使用ISE配置Catalyst 9800 WLC iPSK

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[瞭解iPSK是什麼，它適合哪些場景](#)
[設定9800 WLC](#)
[ISE 組態](#)
[疑難排解](#)
[9800 WLC上的疑難排解](#)
[排除ISE故障](#)

簡介

本文檔介紹在思科9800無線LAN控制器上配置iPSK安全WLAN，並將思科ISE作為RADIUS伺服器。

必要條件

需求

本檔案假設您已熟悉9800上WLAN的基本組態，且能夠調整組態以適應您的部署。

採用元件

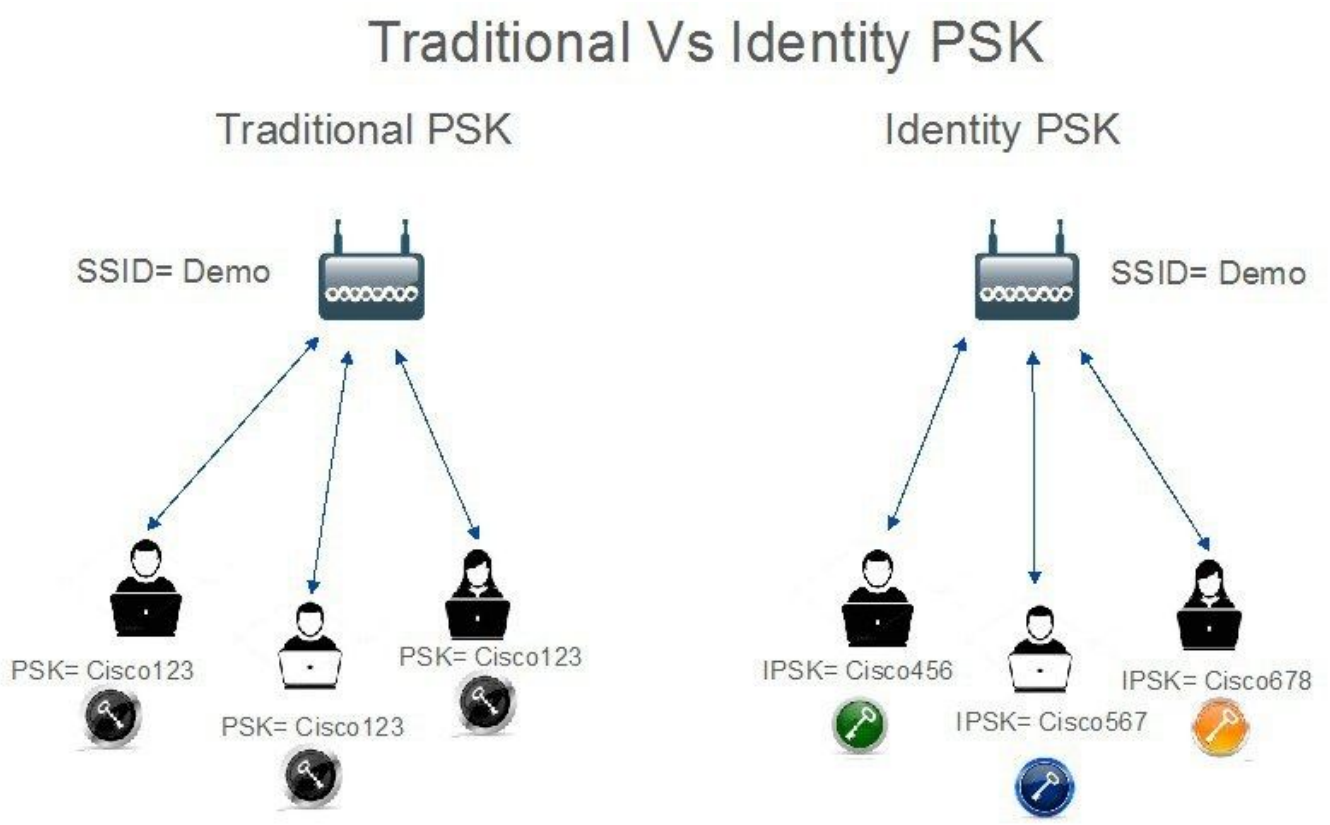
- 執行17.6.3的Cisco 9800-CL WLC
- Cisco ISE 3.0

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。

瞭解iPSK是什麼，它適合哪些場景

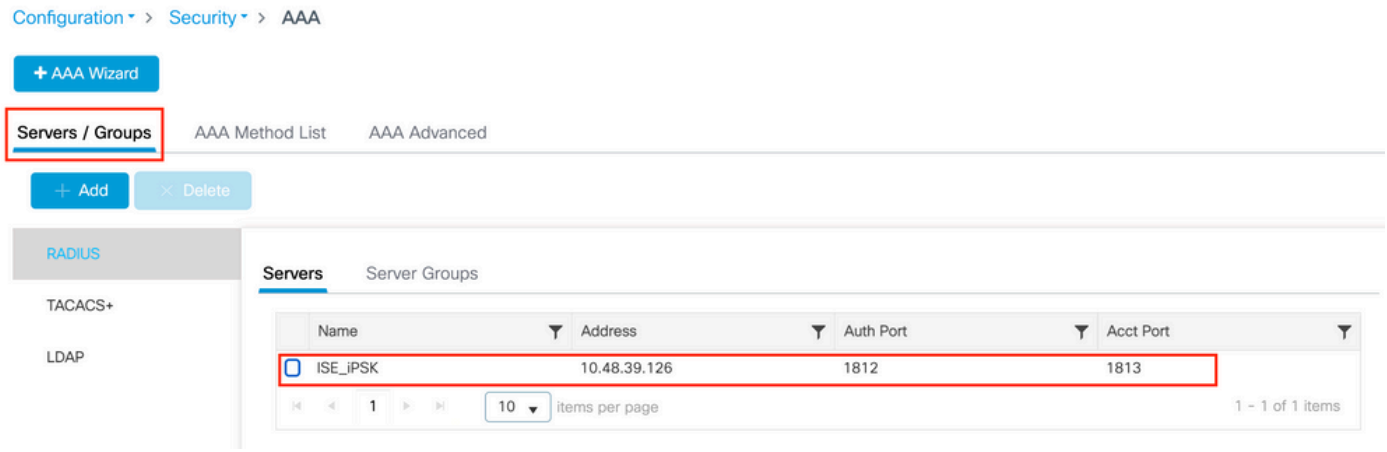
傳統的預共用金鑰(PSK)安全網路對所有連線的客戶端使用相同的密碼。這可能會導致與未經授權的使用者共用金鑰，從而造成安全漏洞和未經授權的網路訪問。對此漏洞最常見的緩解措施是PSK本身的更改，這種更改會影響所有使用者，因為許多終端裝置需要更新新金鑰才能再次訪問網路。

使用身份PSK(iPSK)，在RADIUS伺服器的幫助下為同一SSID上的個人或使用者組建立唯一的預共用金鑰。此類設定對於終端客戶端裝置不支援dot1x身份驗證，但需要更安全和更精細的身份驗證方案的網路極為有用。從客戶端的角度來看，此WLAN看起來與傳統PSK網路完全相同。如果其中一個PSK受到危害，只有受影響的個人或團體需要更新其PSK。連線到WLAN的其餘裝置不受影響。

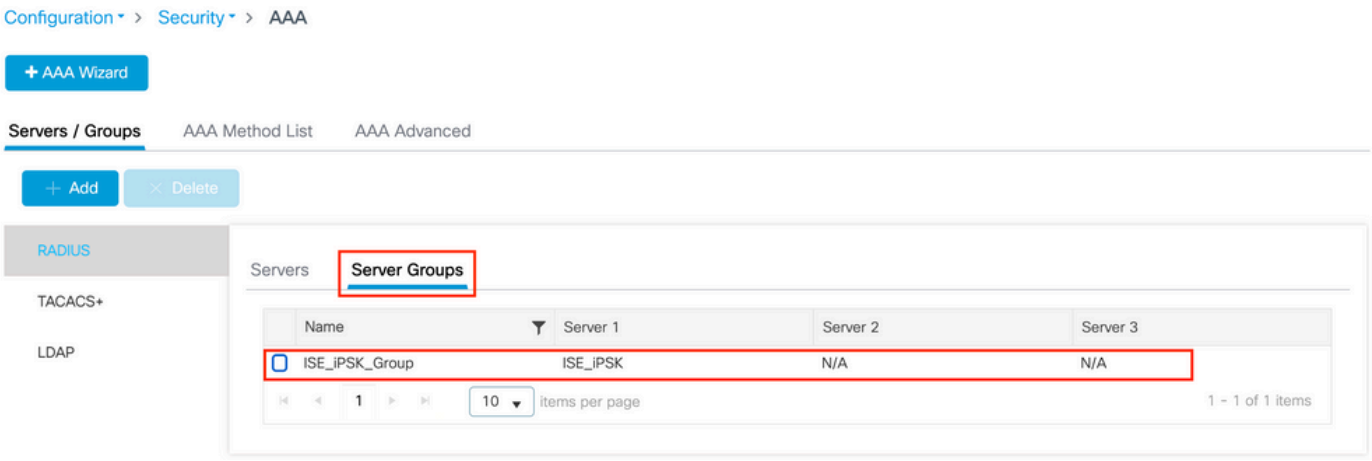


設定9800 WLC

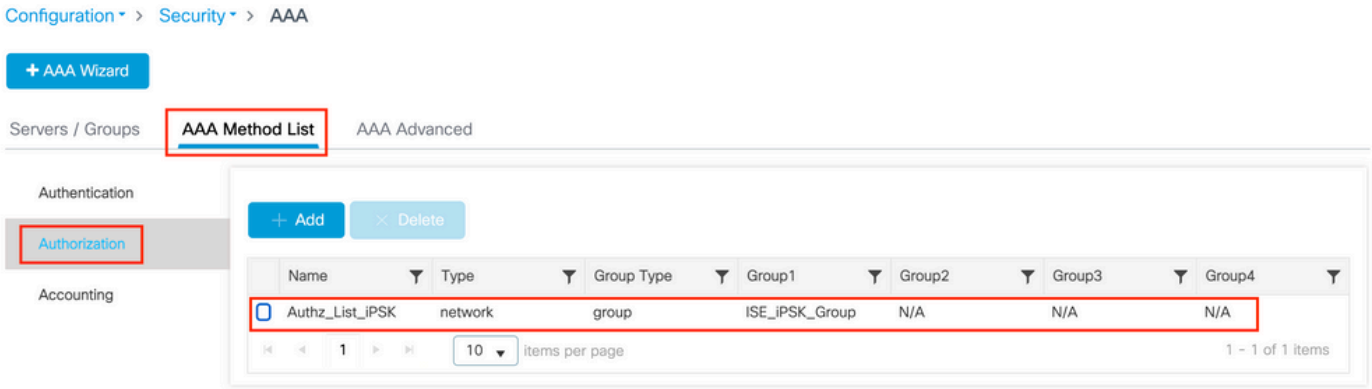
在**Configuration > Security > AAA > Servers/Groups > Servers**下，將ISE新增為RADIUS伺服器：



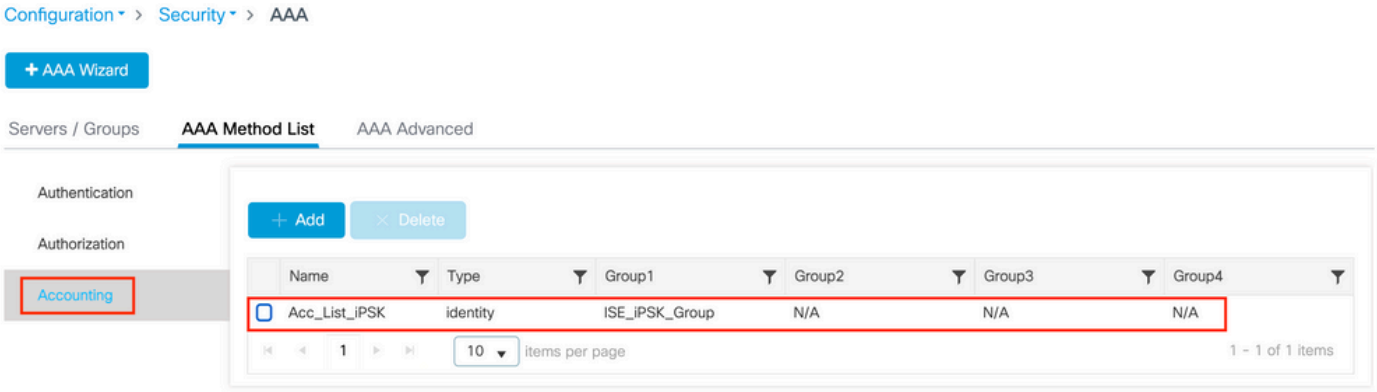
在**Configuration > Security > AAA > Servers/Groups > Server Groups**下，建立RADIUS伺服器組並將先前建立的ISE伺服器新增到其中：



在「**AAA Method List**」索引標籤中，建立一個**Authorization**清單，其中的「Type」為「**network**」，而「Group Type」為「**group**」，指出先前建立的RADIUS伺服器群組：



設定記賬是可選的，但可以通過將型別配置為「**identity**」並將其指向同一RADIUS伺服器組來完成：

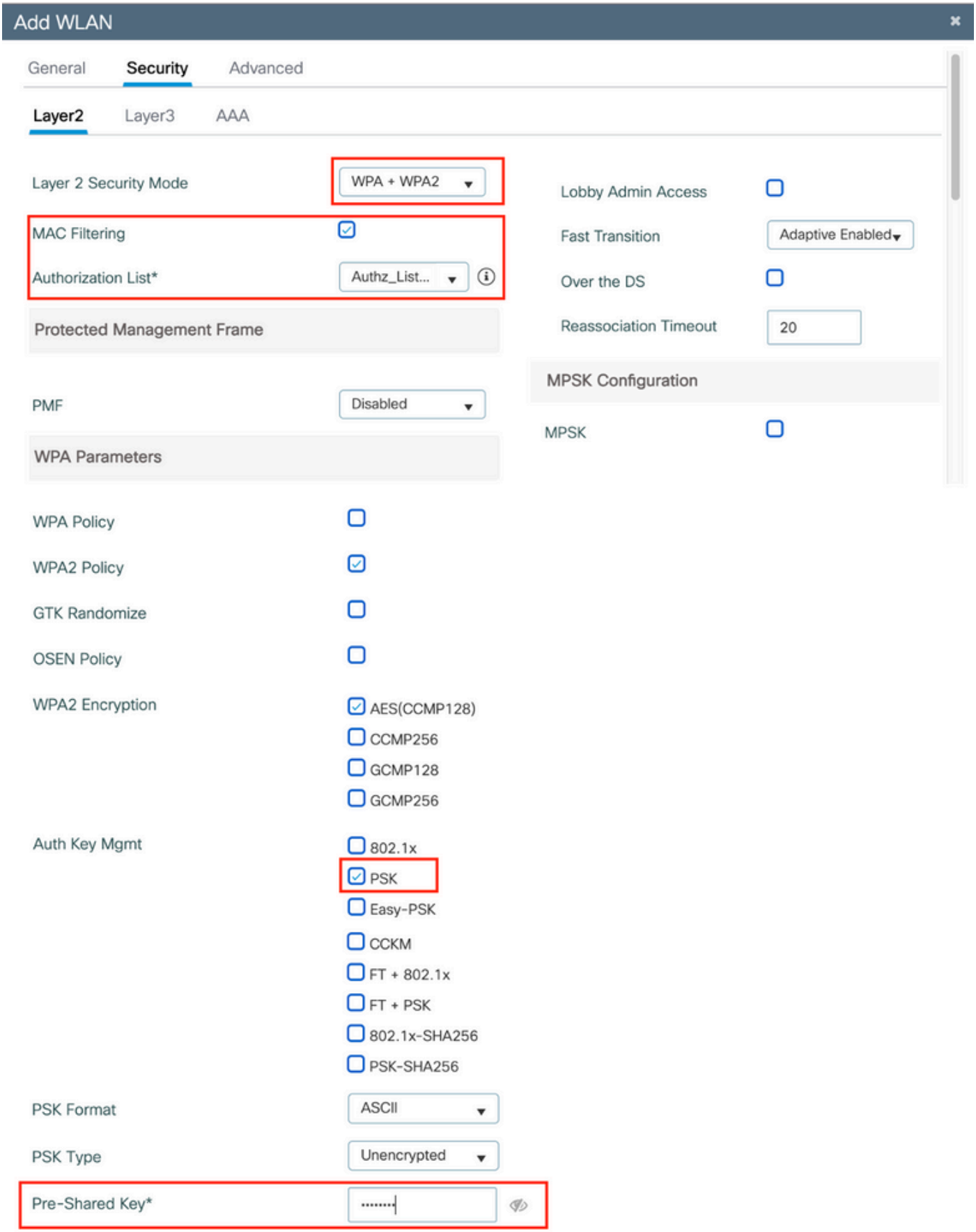


這也可以通過命令列使用以下命令來執行：

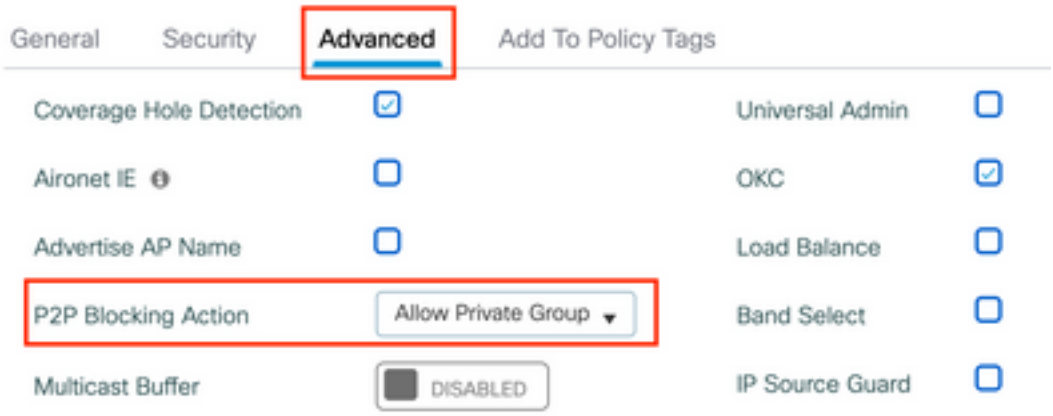
```
radius server
```

在**Configuration > Tags & Profiles > WLANs**下，建立一個新的WLAN。 在第2層配置下：

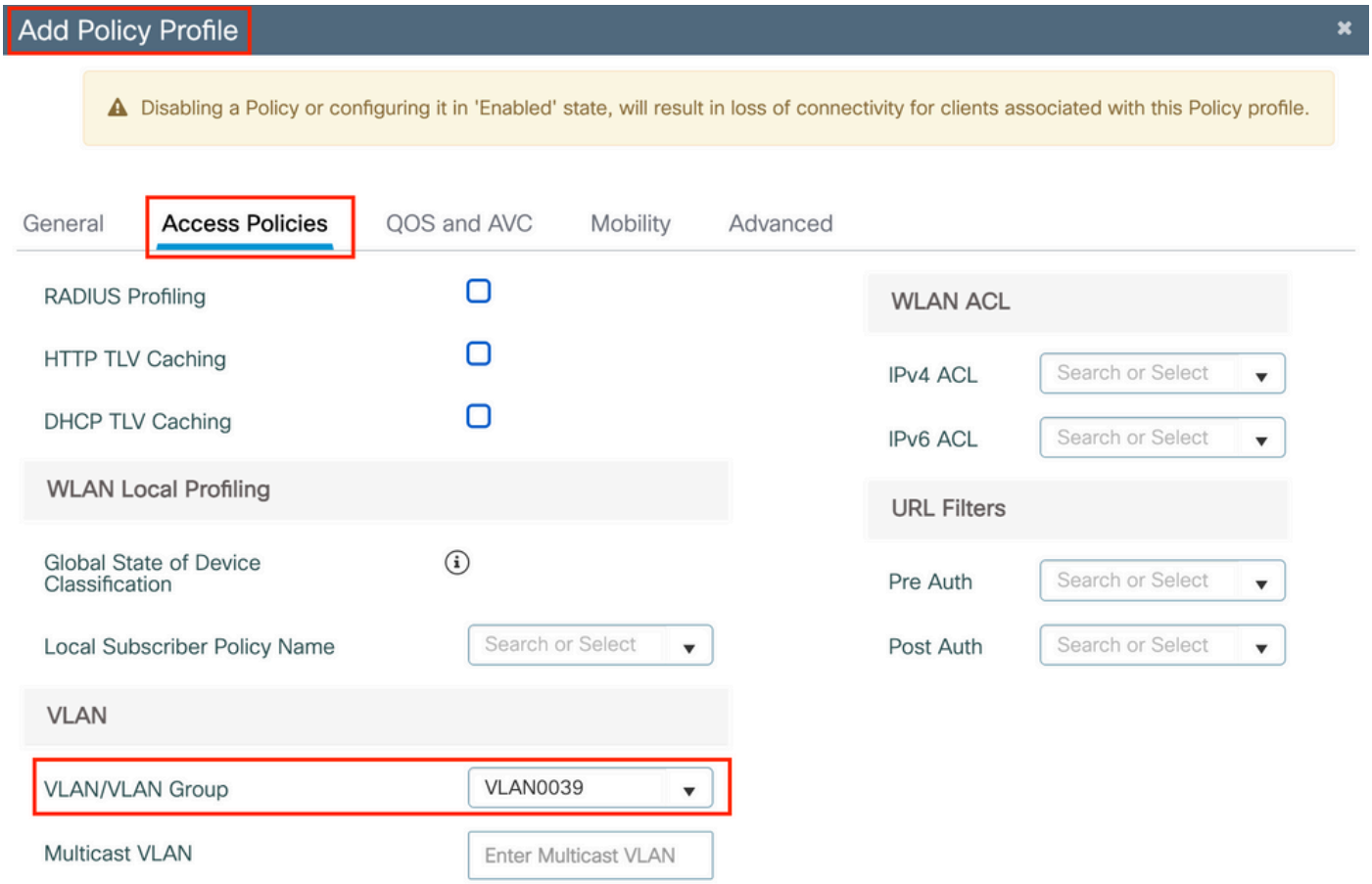
- 啟用MAC過濾並將Authorization List設定為之前建立的清單
- 在**Auth Key Mgmt**下啟用**PSK**
- 預共用金鑰欄位可以填充任何值。這樣做只是為了滿足Web介面設計的要求。沒有使用者能夠使用此金鑰進行身份驗證。在這種情況下，預共用金鑰設定為「12345678」。



