

為安全客戶端VPN使用者配置靜態IP地址分配

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹如何使用LDAP屬性對映為遠端訪問VPN使用者分配靜態IP地址。

必要條件

需求

思科建議您瞭解以下主題：

- Active Directory (AD)
- 輕量型目錄存取通訊協定(LDAP)
- 思科安全防火牆威脅防禦
- Cisco安全防火牆管理中心


採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Windows Server 2022
- FTD 7.4.2版
- FMC 7.4.2版

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。

背景資訊

 注意：Firepower 6.7版或更高版本支援使用領域進行IP地址分配並配置LDAP屬性對映的選項。在繼續操作之前，請確保firepower版本為6.7或更高版本。

設定

步驟 1. 導航到 Devices > Remote Access，然後選擇所需的 Remote Access VPN Policy。選擇所需的 Connection Profile。在 AAA 頁籤下，選擇 Authentication Server 和 Authorization Server 的領域。

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](#)

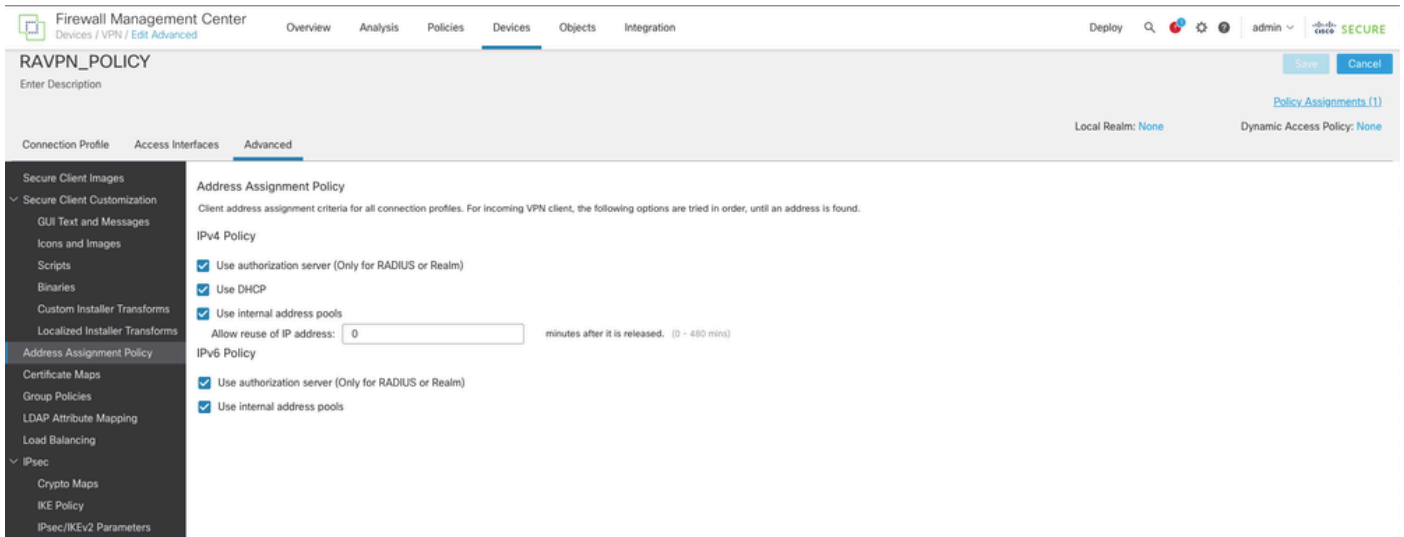
Accounting

Accounting Server: ▾

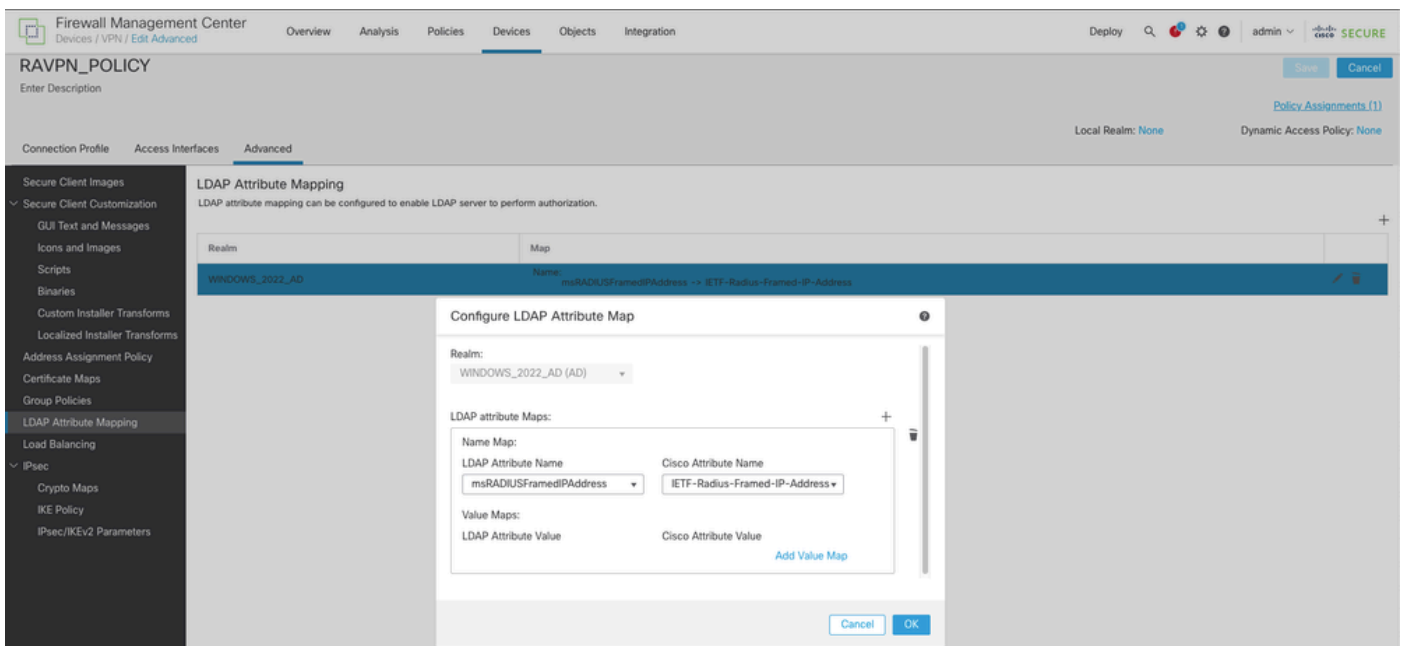
▶ Advanced Settings

[Cancel](#) [Save](#)

步驟 2. 導航到 Devices > Remote Access，然後選擇所需的遠端訪問 VPN 策略。導航到高級 > 地址分配策略，確保啟用使用授權伺服器（僅適用於 RADIUS 或領域）選項。



步驟 3. 導航到 Advanced > LDAP Attribute Mapping 並增加 Name Map，其中 LDAP Attribute Name set to msRADIUSFramedIPAddress，Cisco Attribute Name set to IETF-Radius-Framed-IP-Address。



步驟 4. 在 Windows AD 伺服器上，打開伺服器管理器，然後導航到 工具 > Active Directory 使用者和電腦。按一下右鍵使用者，選擇屬性 > 撥入，然後選中名為分配靜態 IP 地址的框。

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:

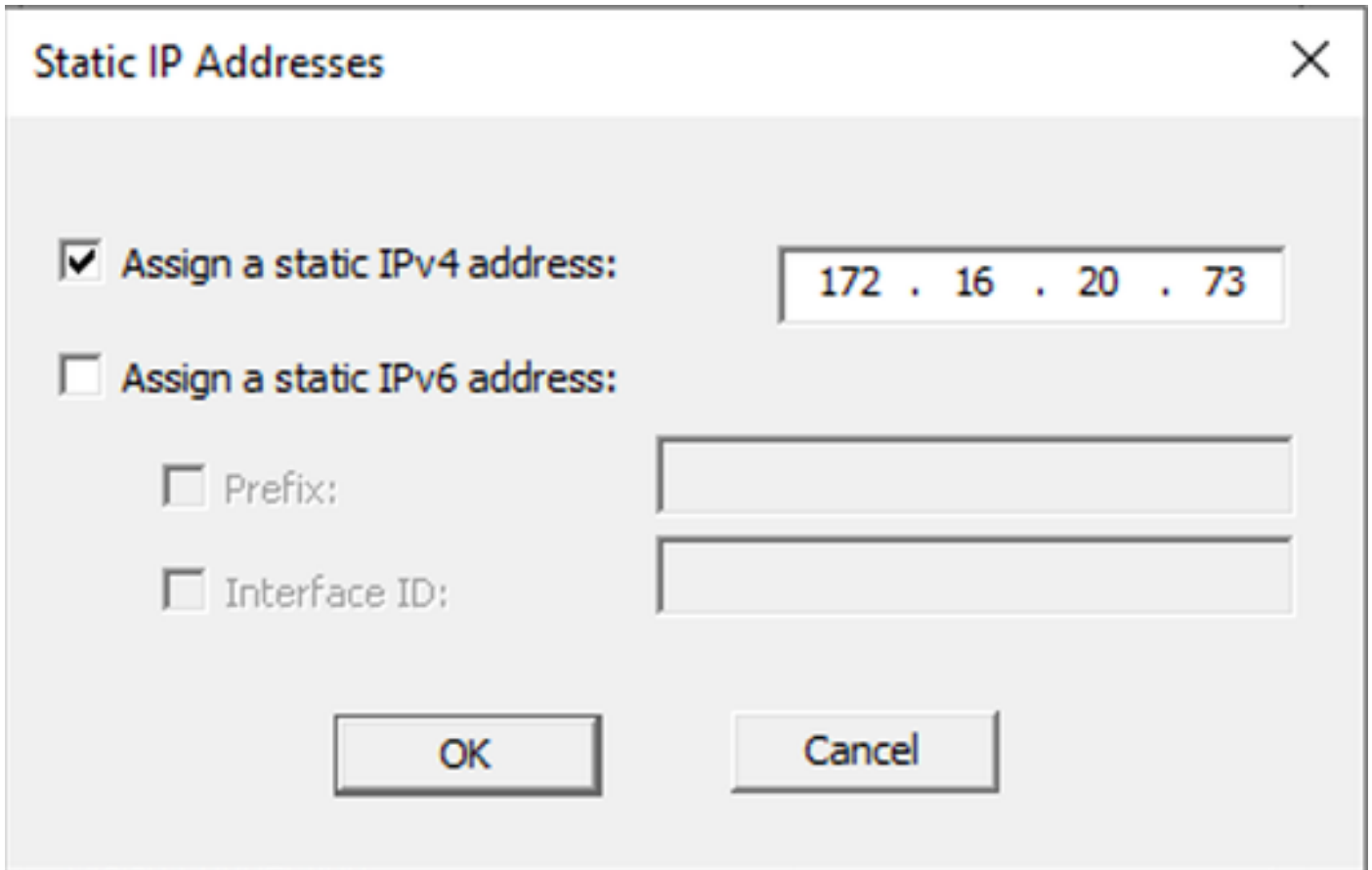
Assign Static IP Addresses

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

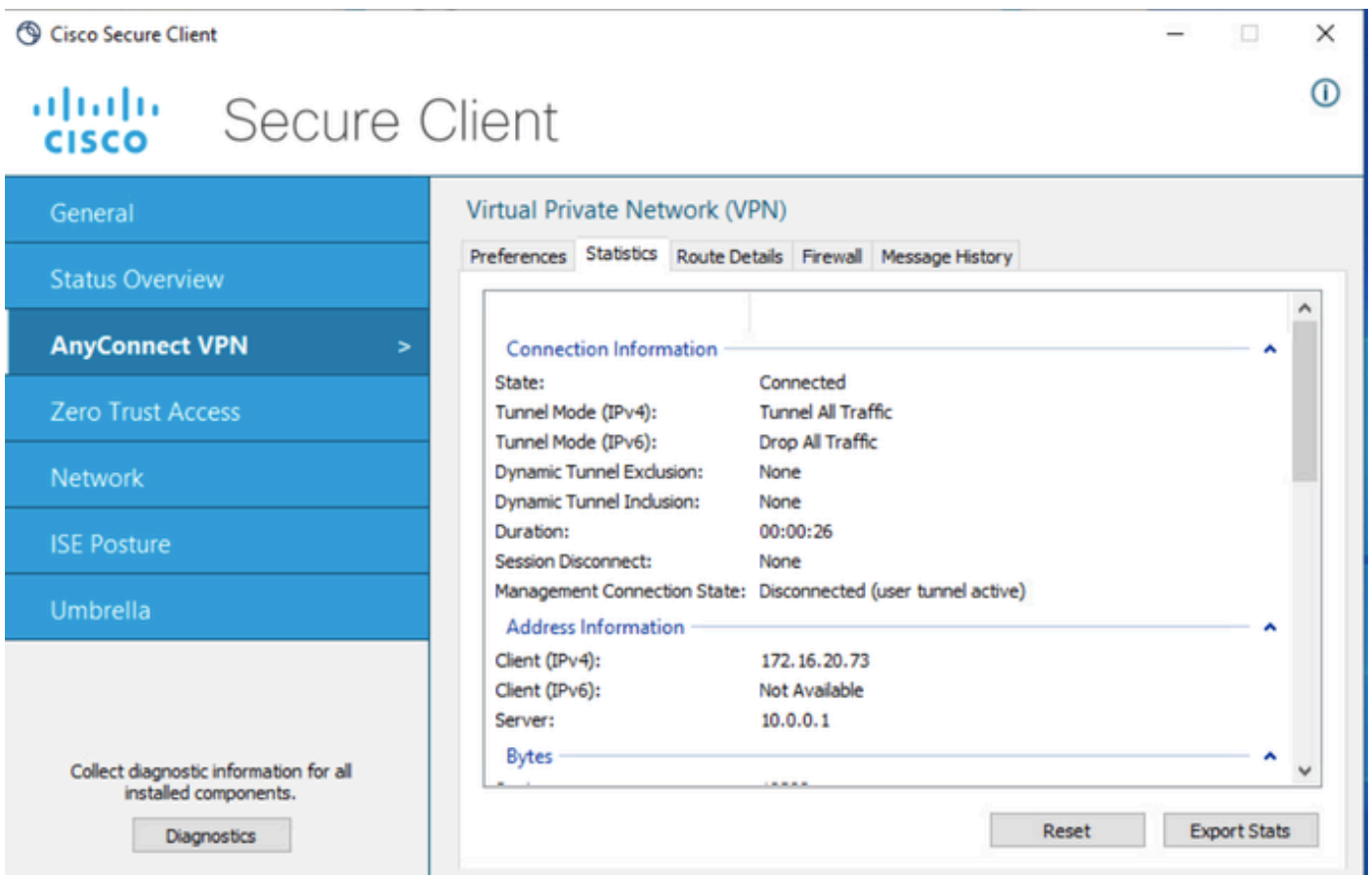
Apply Static Routes

Define routes to enable for this Dial-in connection.

步驟 5.選擇Static IP Addresses並向使用者分配static IP address。



步驟 6.連線到VPN網關並使用Cisco Secure Client登入。系統將為使用者分配您配置的靜態IP地址。



驗證

啟用debug ldap 255並確保檢索到msRADIUSFramedIPAddress LDAP屬性：

```
[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
```

疑難排解

調試命令：

```
debug webvpn 255
```

```
debug ldap
```

用於驗證分配給所需RA VPN使用者的靜態IP地址的命令：

```
show vpn-sessiondb anyconnect filter name <使用者名稱>
```

```
<#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
```

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）。