfg van de Duo-verificatieproxy.

RADIUS

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

Details

[Reset Secret Key](#)

Integration key

 [Copy](#)

Secret key

 [Copy](#)

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

API hostname

 [Copy](#)

DUO - RADIUS

Kopieer deze waarden en ga terug naar de DUO-verificatieproxy en open de `authproxy.cfg` en plak de waarden zoals weergegeven:

Integratiesleutel = sleutel

Geheime sleutel = sleutel

API-hostnaam = 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
```



Opmerking: de sleutel, skey en api_host moeten worden gekopieerd van de Duo-server wanneer u de server configureert, en '10.106.54.143' is het IP-adres van de C8000V-router en 'cisco' is de sleutel die op de router is geconfigureerd onder de radius-serverconfiguratie.

Nadat u deze wijzigingen hebt aangebracht, slaat u het bestand opnieuw op en start u de Duo Security Authentication Proxy Service (`in_services.msc`) opnieuw op.

Stap 3. Gebruikers maken op DUO voor secundaire verificatie.

Navigeer naar `Users > Add User` en typ de gebruikersnaam.



Opmerking: de gebruikersnaam moet overeenkomen met de primaire gebruikersnaam voor verificatie.

Klik op de knop **Add User**. Nadat u deze hebt gemaakt, klikt u onder **Phones** op **Add Phone**, voert u het telefoonnummer in en klikt u op **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 > Add Phone

Add Phone

i

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

Type

☒ Phone

☐ Tablet

Phone number



Show extension field

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

Add Phone

DUO - Telefoon toevoegen

Kies het type authenticatie.

Device Info

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

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

Model
Unknown

OS
Generic Smartphone

DUO - Apparaatgegevens

Kies **Generate Duo Mobile Activation Code** uit.

Dashboard

Policies

Applications

Users

Groups

2FA Devices

Phones

Hardware Tokens

WebAuthn & U2F

Administrators

Reports

Settings

Billing

Need Help?

Upgrade your plan for support.

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

Expiration

24

hours

after generation

Generate Duo Mobile Activation Code

DUO - Telefoon activeren

kiezen 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:

D233.11

Admin Panel:

D233.19

Read Release Notes

Account ID

4149-5271-37

Deployment ID

DUO55

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

DUO - SMS verzenden

Klik op de link die naar de telefoon wordt verzonden en de DUO-app wordt gekoppeld aan het gebruikersaccount in het Device Info gedeelte, zoals weergegeven in de afbeelding:

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: D233.11

Admin Panel: D233.19

Read Release Notes

Account ID: 4149-5271-37

Deployment ID: DUQ55

Helpful Links

Documentation

Dashboard > Phones > [redacted]

Send SMS Passcodes... | Delete Phone



sadks
[redacted]

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
[redacted]



OS
[redacted]

Settings

Number
[redacted] Show extension settings

Device name
[text input]
Optional. Examples: "Work phone", "Old iPod touch"

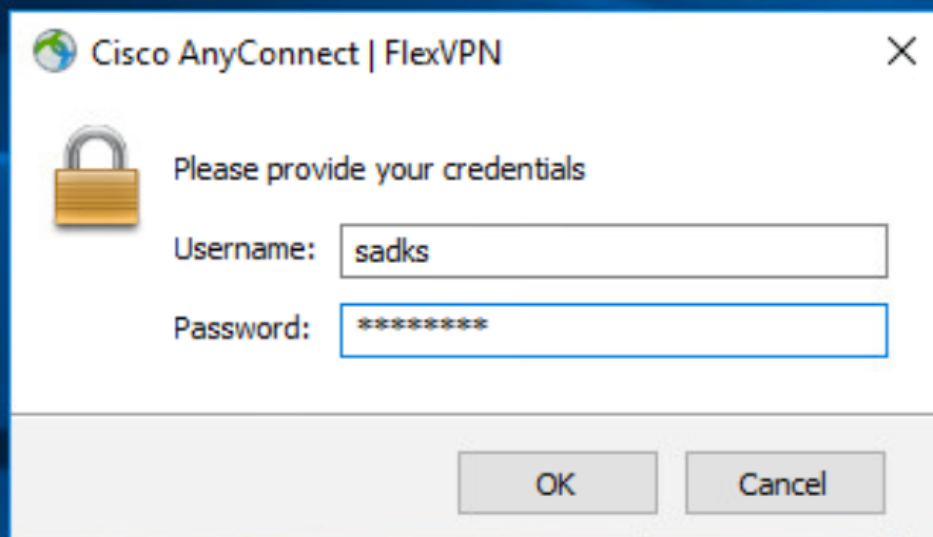
Type
Mobile

DUO - Apparaat gekoppeld

Verifiëren

Als u de verificatie wilt testen, maakt u verbinding met de C8000V vanaf de pc van de gebruiker via AnyConnect.

Typ de gebruikersnaam en het wachtwoord voor de primaire verificatie.



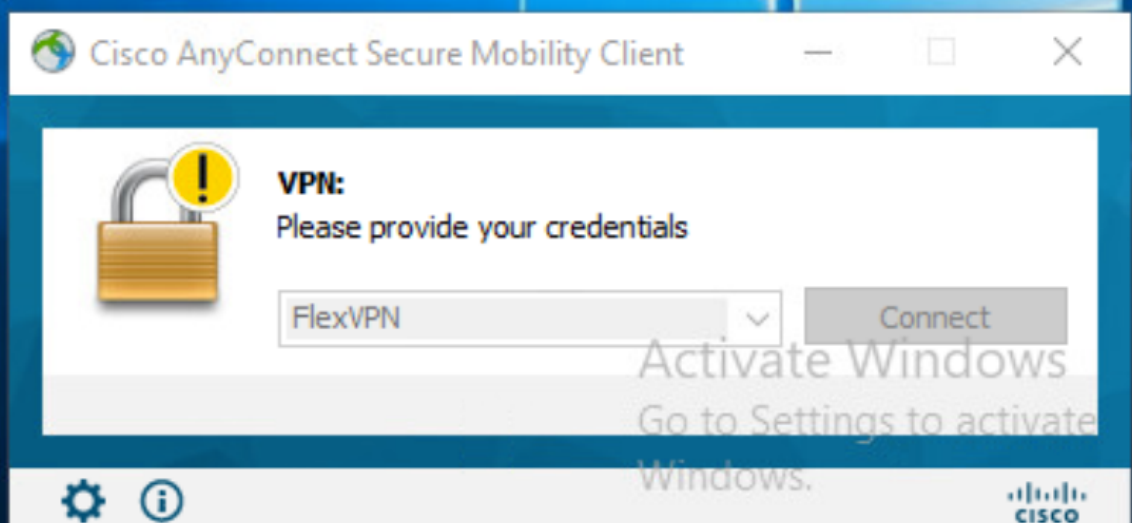
Cisco AnyConnect | FlexVPN

Please provide your credentials

Username:

Password:

OK Cancel



Cisco AnyConnect Secure Mobility Client

VPN: Please provide your credentials

Activate Windows
Go to Settings to activate Windows.

AnyConnect-verbinding

Accepteer vervolgens de DUO-pushes op de mobiel.



(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/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: 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

Navigeer naar [Operations > Live Logs](#) ISE. U kunt het verificatierapport voor de primaire verificatie bekijken.



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 - Live Logs

4. Verification on DUO authentication proxy

Navigeer naar het bestand op 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 ('10.106.54.143', 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>

```

Problemen oplossen

1. Debugs op C8000V.

Voor IKEv2:

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

Voor IPSec:

- debug crypto ipsec
- debug crypto ipsec error

2. Controleer voor de DUO-verificatieproxy de logbestanden met proxy. (C:\Program Files\Duo Security Authentication Proxy\log)

Het fragment voor een foutenlogboek waarin ISE de primaire verificatie afwijst, wordt weergegeven:

<#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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.