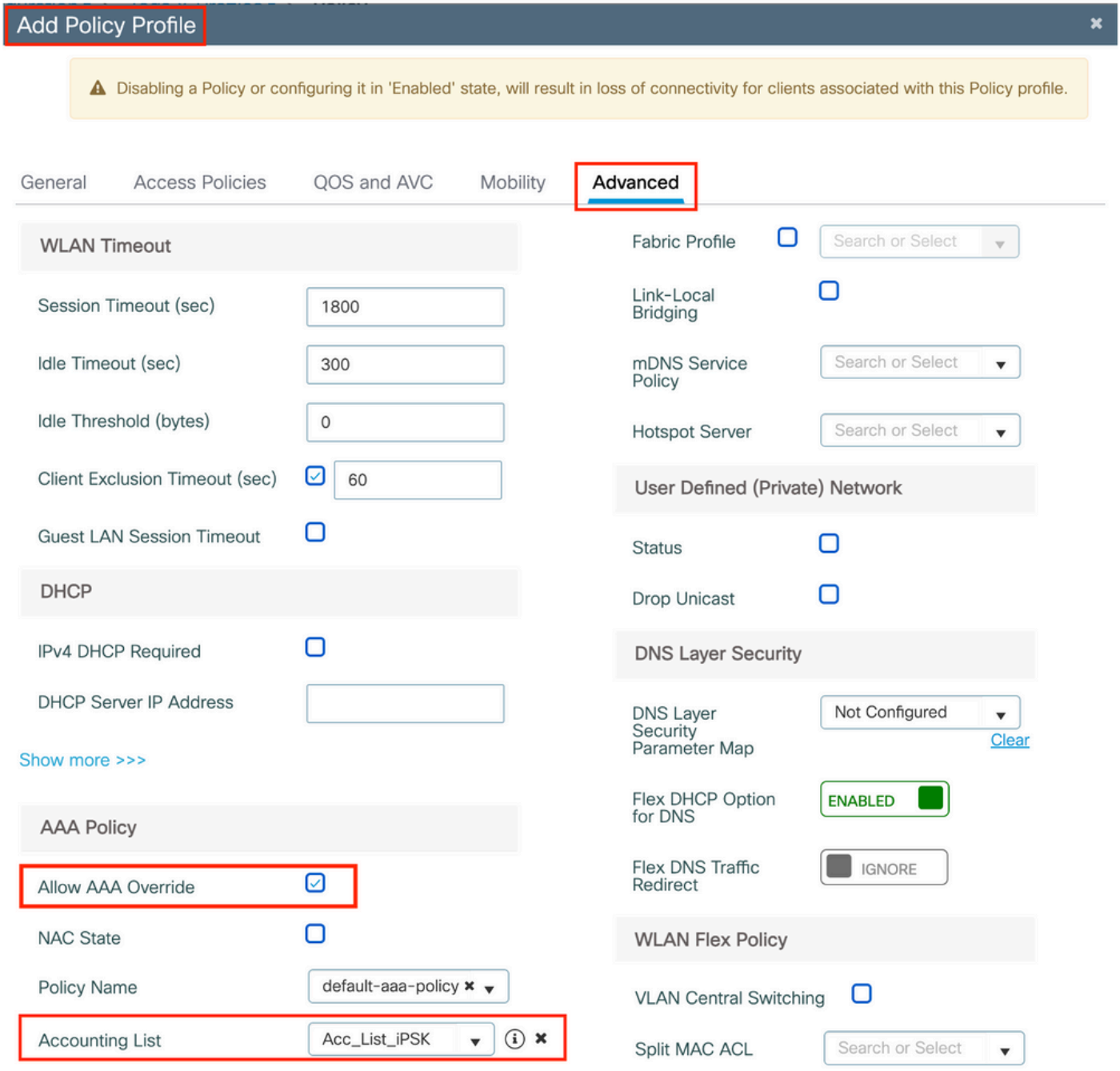
可以在**Advanced**頁籤下實現使用者隔離。將其設定為Allow Private Group可允許使用同一PSK的使用者相互通訊，而使用不同PSK的使用者將被阻止：



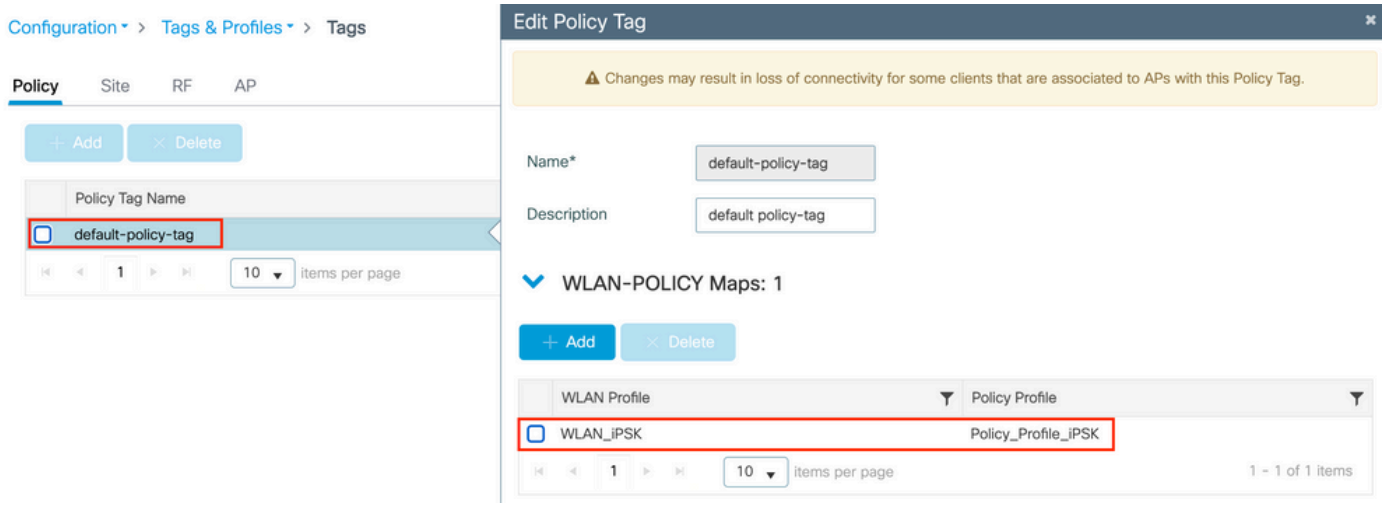
在**Configuration > Tags & Profiles > Policy**下，建立新的策略配置檔案。在**Access Policies**索引標籤中，設定此WLAN使用的VLAN或VLAN群組：



在**Advanced**頁籤中，啟用AAA Override並新增Accounting清單（如果之前已建立）：



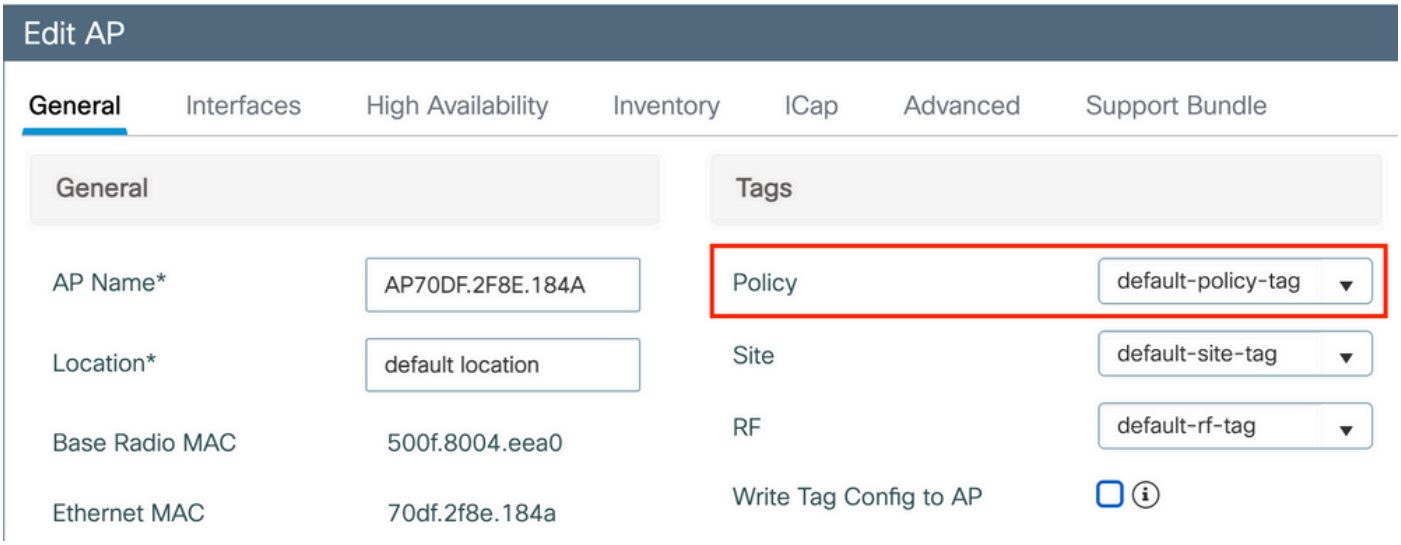
在**Configuration > Tags & Profiles > Tags > Policy**下，確保WLAN已對映到您建立的策略配置檔案：



這也可以通過命令列使用以下命令來執行：

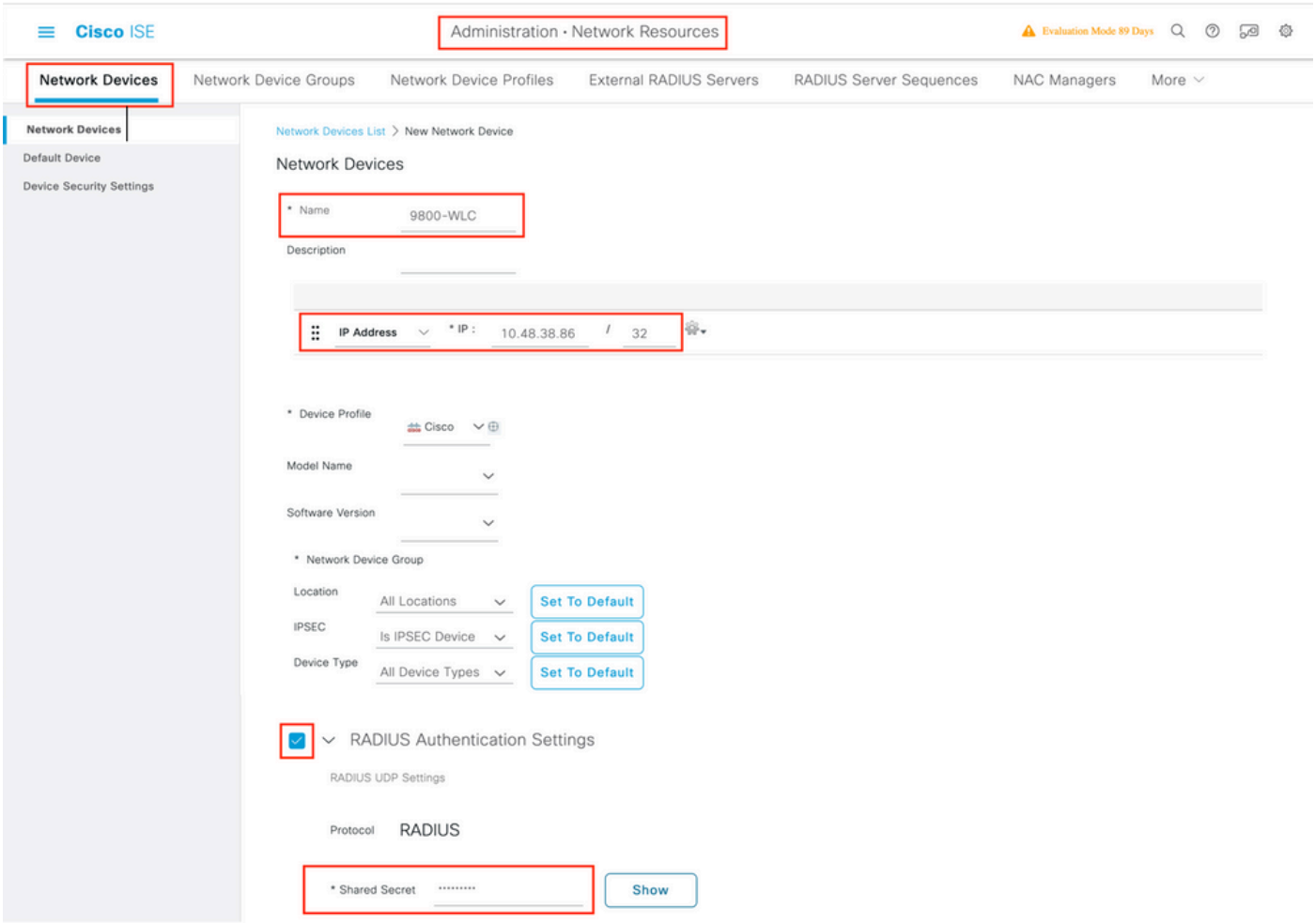
```
wlan
```

在**Configuration > Wireless > Access Points**下，確保此標籤已應用於必須在其上廣播WLAN的接入點：

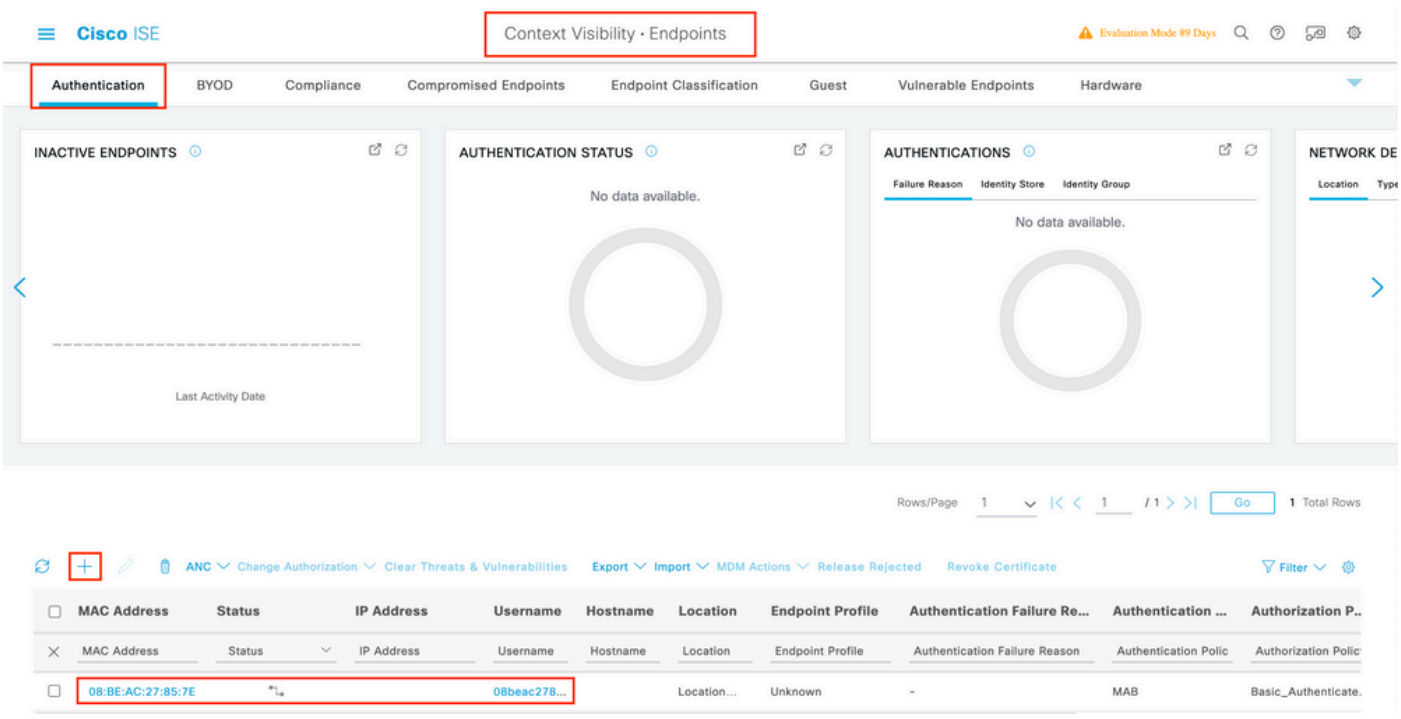


ISE 組態

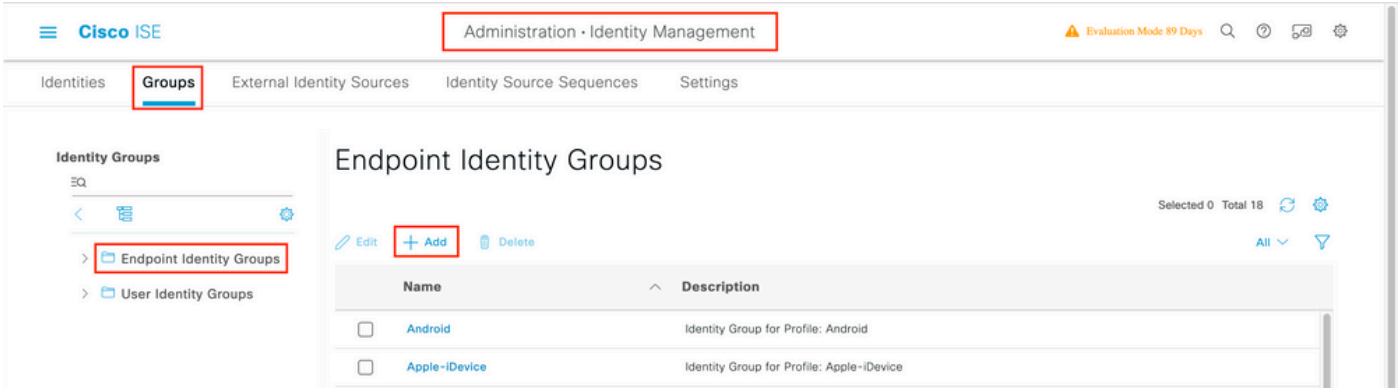
此配置指南介紹根據客戶端MAC地址確定裝置PSK的方案。在**Administration > Network Resources > Network Devices**下，新增新裝置、指定IP地址、啟用RADIUS身份驗證設定並指定RADIUS共用金鑰：

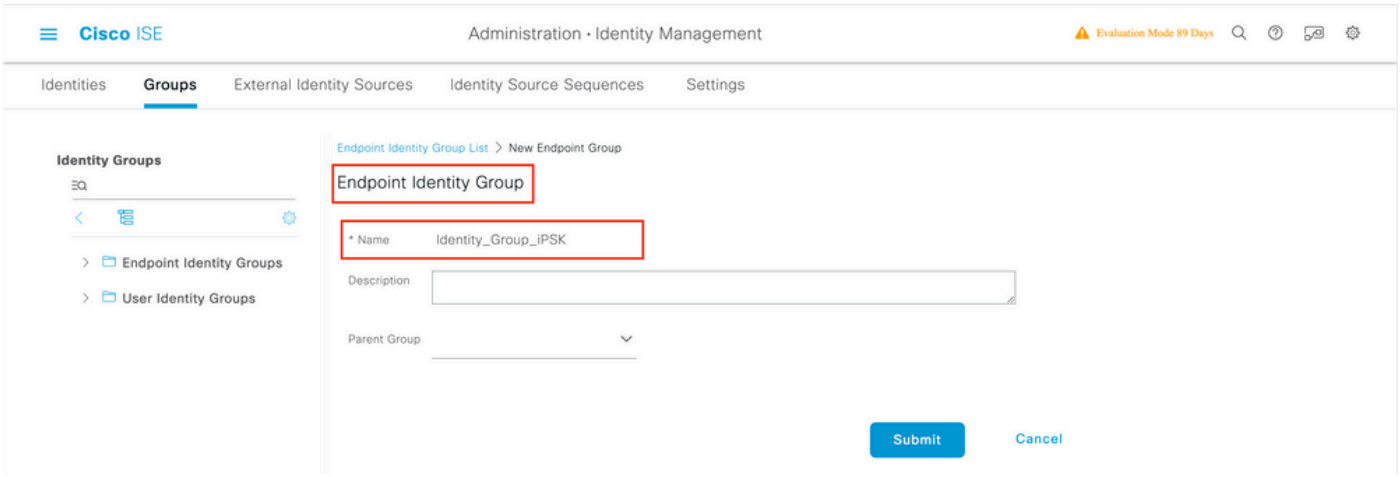


在**Context Visibility > Endpoints > Authentication**下，新增連線到iPSK網路的所有裝置（客戶端）的MAC地址：

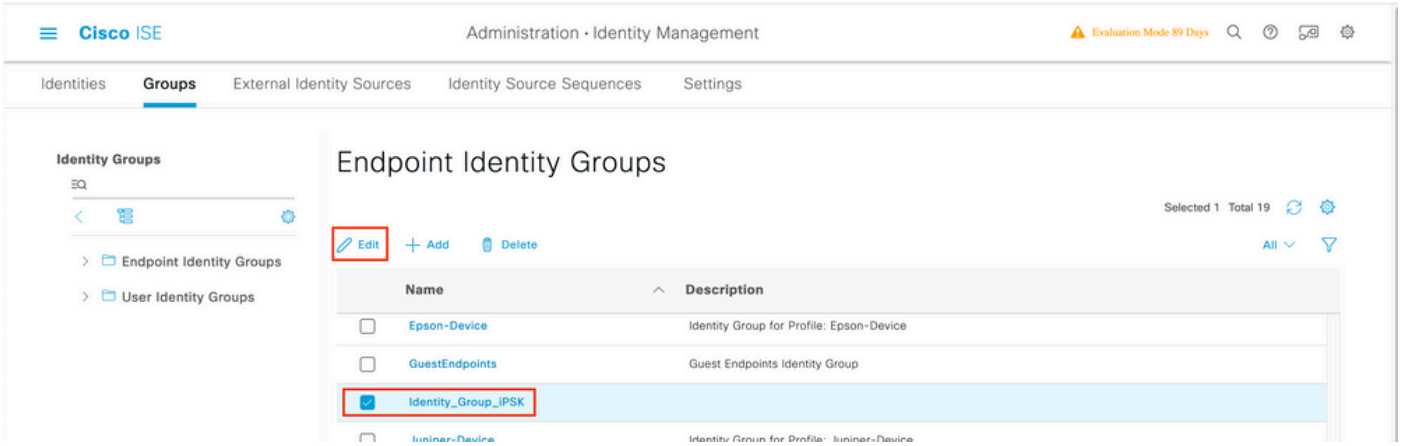


在**Administration > Identity Management>** Groups **> Endpoint Identity Groups**下，建立一個或多個組並將使用者分配給它們。以後可以將每個組配置為使用不同的PSK連線到網路。

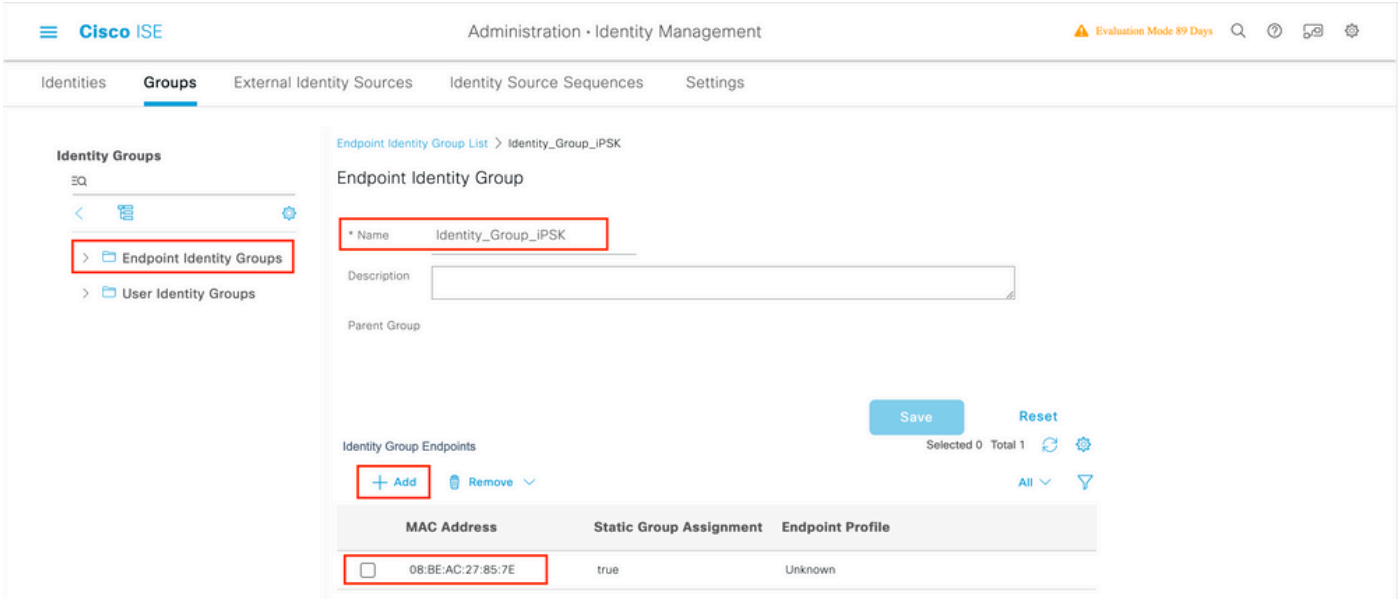




建立組後，您現在可以為其分配使用者。選擇您建立的組，然後按一下「編輯」：



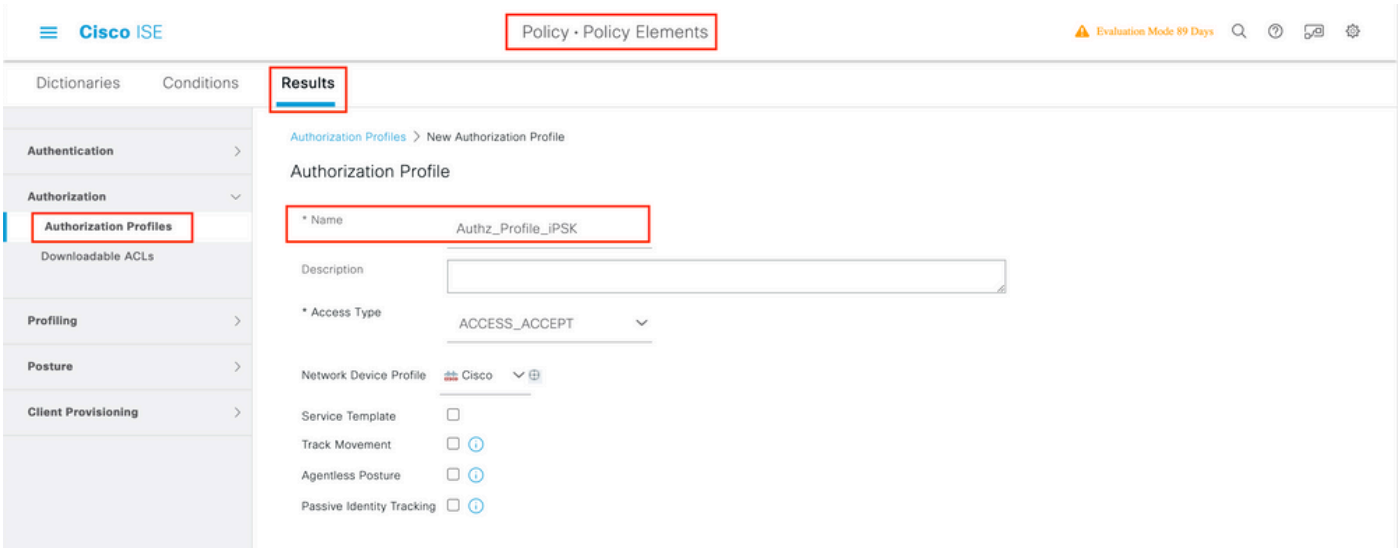
在組配置中，通過按一下「新增」按鈕新增要分配給該組的客戶機的MAC地址：

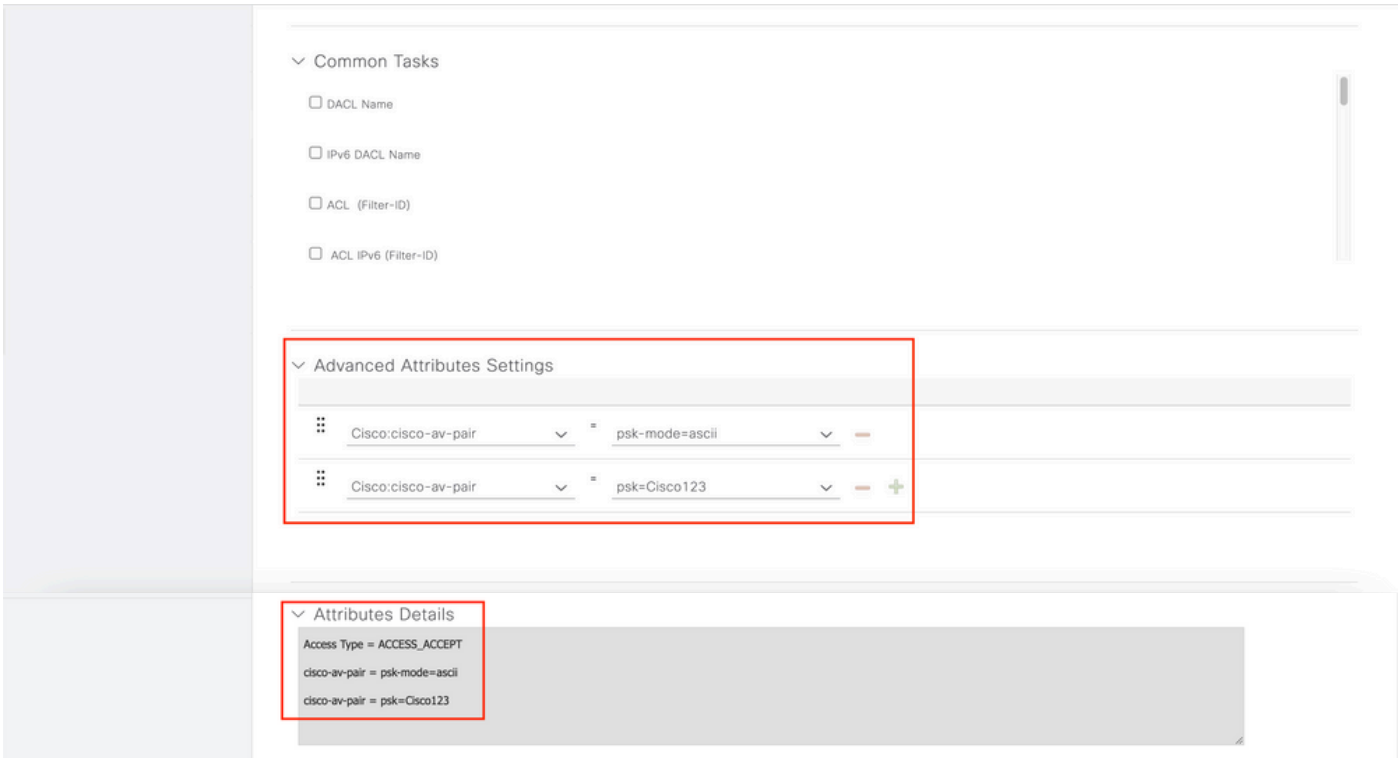


在Policy > **Policy Elements > Results > Authorization > Authorization Profiles**下，建立新的授權配置檔案。將屬性設定為：

```
access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=
```

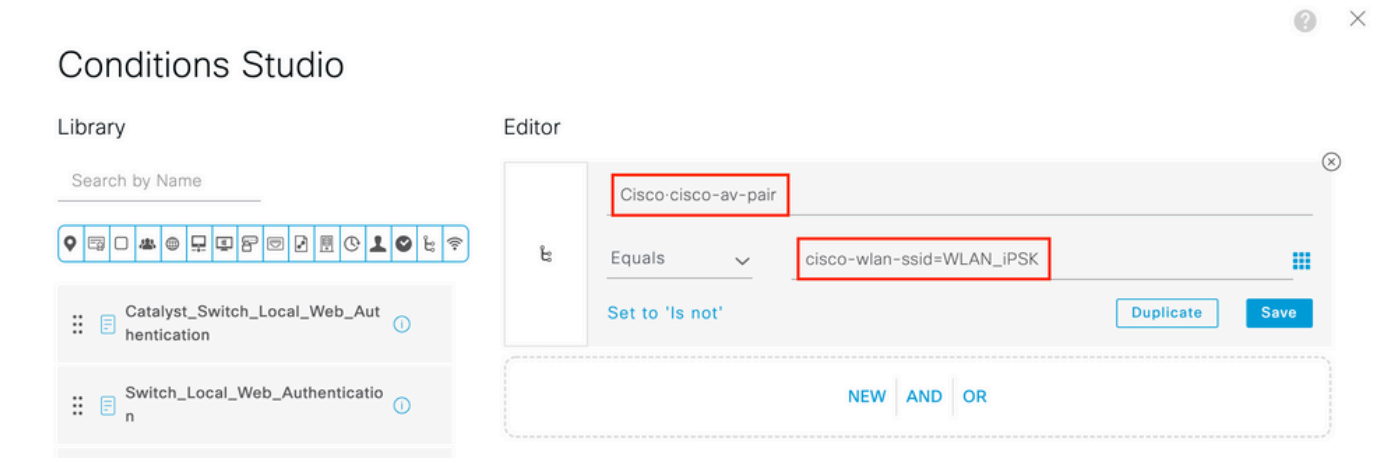
對於必須使用不同PSK的每個使用者組，使用不同的PSK av-pair建立一個附加結果。在此處還可以配置ACL和VLAN覆蓋等其他引數。



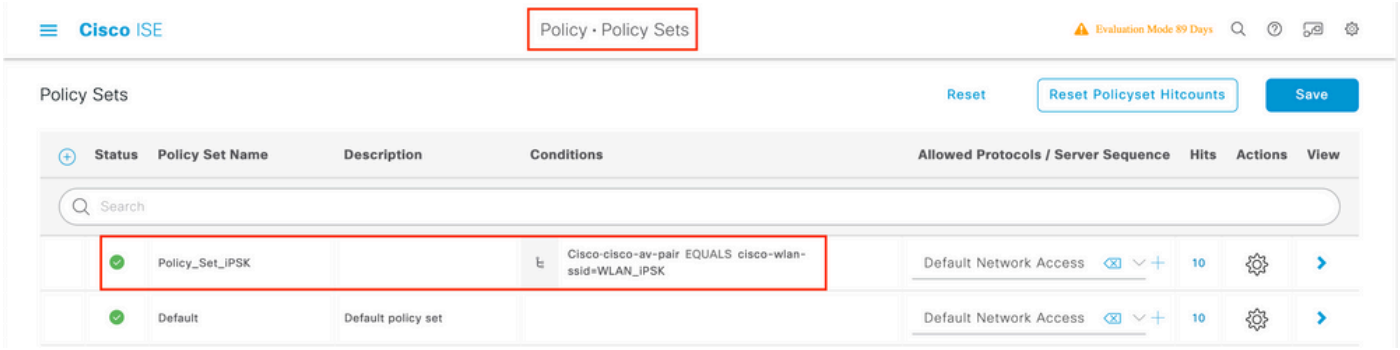


在**Policy > Policy Sets**下，建立一個新策略。要確保客戶端匹配策略集，使用以下條件：

```
Cisco:cisco-av-pair EQUALS cisco-wlan-ssid=WLAN_iPSK    // "WLAN_iPSK" is WLAN name
```

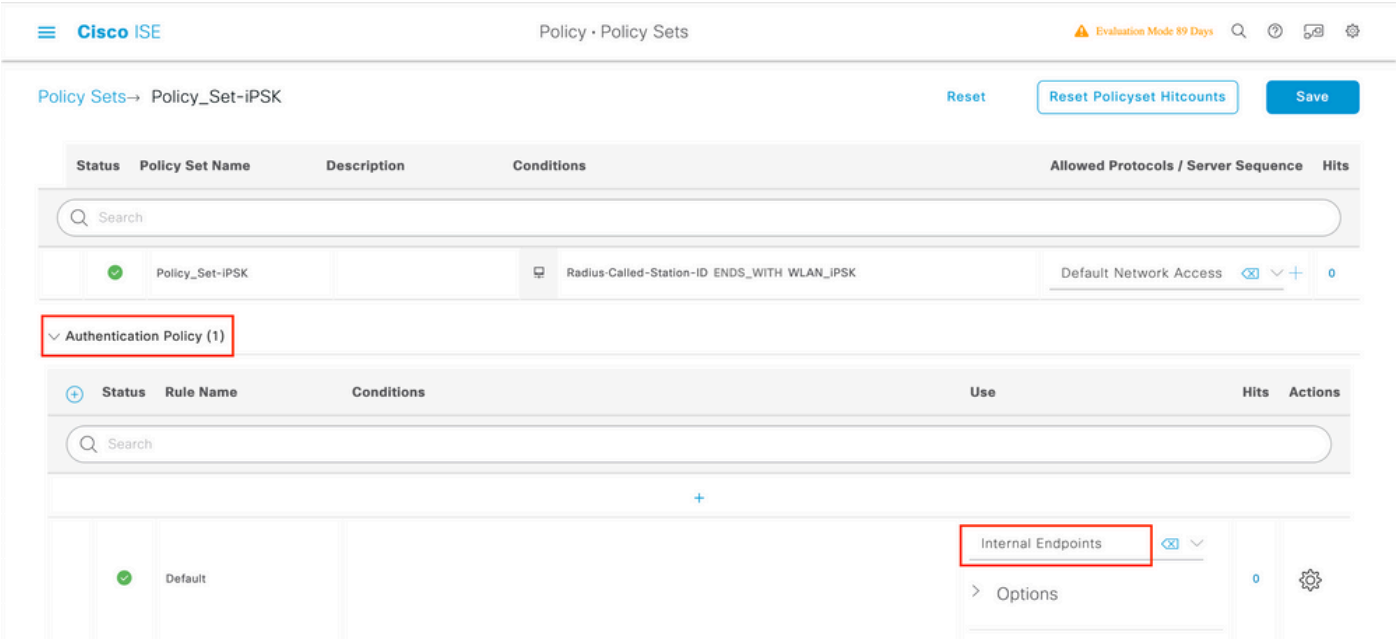


可以新增其他條件以使策略匹配更安全。



按一下「Policy Set（策略集）」行右側的藍色箭頭可訪問新建立的iPSK策略集配置：

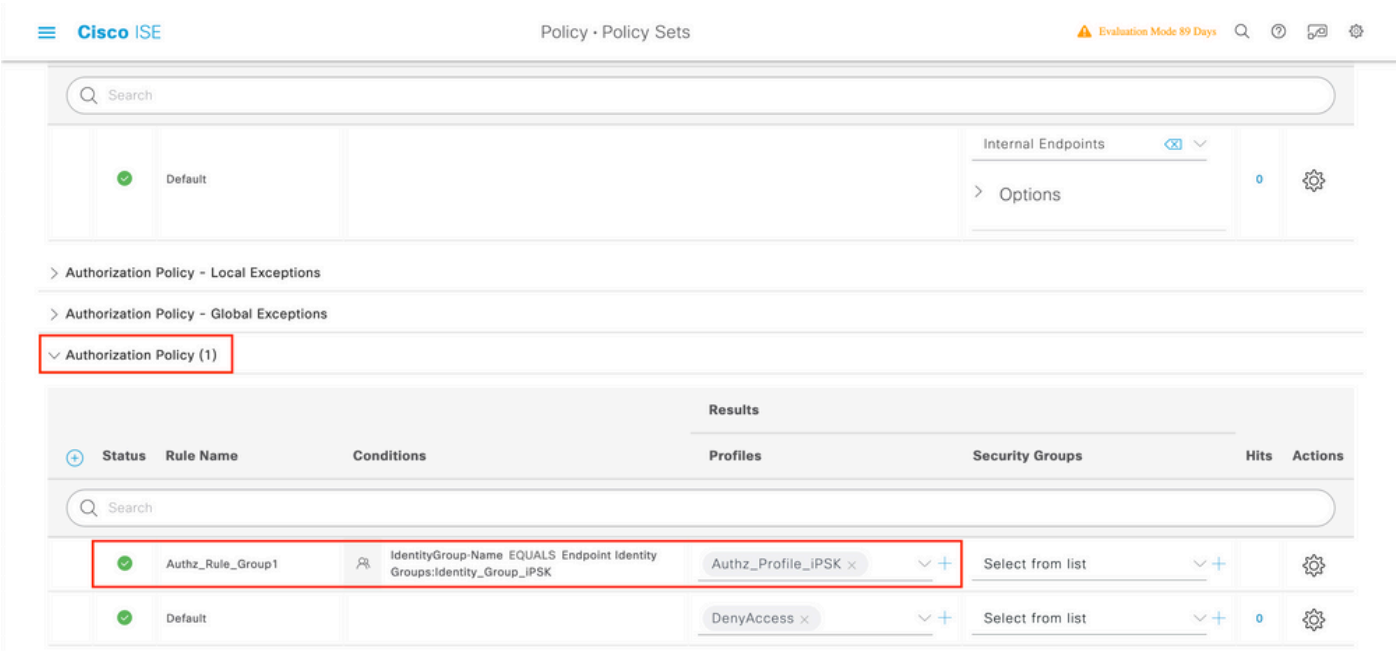
確保**Authentication Policy**設定為「Internal Endpoints」：



在**Authorization Policy**下，為每個使用者組建立一個新規則。作為條件，請使用：

```
IdentityGroup-Name EQUALS Endpoint Identity Group:Identity_Group_iPSK      //
"Identity_Group_iPSK" is name of the created endpoint group
```

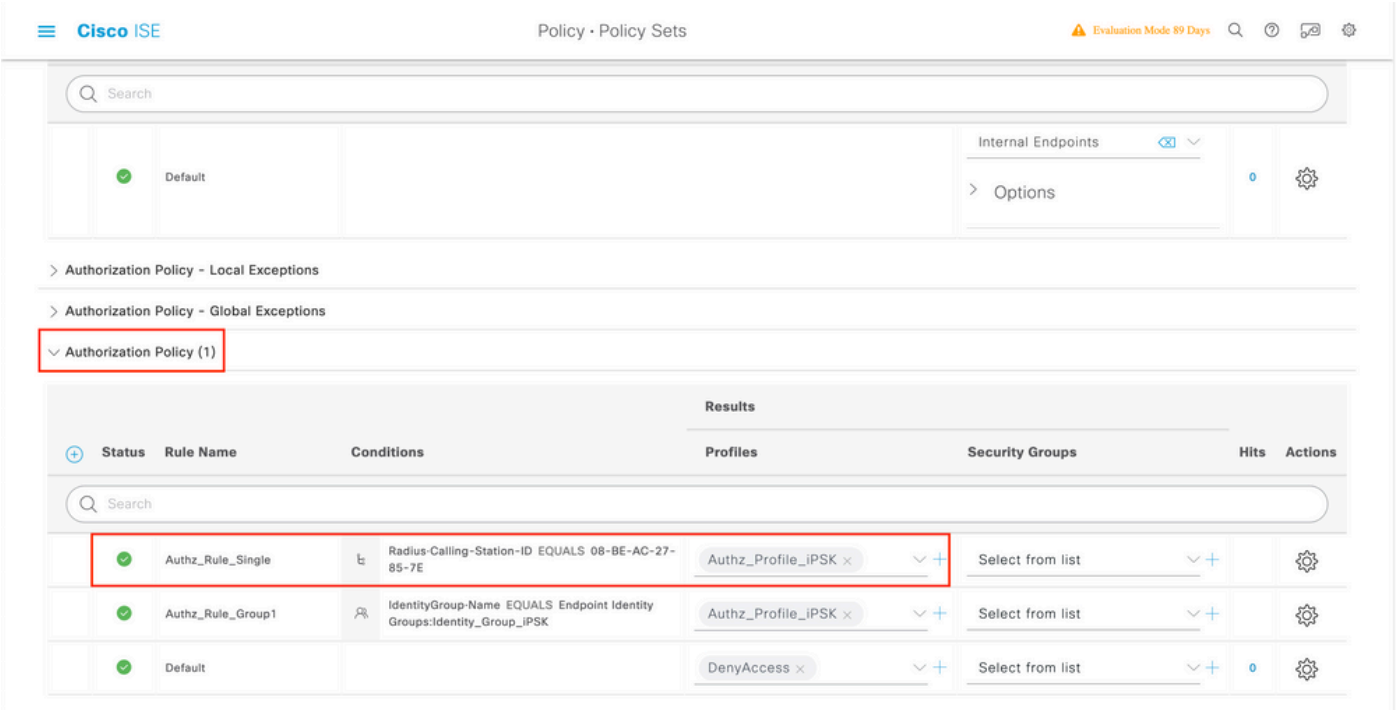
Result是之前建立的Authorization Profile。確保Default Rule位於底部並指向DenyAccess。



如果每個使用者將具有不同的密碼，而不是建立與該終端組匹配的終端組和規則，則可以建立具有此條件的規則：

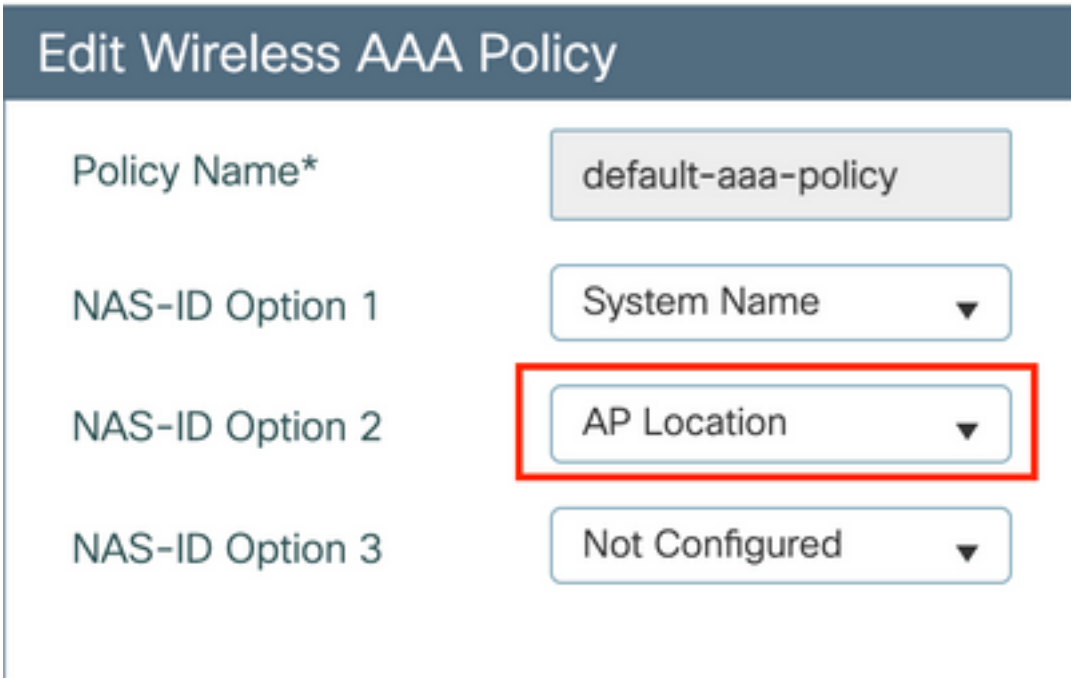
```
Radius-Calling-Station-ID EQUALS <client_mac_addr>
```

附註： MAC位址分隔符可在WLC上的**AAA >AAA Advanced > Global Config > Advanced Settings下設定**。在本示例中，使用了字元「 — 」。



授權策略上的規則允許使用許多其他引數來指定使用者正在使用的密碼。一些最常用的規則是：

1. **基於使用者位置的匹配**
   在此案例中，WLC需要將AP位置資訊傳送到ISE。這允許一個位置的使用者使用一個密碼，而另一個位置的使用者使用不同的密碼。可在**Configuration > Security > Wireless AAA Policy**下配置此功能。



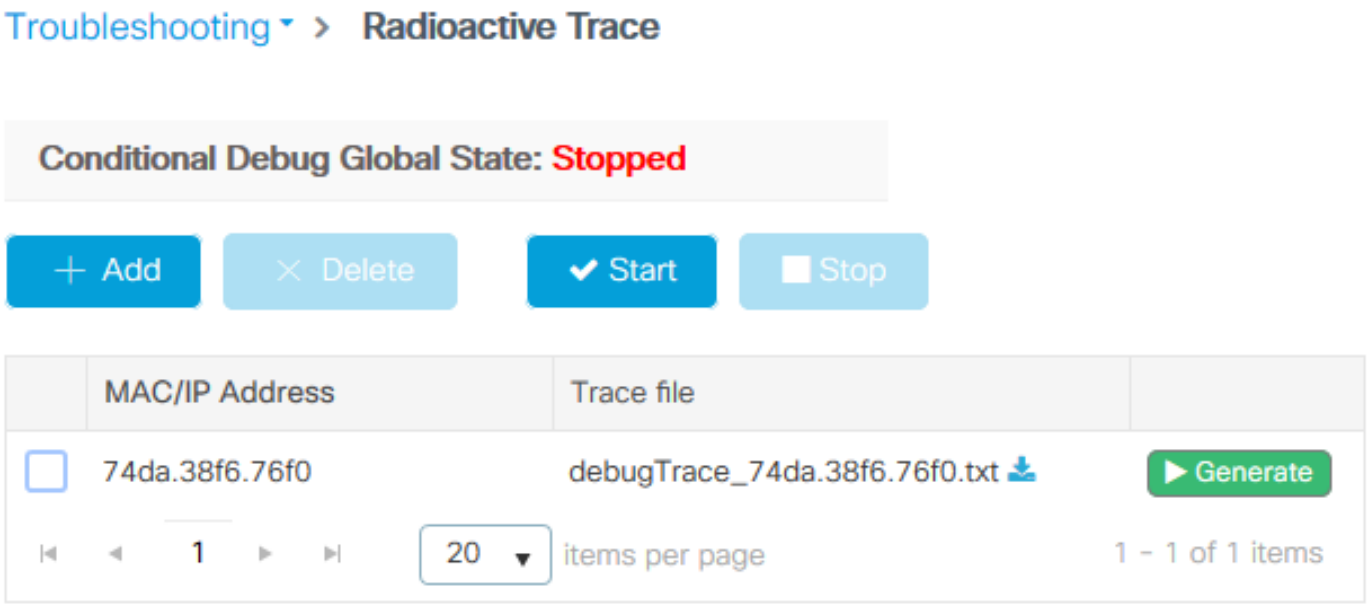
2. **根據裝置分析進行匹配**
   在此案例中，需要將WLC設定為全域性設定裝置設定檔。這允許管理員為筆記型電腦和電話裝置配置不同的密碼。可在**Configuration > Wireless > Wireless Global**下啟用全域性裝置分類。

有關ISE上的裝置分析配置，請參閱ISE分析設計手冊。
除了返回加密金鑰外，由於此授權發生在802.11關聯階段，因此完全可以從ISE返回其他AAA屬性，如ACL或VLAN id。

疑難排解

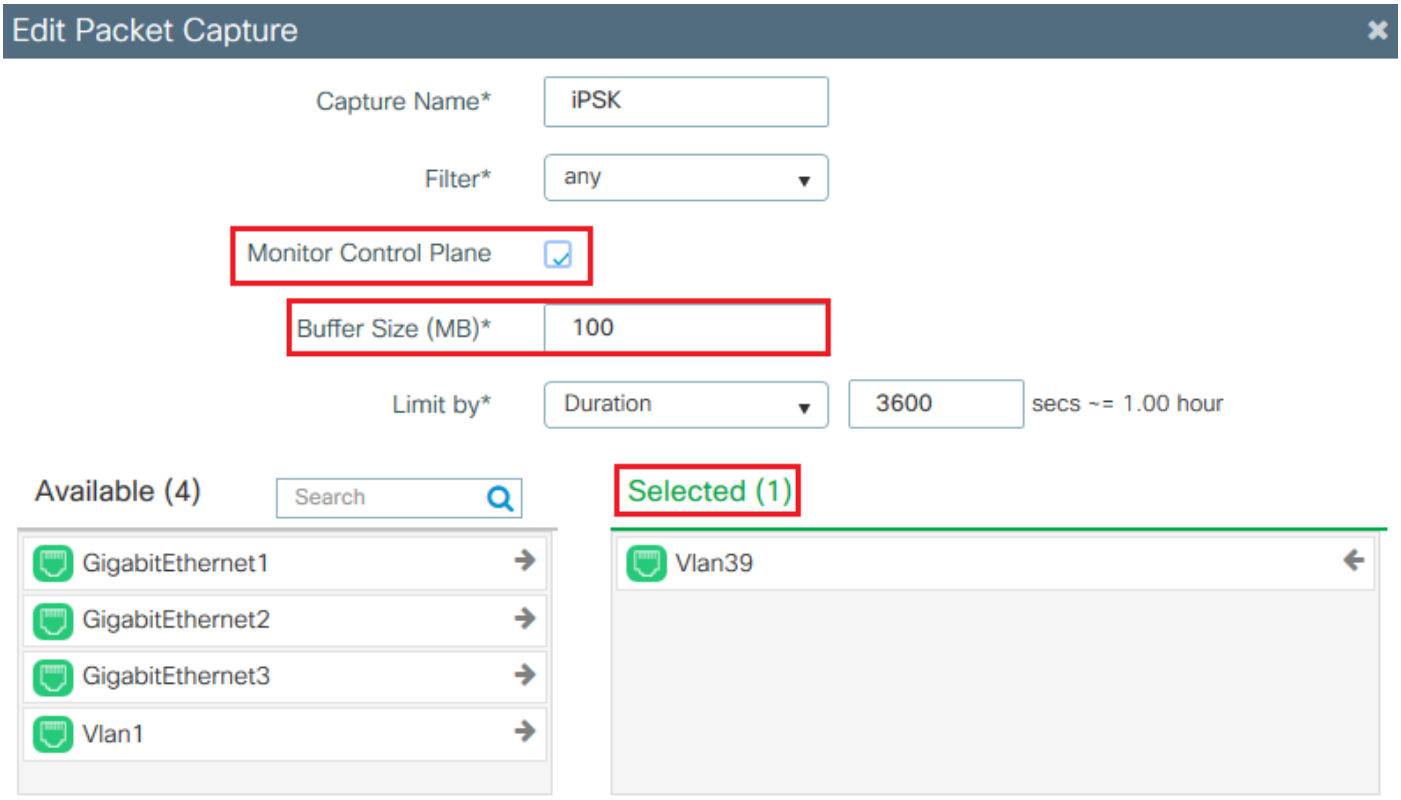
9800 WLC上的疑難排解

在WLC上，收集放射性痕跡必須足以識別大多數問題。可以在WLC Web介面的**疑難排解 > 放射追蹤**下完成此操作。新增客戶端MAC地址，按**開始**並嘗試重現問題。 按一下「**Generate**」以建立檔案並下載：



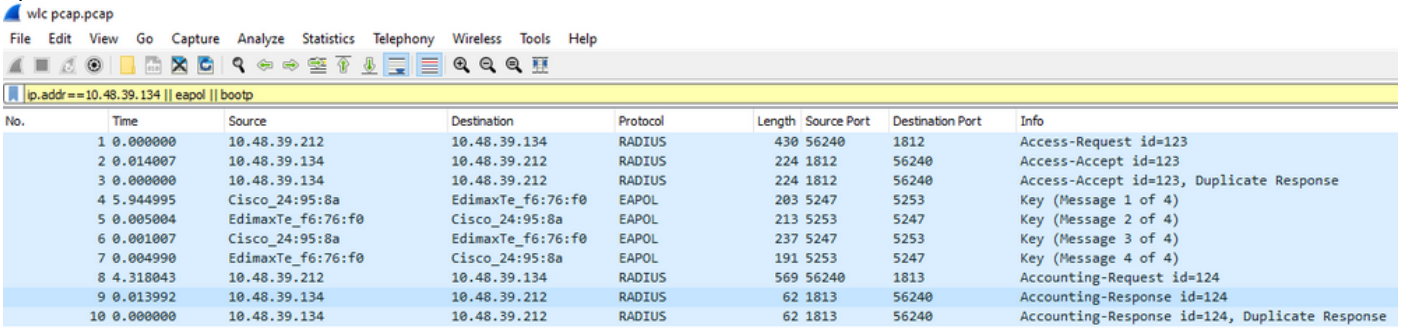
重要資訊:IOS 14和Android 10智慧手機上的iPhone在關聯網路時使用隨機mac地址。此功能可能會完全中斷iPSK配置。請確保此功能已禁用！

如果放射性追蹤不足以識別問題，可以直接在WLC上收集封包擷取。在**Troubleshooting > Packet Capture**下，新增捕獲點。預設情況下，WLC使用無線管理介面進行所有RADIUS AAA通訊。如果WLC有大量使用者端，可將緩衝區大小增加至100 MB:



成功進行身份驗證和記帳嘗試的資料包捕獲如下圖所示。使用此Wireshark過濾器過濾出此客戶端的所有相關資料包：

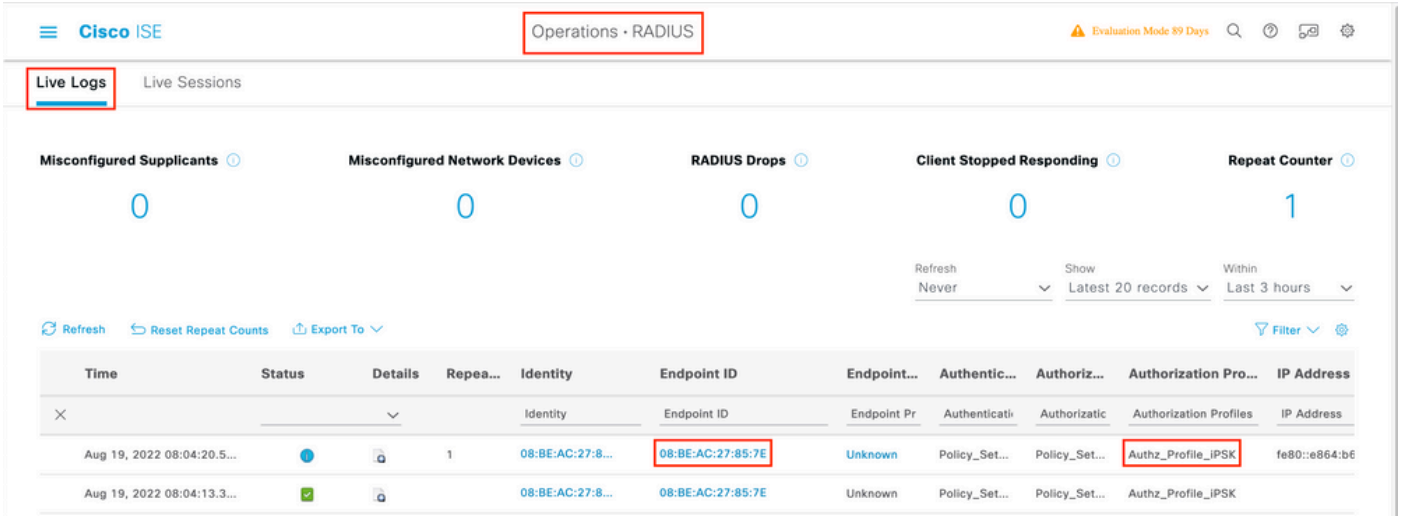
```
ip.addr==
```



No.	Time	Source	Destination	Protocol	Length	Source Port	Destination Port	Info
1	0.000000	10.48.39.212	10.48.39.134	RADIUS	430	56240	1812	Access-Request id=123
2	0.014007	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123
3	0.000000	10.48.39.134	10.48.39.212	RADIUS	224	1812	56240	Access-Accept id=123, Duplicate Response
4	5.944995	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	203	5247	5253	Key (Message 1 of 4)
5	0.005004	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	213	5253	5247	Key (Message 2 of 4)
6	0.001007	Cisco_24:95:8a	EdimaxTe_f6:76:f0	EAPOL	237	5247	5253	Key (Message 3 of 4)
7	0.004990	EdimaxTe_f6:76:f0	Cisco_24:95:8a	EAPOL	191	5253	5247	Key (Message 4 of 4)
8	4.318043	10.48.39.212	10.48.39.134	RADIUS	569	56240	1813	Accounting-Request id=124
9	0.013992	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124
10	0.000000	10.48.39.134	10.48.39.212	RADIUS	62	1813	56240	Accounting-Response id=124, Duplicate Response

排除ISE故障

思科ISE的主要故障排除技術是**即時日誌**頁面，該頁面位於**操作 > RADIUS > 即時日誌**下。可以通過將客戶端的MAC地址放在「終端ID」欄位中對其進行過濾。 開啟完整的ISE報告可提供有關失敗原因的更多詳細資訊。確保客戶端訪問正確的ISE策略：


Cisco ISE
Operations · RADIUS
Evaluation Mode 89 Days
Live Logs
Live Sessions
Misconfigured Supplicants
0
Misconfigured Network Devices
0
RADIUS Drops
0
Client Stopped Responding
0
Repeat Counter
1
Refresh
Never
Show
Latest 20 records
Within
Last 3 hours
Refresh
Reset Repeat Counts
Export To
Filter
Time
Status
Details
Repea...
Identity
Endpoint ID
Endpoint...
Authentic...
Authoriz...
Authorization Pro...
IP Address
Identity
Endpoint ID
Endpoint Pr
Authenticati
Authorizatic
Authorization Profiles
IP Address
Aug 19, 2022 08:04:20.5...
1
08:BE:AC:27:8...
08:BE:AC:27:85:7E
Unknown
Policy_Set...
Policy_Set...
Authz_Profile_iPSK
fe80::e864:b6
Aug 19, 2022 08:04:13.3...
08:BE:AC:27:8...
08:BE:AC:27:85:7E
Unknown
Policy_Set...
Policy_Set...
Authz_Profile_iPSK

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）。