

يـمـدخـتـسـمـل تـبـاـثـل IP نـاـوـنـع نـيـيـعـت نـيـوـكـت لـيـمـعـلـل ةـنـمـآـل VPN

تـاـيـوـتـحـمـلـا

[ةـمـدقـمـلـا](#)

[ةـيـسـاـسـاـلـا تـاـبـلـطـمـلـا](#)

[تـاـبـلـطـمـلـا](#)

[ةـمـدخـتـسـمـلـا تـاـنـوـكـمـلـا](#)

[ةـيـسـاـسـاـتـاـمـوـلـعـم](#)

[نـيـوـكـتـلـا](#)

[ةـحـصـلـا نـمـقـقـحـتـلـا](#)

[اـهـجـاـلـصـاـوـعـاـطـخـاـلـا فـاـشـكـتـسـا](#)

ةـمـدقـمـلـا

نـع لـوـصـوـلـل VPN يـمـدخـتـسـمـل ةـتـبـاـثـل IP نـيـوـانـع صـيـصـخـت ةـيـفـيـك دـنـتـسـمـلـا اذـه حـضـوـي
بـ LDAP تـاـمـس ةـطـيـرـخ مـاـدخـتـسـاـب دـعـب

ةـيـسـاـسـاـلـا تـاـبـلـطـمـلـا

تـاـبـلـطـمـلـا

ةـيـلـاـتـلـا عـيـضـاـوـمـلـا بـ ةـفـرـعـم كـيـدـل نـوـكـت نـأـب Cisco يـصـوـت

- ةـمـدخـ Active Directory (AD)
- لـيـلـدـلـل لـوـصـوـلـل فـيـفـخـل لـوـكـوـتـوـرـبـلـا (LDAP)
- نـم نـمـآـلـا ةـيـاـمـحـلـا رـاـدج دـيـدـهـت دـض عـاـفـدـلـا Cisco
- نـم نـمـآـلـا ةـيـاـمـحـلـا رـاـدج ةـرـاـدـا زـكـرـم Cisco

ةـمـدخـتـسـمـلـا تـاـنـوـكـمـلـا

ةـيـلـاـتـلـا ةـيـدـاـمـلـا تـاـنـوـكـمـلـا وـاـجـمـاـرـبـلـا تـاـرـاـدـصـاـلـا دـنـتـسـمـلـا اذـه فـي ةـدـرـاـوـلـا تـاـمـوـلـعـمـلـا دـنـتـسـت

- Windows Server 2022 لـيـغـشـتـلـا مـاـظـن
- 7.4.2 رـاـدـصـاـلـا FTD
- 7.4.2 رـاـدـصـاـلـا FMC

ةـصـاـخ ةـيـلـمـعـم ةـئـيـب فـي ةـدـوـجـوـمـلـا ةـزـهـجـاـلـا نـم دـنـتـسـمـلـا اذـه فـي ةـدـرـاـوـلـا تـاـمـوـلـعـمـلـا عـاـشـنـا مـت
تـنـاـك اذـا. (يـضـاـرـتـفـا) حـوـسـمـم نـيـوـكـتـب دـنـتـسـمـلـا اذـه فـي ةـمـدخـتـسـمـلـا ةـزـهـجـاـلـا عـيـمـج تـأـدـب
رـمـأ يـاـل لـمـتـحـمـلـا رـيـثـأـتـلـل كـمـهـف نـم دـكـأـتـف، لـيـغـشـتـلـا دـيـق كـتـكـبـش

آساساً تامول عم

ف LDAP تامس طئارخ نڤوكتو IP ناونع نڤيعل قاطن مادختسا راڤخ معد متي: ةظحالم رادصا 6.7 وا FirePOWER رادصا نا نم دكات. ثدحا رادصا وا FirePOWER نم 6.7 رادصا لادصا لبق ثدحا ةعباتملا لبق ثدحا.

نڤوكتل

دعب نع لوصول VPN ةسايس ددحو دعب نع لوصول > زهجالا لىل لقتنا 1. ةوطخلا مداخل املاع ددح، AAA بڤوبتلا ةمالع تحت. بولطملا لىصوتلا فىصوت ددح. ةبولطملا ضيوفتلا مداخو ةقداصملا.

Edit Connection Profile



Connection Profile:* RAVPN_PROFILE

Group Policy:* DfltGrpPolicy +

[Edit Group Policy](#)

Client Address Assignment AAA Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: WINDOWS_2022_AD (AD)

Fallback to LOCAL Authentication

Use secondary authentication

Authorization

Authorization Server: Use same authentication server

Allow connection only if user exists in authorization database

[Configure LDAP Attribute Map](#)

Accounting

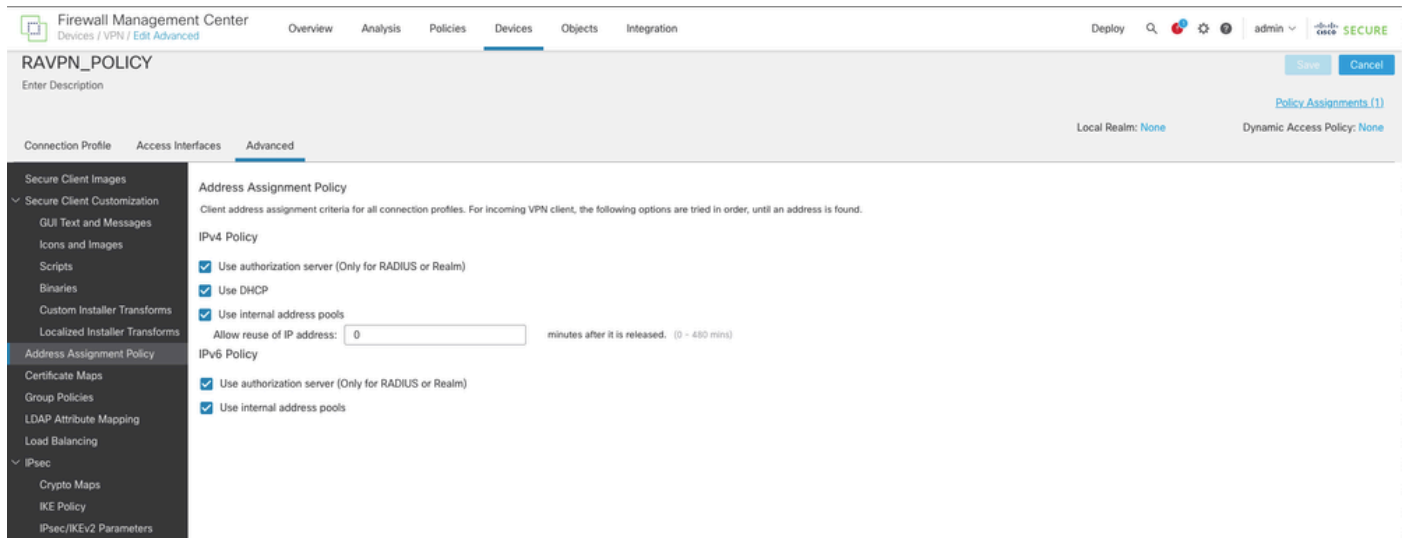
Accounting Server:

▶ Advanced Settings

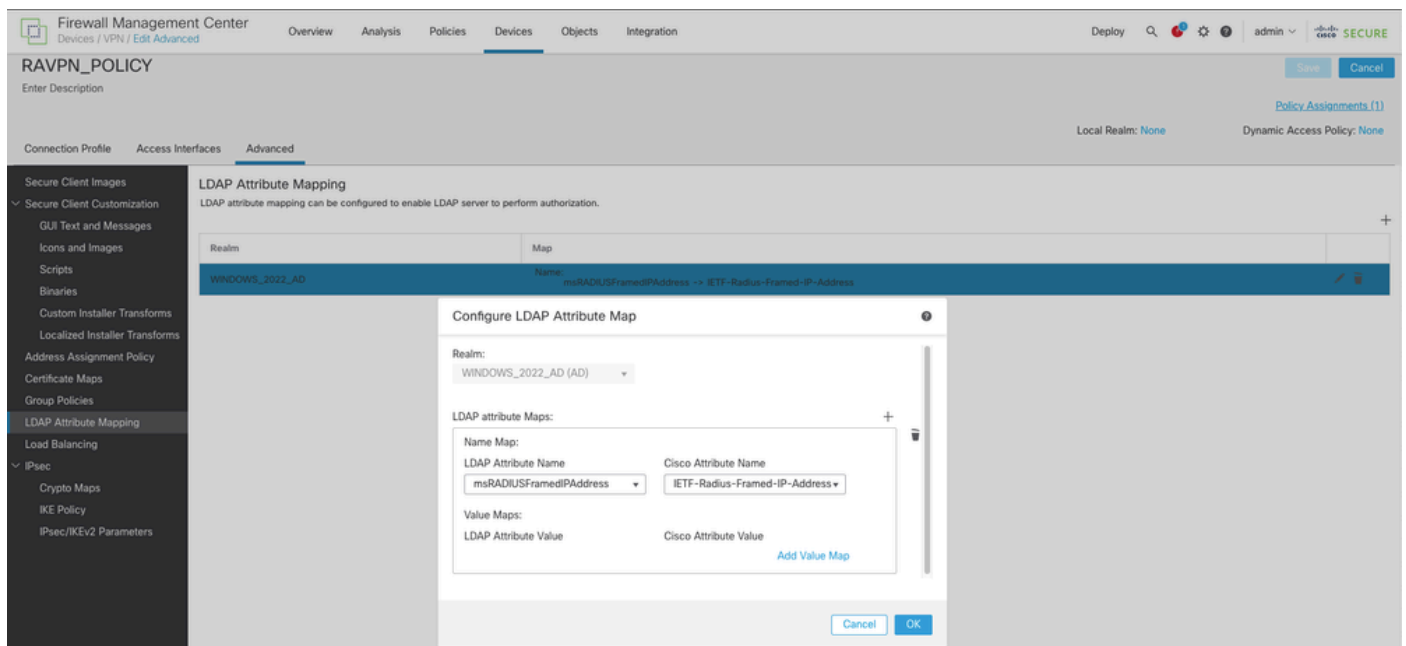
Cancel

Save

ب. لولطم لا دع ب نع لوصولل VPN جهن ددحو دع ب نع لوصولا > ةزهجالا ىلإ لقتنا 2. ةوطخلال
ضىو فتلا م داخ مادختسا راىخ ني كمت نم دكأتو ناو نعلال نيي عت ةسايس > مدقتم ىلإ لقتنا
(ق اطنلا وأ RADIUS ل طقف).



LDAP ةمس مساب مسا ةطيرخ فضا أو LDAP ةمس نيي عت > مدقتم ىلإ لقتنا 3. ةوطخلال
IETF-Radius-Framed-IP-Address ىلإ ةطوبضم و cisco attribute name و msRADIOusfRamedIPAddress ىلإ ةطوبضم



Active Directory م دختسم > تاودأ ىلإ لقتنا و م داخال ةرادا حتفا، Windows AD م داخ ىلإ 4. ةوطخلال
ب ل ط > صئاصخ ددح، م دختسم قوف نم ألس وامل رزب رقنا. رتوي بمكلا ةزهجالا و Active Directory
ةتباثلال IP نيوانع نيي عت ىم سملال ب رملال ددحو يفتاه.

John Doe Properties



Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of	Dial-in		Environment		Sessions

Network Access Permission

- Allow access
- Deny access
- Control access through NPS Network Policy

Verify Caller-ID:

Callback Options

- No Callback
- Set by Caller (Routing and Remote Access Service only)
- Always Callback to:

Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

Static IP Addresses ...

Apply Static Routes

Define routes to enable for this Dial-in connection.

Static Routes ...

OK

Cancel

Apply

Help

مدخست مسملل يكي تاتاسا نكاس IP ناونع تني عو ة تباثال IP نيوانع دح. 5 ةوطخال

Static IP Addresses

Assign a static IPv4 address:

Assign a static IPv6 address:

Prefix:

Interface ID:

لمعتسملال ني عي Cisco Secure Client م ادختساب لوخدلا لچسو VPN ةباوبب لصتا 6 ةوطخلال لتكش تنأ نأ يكي تاتسا نكاس ناوعلا

Cisco Secure Client

CISCO Secure Client

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Connection Information

State:	Connected
Tunnel Mode (IPv4):	Tunnel All Traffic
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:26
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information

Client (IPv4):	172.16.20.73
Client (IPv6):	Not Available
Server:	10.0.0.1

Bytes

General

Status Overview

AnyConnect VPN

Zero Trust Access

Network

ISE Posture

Umbrella

Collect diagnostic information for all installed components.

ةحصل لا نم ققحت لا

مق msRADIOamedIPAddress LDAP: ةمس دادر تس لا نم دكأتو 255 debug ldap نم كمتب مق

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = .....fA.f...;.,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = .....Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
[13] sAMAccountType: value = 805306368
```

```
[13] userPrincipalName: value = jdoe@test.example
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASavedFramedIPAddress: value = -1408232375
[13] dScorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

اهحال صإو ءاطخأل فاشك تسأ

ححصت لل رم أوأ:

```
debug webVPN 255
```

```
debug ldap
```

ببول طم لل RA VPN م دختسم لآ ن ع م لآ تباثل ل IP ناو نع ءحص نم ققحت لل رمأ:

```
show vpn-sessionDB AnyConnect filter name <username>
```

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect filter name jdoe
```

Session Type: AnyConnect

Username : jdoe Index : 7

Assigned IP : 172.16.20.73 Public IP : 10.0.0.10

Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel

License : AnyConnect Premium

Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384

Bytes Tx : 14664 Bytes Rx : 26949

Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE

Login Time : 11:45:48 UTC Sun Sep 29 2024

Duration : 0h:38m:59s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : cb0071820000700066f93dec

Security Grp : none Tunnel Zone : 0

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل