

مادختساب AnyConnect FlexVPN نيوكت

DUO و EAP ةقداصم

تايوتحمل

[ةمدقملا](#)

[ةيساسالابلاتطتملا](#)

[تابلطتملا](#)

[ةمدختسملاتانوكملا](#)

[ةقداصملا قفدت](#)

[قفدتلاليطيطخاتلامسرلا](#)

[لباصتالاةيلمع](#)

[نيوكتلا](#)

[VPN ةكبشبةصاخلا ثبلالاولابقتسالاةدحو C8000V ىلع نيوكتلاتاوطخ](#)

[\(XML فيرعت فلم\) لىمعلما فيرعت فلم نم ةصااصق](#)

[DUO ةقداصم لىك وىلع نيوكتلاتاوطخ](#)

[ISE ىلع نيوكتلاتاوطخ](#)

[Duo قرادالخدم ىلع نيوكتلاتاوطخ](#)

[ةحصلالانم ققحتلا](#)

[اهخالصاواطاخالافاشكتسا](#)

ةمدقملا

AnyConnect لاصتال ةيجراخال لاماولا ةيئانث ةقداصم نيوكت ةيفيك دنتسملا اذه حضوي
Cisco IOS® XE هجوم ب IPsec.

ةكرش نم Rishah Aggarwal و Sadhana K S ةكرش نم TAC يسندنم لبق نم ةمهاسملا تمت
Cisco TAC.

ةيساسالابلاتطتملا

تابلطتملا

ةيلاتال عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- هجوم ىلع RA VPN نيوكت عم ةبجتل
- (ISE) ةيوهلا تامدخ كرحم قرادا

ةمدختسملاتانوكملا

ةيلاتال ةيدامل تانوكملا وجماربل تارادصا ىل دنتسملا اذه يف ةدراولا تامولعمل دنتست

- Cisco Catalyst 8000V (C8000V) ةغيصض كيري 17.10.01a

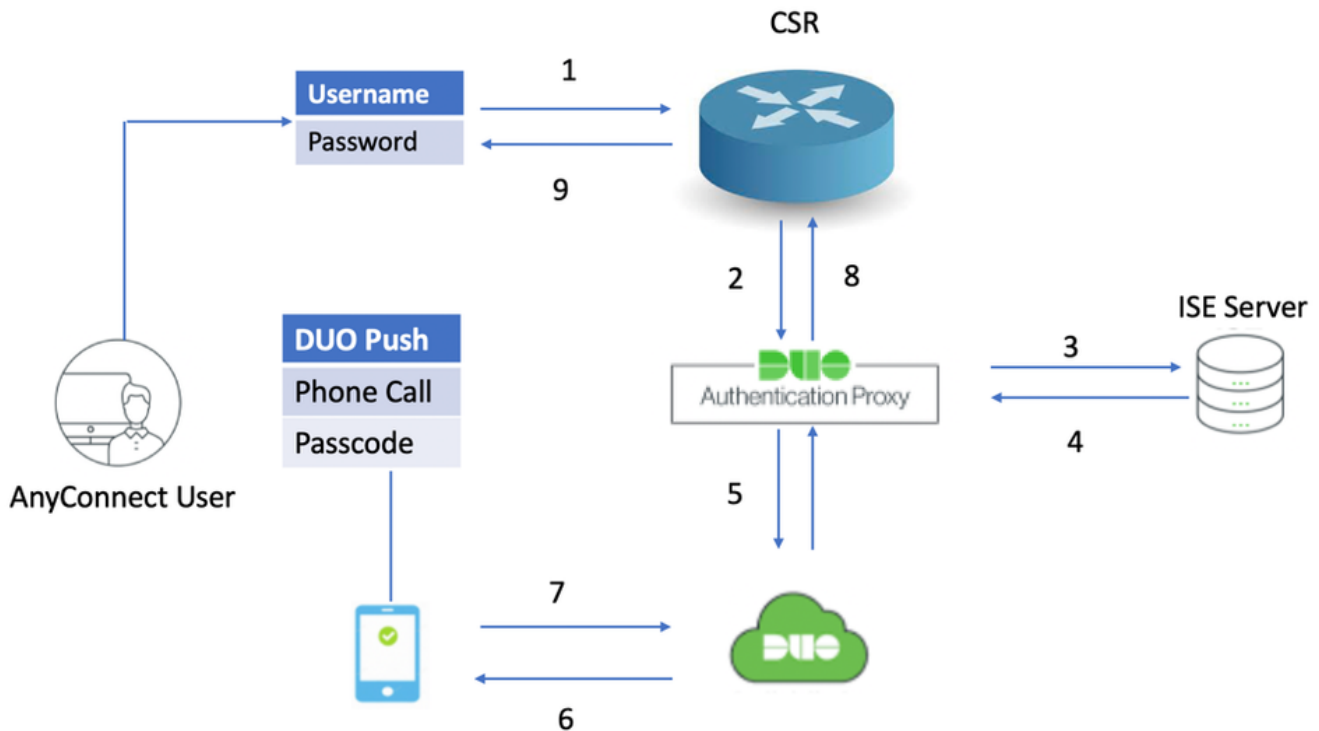
- Cisco AnyConnect Secure Mobility Client، رادصلإا 4.10.04071
- Cisco ISE Running، رادصلإا 3.1.0
- لمعي رتويبمك زاهج ياً وأ Windows 10 لئغشتل ماطن) ئانثلا ةقداصلم لئك و مداخ Linux لئغشتل ماطن ب
- بيولل ع Duo باسح
- AnyConnect هئلع تبتلم لئمعل رتويبمك

