設定 Catalyst 9800 無線控制器的 MAC 驗證 SSID

目錄

簡介

本文件說明如何使用 Cisco Catalyst 9800 WLC 的 MAC 驗證安全性設定無線區域網路 (WLAN)。

必要條件

需求

思科建議您瞭解以下主題：

- MAC 地址
- Cisco Catalyst 9800 系列無線控制器
- 身分識別服務引擎 (ISE)

採用元件

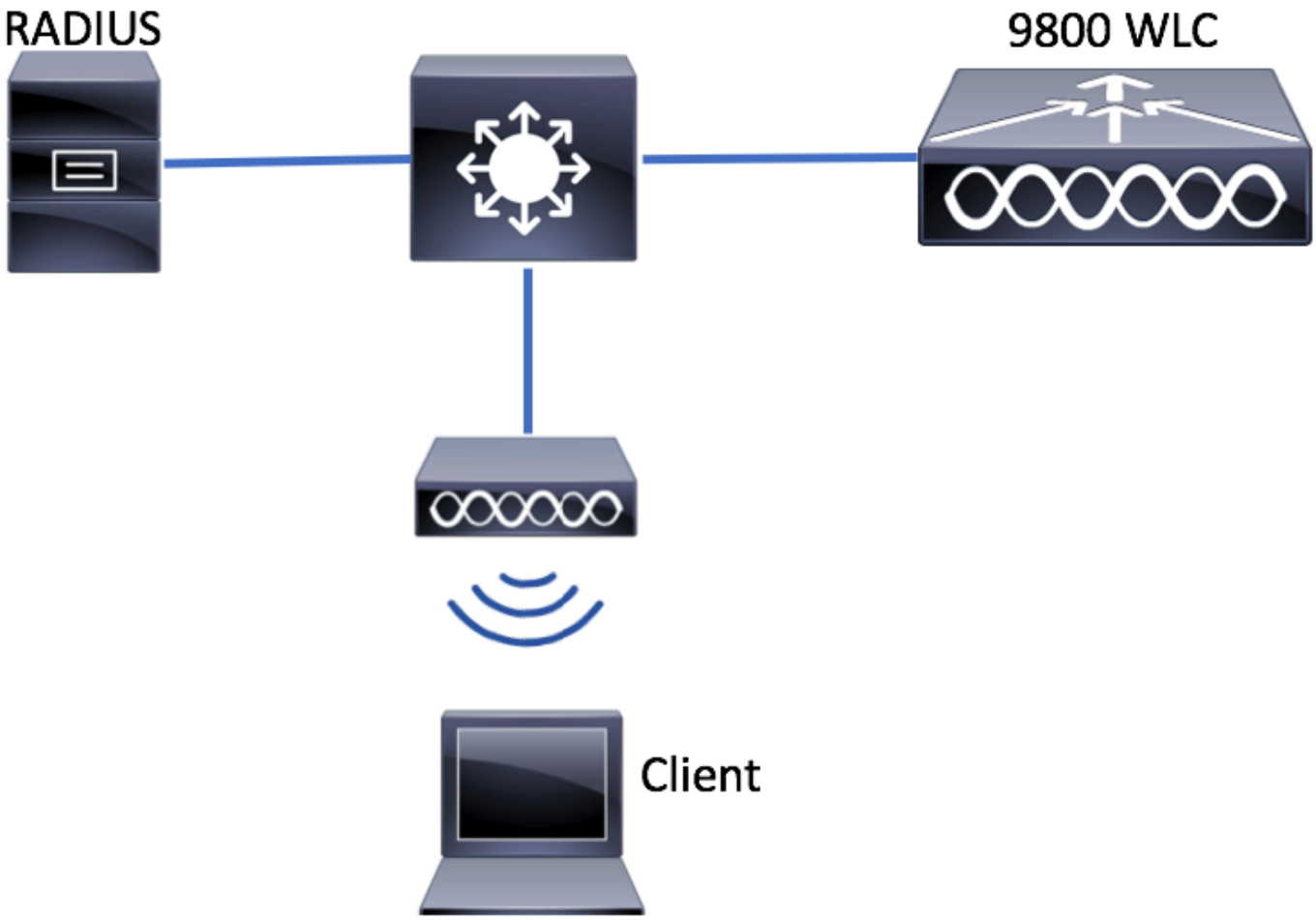
本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS® XE 直布羅陀 v16.12 版
- ISE v2.2

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



9800 WLC 的 AAA 組態

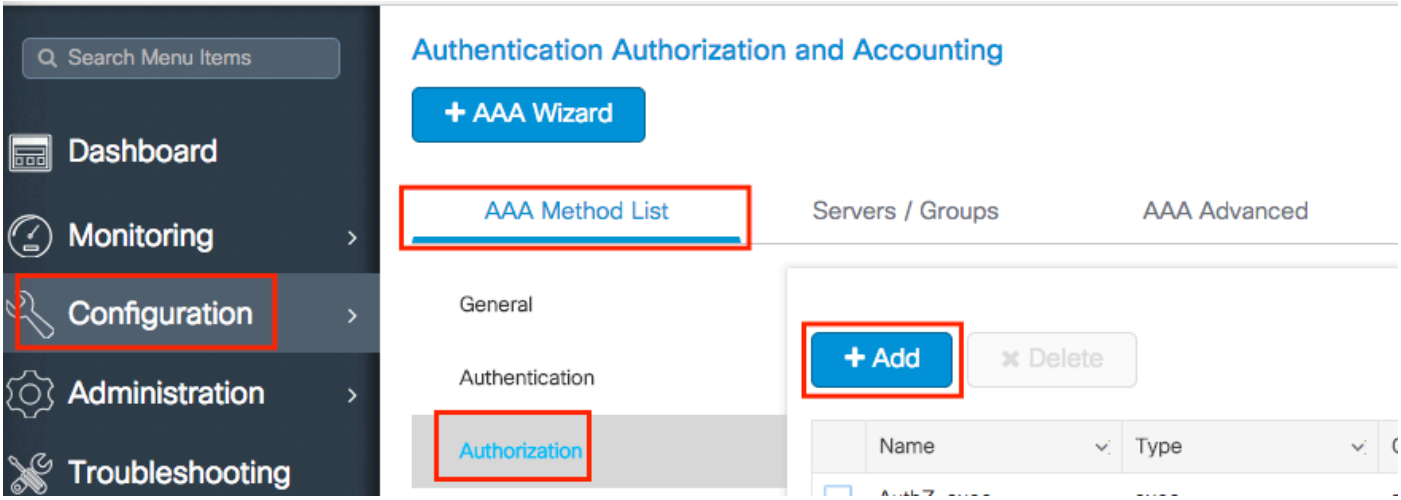
透過外部伺服器驗證用戶端

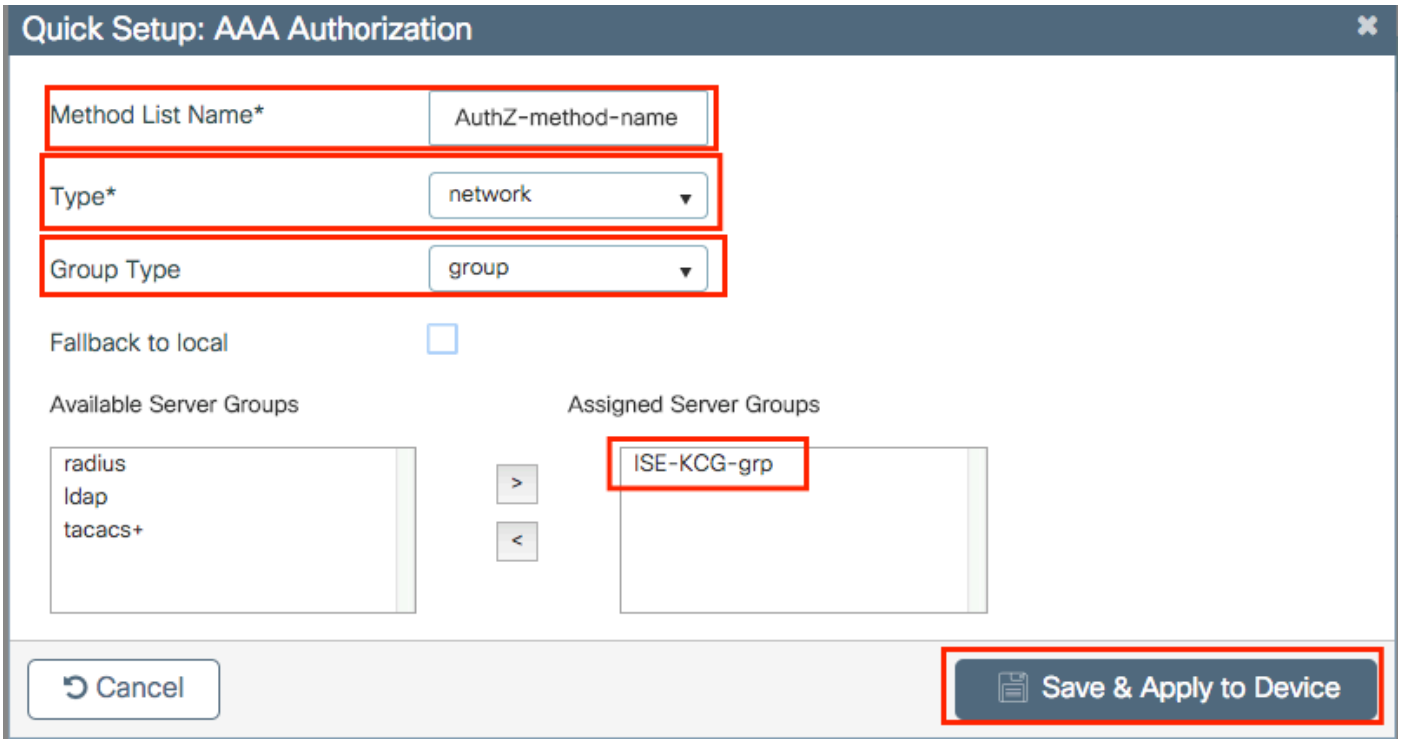
GUI：

閱讀9800系列WLC上的AAA配置部分的步驟1-3。

步驟 4.建立授權網路方法。

導航到Configuration > Security > AAA > AAA Method List > Authorization > + Add 並建立它。





CLI :

config t
aaa new-model

radius server <radius-server-name>
address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
timeout 300
retransmit 3
key <shared-key>
exit

aaa group server radius <radius-grp-name>
server name <radius-server-name>
exit

aaa server radius dynamic-author

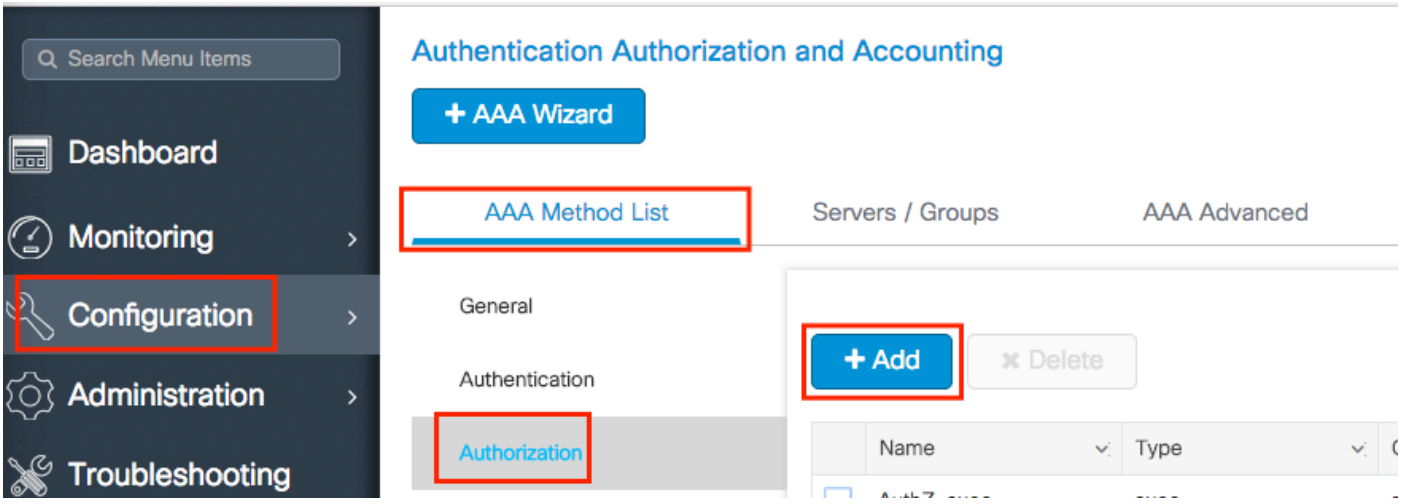
client <radius-server-ip> server-key <shared-key>

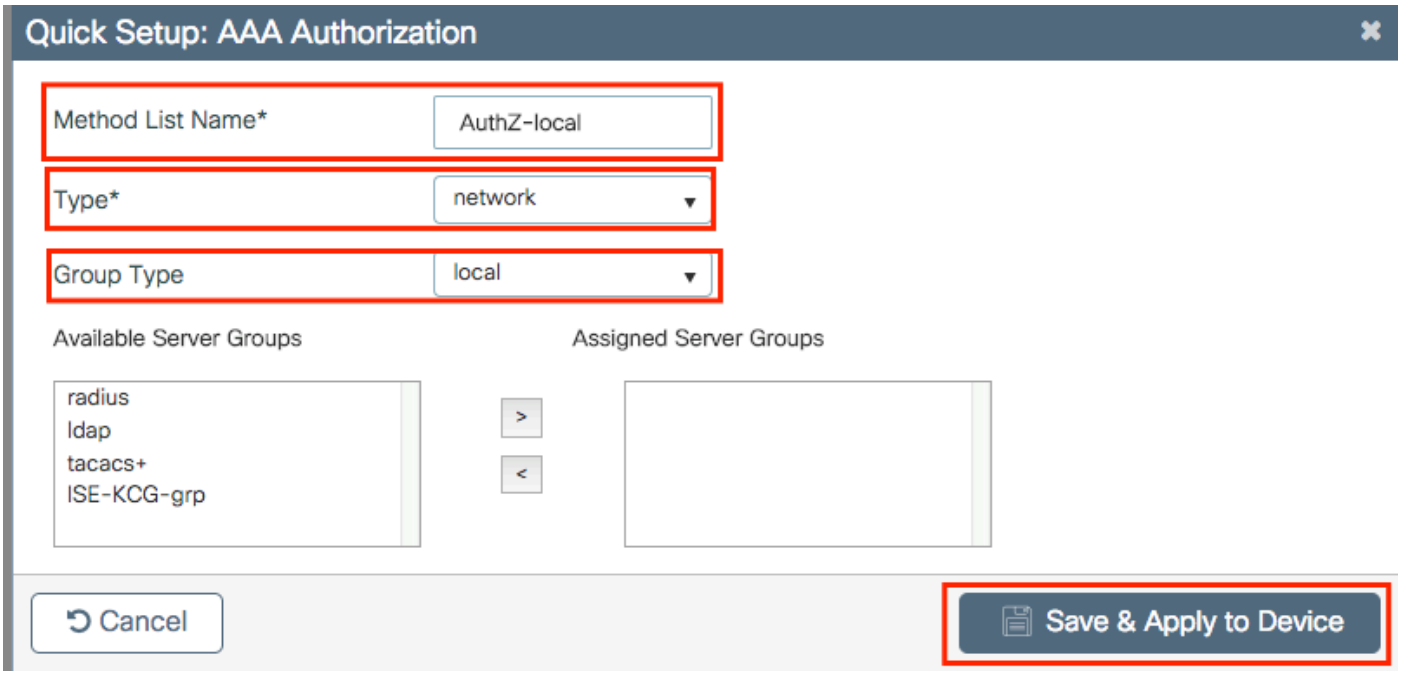
aaa authorization network <AuthZ-method-name> group <radius-grp-name>

在本機驗證用戶端

建立本機授權網路方法.

導航到Configuration > Security > AAA > AAA Method List > Authorization > + Add 並建立它。





CLI：

config t
aaa new-model

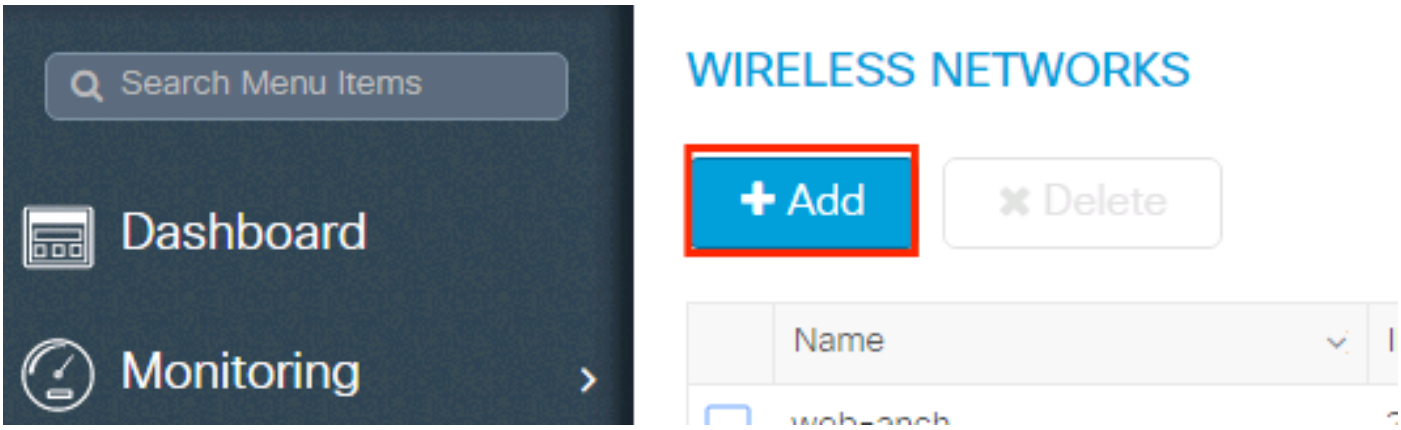
aaa authorization network AuthZ-local local

WLAN配置

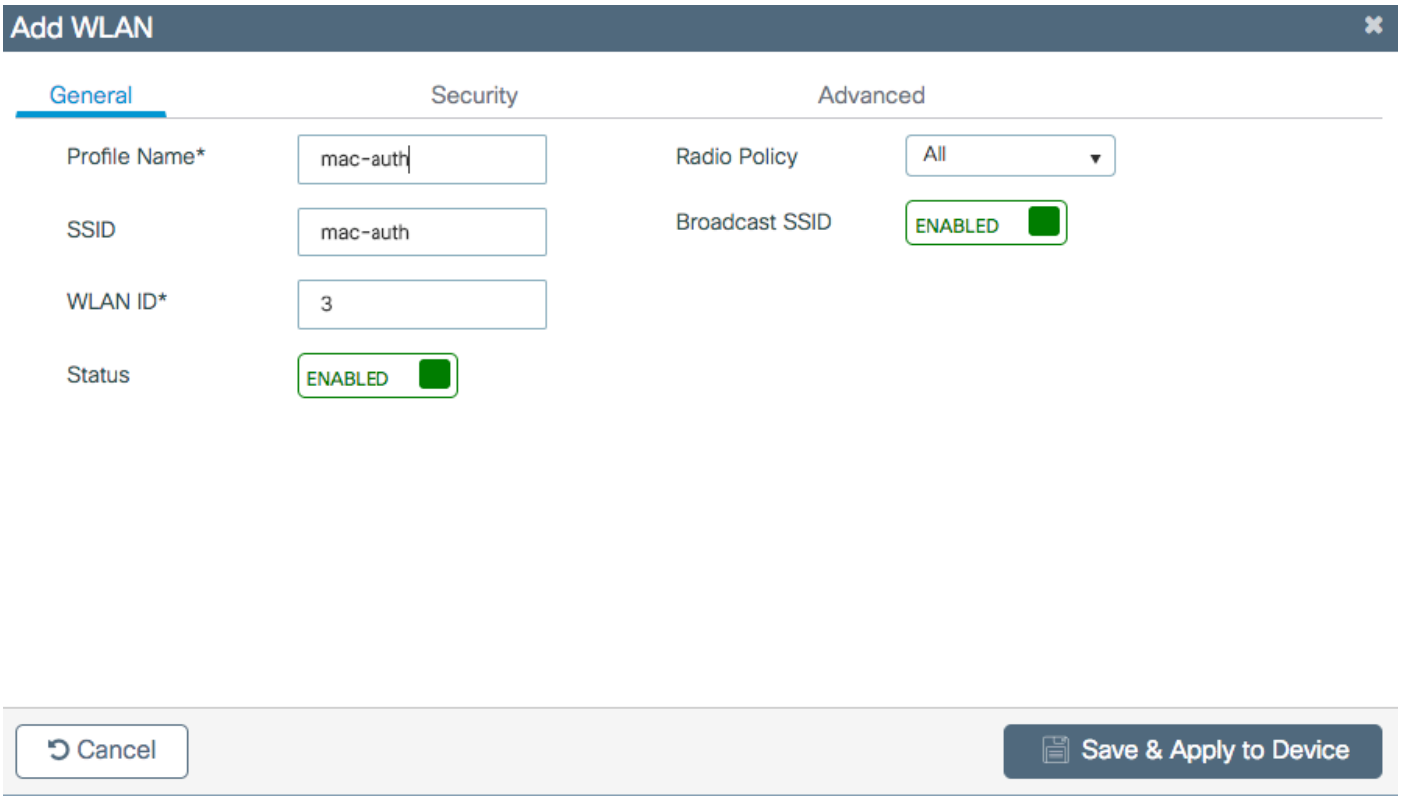
GUI：

步驟 1.建立WLAN。

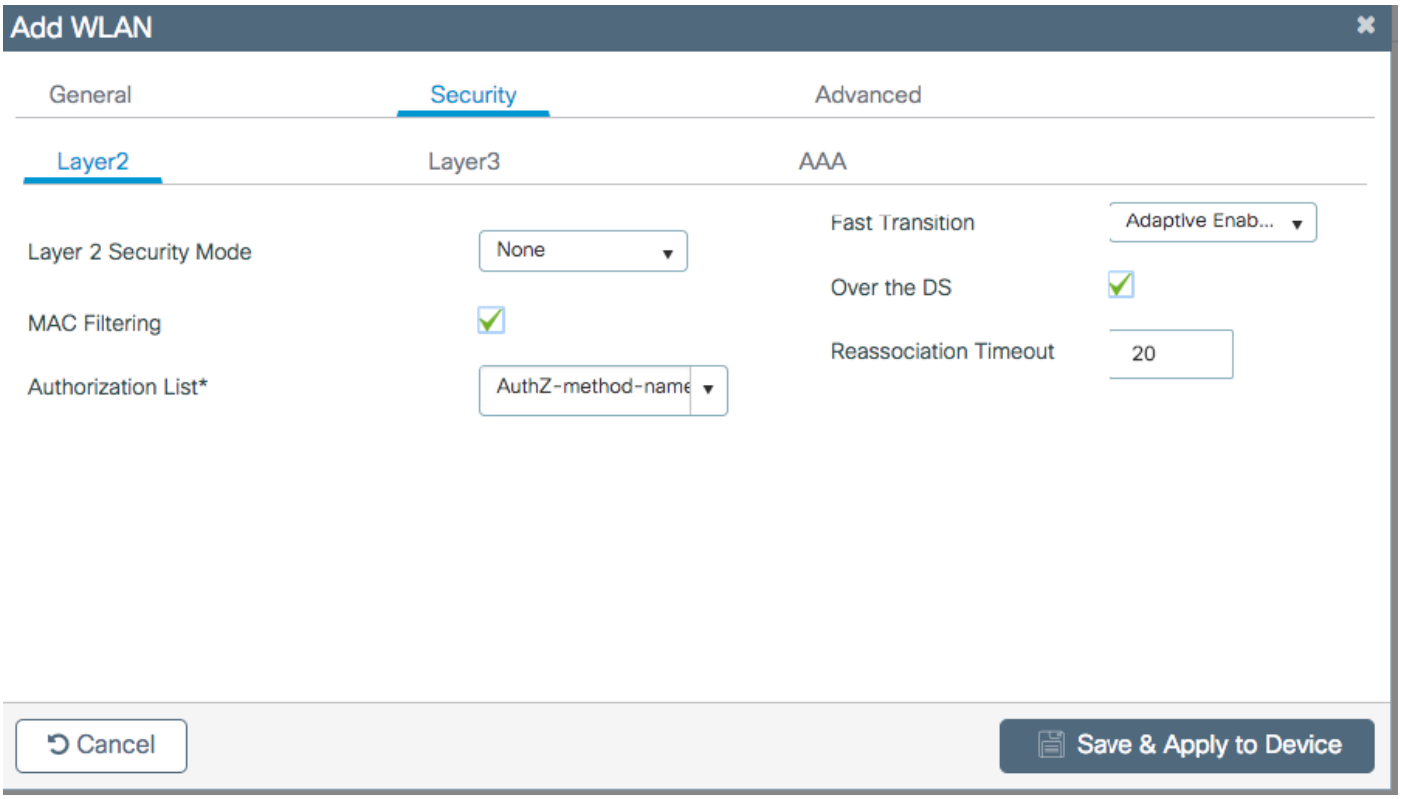
根據需要導航到Configuration > Wireless > WLANs > + Add 並配置網路。



步驟 2.輸入WLAN資訊。



步驟 3.導航到Security 頁籤，然後停用Layer 2 Security Mode 並啟用MAC Filtering。從Authorization List中，選擇上一步中建立的授權方法。然後按一下Save & Apply to Device。



CLI：

```
# config t # wlan <profile-name> <wlan-id> <ssid-name> # mac-filtering <authZ-network-method>
# no security wpa akm dot1x
# no security wpa wpa2 ciphers aes
# no shutdown
```

原則設定檔組態

您必須在策略配置檔案中啟用aaa-override，以確保每個SSID的Mac過濾可以正常運行。

9800 WLC 的原則設定檔組態

原則標籤組態

9800 WLC 的原則標籤

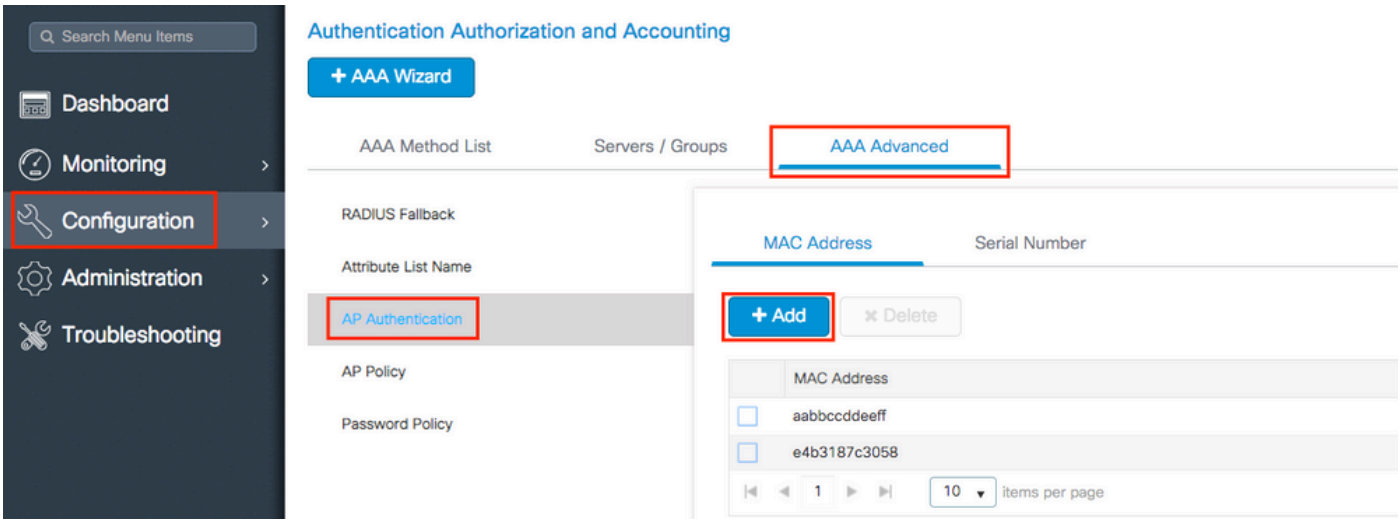
原則標籤指定

9800 WLC 的原則標籤指定

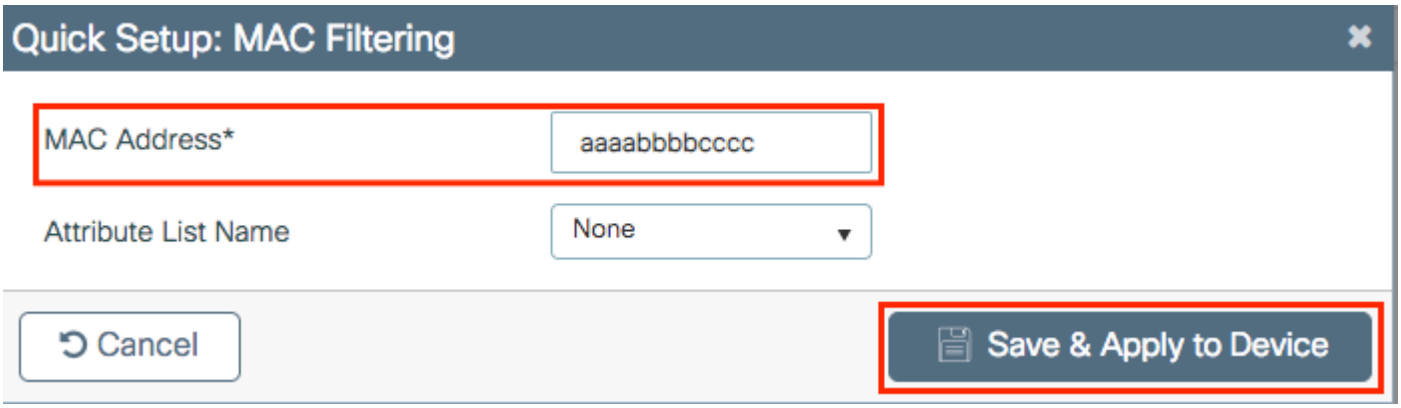
註冊允許的MAC地址。

在本機的 WLC 上註冊 MAC 位址，以進行本機驗證

導航到Configuration > Security > AAA > AAA Advanced > AP Authentication > + Add。



寫下不帶分隔符的所有小寫MAC地址，然後按一下Save & Apply to Device。



注意：在17.3之前的版本中，Web使用者介面(UI)會將您輸入的任何MAC格式變更為圖中所示的**無分隔**格式。在17.3及更高版本中，Web UI尊重您輸入的任何設計，因此，不輸入任何分隔符非常重要。增強型漏洞Cisco漏洞ID CSCvv43870可以跟蹤多種格式的MAC身份驗證支援。

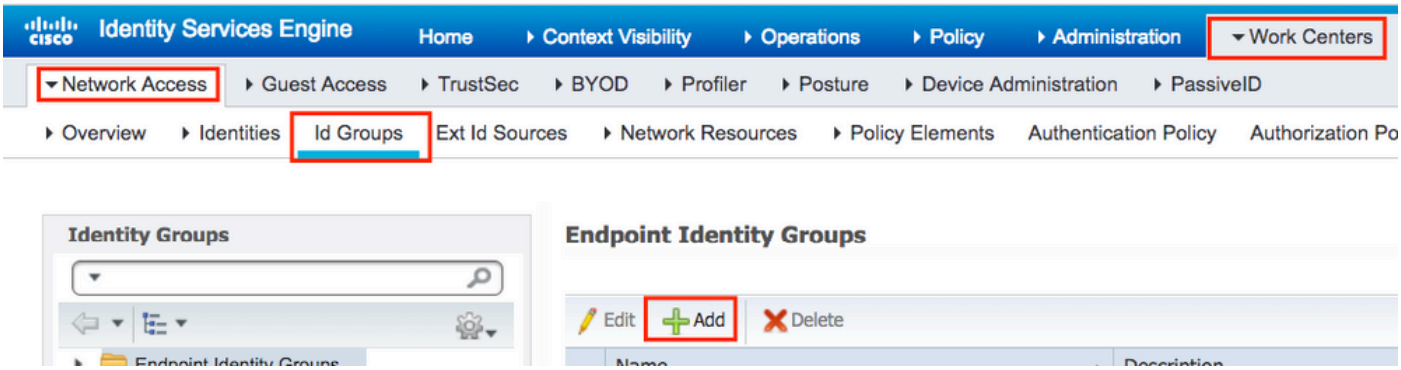
CLI：

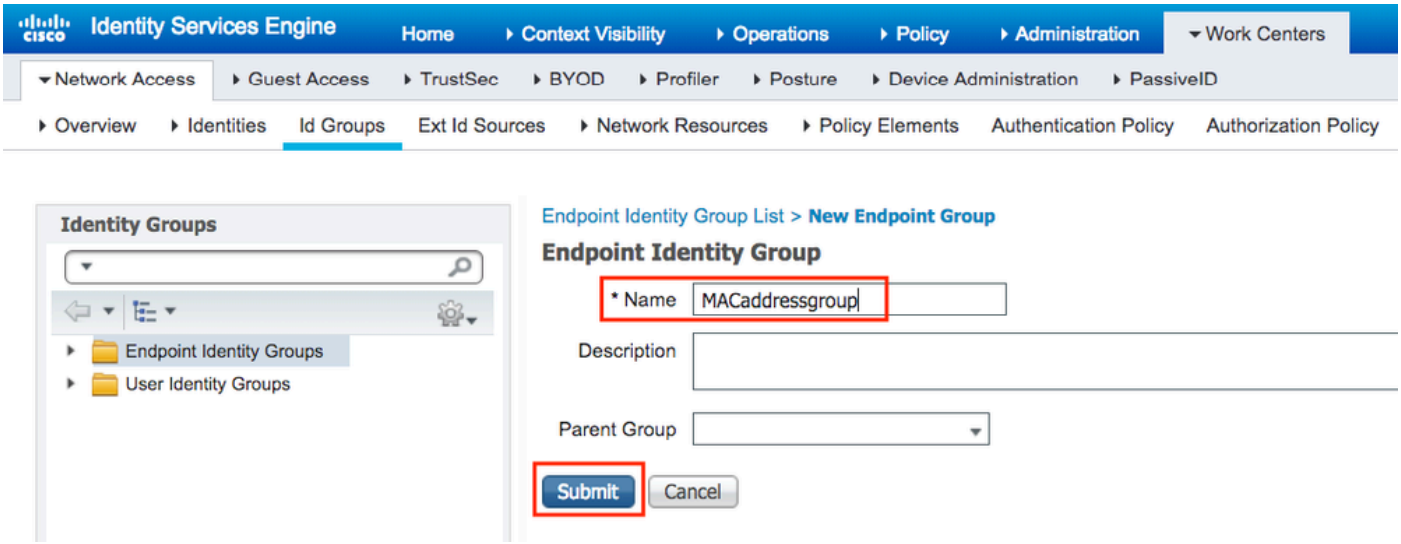
config t # username <aabbccddeeff> mac

輸入ISE終端資料庫上的MAC地址

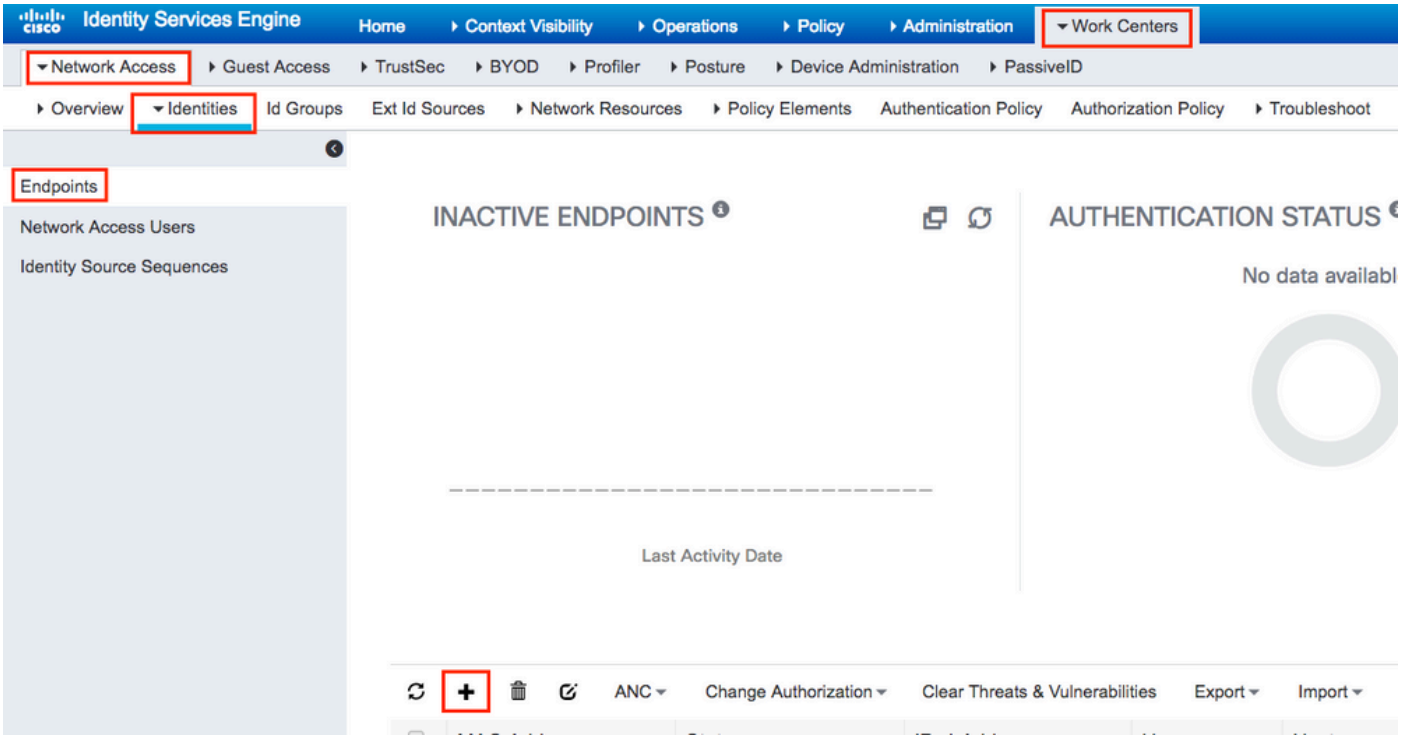
步驟 1.（選用）建立新的端點群組。

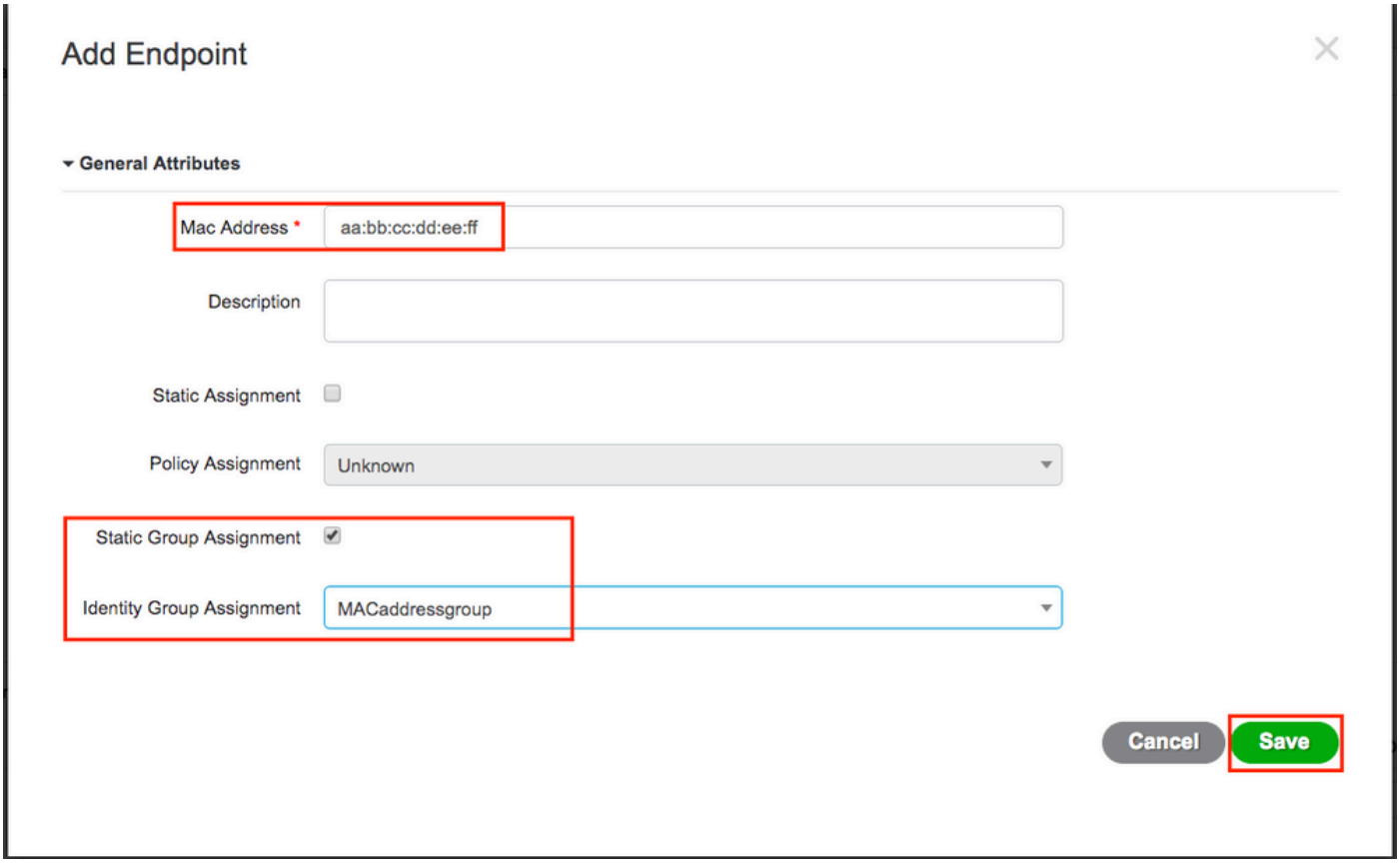
導航到Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add。





步驟 2.導航到Work Centers > Network Access > Identities > Endpoints > +Add。





ISE 組態

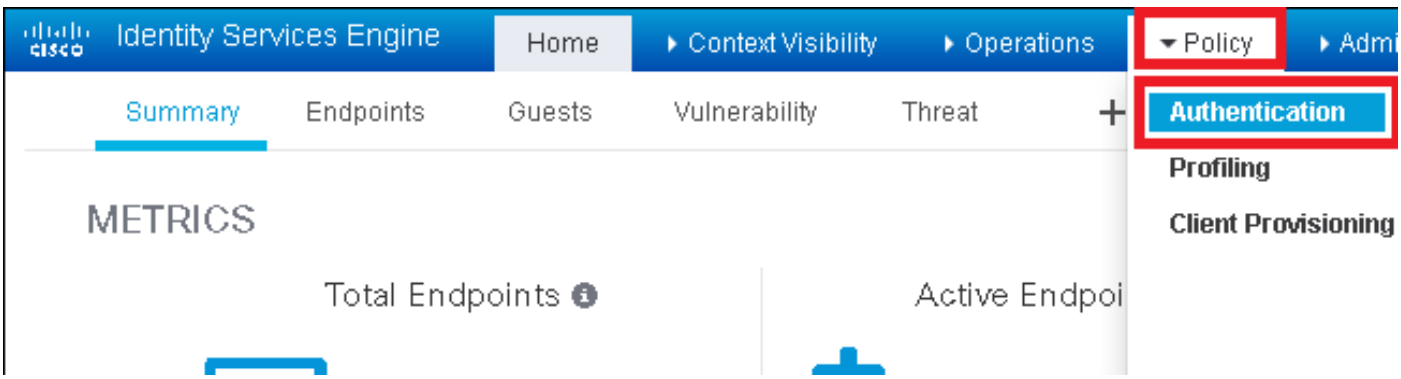
將 9800 WLC 新增至 ISE.

閱讀此連結中的說明：向ISE宣告WLC。

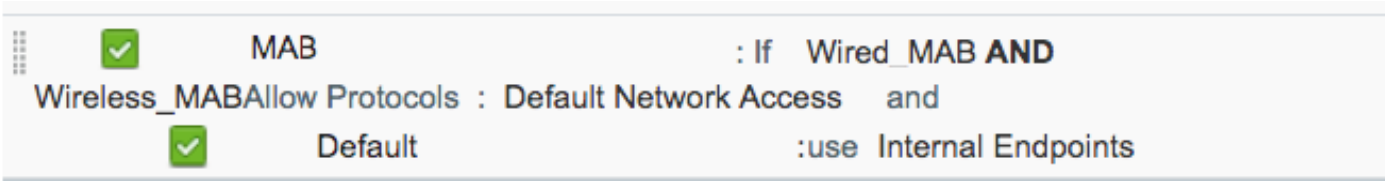
建立驗證規則

驗證規則可用於驗證使用者的認證是否正確（驗證使用者的真實身分正確無誤），並限制其所允許使用的驗證方法。

步驟 1.導覽至Policy > Authentication，如下圖所示。
確認ISE上存在預設MAB規則。



步驟 2.驗證MAB的預設身份驗證規則已存在：

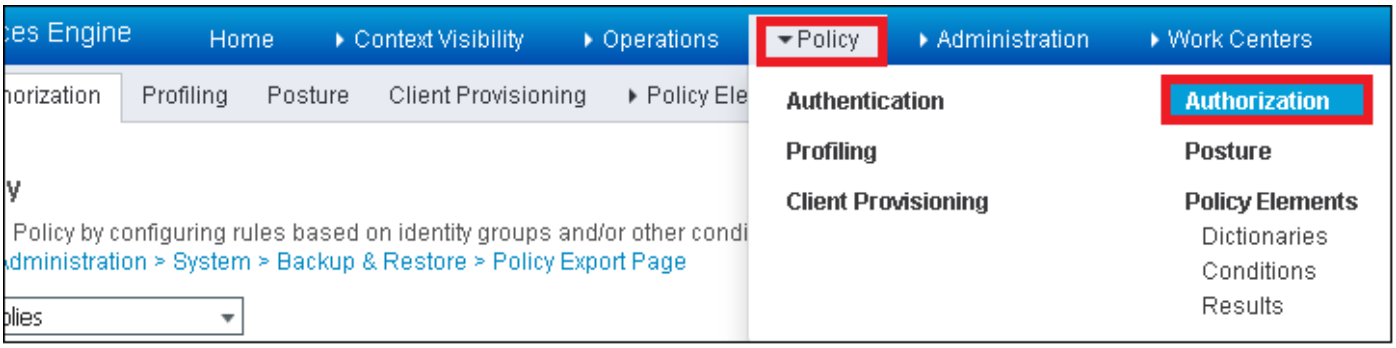


否則，請在按一下Insert new row above時增加新條目。

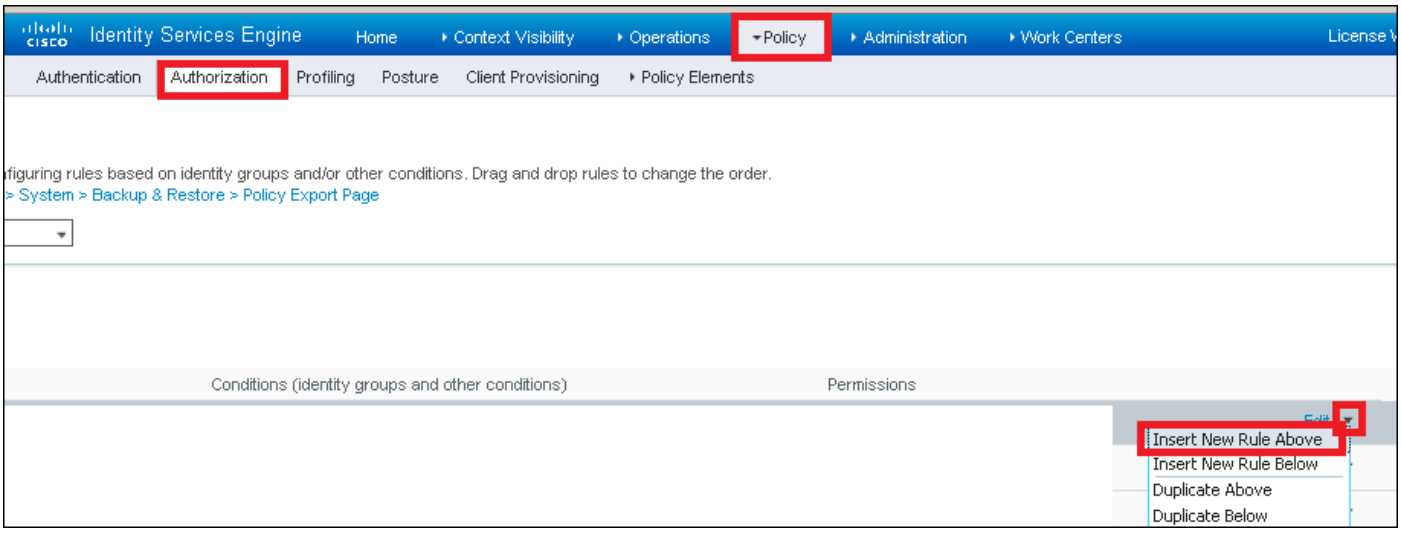
授權規則建立

授權規則為負責決定哪個權限（哪個授權設定檔）結果套用至用戶端的項目。

步驟 1.導覽至Policy > Authorization，如下圖所示。

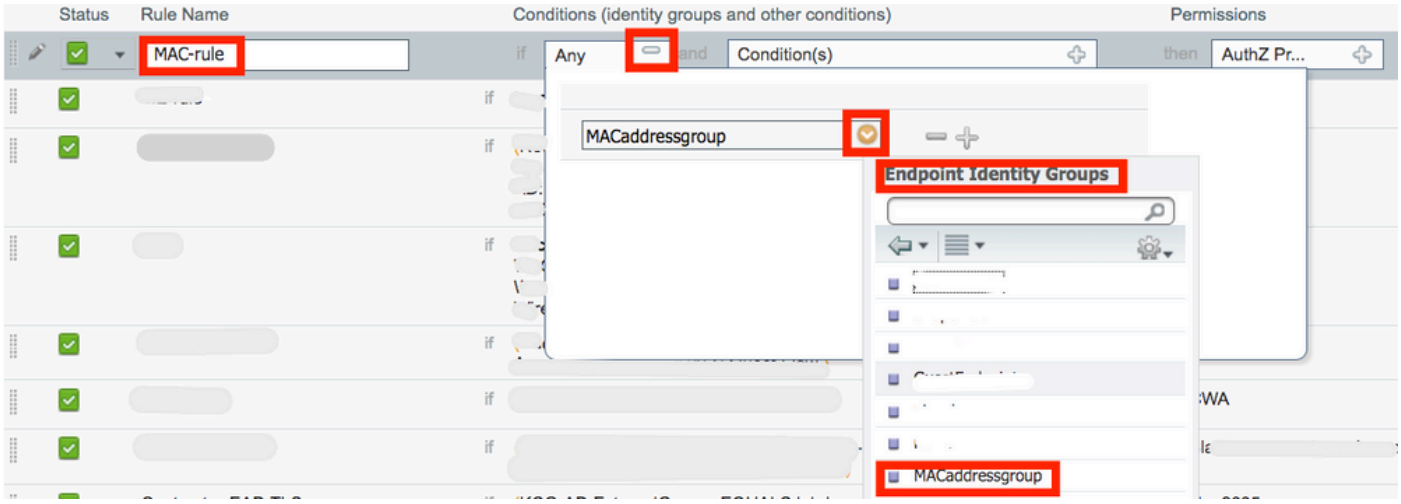


步驟 2.插入新規則，如下圖所示。

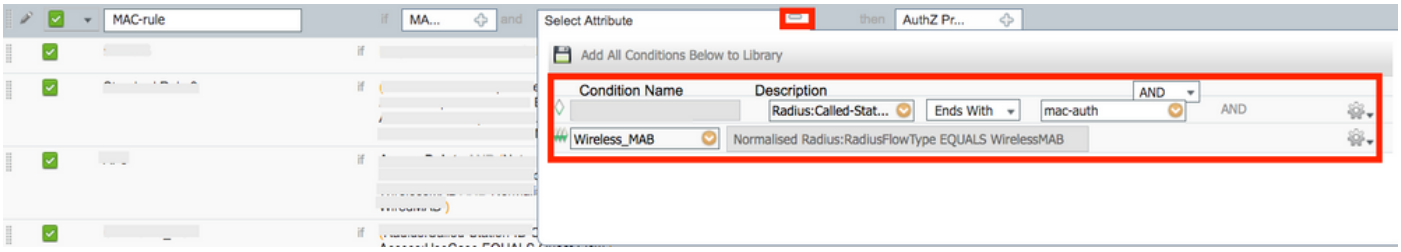


步驟 3.輸入值。

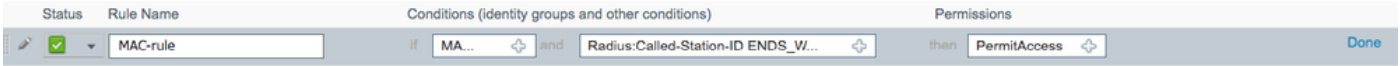
首先，選擇規則名稱以及儲存終端的身份組(**MACaddressgroup**)，如圖所示。



之後，選擇執行授權流程的其他條件以屬於此規則。在本例中，如果授權進程使用無線MAB，並且其被叫站ID（SSID的名稱）以mac-auth結尾，則授權進程會點選此規則，如圖所示。



最後，選擇分配給符合該規則的客戶端的授權配置檔案PermitAccess(在本例中)。按一下Done並儲存它。



驗證

使用以下命令可驗證當前配置：

show wlan { summary | id | name | all } # show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config
show ap tag summary
show ap name <AP-name> tag detail
show wlan { summary | id | name | all }
show wireless tag policy detailed <policy-tag-name>
show wireless profile policy detailed <policy-profile-name>

疑難排解

WLC 9800提供永遠開啟追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別的消息持續記錄，並且您可以在事件發生後檢視事件或故障條件的日誌。

注意：雖然這取決於生成的日誌量，但您可以返回幾小時到幾天。

為了檢視9800 WLC預設收集的跟蹤，您可以透過SSH/Telnet連線到9800 WLC並閱讀以下步驟（確保將會話記錄到文本檔案中）。

步驟 1.檢查控制器的當前時間，以便從發生問題的時間開始跟蹤日誌。

show clock

步驟 2.根據系統配置的指示，從控制器緩衝區或外部系統日誌收集系統日誌。這樣可以快速檢視系統的運行狀況和錯誤（如果有）。

show logging

步驟 3.驗證是否啟用了任何調試條件。

show debugging IOSXE Conditional Debug Configs: Conditional Debug Global State: Stop IOSXE Packet Tracing Configs: Packet Infra debugs: Ip Add

---

注意：如果發現列出任何條件，則意味著所有遇到啟用條件（MAC地址、IP地址等）的進程的跟蹤將記錄到調試級別。這將

增加日誌的量。因此，建議在不主動調試時清除所有條件。

步驟 4.如果測試中的MAC地址未列為步驟3中的條件，請收集特定MAC地址的「永遠線上」通知級別跟蹤。

show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>

您可顯示作業階段中的內容，或可將檔案複製到外部 TFTP 伺服器。

more bootflash:always-on-<FILENAME.txt>
or
copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>

條件式偵錯和無線電主動式追蹤

如果永遠線上的追蹤無法提供足夠資訊來判斷觸發調查中問題的原因，您可以啟用條件式偵錯並擷取「無線電作用中(RA)」追蹤，此追蹤會為與指定條件（此案例為使用者端mac位址）互動的所有處理作業提供偵錯層級追蹤。要啟用條件調試，請閱讀以下步驟。

步驟 5.確保未啟用調試條件。

clear platform condition all

步驟 6.為要監控的無線客戶端MAC地址啟用調試條件。

以下命令會開始監控提供的 MAC 位址 30 分鐘（1800 秒）。您可選擇將此時間增加至 2085978494 秒。

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}

注意：要同時監控多個客戶端，請對每個mac地址運行debug wireless mac<aaaa.bbbb.cccc>命令。

注意：您不會在終端會話中看到客戶端活動的輸出，因為所有內容都在內部進行緩衝以便以後檢視。

步驟 7.重現您要監控的問題或行為。

步驟 8.如果在預設或配置的監控時間之前重現問題，則停止調試。

no debug wireless mac <aaaa.bbbb.cccc>

一旦經過監控時間或停止偵錯無線，9800 WLC會產生具有以下名稱的本機檔案
： ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

步驟 9. 收集 MAC 位址活動的檔案。 您可以將ra trace .log 複製到外部伺服器，或直接在螢幕上顯示輸出。

檢查 RA 追蹤檔案的名稱:

dir bootflash: | inc ra_trace

將檔案複製到外部伺服器：

copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt

顯示內容：

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

步驟 10.如果根本原因仍不明顯，請收集內部日誌，這些日誌是調試級別日誌的更詳細檢視。您不需要再次調試客戶端，因為您只需進一步詳細檢視已收集並內部儲存的調試日誌。

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt
```

注意：此命令輸出返回所有進程的所有日誌記錄級別的跟蹤，而且輸出量非常大。請與Cisco TAC聯絡，幫助您分析這些跟蹤。

您可以將ra-internal-FILENAME.txt複製到外部伺服器，或直接在螢幕上顯示輸出。

將檔案複製到外部伺服器：

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

顯示內容：

```
# more bootflash:ra-internal-<FILENAME>.txt
```

步驟 11.移除偵錯條件。

```
# clear platform condition all
```

注意：請確保在故障排除會話結束後始終刪除調試條件。

相關資訊

- 思科技術支援與下載

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）。