配置FlexVPN遠端使用者的RADIUS屬性對映

目錄

簡介

本文檔介紹如何使用思科身份服務引擎(ISE)配置FlexVPN以驗證身份並執行屬性組對映。

必要條件

需求

思科建議您瞭解以下主題：

- 透過CLI在Cisco IOS® XE路由器上配置具有IKEV2/IPsec的遠端訪問虛擬專用網路(RAVPN)
- 思科身份服務引擎(ISE)配置
- 思科安全使用者端(CSC)
- RADIUS通訊協定

採用元件

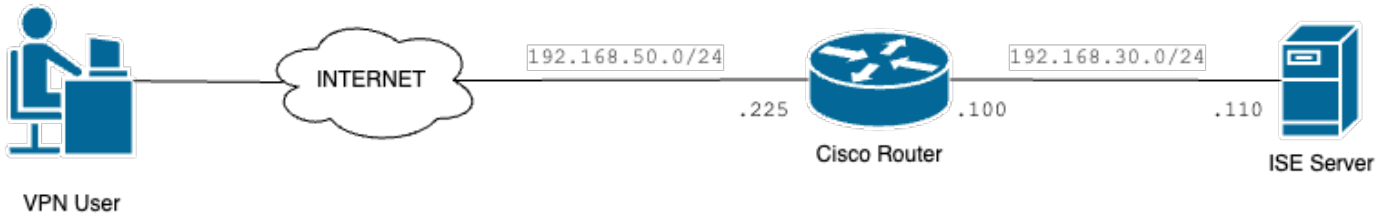
本檔案根據這些軟體和硬體版本：

- Cisco CSR1000V (VXE) - 17.03.04a版
- 思科身分辨識服務引擎(ISE) - 3.1
- 思科安全使用者端(CSC) - 5.0.05040版
- Windows 11

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。

設定

網路圖表



基本網路圖表

組態

路由器配置

步驟 1.在裝置上配置RADIUS伺服器進行身份驗證和本地授權：

```
aaa new-model
aaa group server radius FlexVPN-Authentication-Server
server-private 192.168.30.110 key Cisco123
aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server
aaa authorization network FlexVPN-Authorization-List local
```

aaa authentication login <list_name>命令是指身份驗證、授權和記帳(AAA)組（用於定義RADIUS伺服器）。

aaa authorization network <list_name> local命令宣告將使用本地定義的使用者/組。

步驟2. 配置信任點以儲存路由器證書。由於路由器的本地身份驗證型別為RSA，因此裝置要求伺服器使用證書對自身進行身份驗證：

```
crypto pki trustpoint FlexVPN-TP
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
revocation-check none
rsakeypair FlexVPN_KEY
```

步驟 3.為每個不同的使用者組定義IP本地池：

```
ip local pool group1 172.16.10.1 172.16.10.50
ip local pool group2 172.16.20.1 172.16.20.50
```

步驟 4. 配置本地授權策略：

```
crypto ikev2 authorization policy FlexVPN-Local-Policy
```

由於身份驗證伺服器負責根據使用者所屬的組傳送相關值（DNS、池、受保護的路由等），因此無需對授權策略進行配置。但是，必須將其配置為在本地授權資料庫中定義使用者名稱。

步驟5 （可選）。建立IKEv2方案和策略（如果未配置，則使用智慧預設值）：

```
crypto ikev2 proposal IKEv2-prop
 encryption aes-cbc-256
 integrity sha256
 group 14

crypto ikev2 policy IKEv2-pol
 proposal IKEv2-prop
```

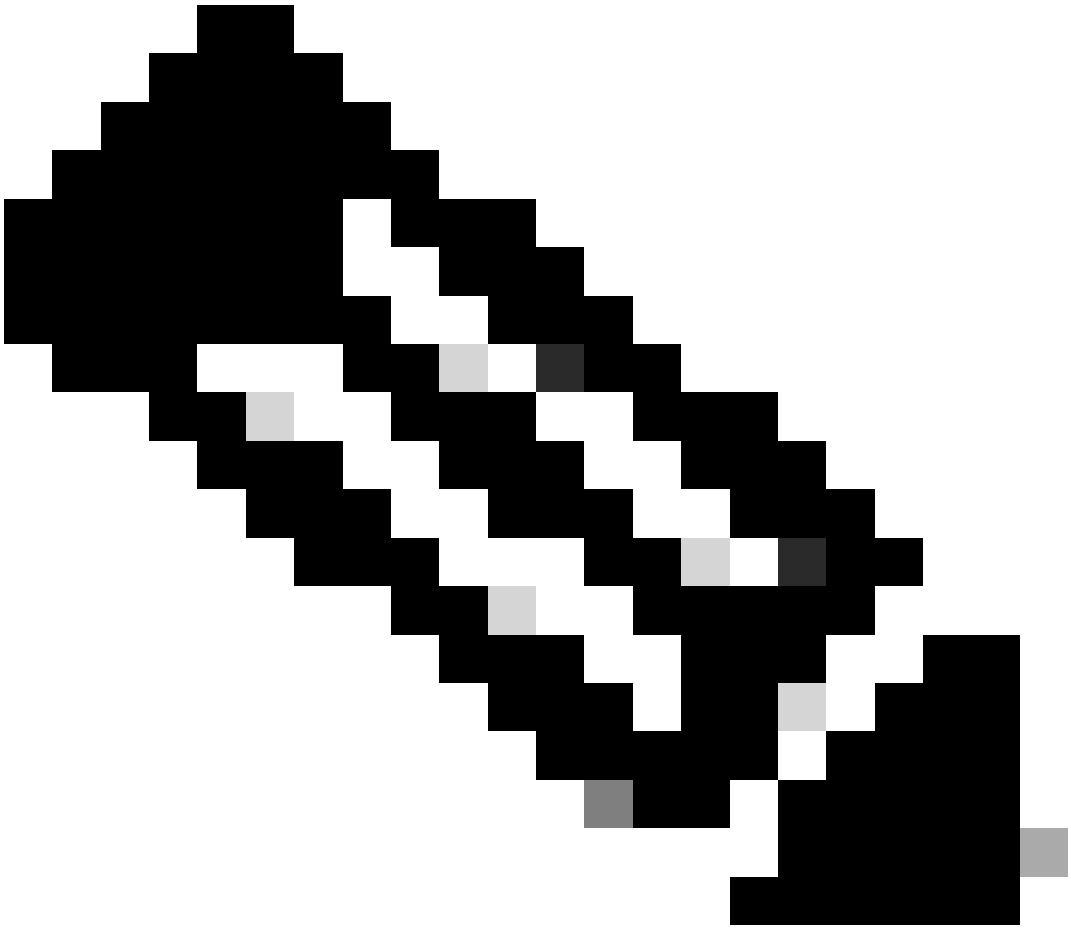
步驟6 （可選）。配置轉換集（如果未配置，則使用智慧預設值）：

```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel
```

步驟 7. 使用正確的本地和遠端身份、身份驗證方法（本地和遠端）、信任點、AAA以及用於連線的虛擬模板介面配置IKEv2配置檔案：

```
crypto ikev2 profile FlexVPN-IKEv2-Profile
match identity remote key-id cisco.example
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FlexVPN-TP
aaa authentication eap FlexVPN-Authentication-List
aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy
aaa authorization user eap cached
virtual-template 100
```

命令aaa authorization user eap cached指定必須快取在EAP身份驗證期間接收的屬性。 此命令對於配置非常重要，因為如果沒有此命令，則不會使用身份驗證伺服器傳送的資料，從而導致連線失敗。



注意：遠端金鑰ID必須與XML檔案中的金鑰ID值匹配。如果未在XML檔案中對其進行修改，將使用預設值(*$AnyConnectClient$*)，並且必須在IKEv2配置檔案中進行配置。

步驟 8. 配置IPsec配置檔案並分配轉換集和IKEv2配置檔案：

```
crypto ipsec profile FlexVPN-IPsec-Profile
set transform-set TS
set ikev2-profile FlexVPN-IKEv2-Profile
```

步驟 9. 配置環回介面。虛擬訪問介面從它借用IP地址：

```
interface Loopback100
ip address 10.0.0.1 255.255.255.255
```

步驟 10. 建立將用於建立不同虛擬訪問介面的虛擬模板，並連結第8步中建立的IPSec配置檔案：

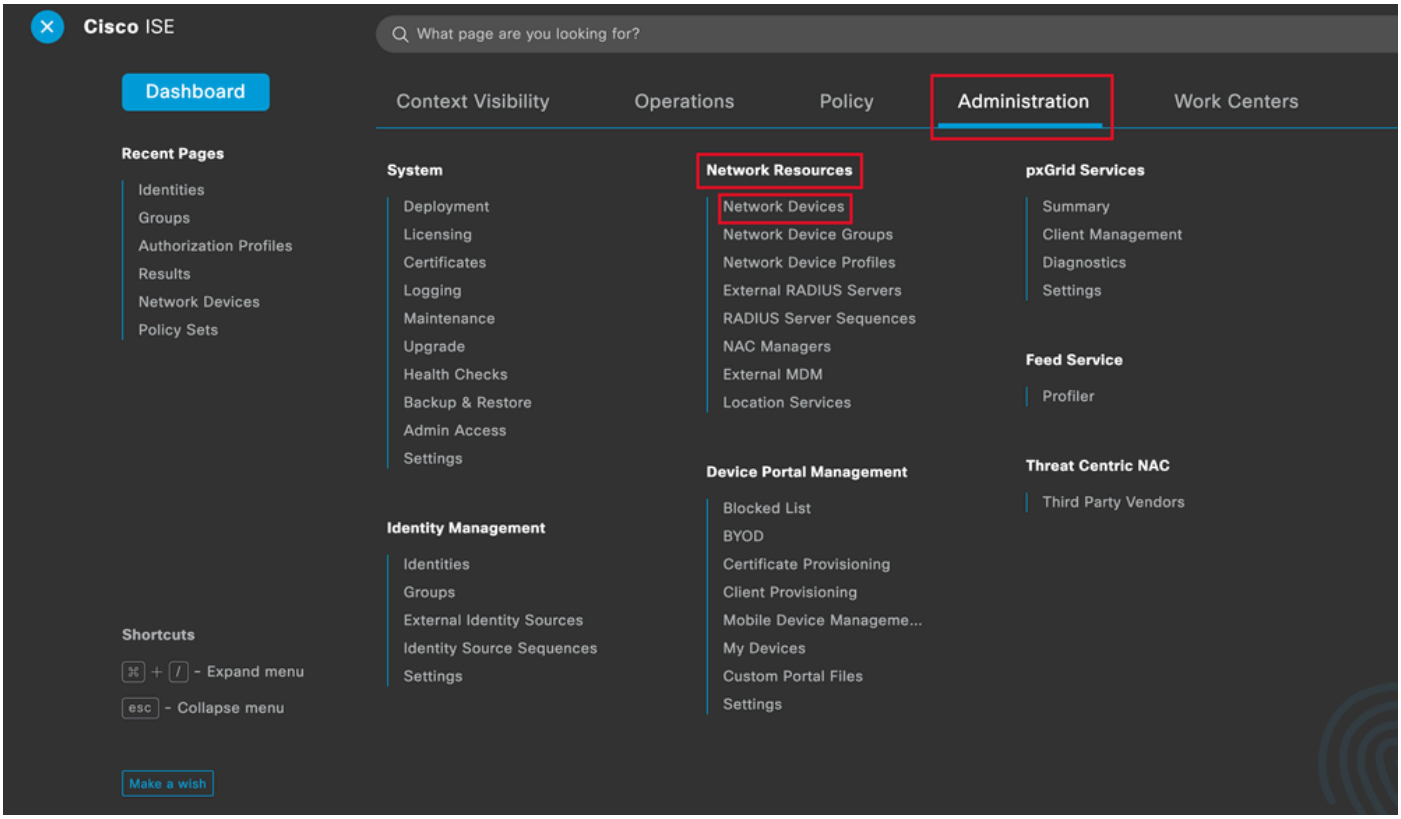
```
interface Virtual-Template100 type tunnel
ip unnumbered Loopback100
tunnel mode ipsec ipv4
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

步驟 11.在路由器上停用基於HTTP-URL的證書查詢和HTTP伺服器：

```
no crypto ikev2 http-url cert
no ip http server
no ip http secure-server
```

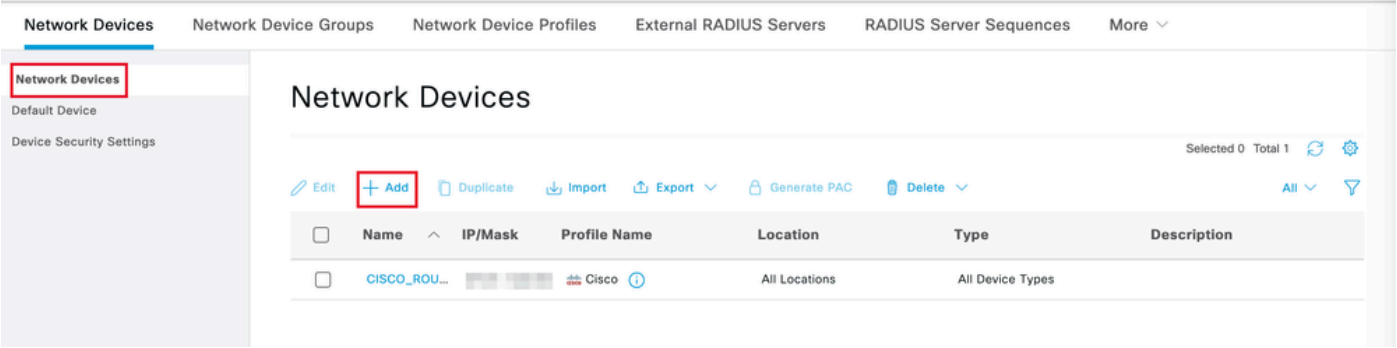
身份服務引擎(ISE)配置

步驟 1.登入到ISE伺服器並導航到管理>網路資源>網路裝置：



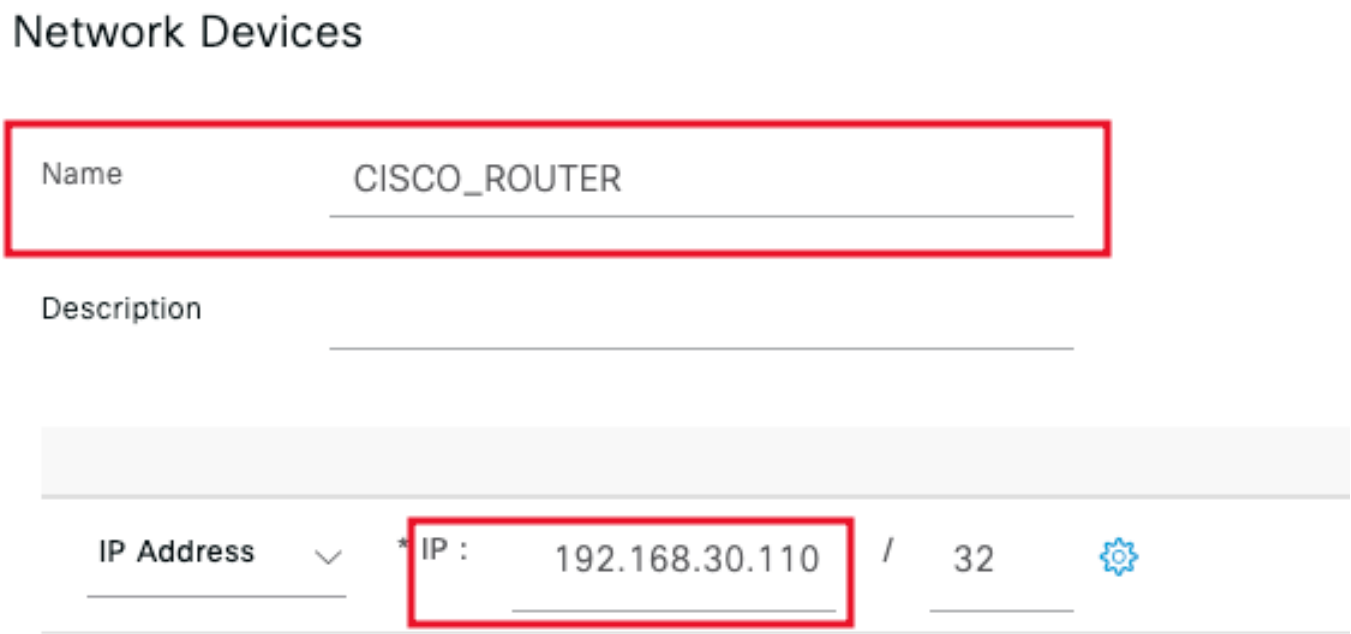
ISE常規選單

步驟 2.按一下Add將路由器配置為AAA客戶端：

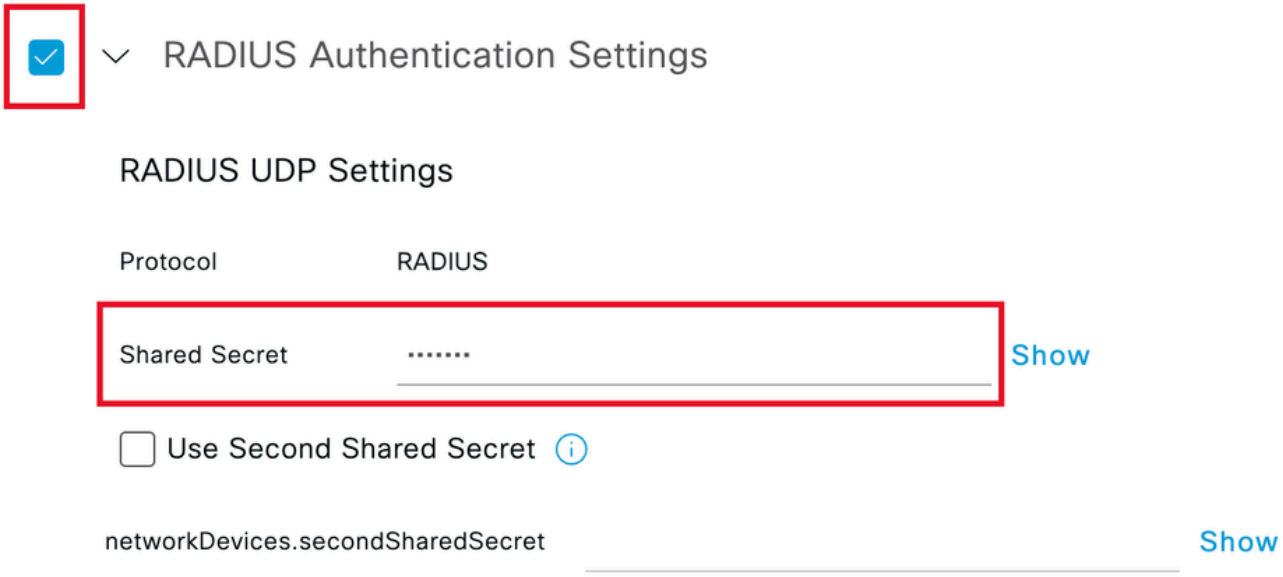


增加新網路裝置

輸入網路裝置名稱和IP地址欄位，然後選中RADIUS Authentication Settings框並增加共用金鑰，此值必須與建立路由器上的RADIUS伺服器對象時使用的金鑰相同。



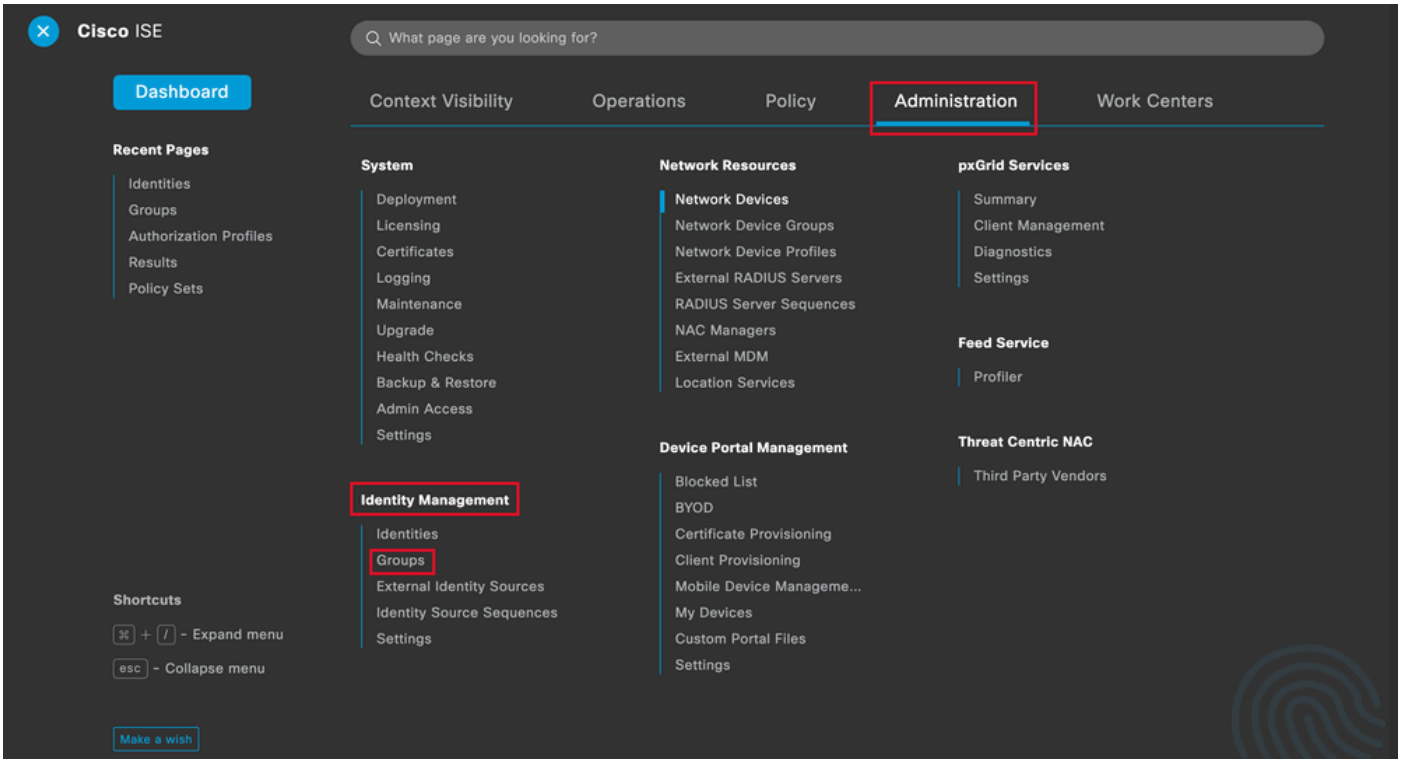
名稱和IP地址



Radius密碼

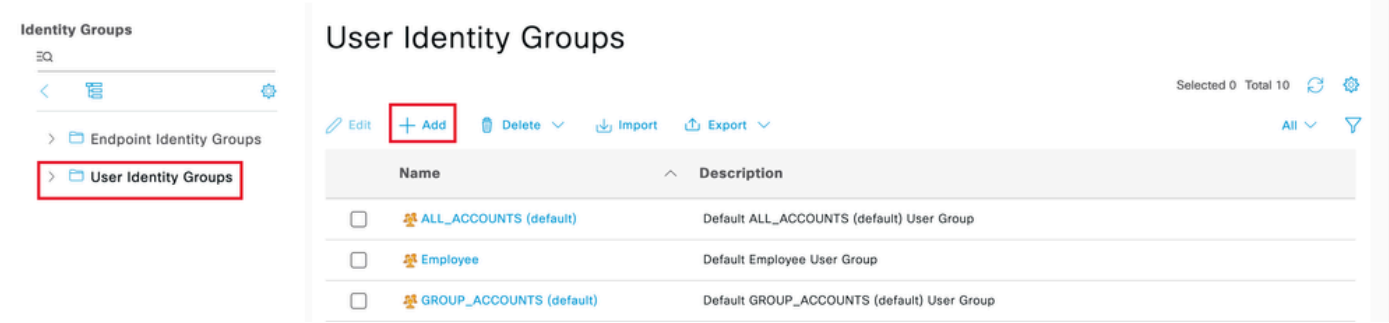
按一下Save。

步驟 3.導航到管理>身份管理>組：



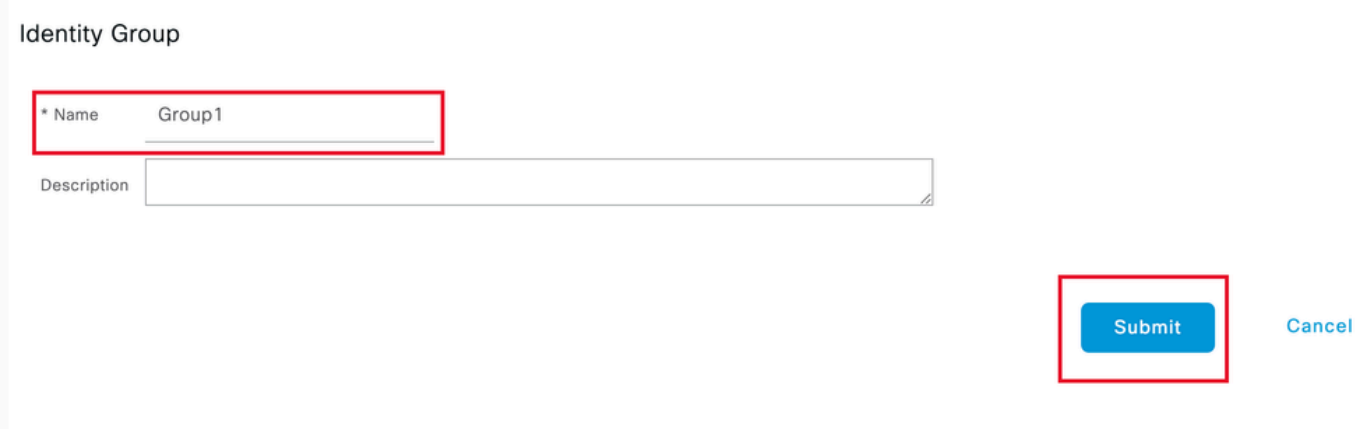
ISE常規選單

步驟 4.按一下User Identity Groups，然後按一下Add：

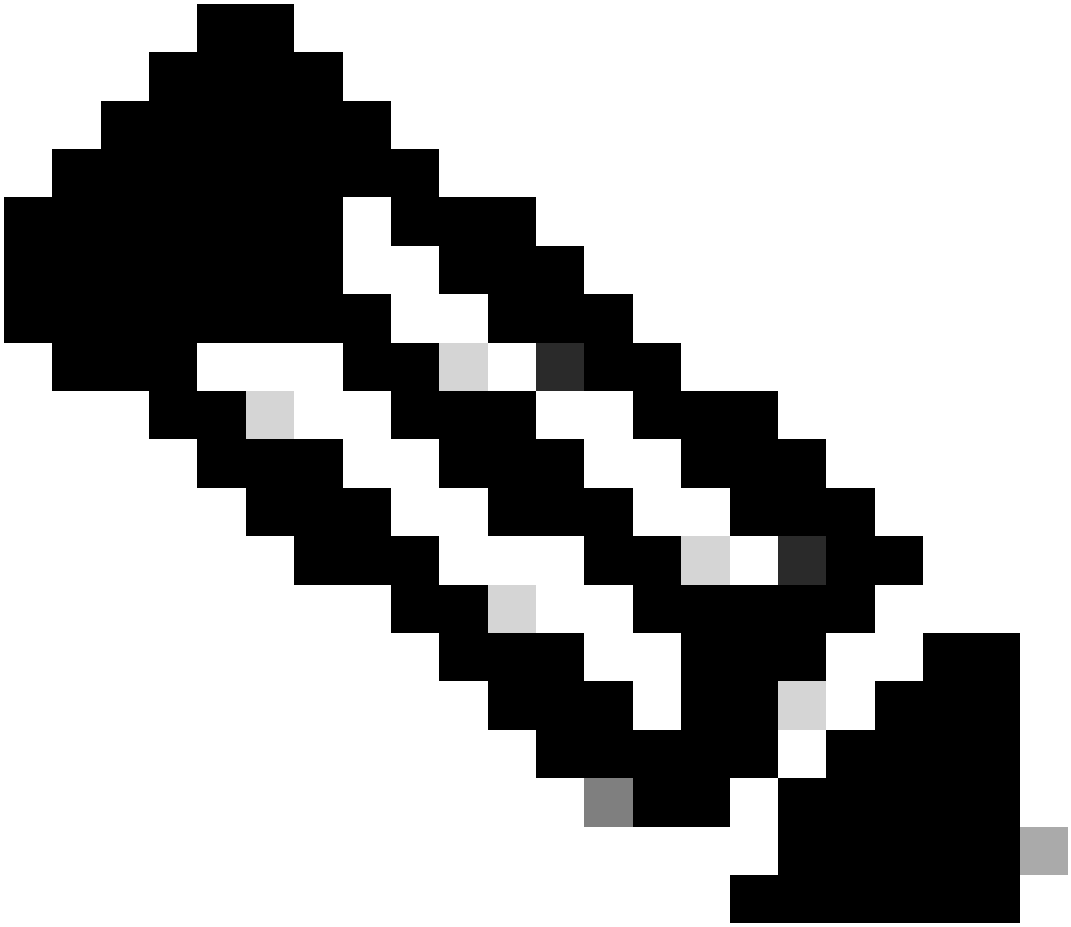


增加新組

輸入組Name，然後按一下Submit。

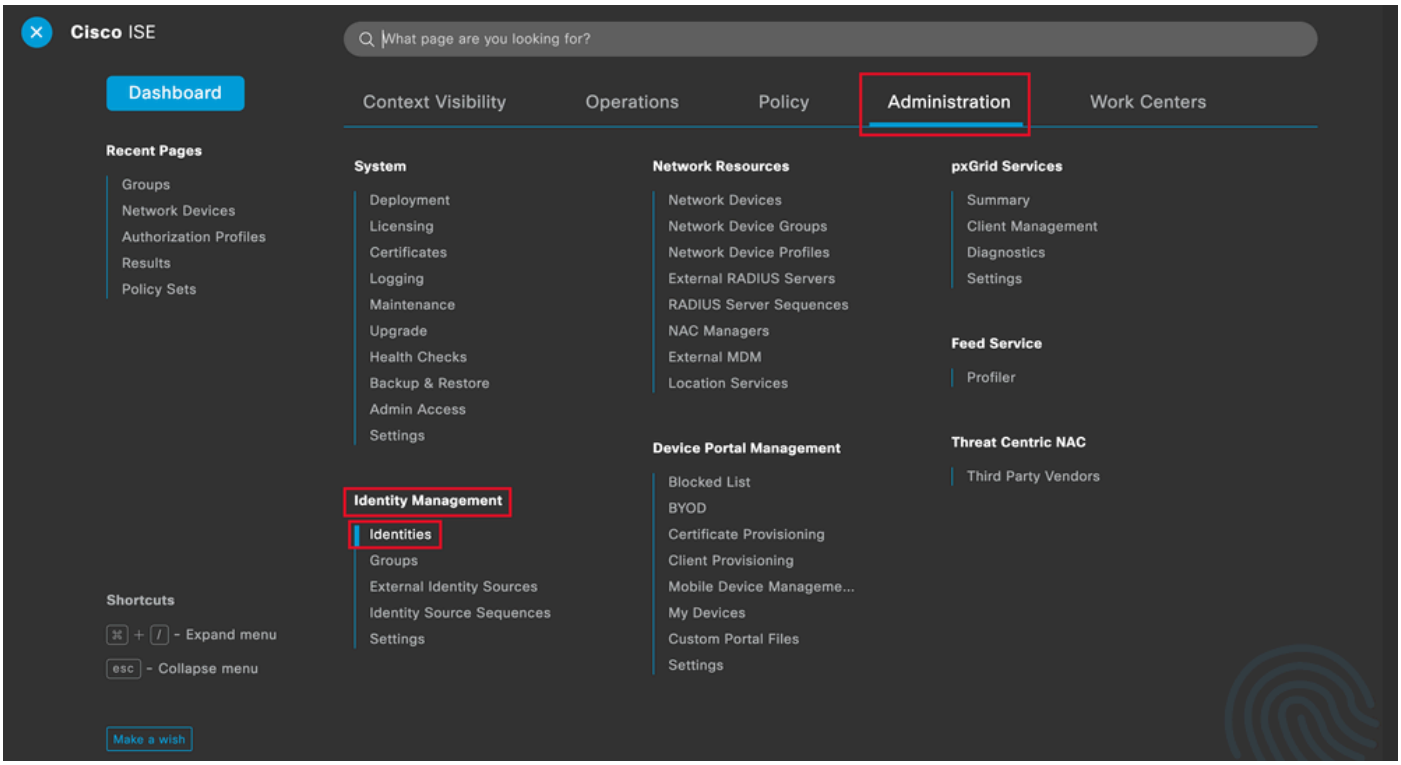


群組資訊



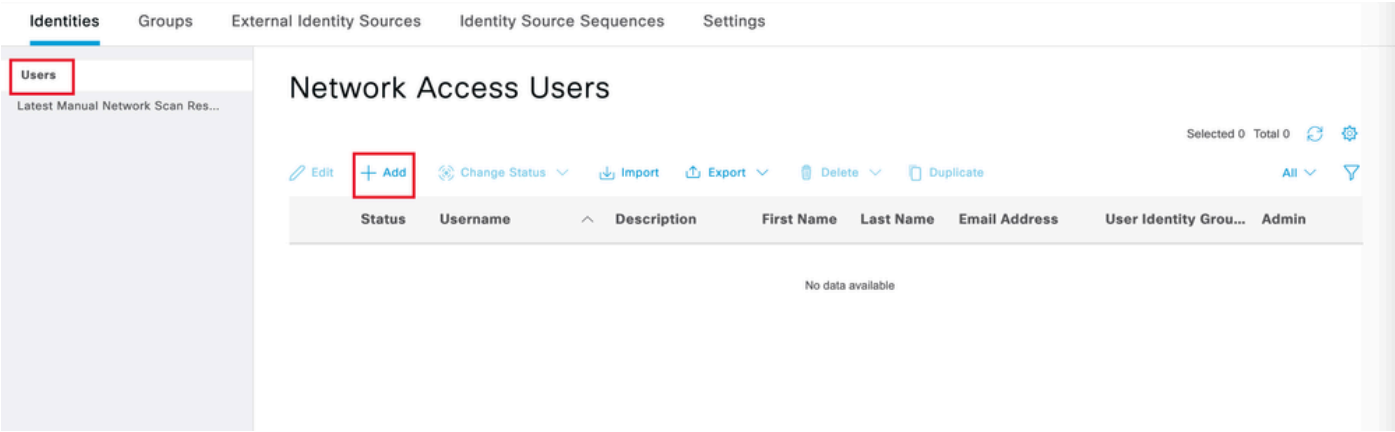
注意：重複步驟3和4，根據需要建立多個組。

步驟 5. 導航到管理>身份管理>身份：



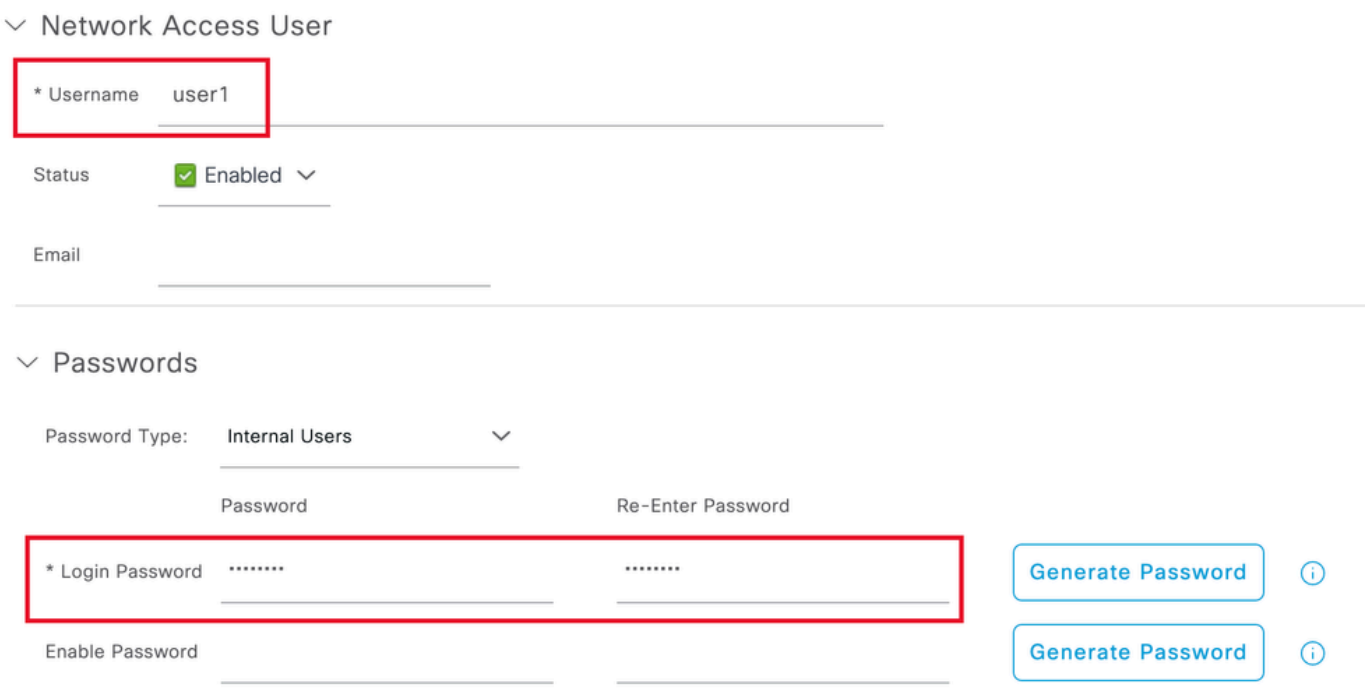
ISE常規選單

步驟 6.按一下Add，以便在伺服器本地資料庫中建立新使用者：

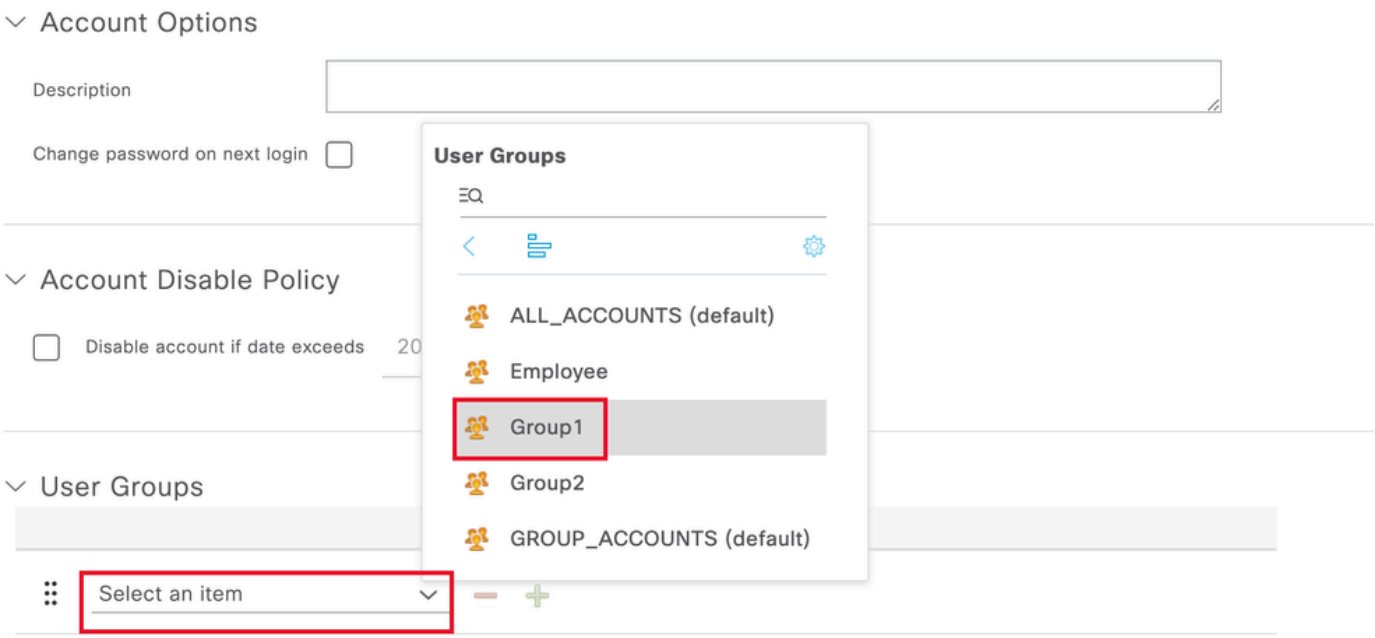


新增使用者

輸入Username 和Login Password。然後，導航到此頁面末尾，選擇User Group：

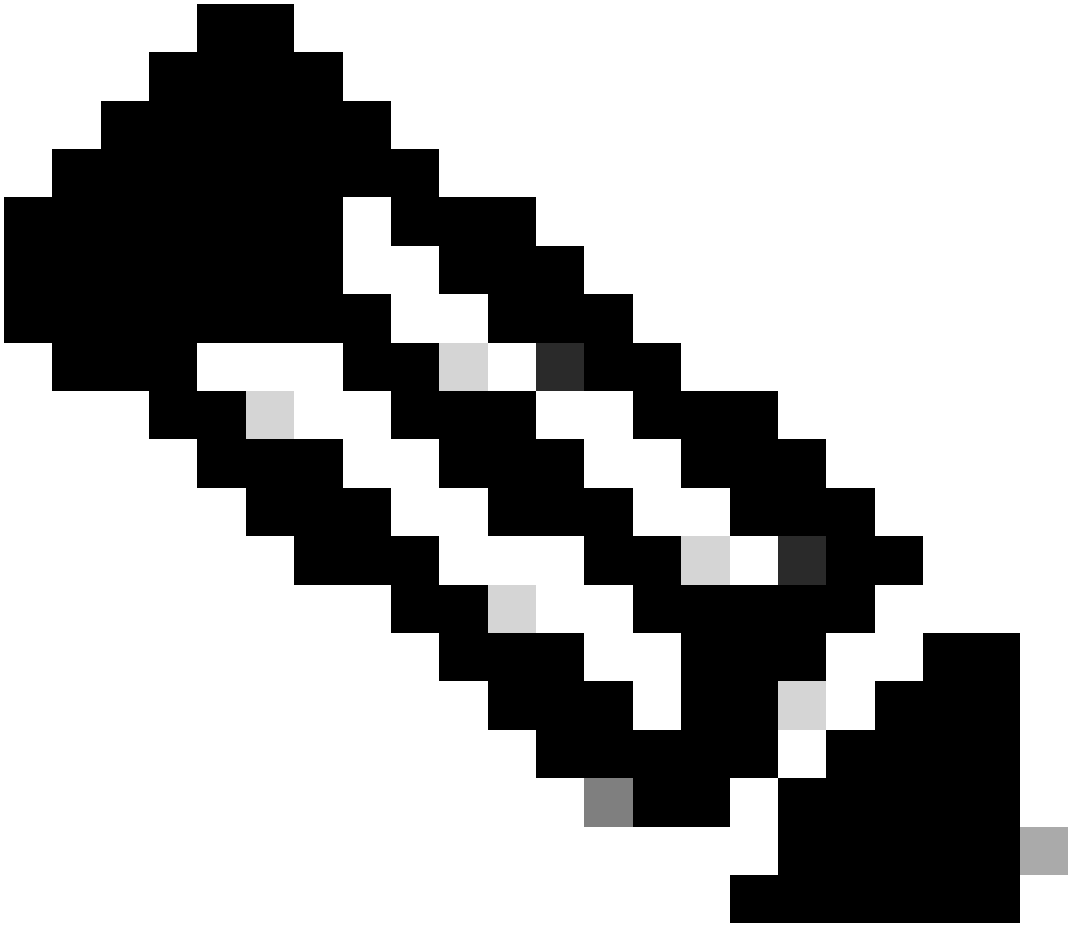


使用者名稱和密碼



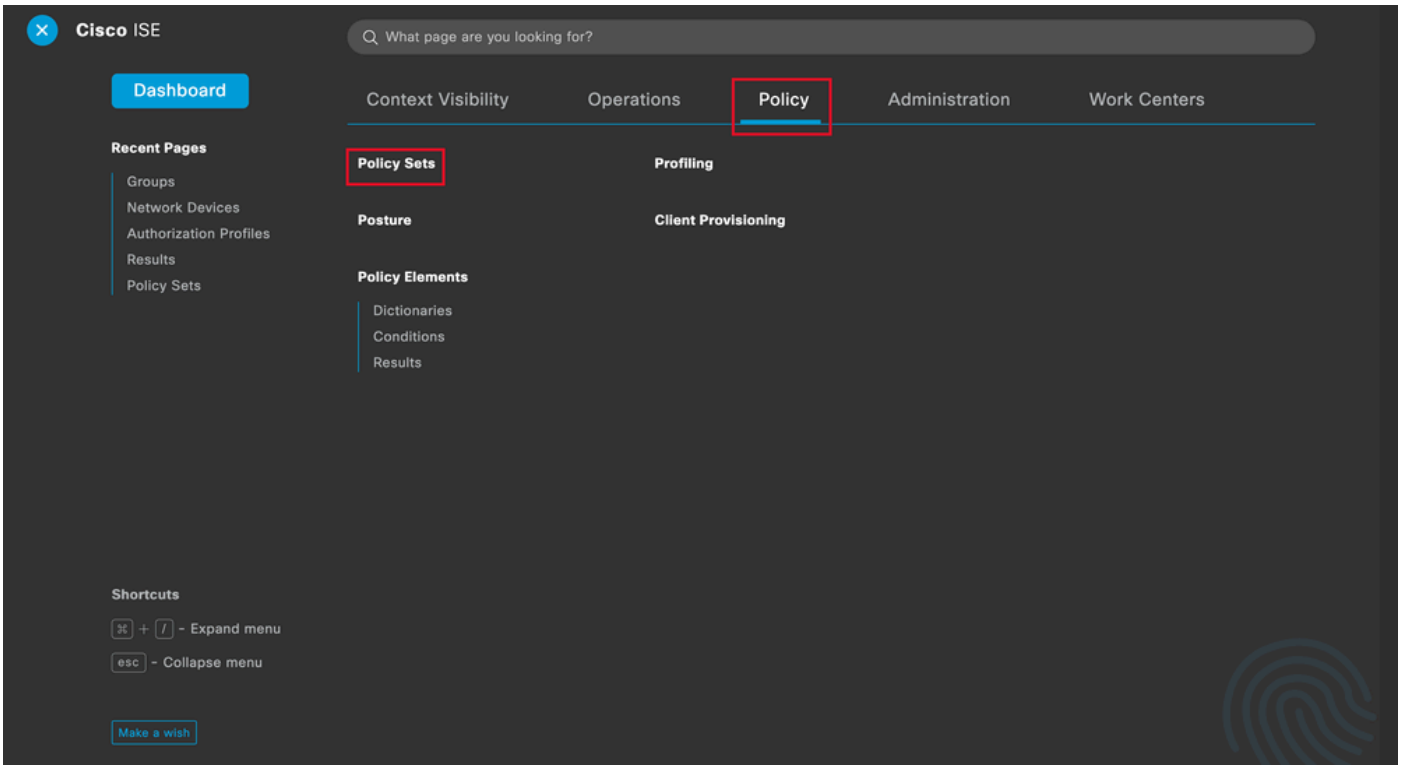
將正確的群組指派給使用者

按一下Save。



附註：重複步驟5和6，建立您需要的使用者，並將他們指派給對應的群組。

第7步：導航到策略>策略集：

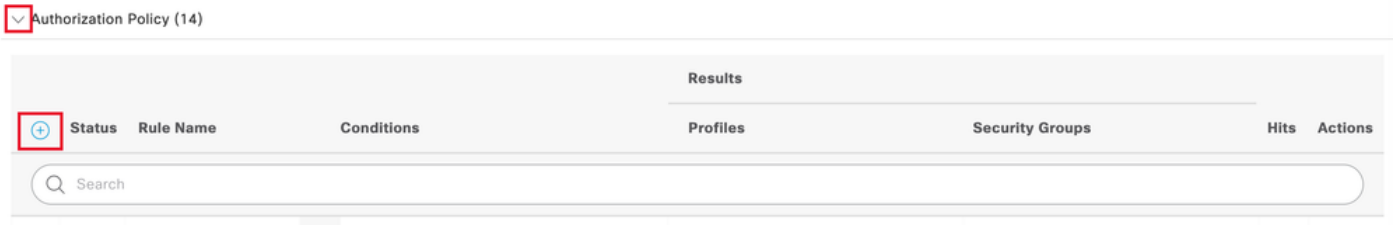


ISE常規選單

透過按一下螢幕右側的箭頭來選擇預設授權策略：

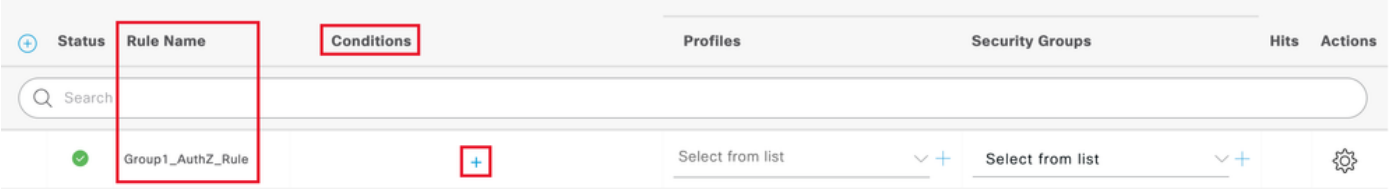
選擇授權策略

步驟 8. 點選Authorization Policy旁邊的下拉選單箭頭以展開它。然後，按一下add (+)圖示以增加新規則：



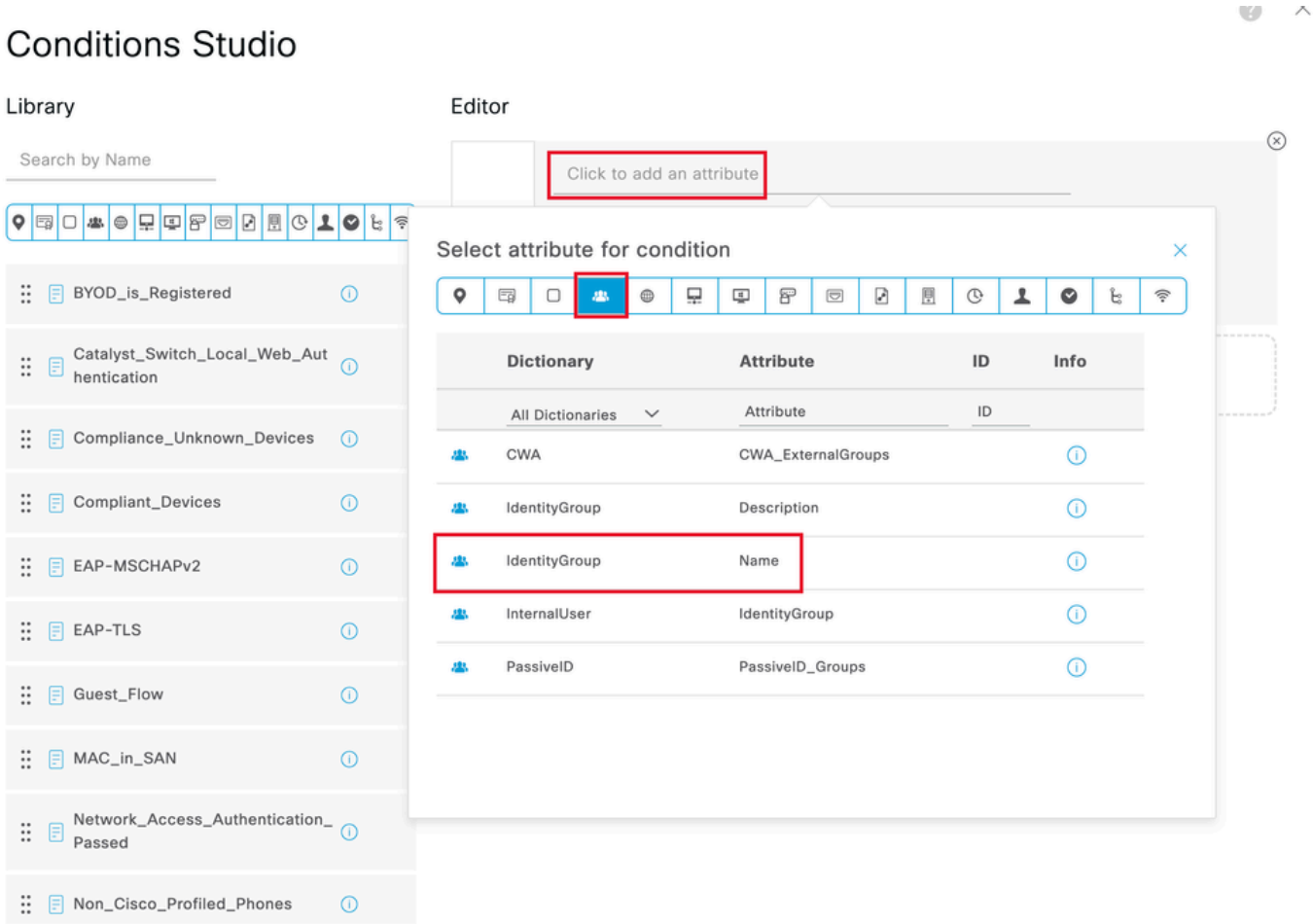
增加新授權規則

輸入規則的名稱，然後在條件欄下選取add (+)圖示：



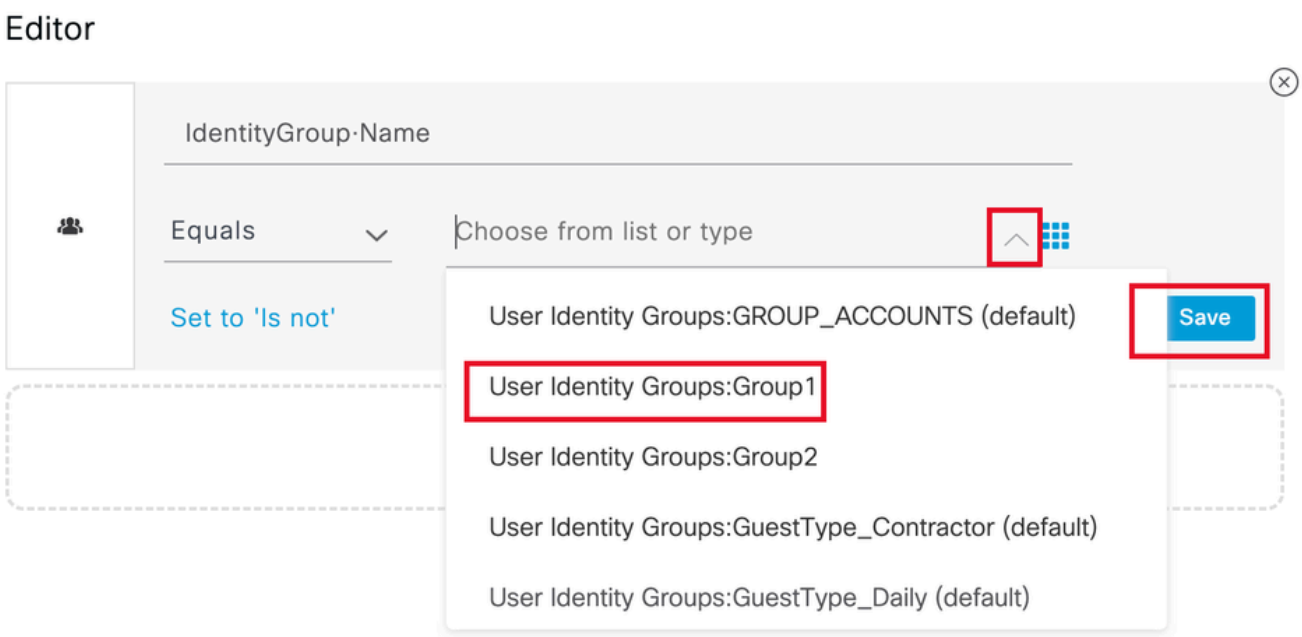
增加條件

步驟 9. 在「屬性編輯器」文字方塊中按一下，然後按一下Identity群組。選擇Identity group - Name屬性：



選取條件

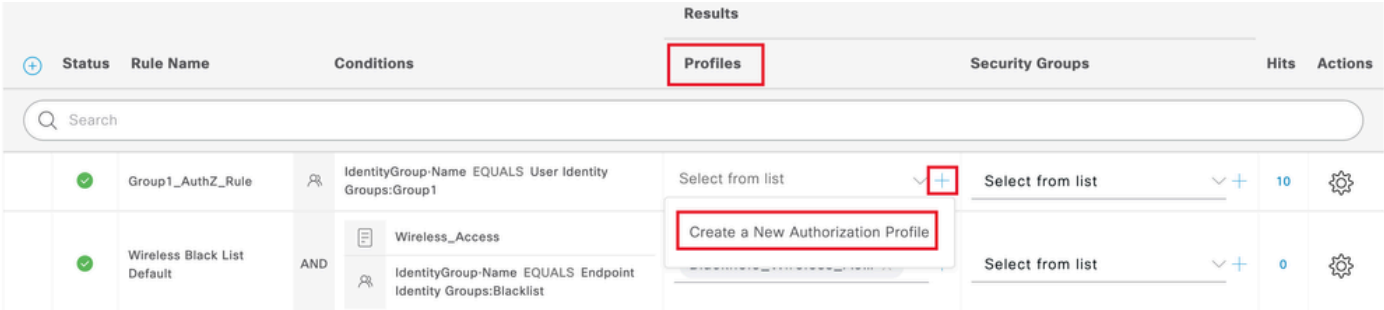
選擇與運算子相同，然後按一下下拉選單箭頭以顯示可用選項，然後選擇使用者身份組：<GROUP_NAME>。



選取群組

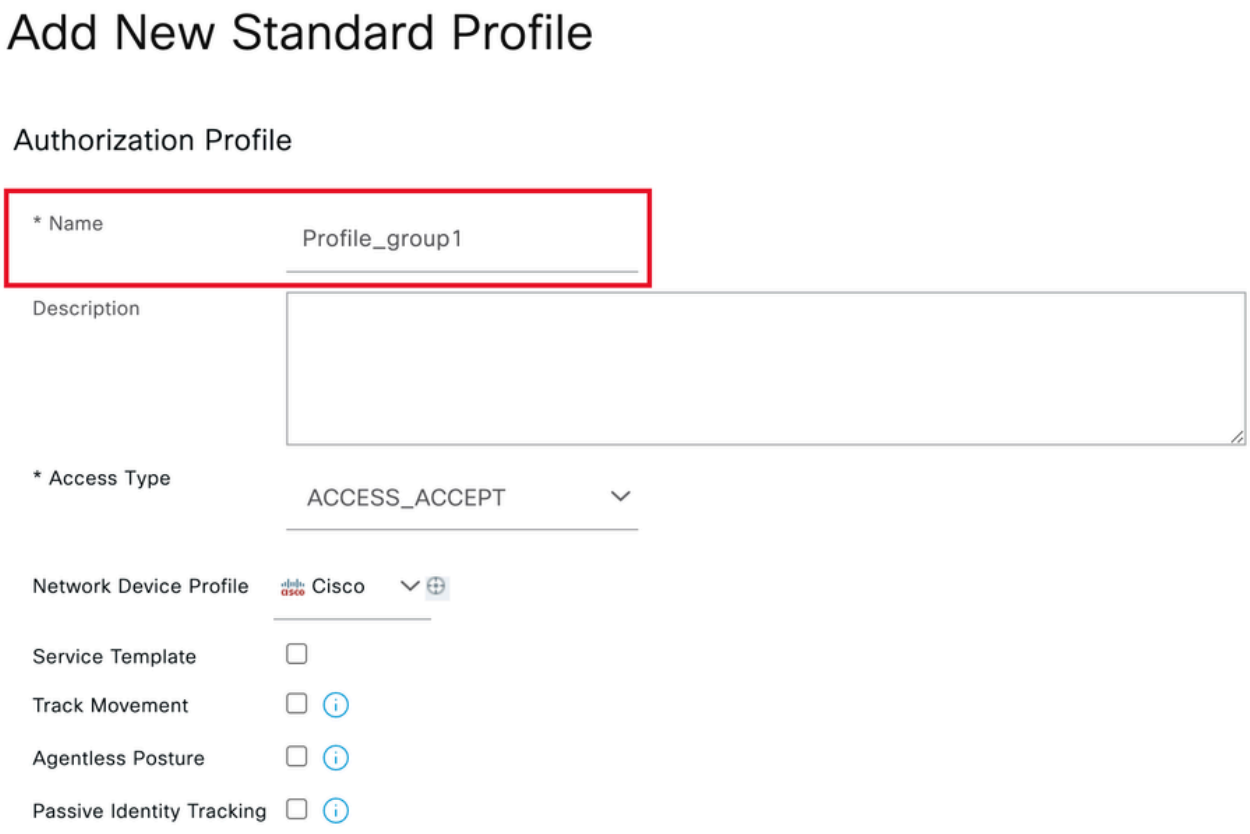
按一下「儲存」。

第10步：在配置檔案列中，點選增加(+)圖示並選擇建立新授權配置檔案：



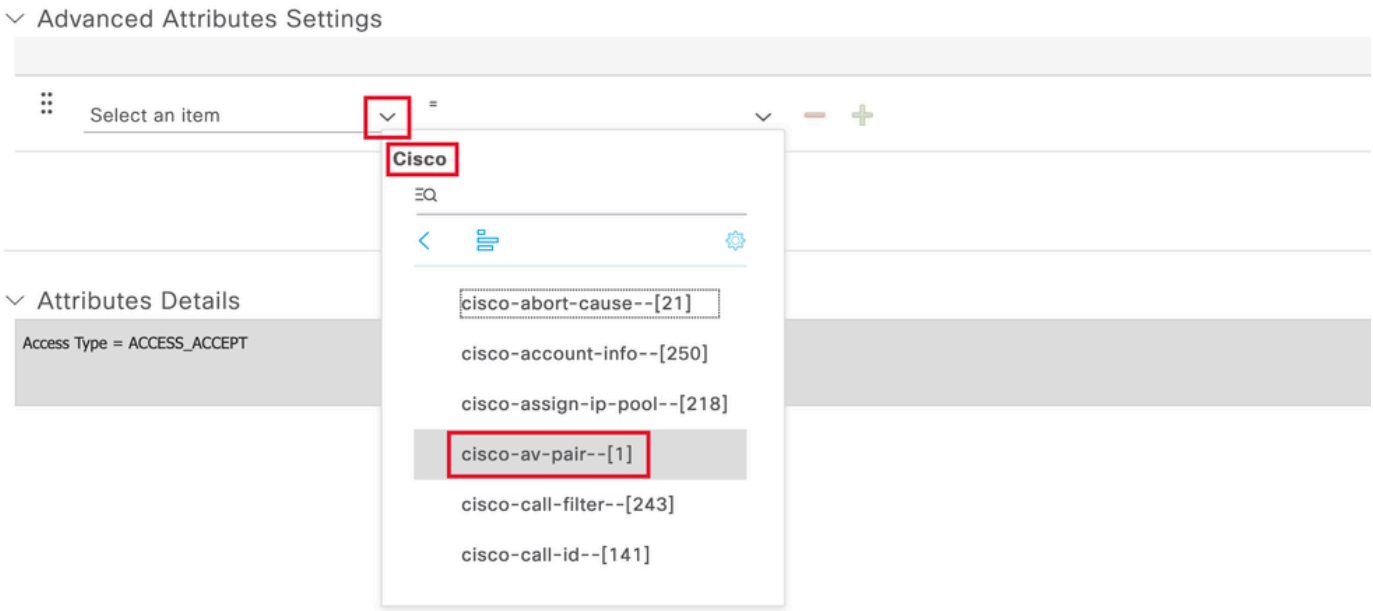
建立授權配置檔案

輸入設定檔名稱



設定檔資訊

瀏覽至此頁末的進階屬性設定，然後按一下下拉式功能表箭頭。然後按一下Cisco，然後選擇cisco-av-pair—[1]：

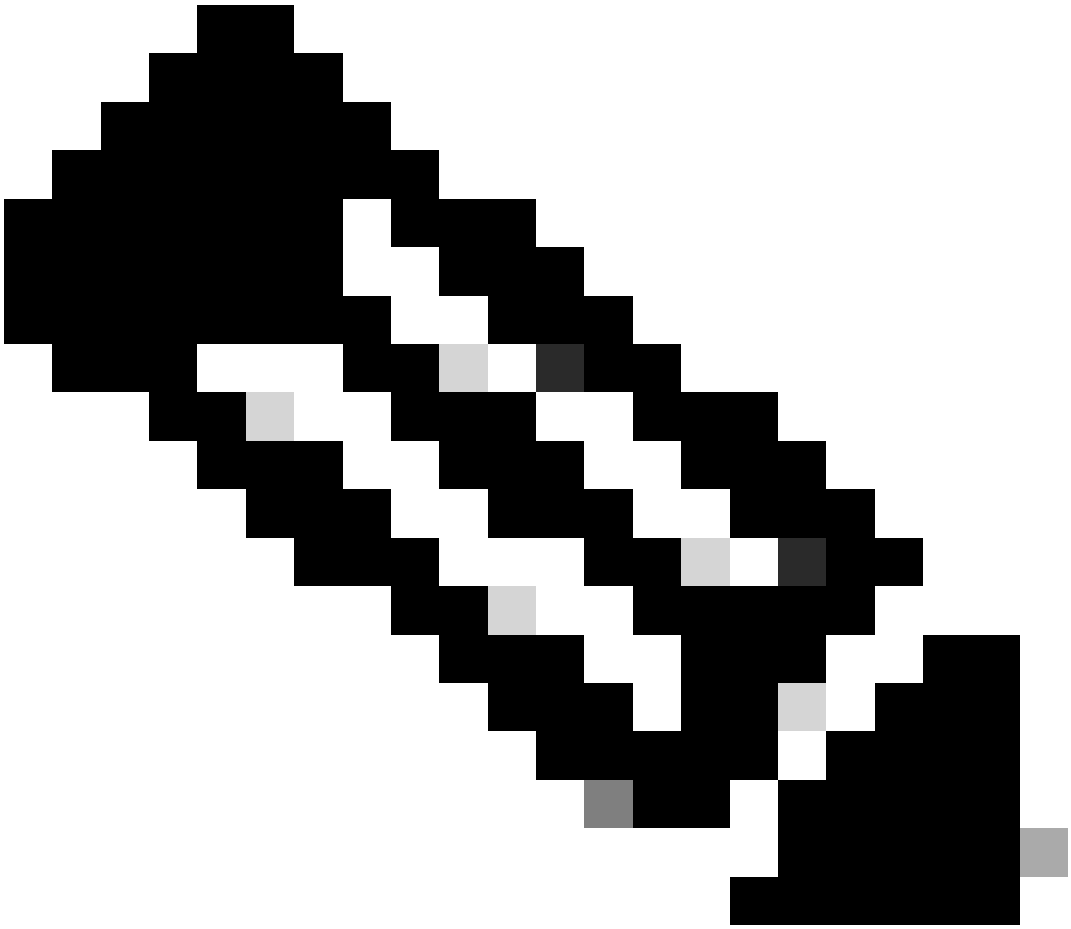


選取屬性型別

。

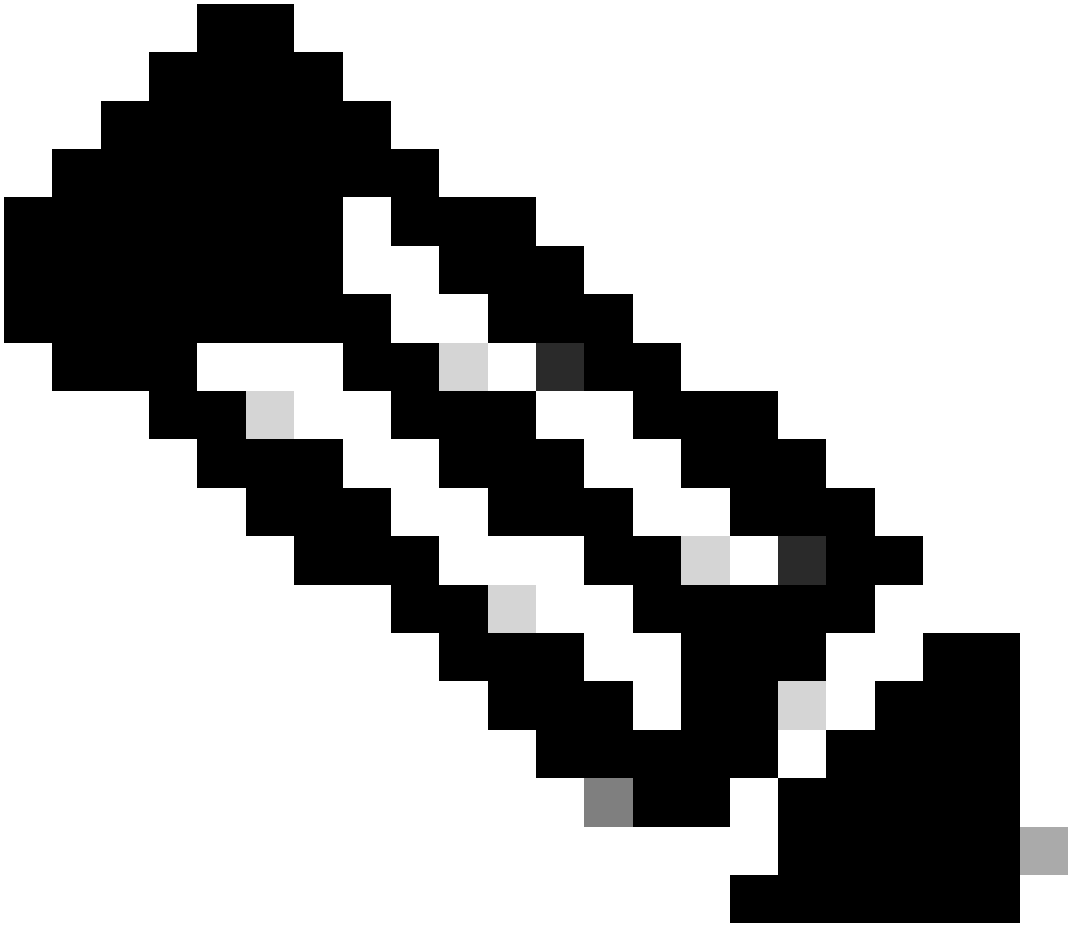
增加要配置的cisco-av-pair屬性，並按一下add (+)圖示增加另一個屬性：

配置屬性



注意：有關屬性規範（名稱、語法、說明、示例等），請參閱FlexVPN RADIUS屬性配置指南：

[FlexVPN和網際網路金鑰交換版本2配置指南，Cisco IOS XE Fuji 16.9.x -支援的RADIUS屬性]

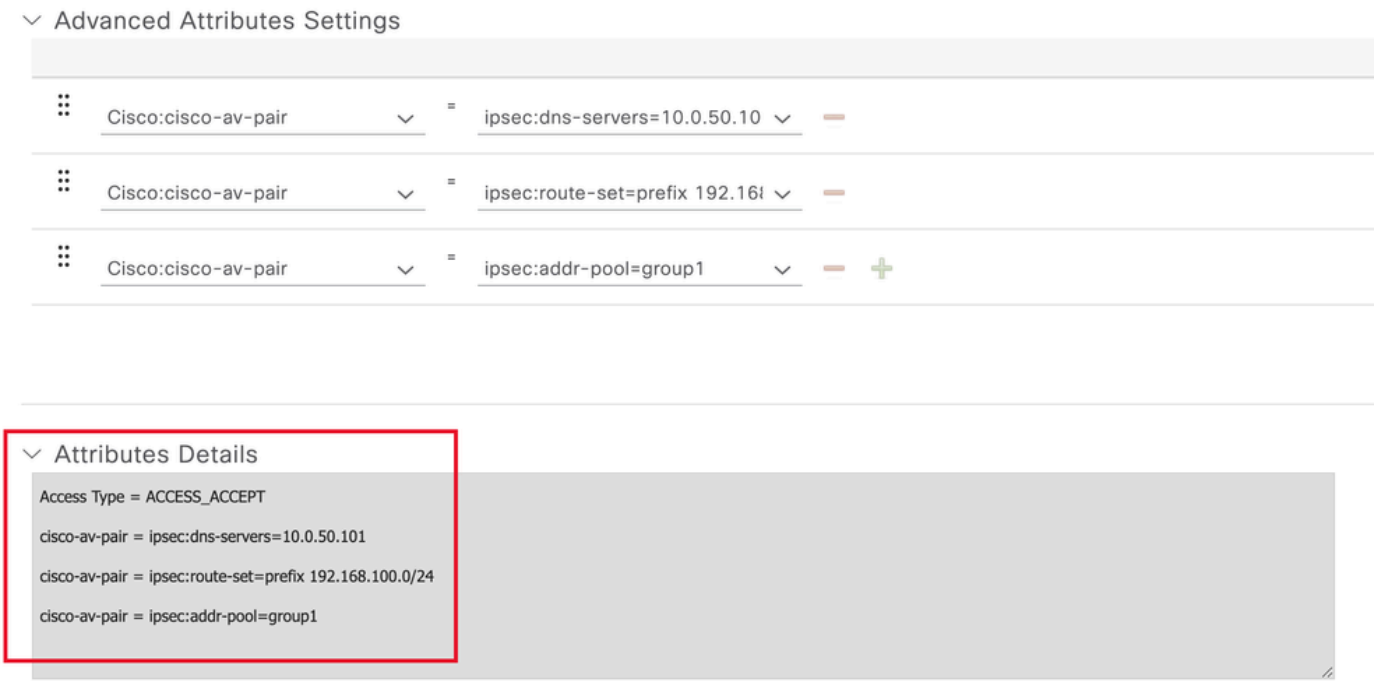


附註：重複上一步以建立必要的屬性。

按一下Save。

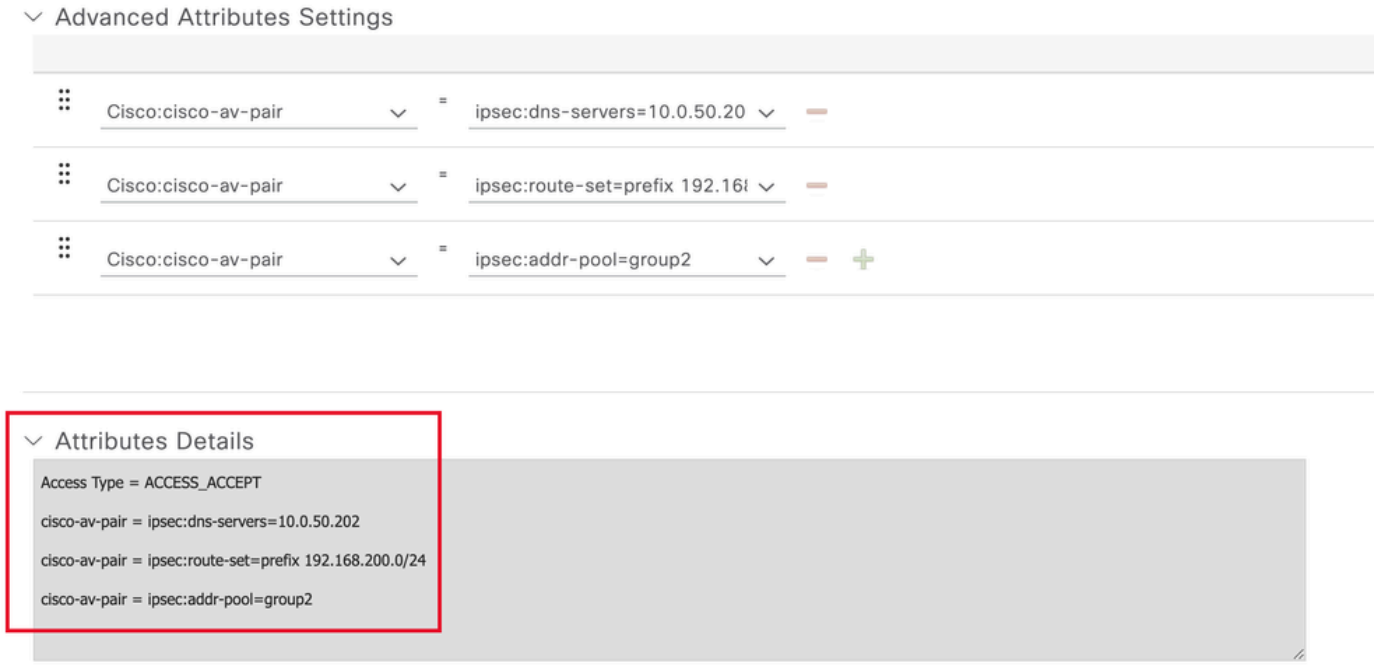
接下來的屬性已指定給每個群組：

- 群組1屬性：



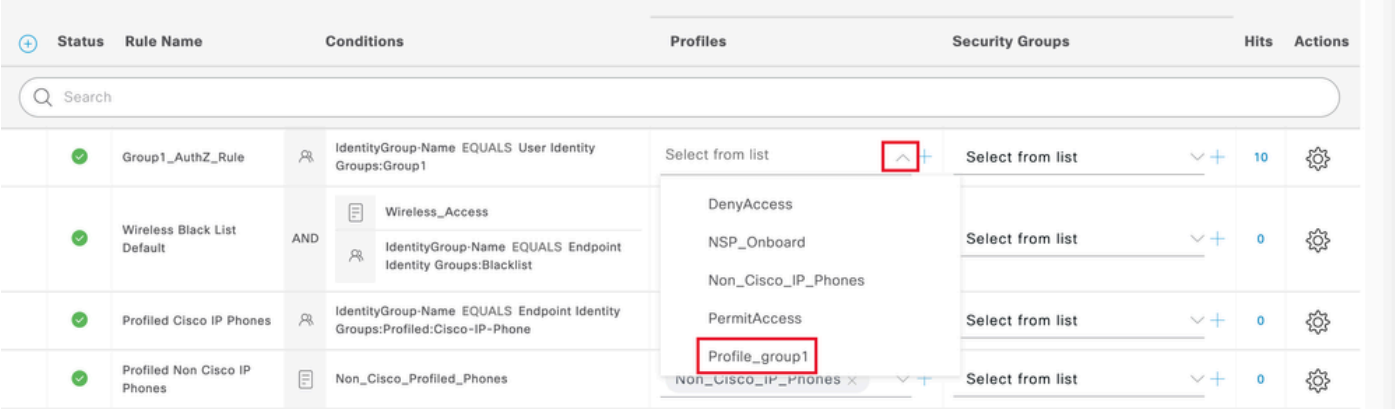
Group1屬性

- 群組2屬性：



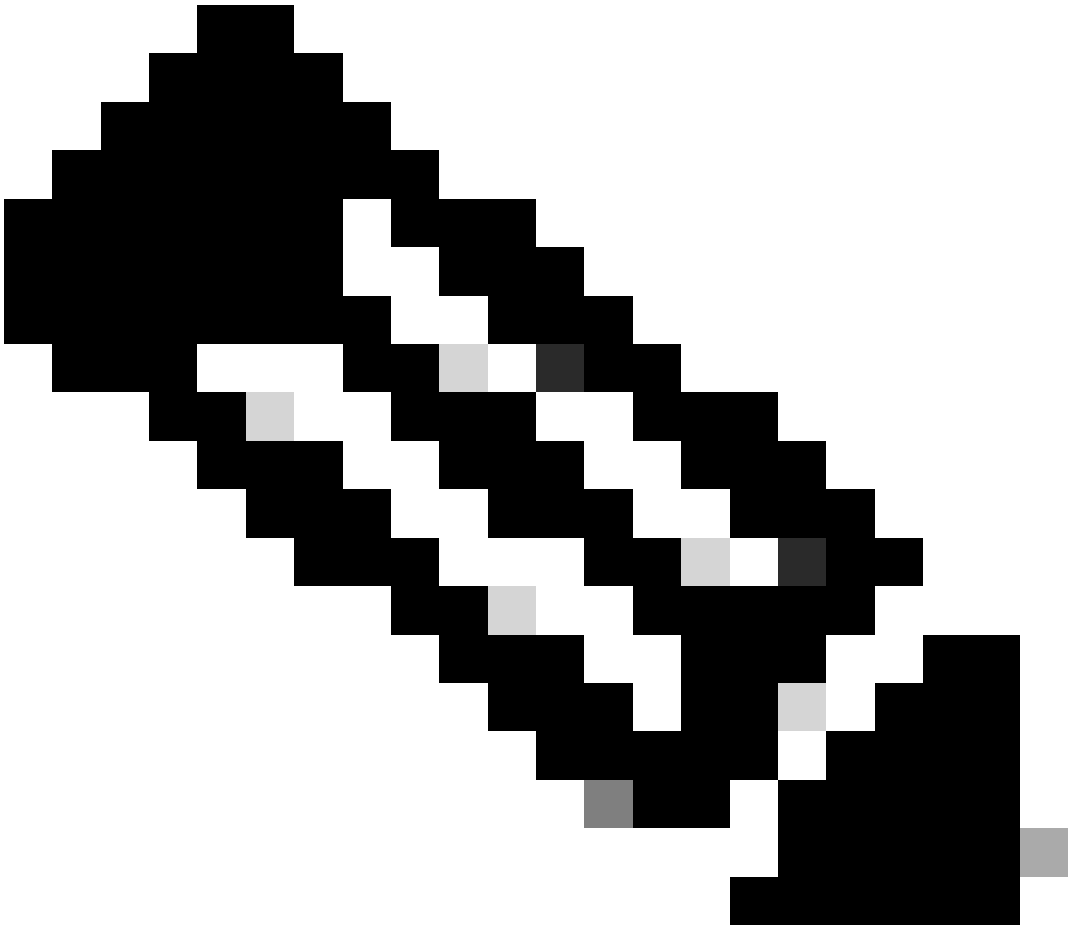
群組2屬性

第11步：點選下拉選單箭頭，選擇第10步中建立的授權配置檔案：



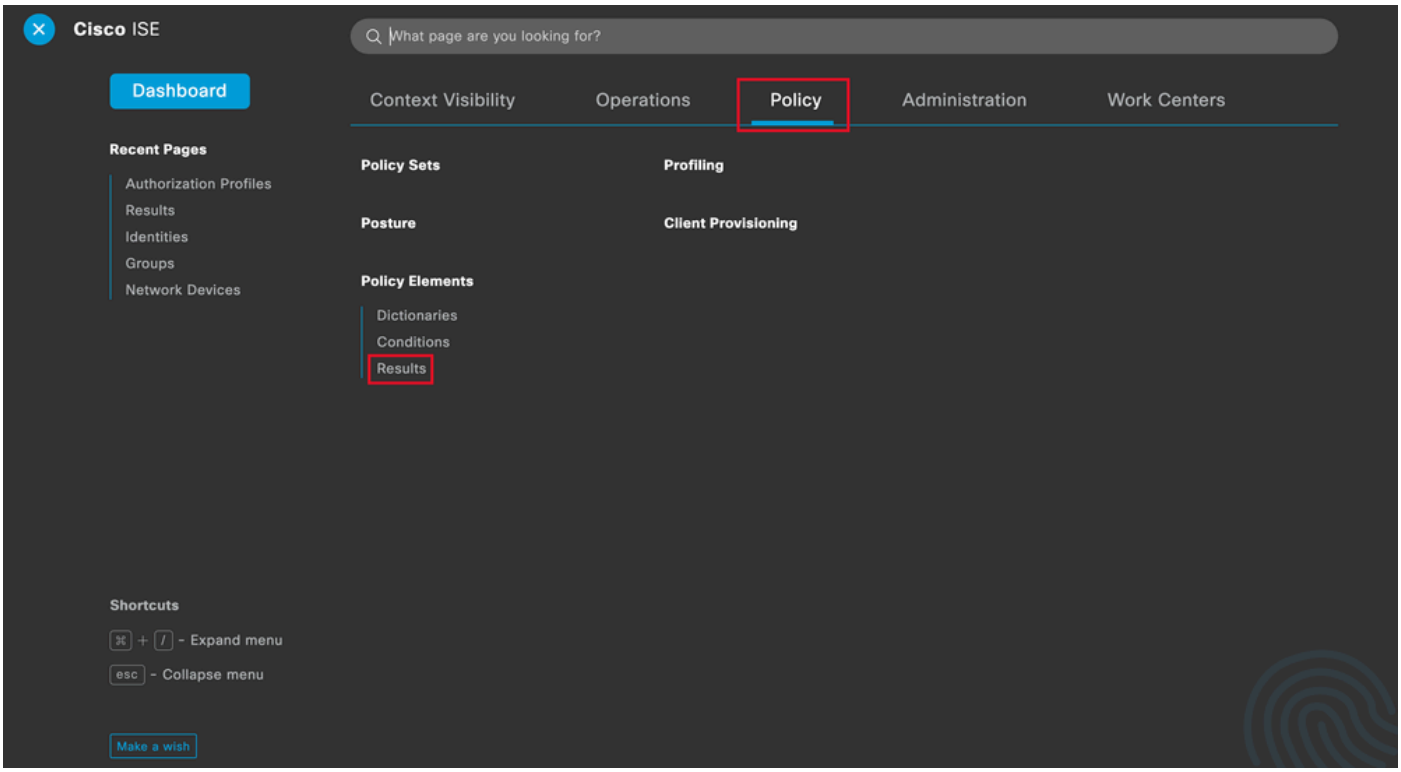
分配授權配置檔案

按一下Save。



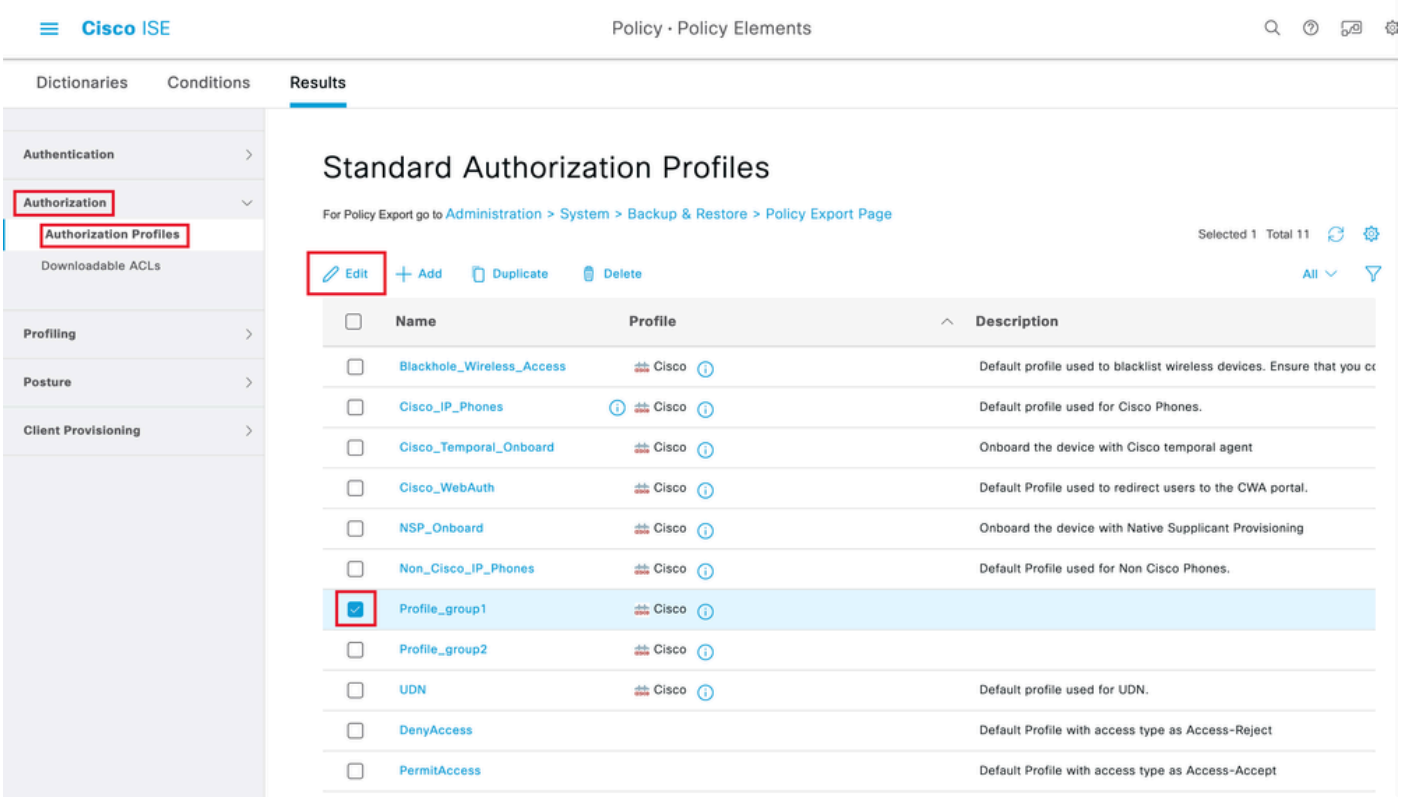
注意：重複步驟8到11為每個組建立必要的授權規則。

步驟12（可選）。 如果需要編輯授權配置檔案，請導航到策略>結果：



ISE常規選單

導航到授權>授權配置檔案。按一下要修改的配置檔案的覈取方塊，然後按一下Edit：



編輯授權配置檔案

客戶端配置

步驟 1.使用XML配置檔案編輯器建立XML配置檔案。以下範例是用來建立本檔案的範例：

<#root>


```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreLinux>All</CertificateStoreLinux>
<CertificateStoreOverride>true</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">
true
<AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">
Disable
<PPPExclusionServerIP UserControllable="false"/>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">
false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>
```


FlexVPN HUB


```
</HostName>
<HostAddress>
```


192.168.50.225


```
</HostAddress>
<PrimaryProtocol>
```


IPsec

```
<StandardAuthenticationOnly>
true
<AuthMethodDuringIKENegotiation>
```

EAP-MD5

```
</AuthMethodDuringIKENegotiation>
<IKEIdentity>
```

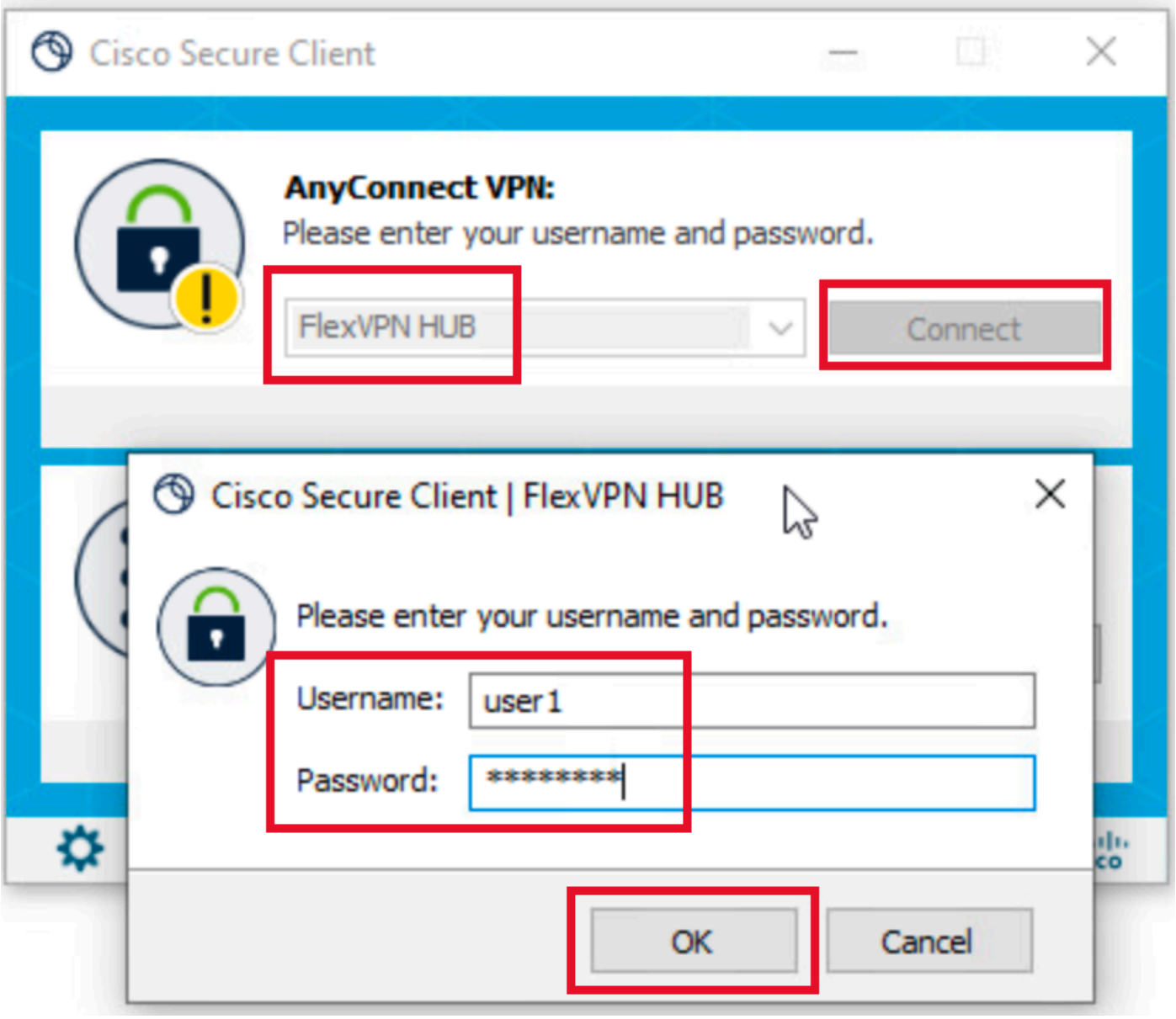
cisco.example

```
</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

- **<主機名>** -用於表示主機、IP地址或完全限定域名(FQDN)的別名。這會顯示在CSC方塊中。
- **<HostAddress>** - FlexVPN集線器的IP地址或FQDN。
- **<PrimaryProtocol>** -必須設定為IPsec以強制客戶端使用IKEv2/IPsec而不是SSL。
- **<AuthMethodDuringIKENegotiation>** -必須設定為在EAP中使用EAP-MD5。這是根據ISE伺服器進行身份驗證所必需的。
- **<IKEIdentity>** -此字串由客戶端作為ID_GROUP型別ID負載傳送。這可用於將客戶端與中心上的特定IKEv2配置檔案進行匹配。

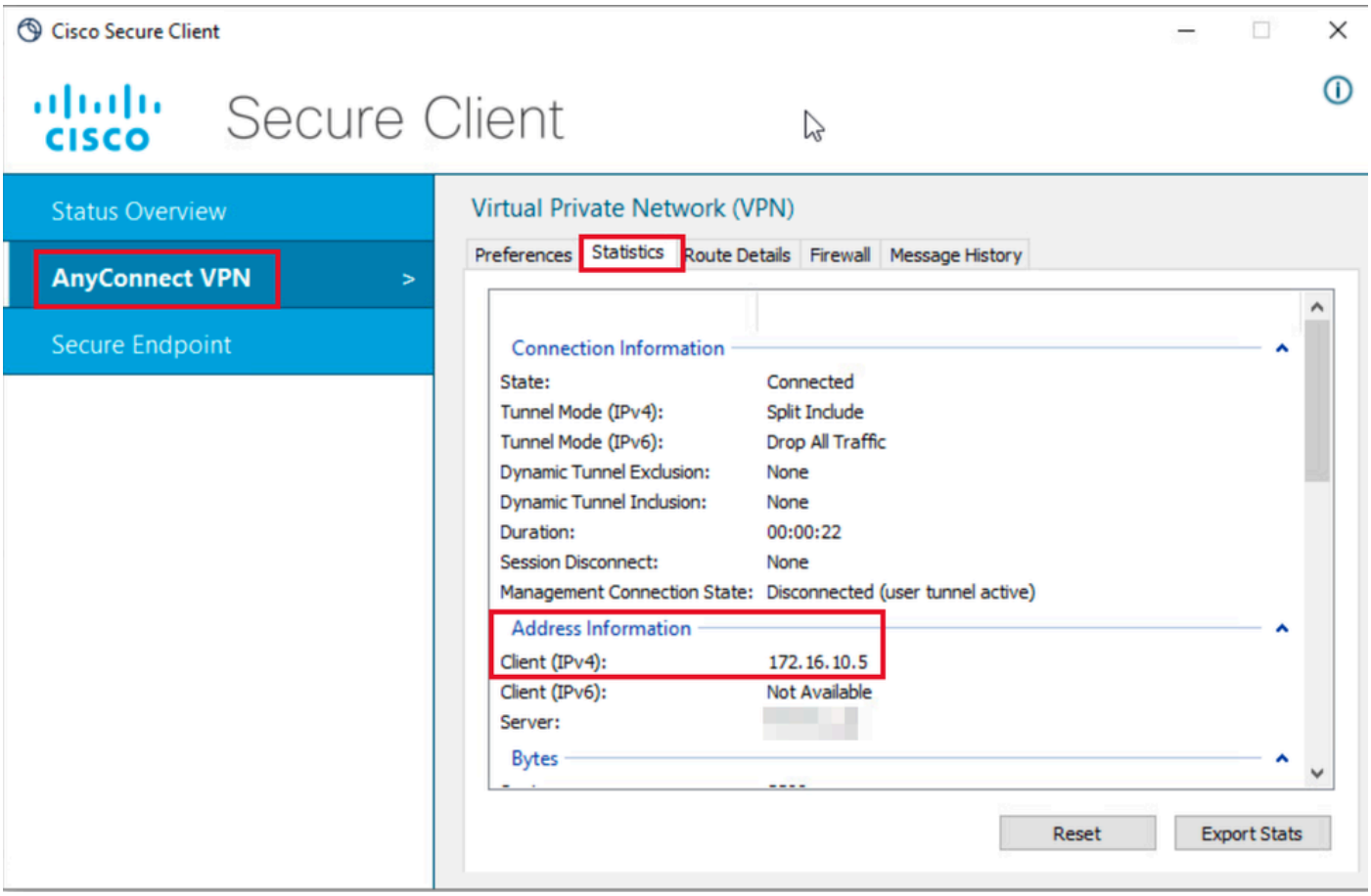
驗證

步驟 1.導航到安裝CSC的客戶端電腦。連線到FlexVPN中心並輸入user1憑證：



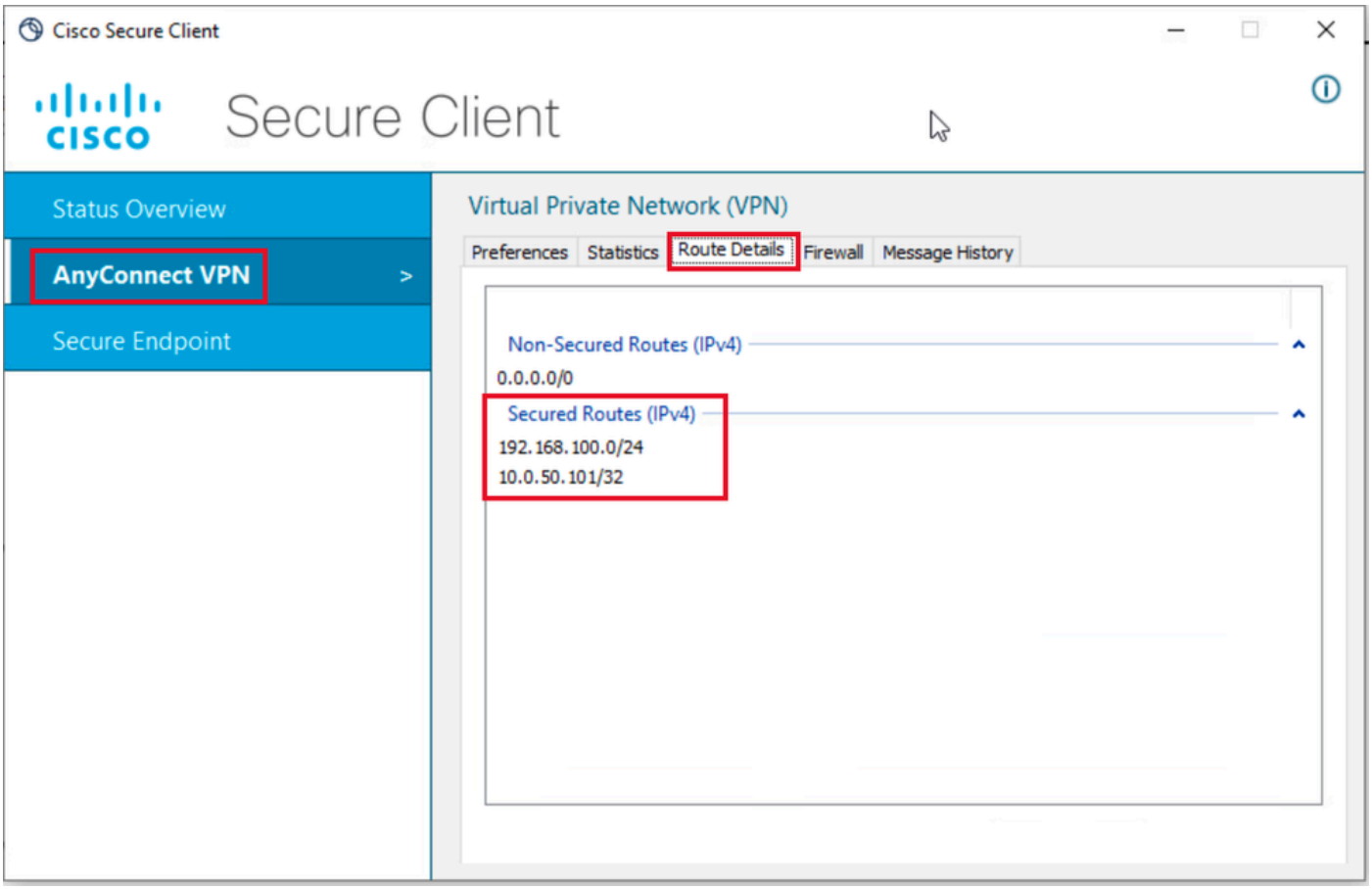
User1身份證明

步驟 2.建立連線後，點選齒輪圖示（左下角）並導航到AnyConnectVPN > Statistics。 在Address Information 部分中確認所分配的IP地址屬於為組1配置的池：



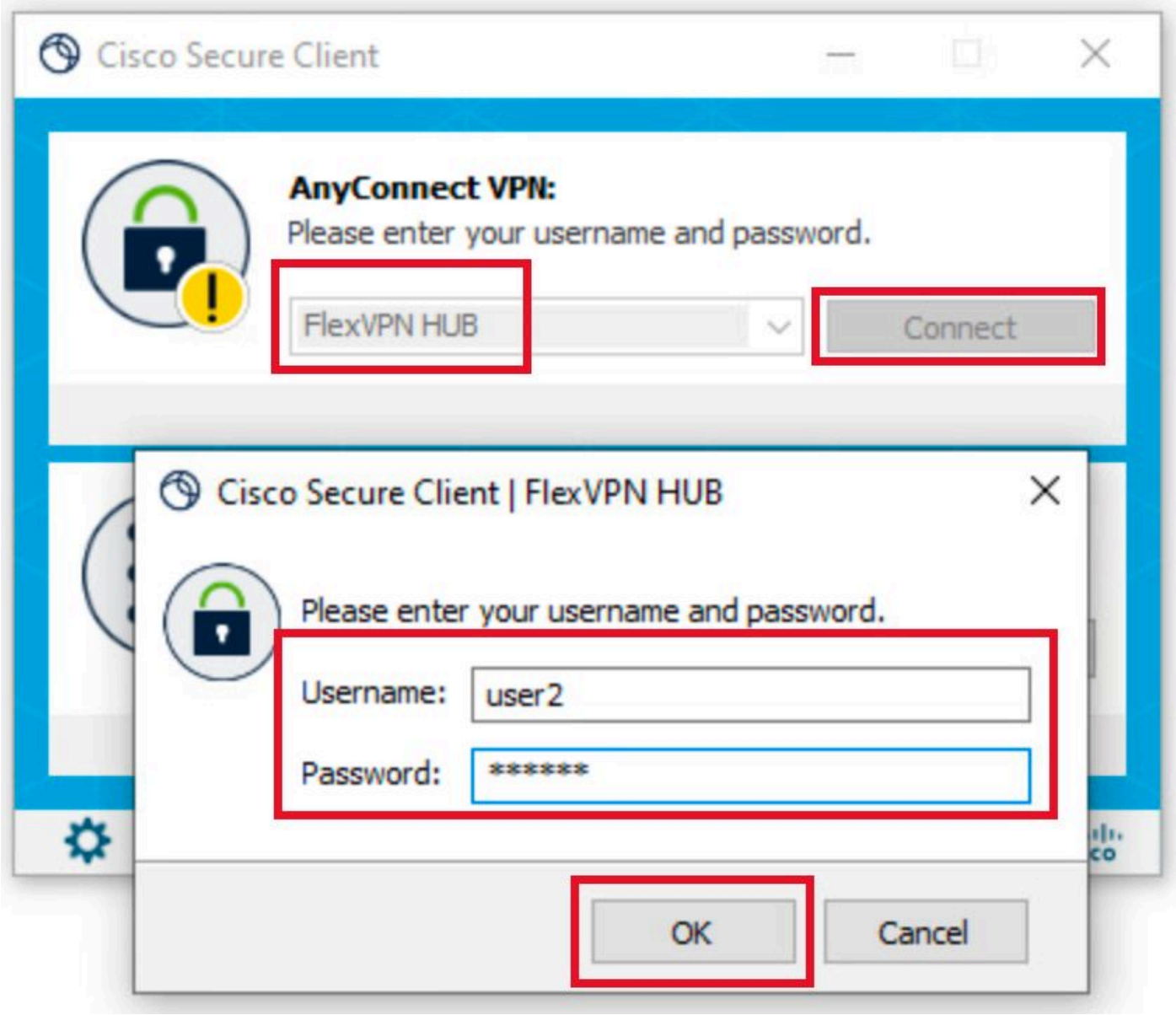
User1統計

導航到AnyConnectVPN > Route details，確認顯示的資訊對應於為group1配置的安全路由和DNS：

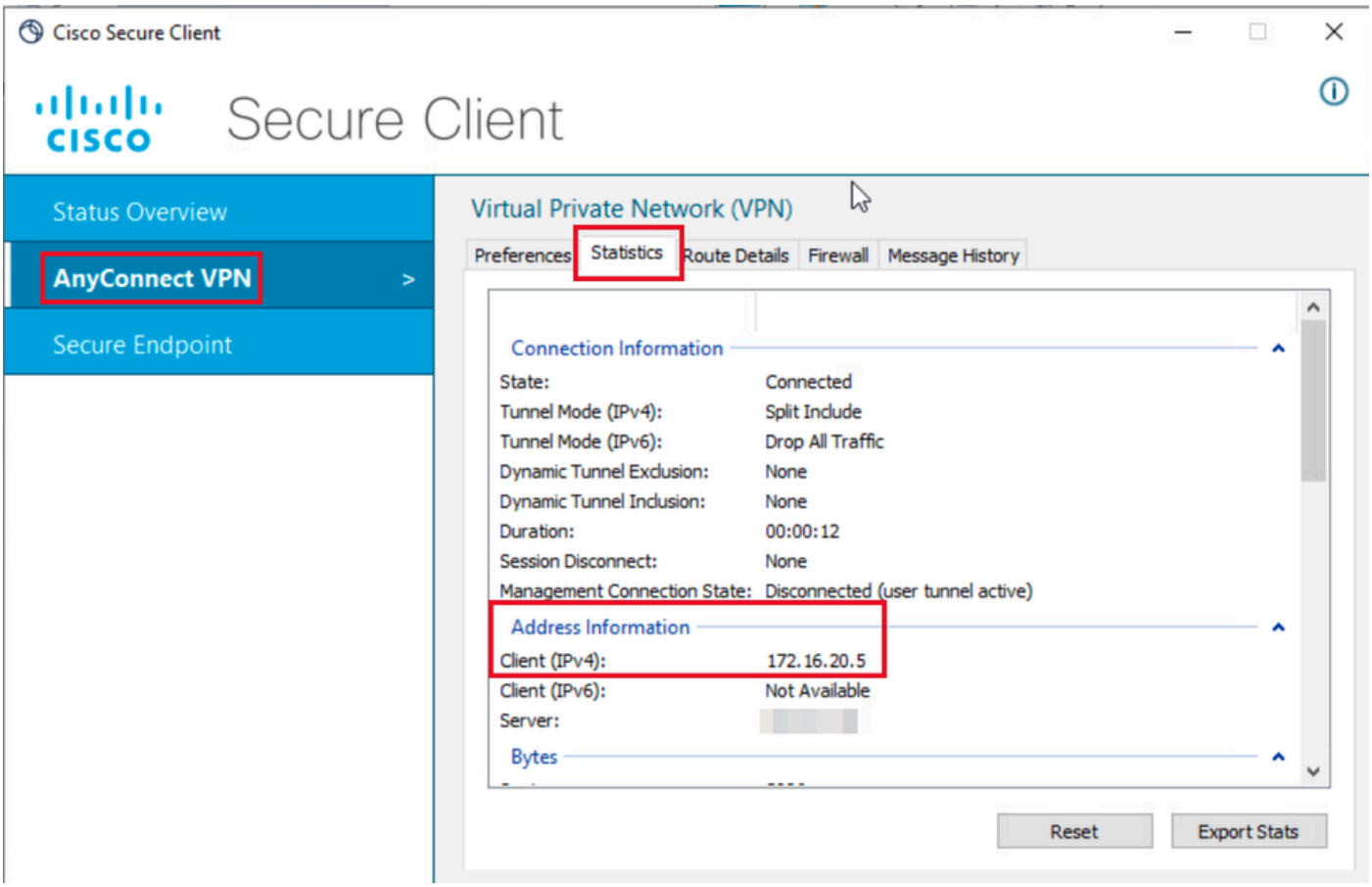


User1路由詳細資訊

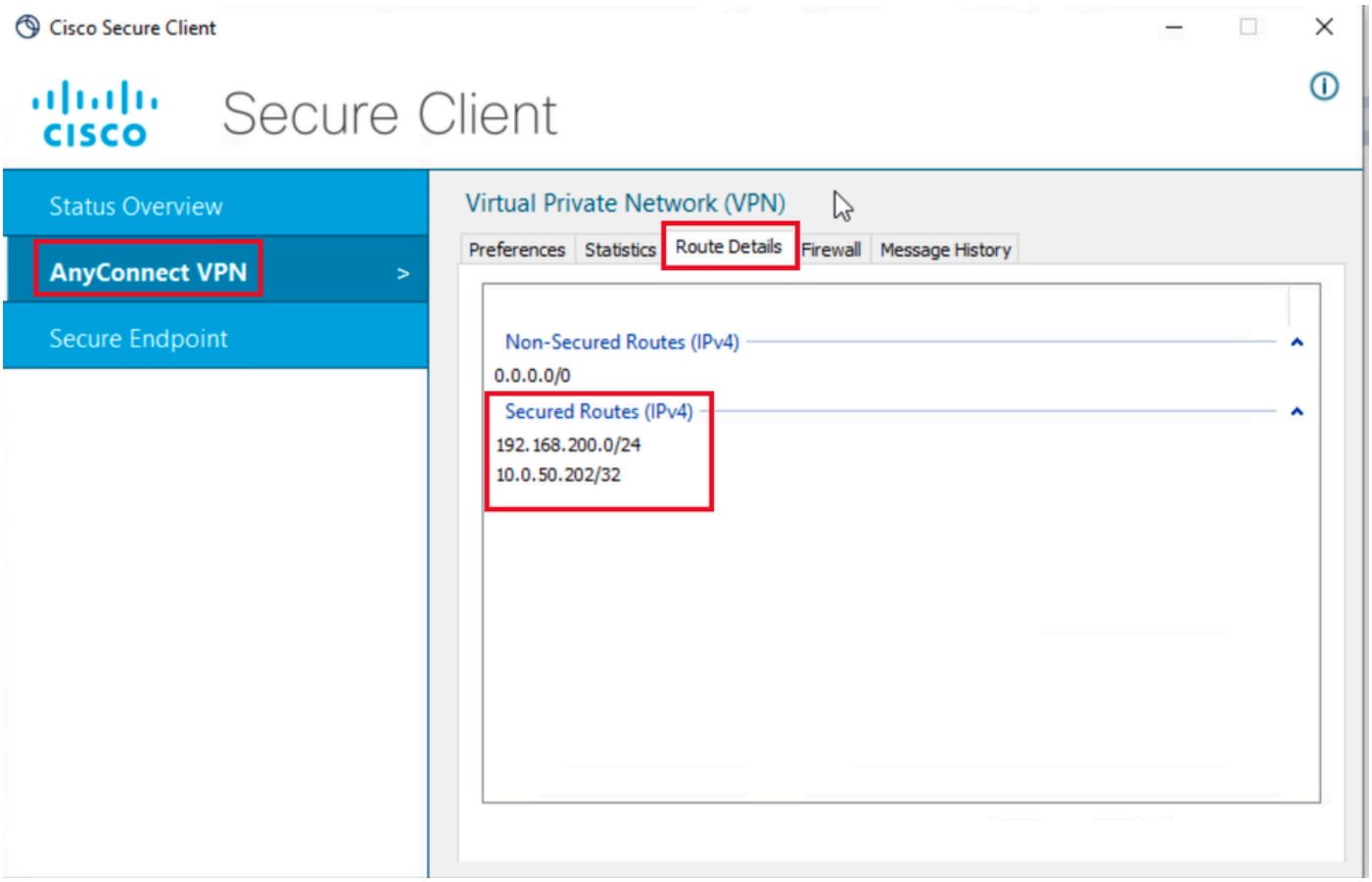
步驟 3.對使用者2憑證重複第1步和第2步，檢查資訊是否與在ISE授權策略上為此組配置的值匹配：


Cisco Secure Client
AnyConnect VPN:
Please enter your username and password.
FlexVPN HUB
Connect
Cisco Secure Client | FlexVPN HUB
Please enter your username and password.
Username:
user2
Password:
******
OK
Cancel

使用者2身份證明



使用者2統計資訊



使用者2路由詳細資訊

疑難排解

調試和日誌

在Cisco路由器上：

1. 使用IKEv2和IPSec調試來驗證頭端和客戶端之間的協商：

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. 使用AAA調試驗證本地和/或遠端屬性的分配：

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

在ISE上：

- RADIUS即時日誌

工作案例

以下輸出是成功連線的示例：

- User1調試輸出：

<#root>

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.088: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.088: idb is NULL
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.089: RADIUS/ENCODE(000000FF): acct_session_id: 4245
Jan 30 02:57:21.089: RADIUS(000000FF): sending
```

```
Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.089: RADIUS(000000FF):
```

Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229

```
RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34
Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194CAE2Z
Jan 30 02:57:21.089: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1]
Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18
RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II*?O]
Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.089: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.090: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.094: RADIUS:
```

Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137

```
RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5
Jan 30 02:57:21.094: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8
RADIUS: 01 52 00 06 0D 20 [ R ]
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@OXH6]
Jan 30 02:57:21.094: RADIUS(000000FF): Received from id 1645/85
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.097: idb is NULL
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): acct_session_id: 4245
```

```
Jan 30 02:57:21.097: RADIUS(000000FF): sending
Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.097: RADIUS(000000FF):
```

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

```
RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC
Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194CAE2Z
Jan 30 02:57:21.098: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8
RADIUS: 02 52 00 06 03 04 [ R]
Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18
RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g$D&d]
Jan 30 02:57:21.098: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.101: RADIUS:
```

Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161

```
RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1
Jan 30 02:57:21.101: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32
RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC 0F B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai
Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18
RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL!]
Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes
Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.103: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.104: idb is NULL
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.104: RADIUS/ENCODE(000000FF): acct_session_id: 4245
Jan 30 02:57:21.104: RADIUS(000000FF): sending
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.104: RADIUS(000000FF):
```

Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332

```
RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46
Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194CAE2Z
Jan 30 02:57:21.104: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24
RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/]
Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>;Tv]
Jan 30 02:57:21.104: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.170: RADIUS:
```

Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233

```
RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6
Jan 30 02:57:21.170: RADIUS: User-Name [1] 7
```

"user1"

```
Jan 30 02:57:21.170: RADIUS: Class [25] 68
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6ZO2L42F2F016FZH]
RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE]
```

```
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams(]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31
```

"ipsec:dns-servers=10.0.50.101"

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41
```

"ipsec:route-set=prefix 192.168.100.0/24"

```
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24
```

"ipsec:addr-pool=group1"

```
Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f
Jan 30 02:57:21.175: AAA/AUTHOR (0x100):
```

Pick method list 'FlexVPN-Authorization-List'

```
Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
Jan 30 02:57:21.192: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:
```

Line protocol on Interface Virtual-Access1, changed state to up

- 使用者2調試輸出：

<#root>

```
Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f
Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.103: RADIUS(00000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229

```
RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64
Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194E444Z
Jan 30 03:28:58.104: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]
Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]
Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.109: RADIUS:
```

Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137

```
RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43
Jan 30 03:28:58.109: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8
RADIUS: 01 35 00 06 0D 20 [ 5 ]
Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18
RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]
Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.113: idb is NULL
Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.113: RADIUS(00000103): sending
Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.113: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316

```
RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C
Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194E444Z
Jan 30 03:28:58.113: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8
RADIUS: 02 35 00 06 03 04 [ 5]
Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18
RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]
Jan 30 03:28:58.113: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.116: RADIUS:
```

Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161

```
RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02
Jan 30 03:28:58.116: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32
RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM
Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18
RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]
Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes
Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.118: idb is NULL
```

```
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.118: RADIUS(00000103): sending
Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.119: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332

```
RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE
Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30
```

"isakmp-phase1-id=cisco.example"

```
Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116ZO2L42F2F016FZH1194E444Z
Jan 30 03:28:58.119: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24
RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w]
Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18
RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo]
Jan 30 03:28:58.119: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116ZO2L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233
RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD
Jan 30 03:28:58.186: RADIUS: User-Name [1] 7
```

"user2"

```
Jan 30 03:28:58.186: RADIUS: Class [25] 68
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6ZO2L42F2F016FZH]
RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 33 30 [ 30]
Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6
RADIUS: 03 36 00 04 [ 6]
Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18
RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S]
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31
```

"ipsec:dns-servers=10.0.50.202"

```
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41
```

"ipsec:route-set=prefix 192.168.200.0/24"

```
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24
```

"ipsec:addr-pool=group2"

```
Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f
Jan 30 03:28:58.190: AAA/AUTHOR (0x104):
```

Pick method list 'FlexVPN-Authorization-List'

```
Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to
Jan 30 03:28:58.209: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:
```

Line protocol on Interface Virtual-Access2, changed state to up

相關資訊

- 思科技術支援與下載