ةصاخ ةئيم ةئيب ي ف ةدوجومل ةزهجال نم دنتسلمل اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا). (يضا رتفا) حوسمم نيوكتب دنتسلمل اذه ي ف ةمدختسمل ةزهجال عيمج تادب رما يال لمحتلمل ريثاتلل كمهف نم دكأتف ، لئغشتل دي ق ك تكبش

ةقداصلم لقفت

لسري ISE. مداخل ع رورم ةملكو مدختسم مسا مادختساب AnyConnect مدختسم ةقداصلم متت لومحمل زاهج لئ ع ف د مالع لئش ي ف ةيفاضل ةقداصلم اضيأ Duo Authentication Proxy مداخ مدختسم لابل صاخال

قفدتل لئطختل مسرل



ةقداصلم لقفت ططخم

لاصلال ةئلمع

1. رورم ةملكو مدختسم مسا رفويو C8000V لئ RAVPN لاصلتا ةئيب مت مدختسمل موقي ي . ةئساسال ةقداصلم لل
2. Duo ةقداصلم لئكو لئ ةقداصلم بلط C8000V زارطلل لسري

3. أو Active Directory مداخل إلى أساسيات بلطال يئانثال ةقداصملا ليكول لسري مٲ . RADIUS.
4. ةقداصملا ليكول إلى رخأ ةرم ةقداصملا ةباجتسا لاسرا مٲي .
5. ةيوناث ةقداصم يئانثال ةقداصملا ليكول بلطي ، ةيساسال ةقداصملا حاجن درجمب Duo مداخل ربع .
6. ، ةفدل) ةيوناثال ةقداصملا ةقيرط إلى عانب ، مدختسملا ةقداصمب Duo ةمدخ موقت مٲ (رورملا زمر ، ةيفتاهل ةملاكمل .
7. ةقداصملا ةباجتسا Duo ةقداصم ليكول ملتسي .
8. C8000v إلى ةباجتسال لاسرا مٲي .
9. AnyConnect لاصتا سيسيأت مٲي ، ءارجال اذه حاجن ةلاح ي ف .

