تكوين تعيين عنوان IP الثابت لمستخدمي VPN الآمنة للعميل

المحتويات

المقدمة

يوضح هذا المستند كيفية تخصيص عناوين IP الثابتة لمستخدمي VPN للوصول عن بعد باستخدام خريطة سمات LDAP.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- خدمة Active Directory (AD)
- البروتوكول الخفيف للوصول للدليل (LDAP)
- الدفاع ضد تهديد جدار الحماية الآمن من Cisco
- مركز إدارة جدار الحماية الآمن من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- نظام التشغيل Windows Server 2022
- FTD الإصدار 7.4.2
- FMC، الإصدار 7.4.2

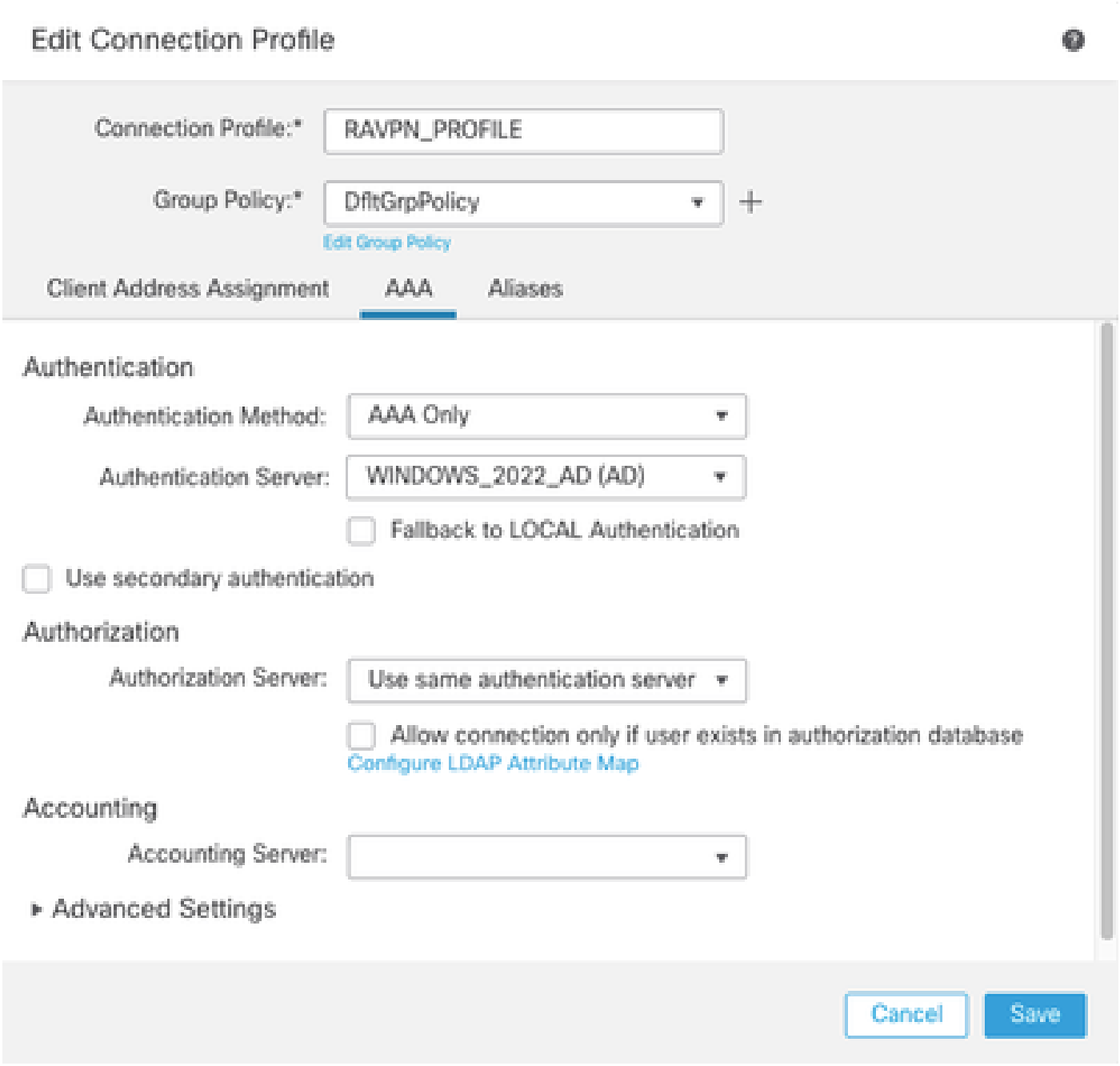
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

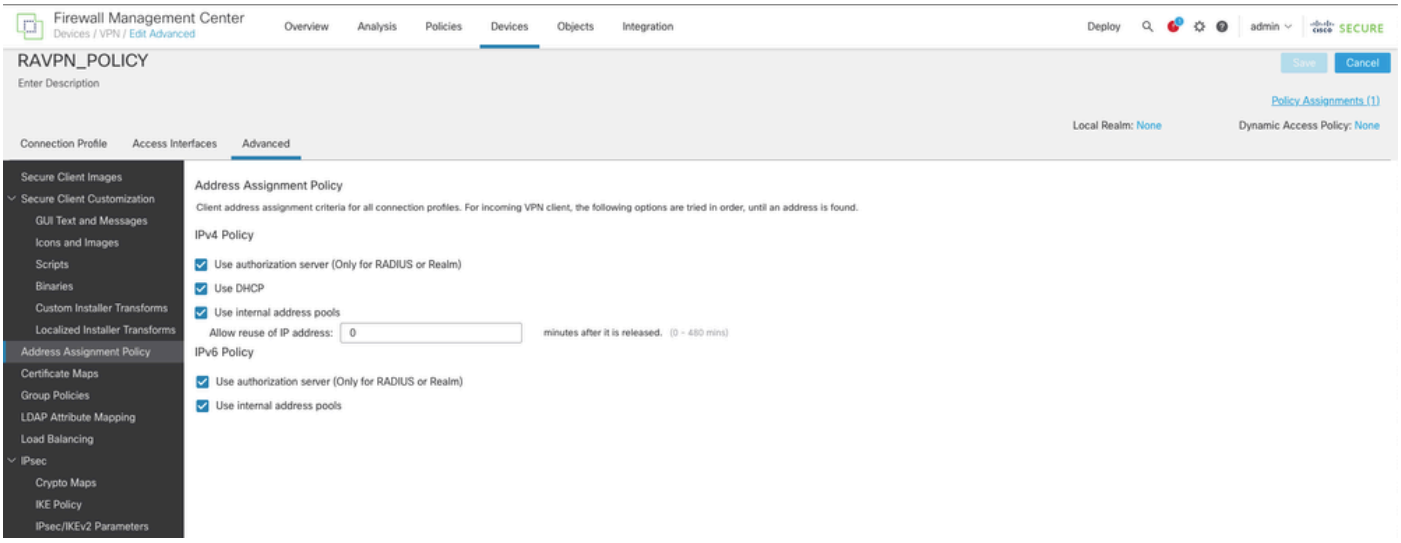
ملاحظة: يتم دعم خيار إستخدام نطاق لتعييني عنوان IP وتكوين خرائط سمات LDAP في الإصدار 6.7 من FirePOWER وأ إصدار أحدث. تأكد من أن إصدار FirePOWER هو 6.7 وأ إصدار أحدث قبل المتابعة.

التكوين

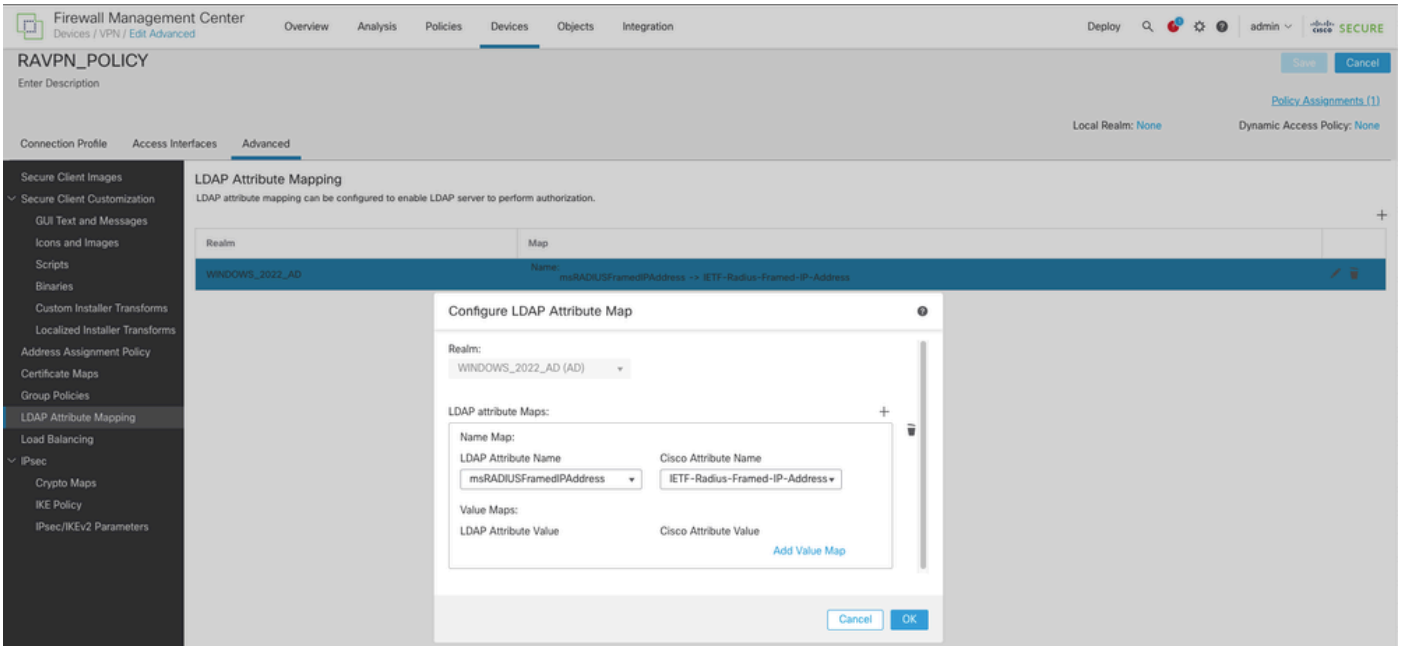
الخطوة 1. انتقل إلى الأجهزة > الوصول عن بعد وحدد سياسة VPN للوصول عن بعد المطلوبة. حدد توصيف التوصيل المطلوب. تحت علامة التبويب AAA، حدد عالم لخادم المصادقة وخادم التفويض.



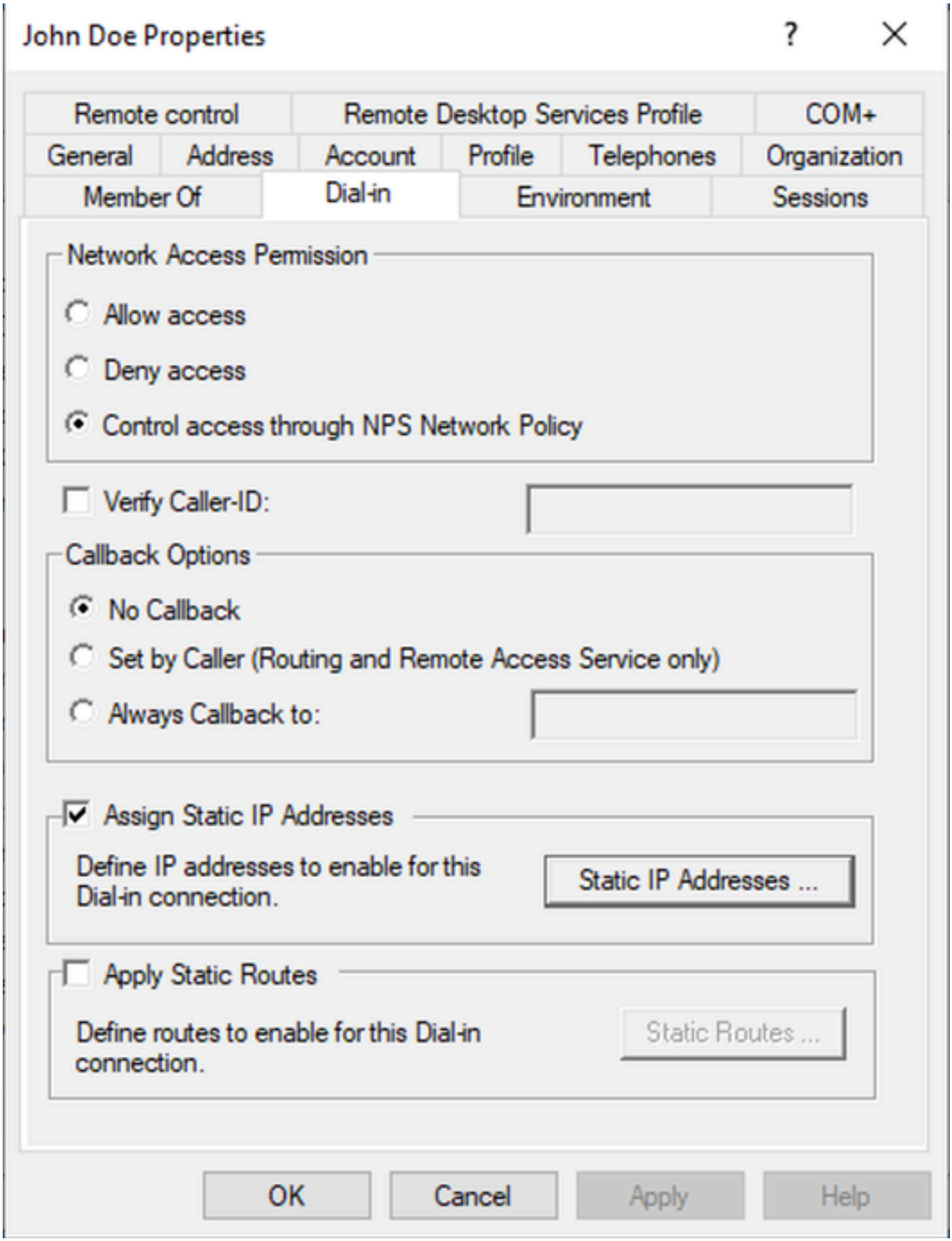
الخطوة 2. انتقل إلى الأجهزة > الوصول عن بعد وحدد نهج VPN للوصول عن بعد المطلوب. انتقل إلى متقدم > سياسة تعيين العنوان وتأكد من تمكين خيار إستخدام خادم التفويض (فقط ل RADIUS أو النطاق).



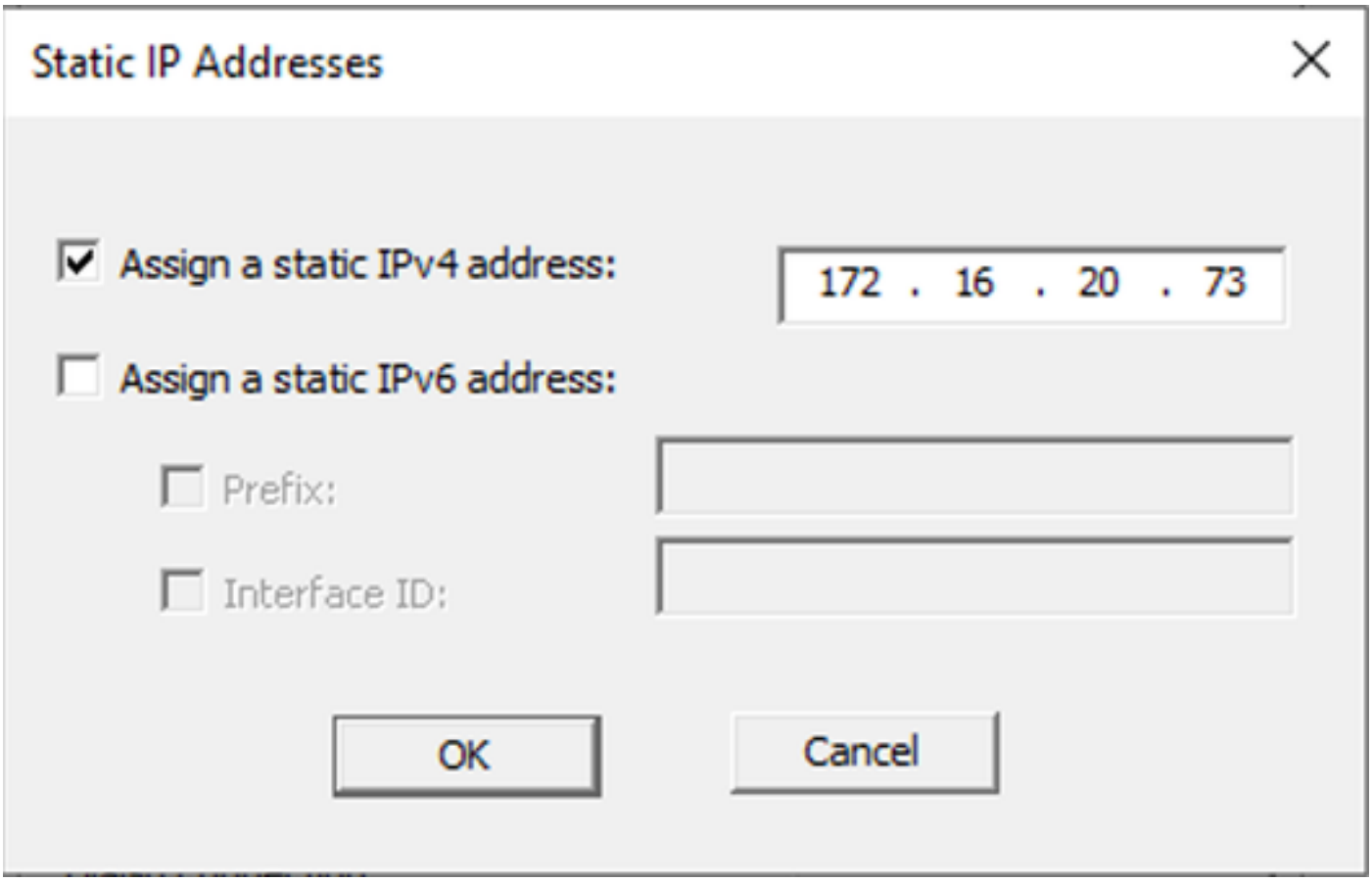
الخطوة 3. انتقل إلى متقدم > تعيين سمة LDAP وأضف خريطة اسم باسم سمة LDAP مضبوطة على msRADIOusfRamedIPAddress وcisco attribute name مضبوطة على IETF-Radius-Framed-IP-Address.



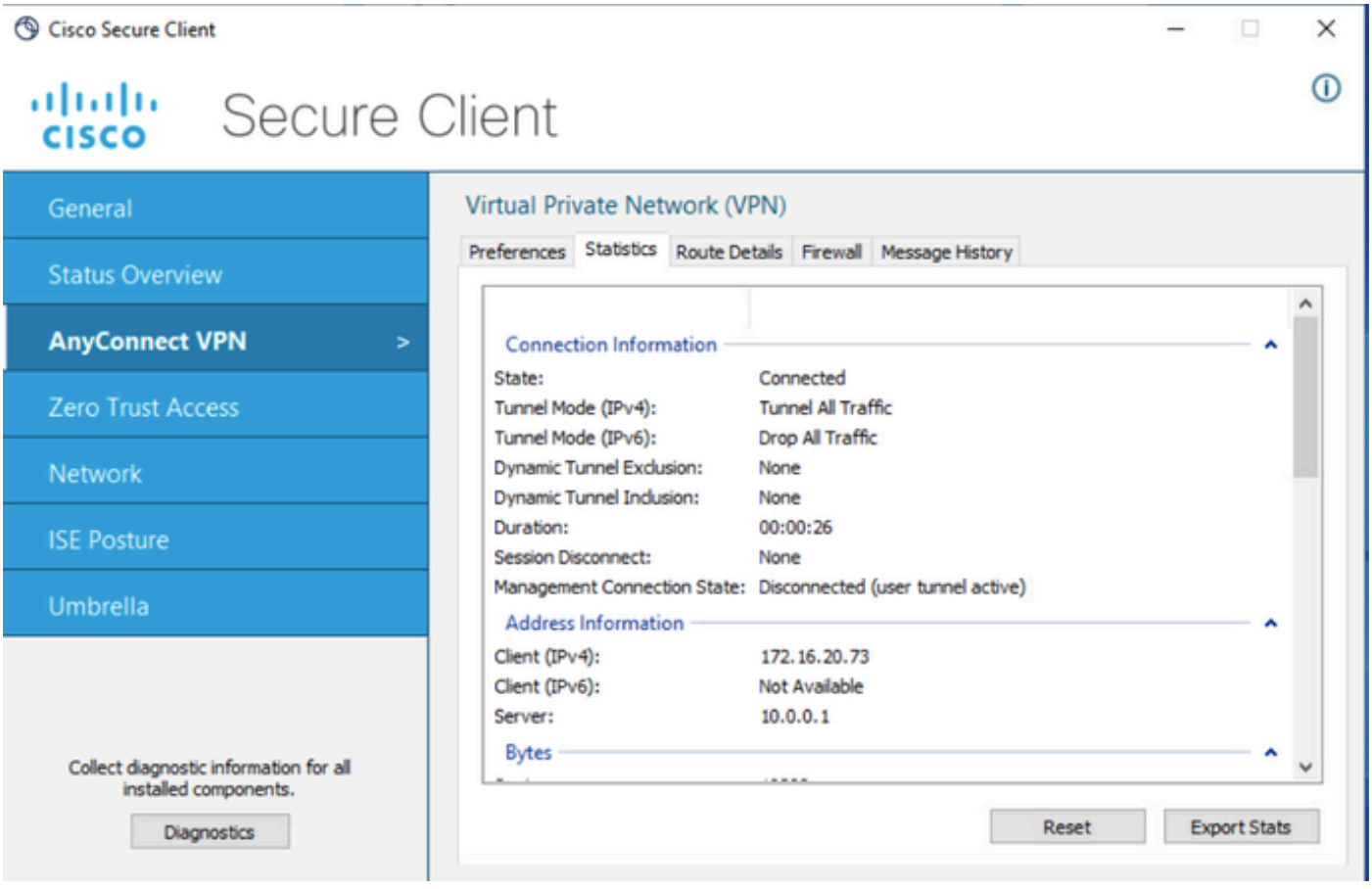
الخطوة 4. على خادم Windows AD، افتح إدارة الخادم وانتقل إلى أدوات > مستخدمي Active Directory وأجهزة الكمبيوتر. انقر بزر الماوس الأيمن فوق مستخدم، حدد خصائص > طلب هاتفي وحدد المربع المسمى تعيين عناوين IP الثابتة.



الخطوة 5. حدد عناوين IP الثابتة وعينت عنوان IP ساكن إستاتيكي للمستخدم.



الخطوة 6. اتصل ببوابة VPN وسجل الدخول باستخدام Cisco Secure Client. يعين المستعمل العنوان ساكن إستاتيكي أن أنت شكلت.



التحقق من الصحة

قم بتمكين debug ldap 255 وتأكد من إستيراد سمة msRADIOramedIPAddress LDAP:

```
[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] msRASSavedFramedIPAddress: 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
```

استكشاف الأخطاء وإصلاحها

أوامر التصحيح:

debug webVPN 255

debug ldap

أمر للتحقق من صحة عنوان IP الثابت المعين إلى مستخدم RA VPN المطلوب:

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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).