نيوكتال

ماسقالا هذه رابتعالا ي ف عض ، نيوكتال لامكإ لجأ نم

(VPN ةكبشب ةصاخلا ثبالاو لابققتسال ةدحو) C8000V إلى نيوكتال تاوطخ

صاخلا IP ناونع وه RADIUS مداخل صاخلا IP ناونع نوكي نأ بجي . RADIUS مداخل نيوكتب مق 1. يئانثال ةقداصملا ليكول

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

2. يلحم مداخل ضيوفتو ةقداصمaaaك RADIUS مداخل نيوكتب مق .

```
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. لعفلاب ةدوجوم نكت مل اذا ، ةيوهال ةداهش تيبتث لجأ نم TrustPoint ءاشنإب مق . نم ديزم إلى لوصحلل [PKI ل ةداهشلا ليچست](#) إلى عوچرلا كنكمي . ةيلحمل ةقداصملا ةداهشلا ءاشنإ لوح ليصافتال

```
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
```

نوكتت. مسقمال قف نلل اهمادختسا متيل ةيسايق لوصو ةمئاق نيوكتب مق (يرايخا). 4. VPN قف نلل نم اهيل لوصولا نكمي يتل ةهجلو تاكبشل نم هذه لوصولا ةمئاق قف نلل نيوكت متي مل اذا VPN قف نلل ربع تانايبل رورم ةكرح عيمج رم، يضارتفا لكشب مسقمال.

```
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 نيوانع عمجت عاشنإ.

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

لاصتا ءانثأ AnyConnect لي عمل IPv4 ناو نع هؤاشنإ مت يذل IP نيوانع عمجت نيغي حاجنب AnyConnect.

6. ليوخت جهن نيوكت.

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

ليوختل جهن نمض كلذلى امو مسقمال قف نلل ةمئاقو DNS و IP عمجت ديدحت متي.



جهن مادختسا متي، صصخم ال IKEv2 ليوخت جهن نيوكت مدع ةلاح ي ف: ةطحالام تامسل عفد اضيأ نكمي. ليوختلل "يضارتفال" ىمسمل يضرارتفال ليوختل RADIUS مداخ ربع IKEv2 ليوخت جهن نمض ةدحمل.

7. IKEv2 ةسايسو حارتقا نيوكت.

```
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. فيرعتل فلم ددحو هجوملل ديهمتلا ةركاذى إلى AnyConnect لي مع فيرعت فلم لي محتب مق 8.
حضم وه امك:

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

9. نمآل HTTP مداخل لي طعت 9.

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

10. فلم ليزننل لي لحم ناونعك هجوملاب صاخال IP WAN ددحو SSL ةسايس نيوكتب مق 10.
فيرعتل.

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

  port 443
```

11. ممقل اي ره اظلال لوصول ةسسؤم عاشنإ هلالخ نم متي يره اظبالق نيوكتب مق 11.
خسننسم

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

(GigabitEthernet1) اهنيوكت مت يثلا ةهجاو لا نم IP ناو نع ىلع مقرملا ريغ رمألا لصحي

دا تامولعم طبرلا طاقن عيجم ىلع يوتحي IKEv2 فيرعت فلم نيوكتب مق 13.

```
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
```

IKEv2: فيرعت فلم في رصانعلا هذه مادختسا متي و

- match identity remote any - لي مع أي نكمتي ىتح انه 'any' نيوكت مت . لي معلا ةي وه ىلى ري شي -
 - authentication remote - لي معلا ةقداصلم EAP لوكتورب مادختسا بجي هنا ىلى ري شي -
 - authentication local - لي معلا ةقداصلم لتاداهشلا مادختسا بجي هنا ىلى راشلا -
 - aaa authentication eap - RADIUS م داخ مدختسي FlexVPN_auth، EAP ةقداصلم اناثا -
 - aaa authorization group eap list - FlexVPN_authz ةكبشلا ةمئاق ، صيخرتلا اناثا -
 - ikev2-authz-policy لي وختلا
 - aaa authorization user eap cached - ي نمضلا مدختسلا صي وفت ني كمت -
 - virtual-template 20 mode auto - هخسن بولطملا يره اظلا بلالقي دحت -
 - anyconnect profile Client_Profile - ىلع انه 8 ةوطخلا في دحمل لي معلا فيرعت فلم قي بطت متي -
- اذه IKEv2 فيرعت فلم

IPSec. فيرعت فلم ولي وحت ةومجم نيوكت 14.

```
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
```

ي.ره اظلا بلالقي ىلى IPSec فيرعت فلم فضا 15.

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

(XML فيرعت فلم) ليمعلا فيرعت فلم نم ةصاصق

ةدحو نم ةيئاقلتلا فيرعتلا فلم تاليزنت رفوتت ال، Cisco IOS XE 16.9.1 لبق
لابقتسالا ةدحو نم فيرعتلا فلم ليزنت نكمملا نم، 16.9.1 دع ب. ثبلالابقتسالا
ثبلالو.

<#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 ةقداصم ليك وىل ع نيوكتل تاوطخ



RADIUS ةقداصم عم طقف MS-CHAPv2 يئانثلا ةقداصم لىك وىل ع دي: ةطخال م

هت يثتو Duo ةقداصم ليك وىل ع مداخل [ليزنت](#) 1. ةوطخال

Duo Authentication Proxy مداخل ت يثت م قو Windows زاه ىل ل وخذل لىجست م ق

صرق ةحاسم و ل قألا ىل ع ةدحاو (CPU) ةيزكرم ةجلاعم ةدحوب دوزم ماظن م ادختساب ىصوي
ت يابايج 4 ةعس (RAM) يئاشع لوصو ةركاذو ت يابايج م 200 غلبت

لك و نيوكتل authproxy.cfg وحتف و C:\Program Files\Duo Security Authentication Proxy\conf\ ىل ل قتنا 2. ةوطخال
ةبسانم ل لىصافتل م ادختساب ةقداصم ل

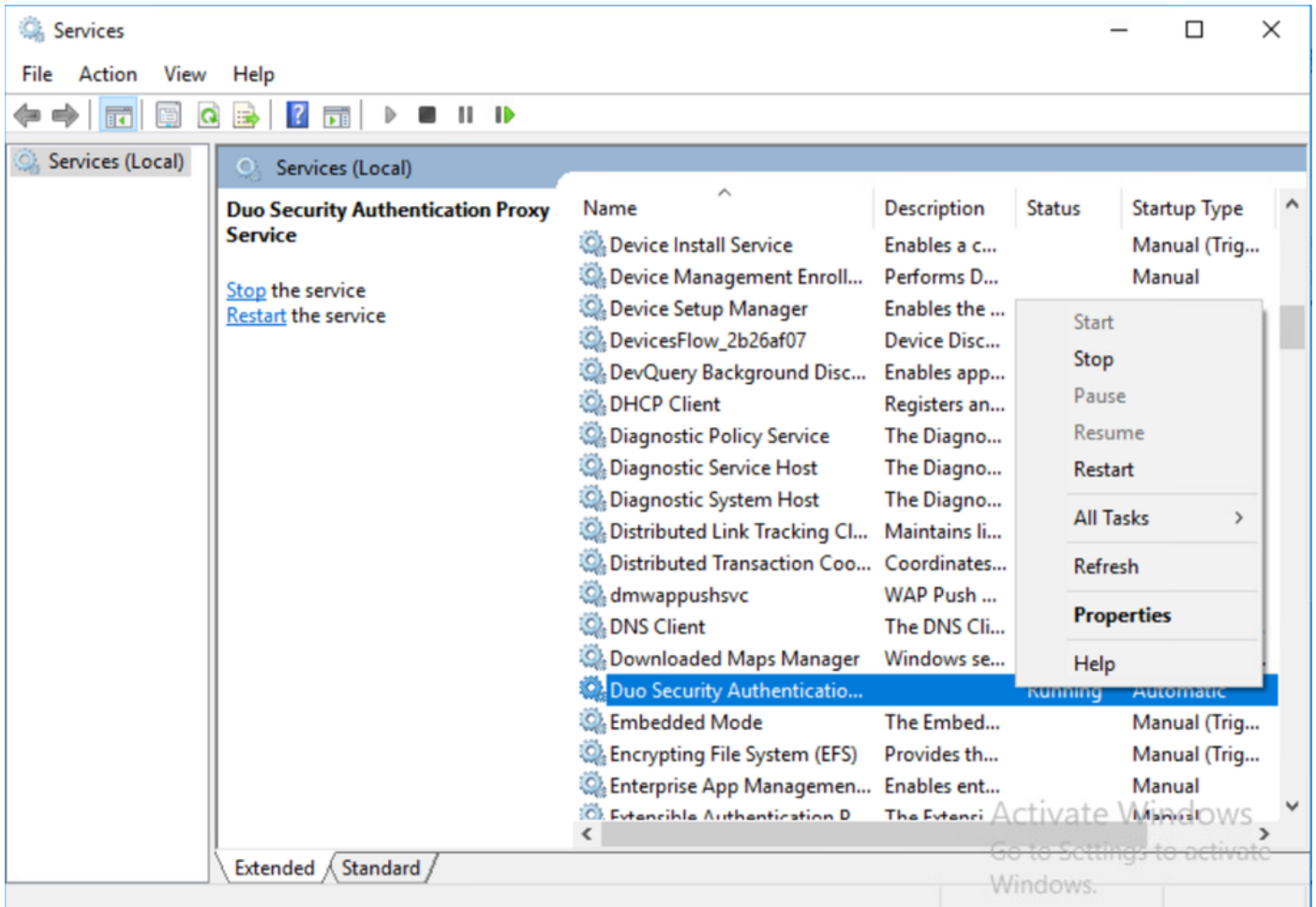
```
[radius_client]
host=10.197.243.116
secret=cisco
```



يتل رورملا ةملك وه 'cisco' و ISE مداخل صاخلا IP ناونع وه '10.197.243.116' انه: ةطخال م
ةيساسالا ةقداصم ل ةحص نم ققحتلل ا ه نيوكت م ت

فللم لظفح م ق ، تاريغتلا هذه ءارج درجم ب

Duo Security Authentication Proxy ليغشتلا ةداع و (services.msc) Windows تامدخ مكحت ةدحوتفا 3. ةوطخال
Service.



يئاتنثل نامألا ةقداصم لىك و ةمدخ

ISE لىل ةنيوكتل تاوطخ

ةكبشلا زاهج ةنيوكتل قوف Add رقناو ، Administration > Network Devices لىل لقنتنا 1. ةوطخل



Duo. ةقداصم لىك و مداخل صاخل IP ناو نعب x.x.x.x لىل ادبتسا : ةطخال

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

Default Device

Device Security Settings

* Name: Sadhana_Duo_Proxy

Description:

IP Address: * IP: x.x.x.x / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations [Set To Default]

IPSEC: No [Set To Default]

Device Type: All Device Types [Set To Default]

authproxy.cfgsecret: في روكذم وه امك رمأل Shared Secret نيوكتب مق 2. ةوطخل

☒ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret Show

Use Second Shared Secret ☐ *i*

Show

CoA Port Set To Default

RADIUS DTLS Settings *i*

DTLS Required ☐ *i*

Shared Secret *i*

CoA Port Set To Default

Issuer CA of ISE Certificates for CoA *i*

DNS Name

General Settings

Enable KeyWrap ☐ *i*

* Key Encryption Key Show

* Message Authenticator Code Key Show

Key Input Format ☒ ASCII ☐ HEXADECIMAL

كترشم رس - ISE

مدختسملا فرعم تلكش Addin order to رتخأ. Administration > Identities > Users. ةوطخل
ةيساسأل AnyConnect ةقداصلم:

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 > sadks

Network Access User

* Name

Status ☒ Enabled

Email

Passwords

Password Type:

Password Re-Enter Password

* Login Password Generate Password *i*

Enable Password Generate Password *i*

نومدختسملا - ISE

Duo ةرادإ لخدم ىل ع نيوكتبلا تاوطخ

كب صاخال Duo باسح ىلإ لوخدلا ليحست 1. ةوطخل

في RADIUS). همادختسإ ديرت يذل قيبطت للProtect رقنا Applications > Protect an Application. ىلإ لقتنا

(ةلإحاله هذه)

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

4149-5271-37

Deployment ID

DUO55

Helpful Links

Documentation

Dashboard > Applications > Protect an Application

Protect an Application

radius

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

قيبطتال - يئانث

(ةلإحاله هذه في RADIUS). همادختسإ ديرت يذلا قيطتاللProtect قوف رقنا 2. ةوطخل

(API) تاقيطتال ةجمر بةهجاو فيضم مساو، يرسلال حاتفملاو، لمكالتال حاتفم خسنا
Duo ةقداصم ليك وauthproxy.cfgىل عهقصلو.

Dashboard > Applications > RADIUS

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

RADIUS - يئانث

امك ميقلال قصلو وauthproxy.cfg حثافاو DUO ةقداصم ليك وىلإ ىرخأ ةرم لقتناو ميقلال هذه خسنا
حضوم وه:

iKey = لمكالتال حاتفم

حاتفم = يرسل الحاتفم

API = api_host فيضم مسا

```
[radius_server_auto]
ikey=xxxxxxxx
skey=xxxxxxxxv1zG
api_host=xxxxxxxx
radius_ip_1=10.106.54.143
radius_secret_1=cisco
failmode=safe
client=radius_client
port=1812
```



مداخل نيوكت دنع Duo مداخل نم api_host و skey و iKey خسن بجي: عظهارم
مت يذل حاتفم الو 'cisco' و، C8000V هجوملاب صاخ ال IP ناوع وه '10.106.54.143' و
Radius مداخل نيوكت نمض هجومل علع هنيوكت

عقداصم ليكو وعمدخ ليغشت دعأ مث رخأ عرم فلمل ظفحب مق، تاريخيغت ال هذه عارج درجب
services.msc). يئانثال نامال

ةيوناثال عقداصم لل duo علع نيمدختسم عاشنإ 3. عوطخل

هباتك وUsers > Add User ممدختسمال مسا ال لقتنا



يساسال عقداصم ممدختسم مسا عم ممدختسمال مسا قباطتي نأ بجي: عظهارم

Add Phone رقناو، فاهال مقرلخدأ، Add Phone رقنا، Phones تحت، اهئاشنإ دنع Add User. رقنا

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

Learn more about Activating Duo Mobile

Type

Phone

Tablet

Phone number

Show extension field

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

Add Phone

فتاه ةفاضل - Duo

ةقداصلال عون رتخا

Device Info

[Learn more about Activating Duo Mobile](#)

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

Model
Unknown

OS
Generic Smartphone

زاهال تامولعم - Duo

رتخا 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 > 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

فتاهال طيشنت - ڤئانث

رتخا 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 لاسر

مدخستسم ل باسحب DUO قيبطت طبرم تي و ف تاهل ال ال ل سرمل طابترال قوف رقنا
ةروصل ال ي ف حضوم وه امك ، عطقم ل Device Info

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
Helpful Links
Documentation

Dashboard > Phones >

Send SMS Passcodes...
Delete Phone

sads

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

Model

OS

Last seen
13 hours ago

Settings

Number

Show extension settings

Device name

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

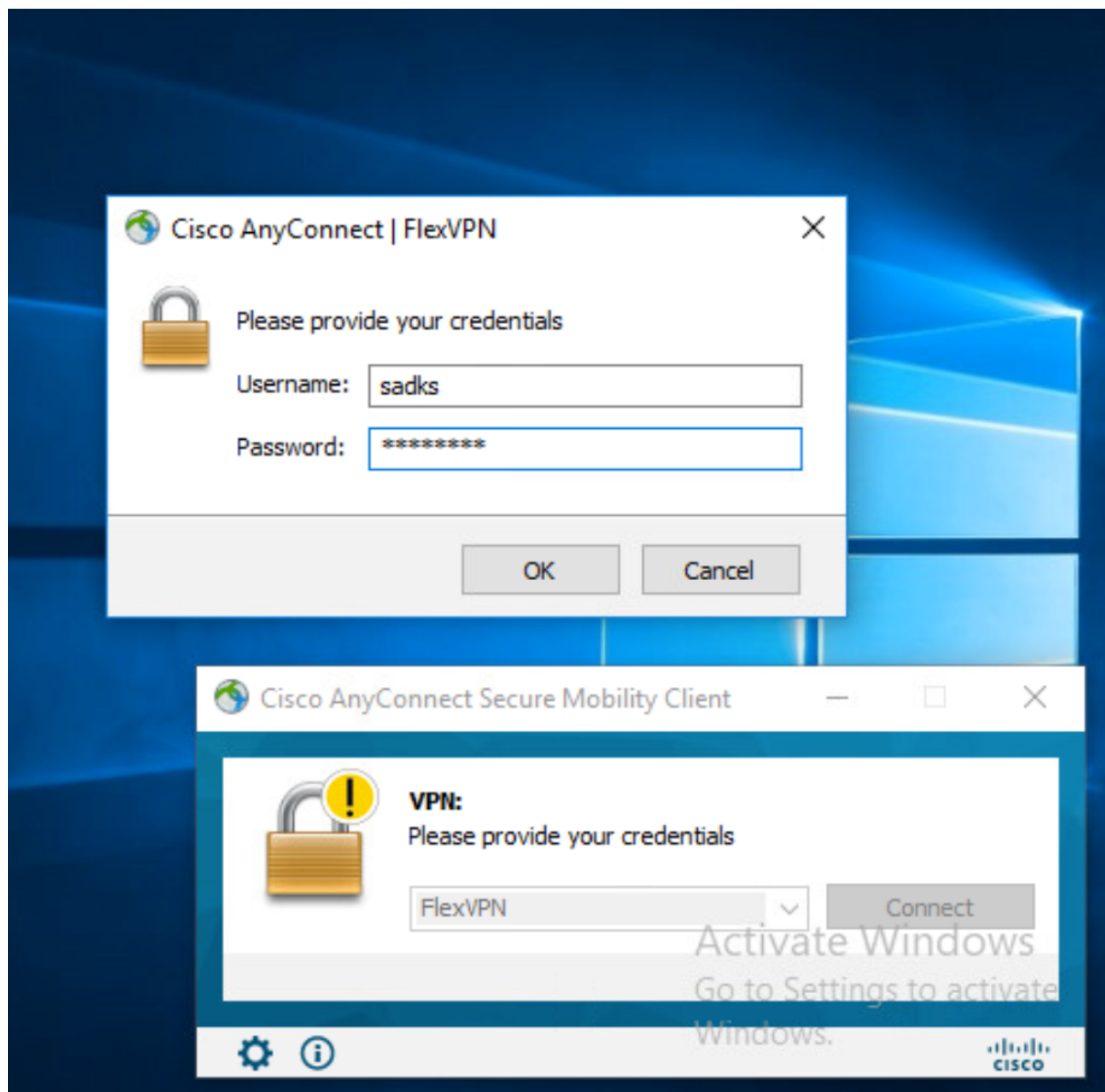
Type

Mobile

Duo - طبرم زاهج

ةحصل ال نم ققحت ال

AnyConnect لالځ نم مدختسم لارتيوېېمك نم C8000V لالاصتالاب مق ،ةقداصم لارابتځال
ةيساسألا ةقداصم لال رورم لال ةملك و مدختسم لال مسا بتكا



AnyConnect لالاصتا

لليابوم لال ىلع يئانثلا طغض يللق ت اهدعبو



(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

ةيساسألأةقداصم للةقداصم لاريقت ضرع كنكمي ISE. Operations > Live Logs إلى لقتنا

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

إرشاب الم تالجال - ISE

4. Verification on DUO authentication proxy

DUO: C:\Program Files\Duo Security Authentication Proxy\log
 ةقداصم ليكوي ف فلملا اذه لىل لقتنا

<#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>
```

اهحال صاوعاطخ ال افاشكتسا

1. C8000v. عاطخ ال احيصت

IKEv2 ل ةبسنلاب

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

ل IPSec:

- debug crypto ipsec
- debug crypto ipsec error

لجسلا فلم ليكوب ةقلعتملا تالجسلا نم ققحت ،DUO ةقداصم ليكول ةبسئلاب 2.

(C:\Program Files\Duo Security Authentication Proxy\log

:ةيساسألا ةقداصملا ضفري ISE ثيح لجسأطخ ل ةصاقل رهظي

<#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

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا