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

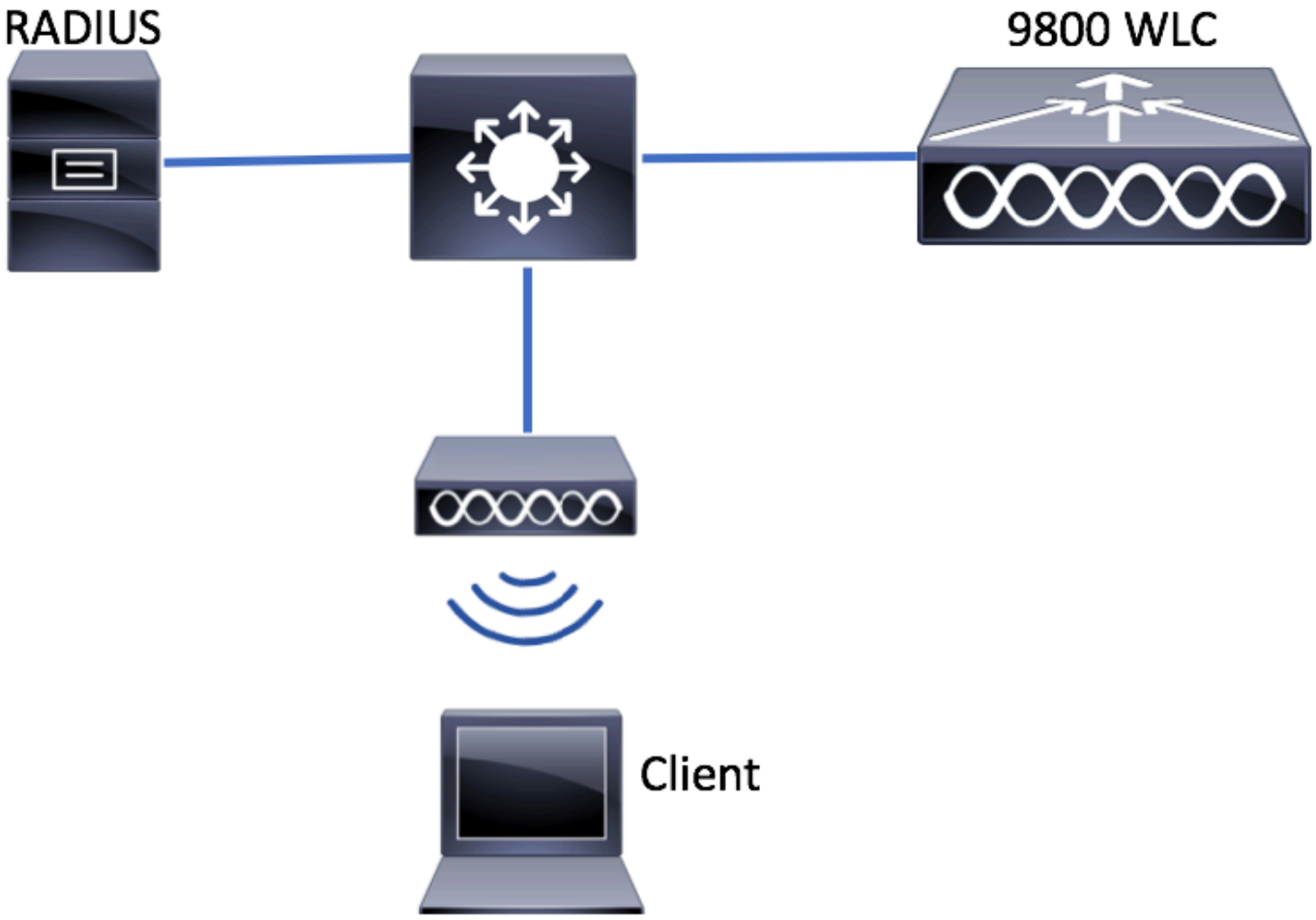
本文中的資訊係根據以下軟體和硬體版本：

- 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

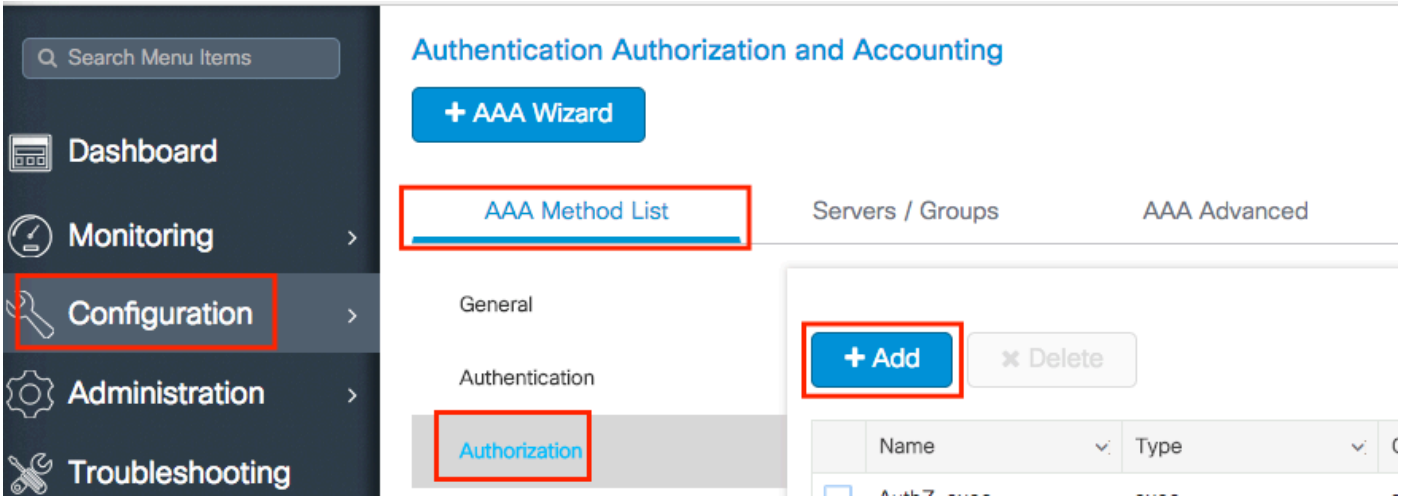
GUI:

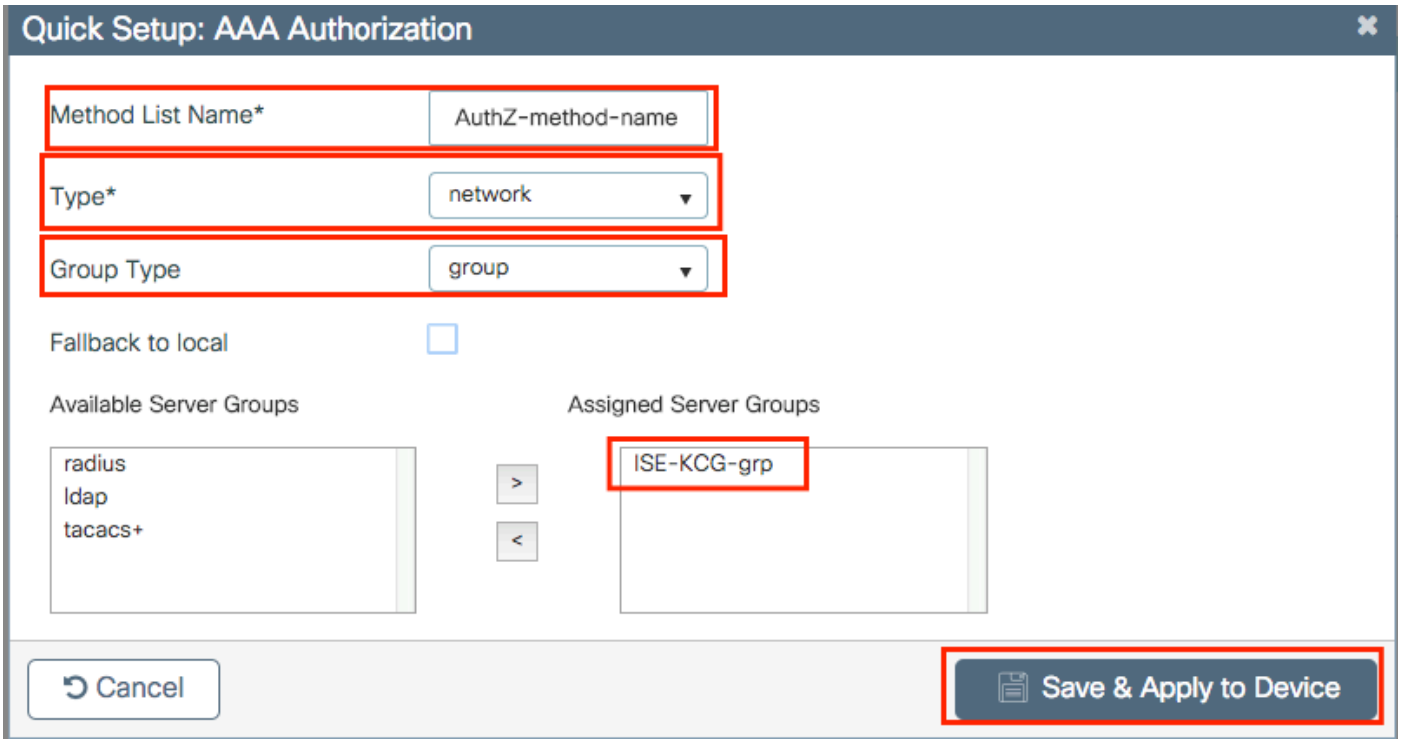
從此連結閱讀「9800 WLC上的AAA配置」一節的步驟1-3:

[9800 系列 WLC 的 AAA 組態]

步驟 4.建立授權網路方法。

導覽至Configuration > Security > AAA > AAA Method List > Authorization > + Add並建立。





CLI:

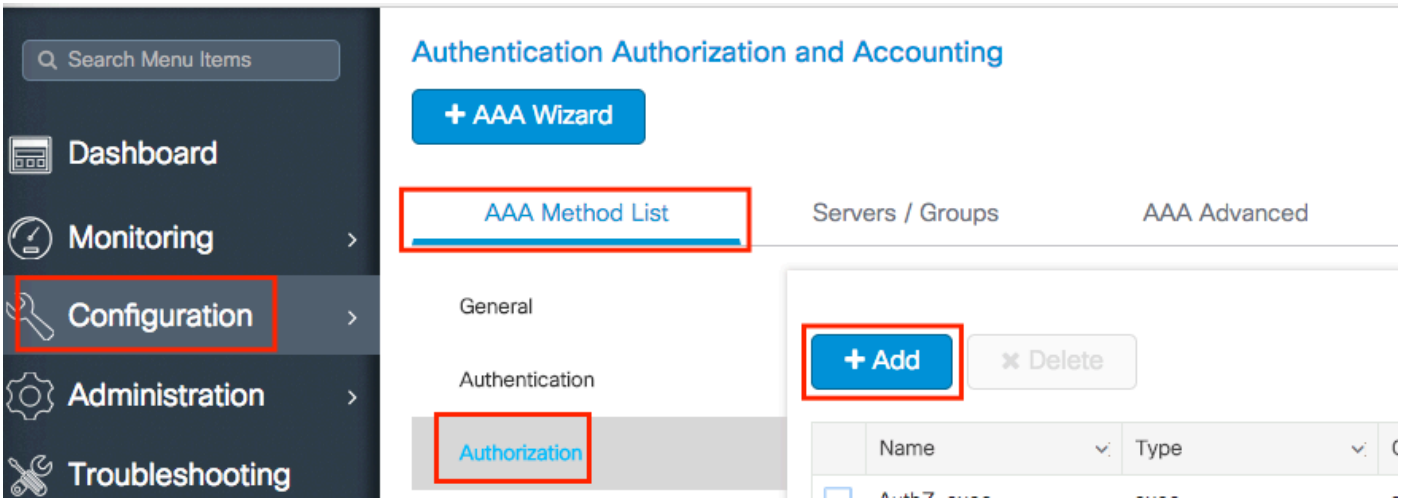
```
# config t
# aaa new-model

# 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
```

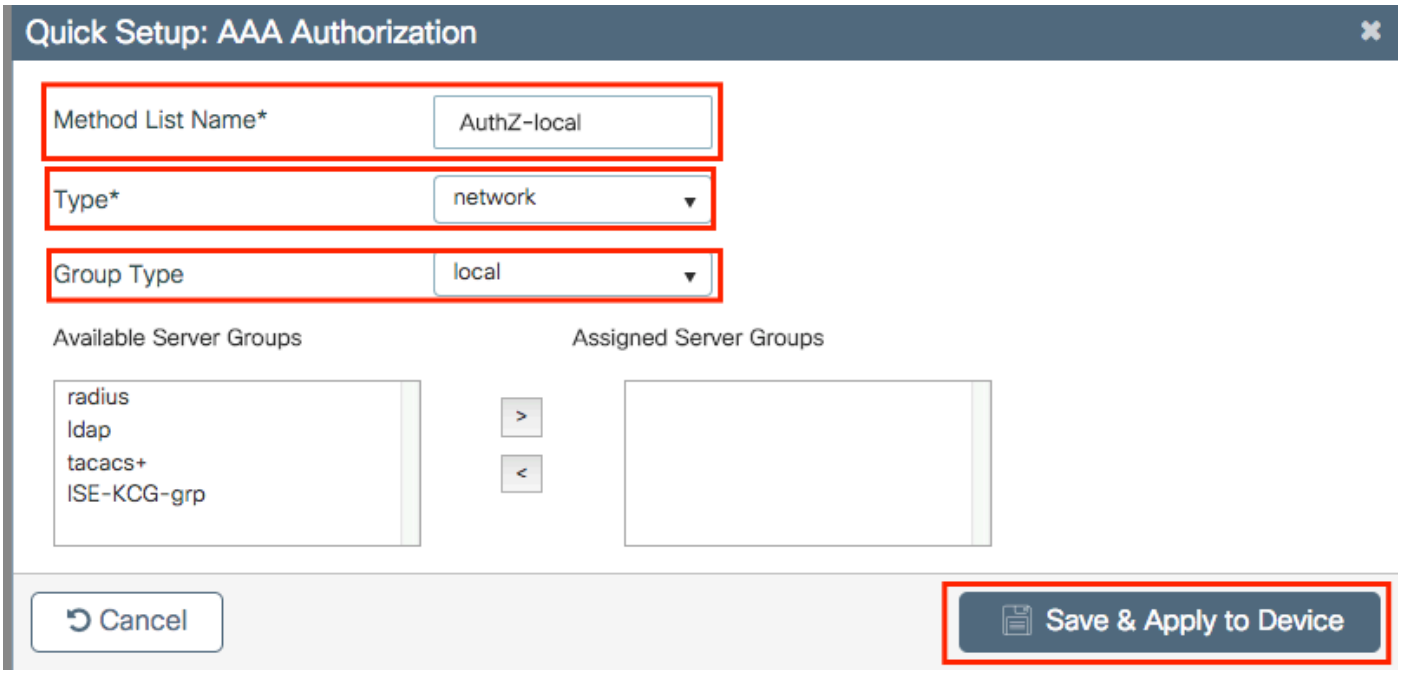
```
# client <radius-server-ip> server-key <shared-key>

# 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.

導覽至Configuration > Security > AAA > AAA Method List > Authorization > + Add並建立。





CLI:

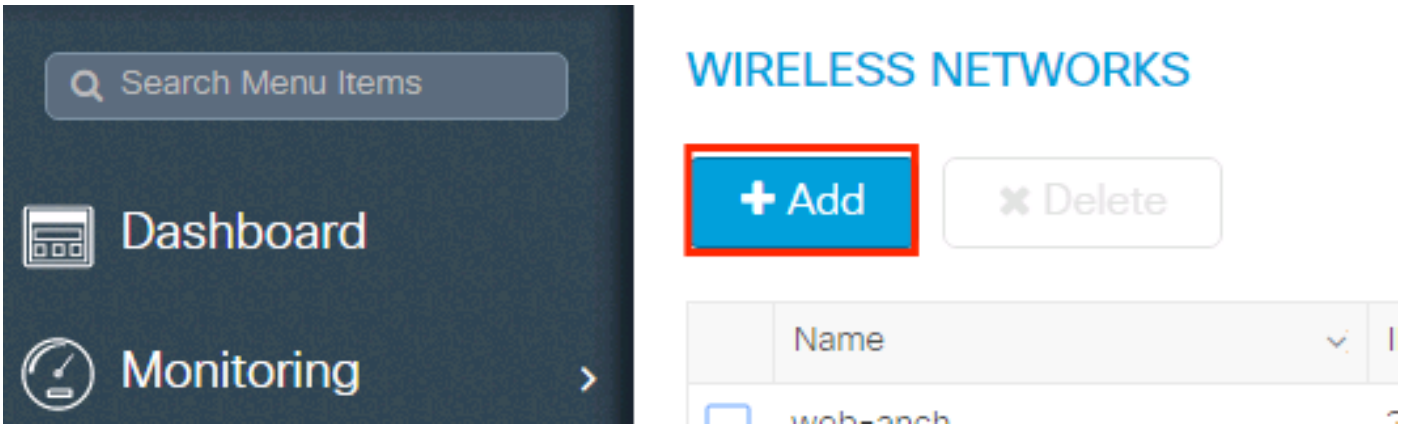
```
# config t
# aaa new-model
# aaa authorization network AuthZ-local local
```

WLAN配置

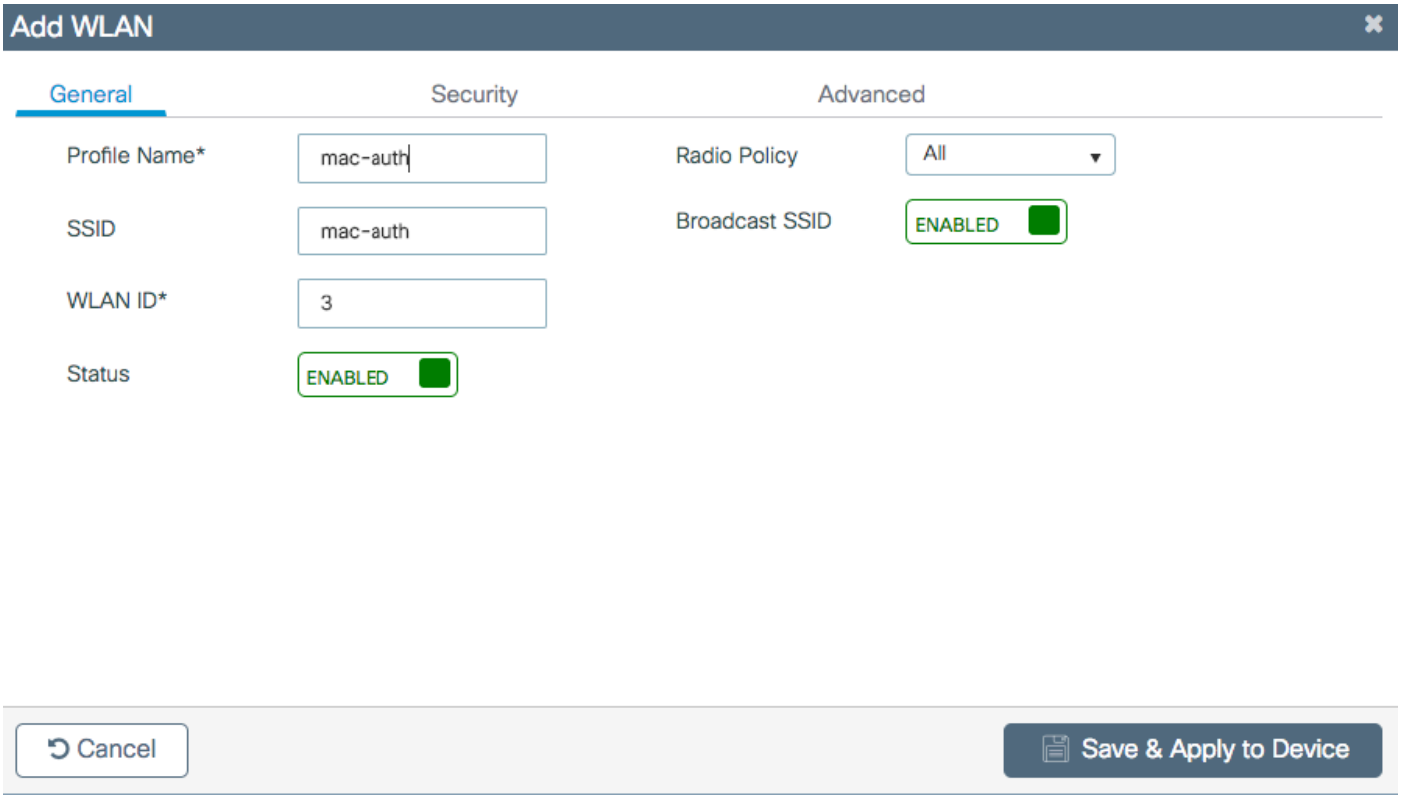
GUI:

步驟 1.建立WLAN。

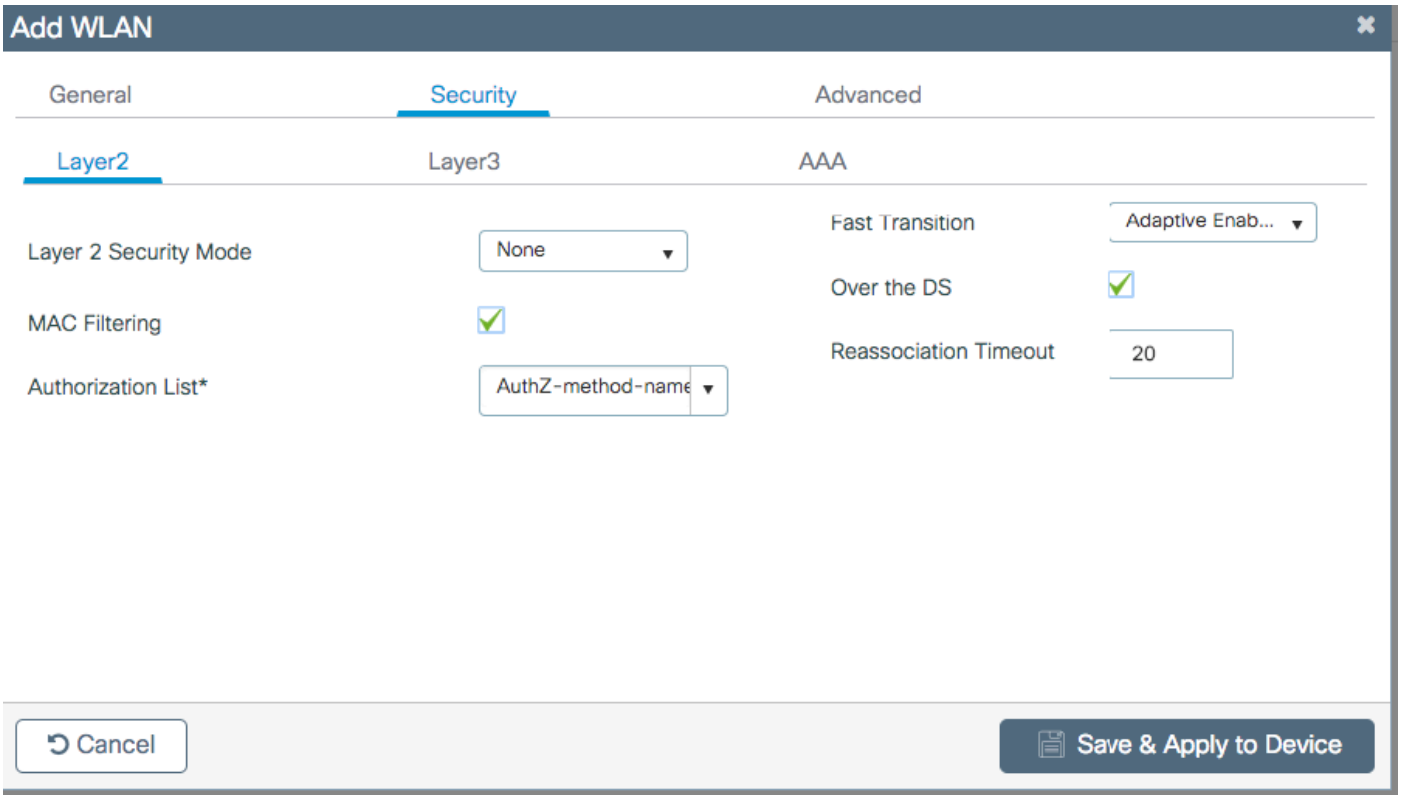
根據需Configuration > Wireless > WLANs > + Add要導航到並配置網路。



步驟 2.輸入WLAN資訊。



步驟 3.導航到選Security項卡並禁用Layer 2 Security Mode和啟用MAC Filtering。 從Authorization List ，選擇在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

必須在策略配置檔案中啟用aaa-override，以確保每個SSID的mac過濾工作正常。

9800 WLC 的原則設定檔組態

原則標籤組態

9800 WLC 的原則標籤

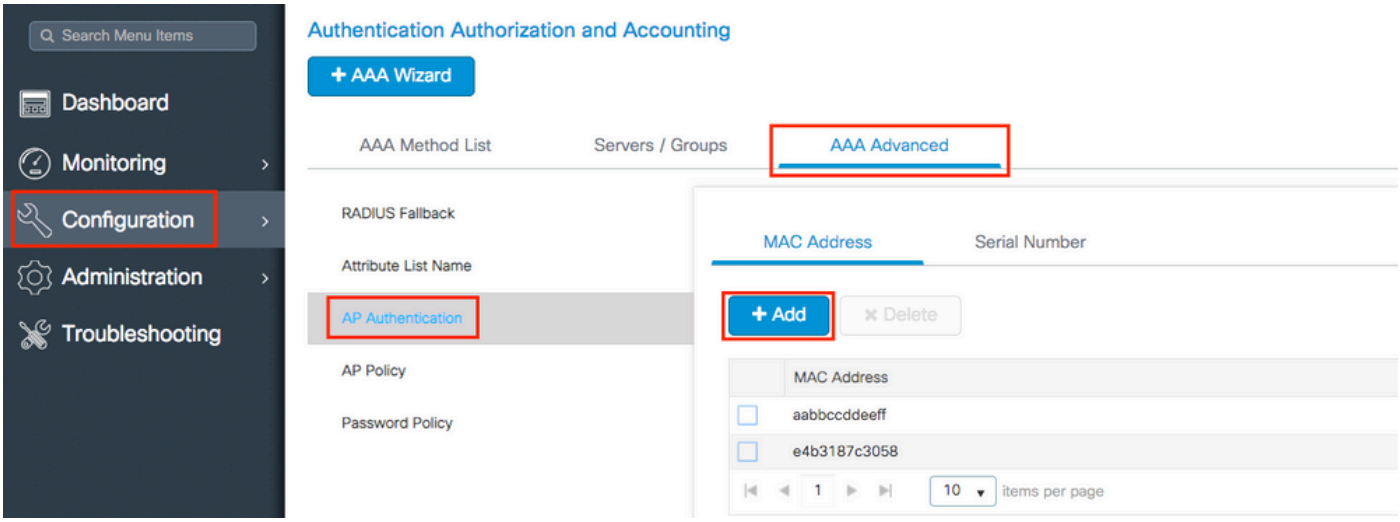
原則標籤指定

[9800 WLC 的原則標籤指定]

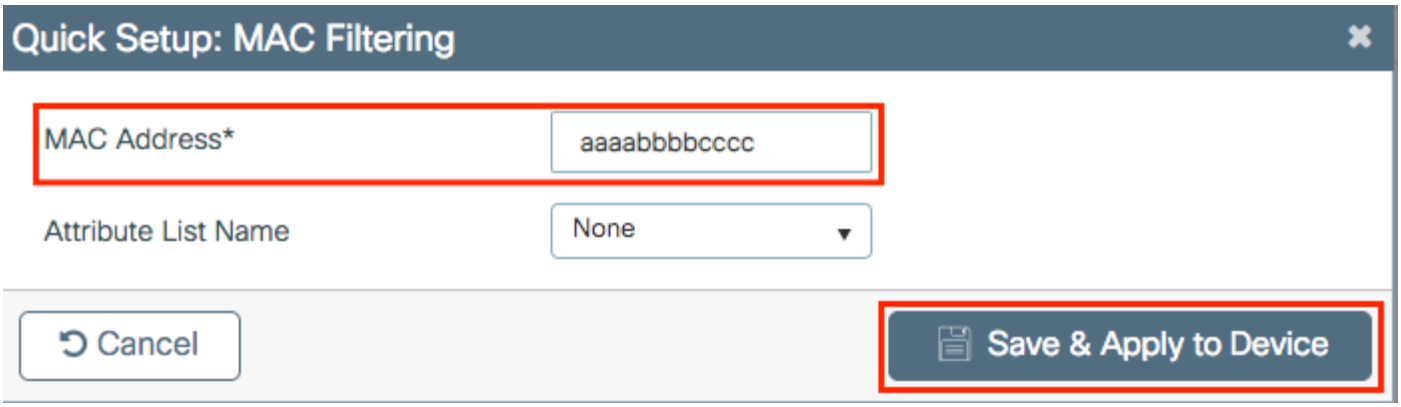
註冊允許的MAC地址。

在本機的 WLC 上註冊 MAC 位址，以進行本機驗證

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



以所有小寫寫出mac地址，不帶分隔符，然後按一下Save & Apply to Device。



註：在17.3以前的版本中，Web UI將您鍵入的任何MAC格式更改為圖中所示的「無分隔符」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，不輸入任何分隔符至關重要。增強功能錯誤Cisco錯誤ID CSCvv43870會追蹤是否支援幾種格式進行MAC驗證。

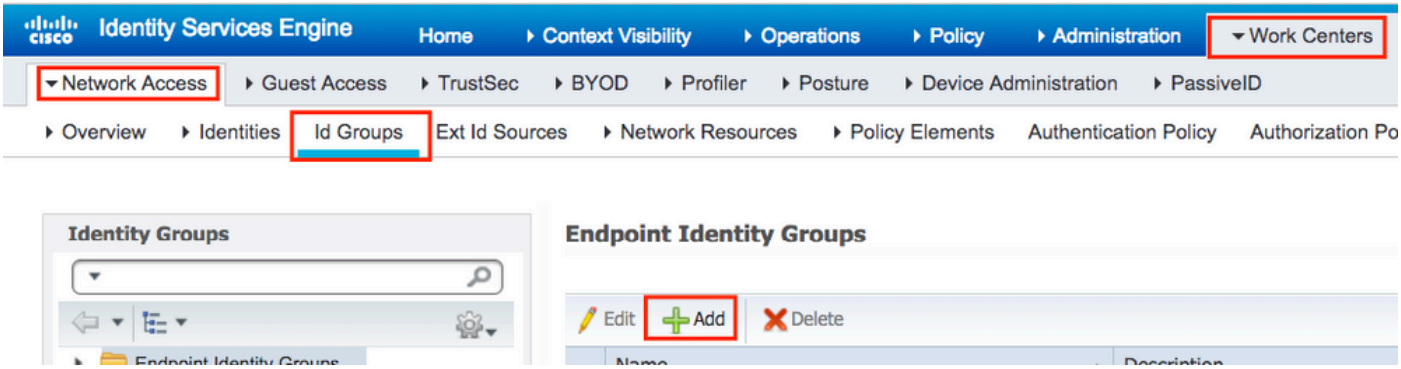
CLI:

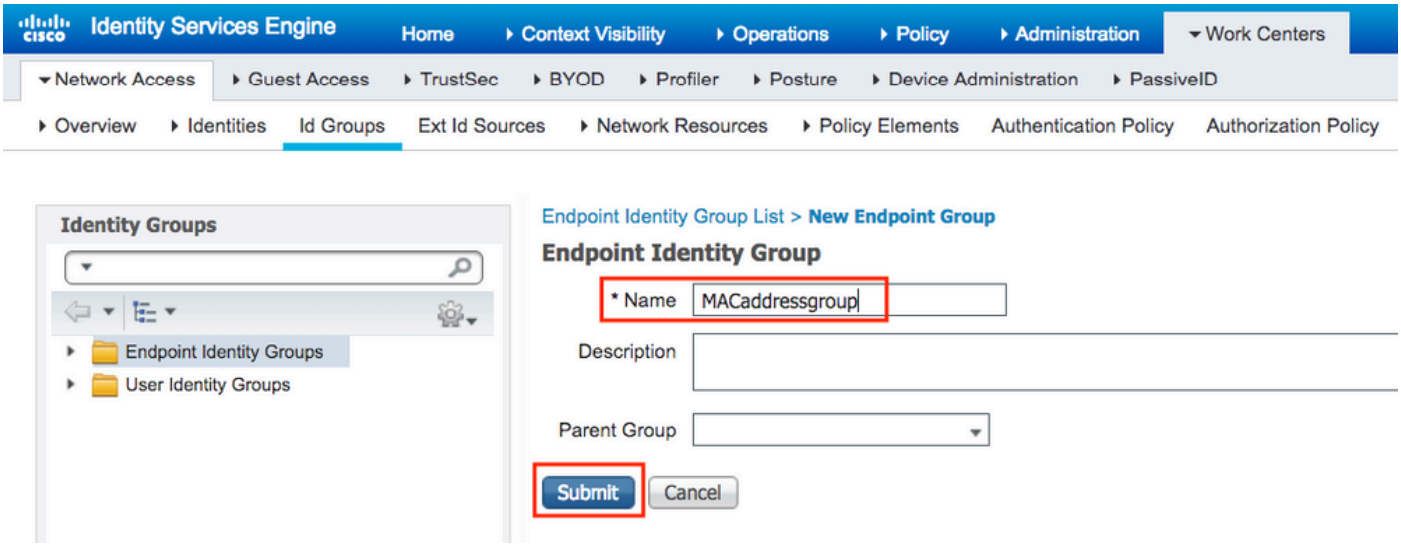
```
# config t
# username <aabbccddeeff> mac
```

在ISE終端資料庫上輸入MAC地址

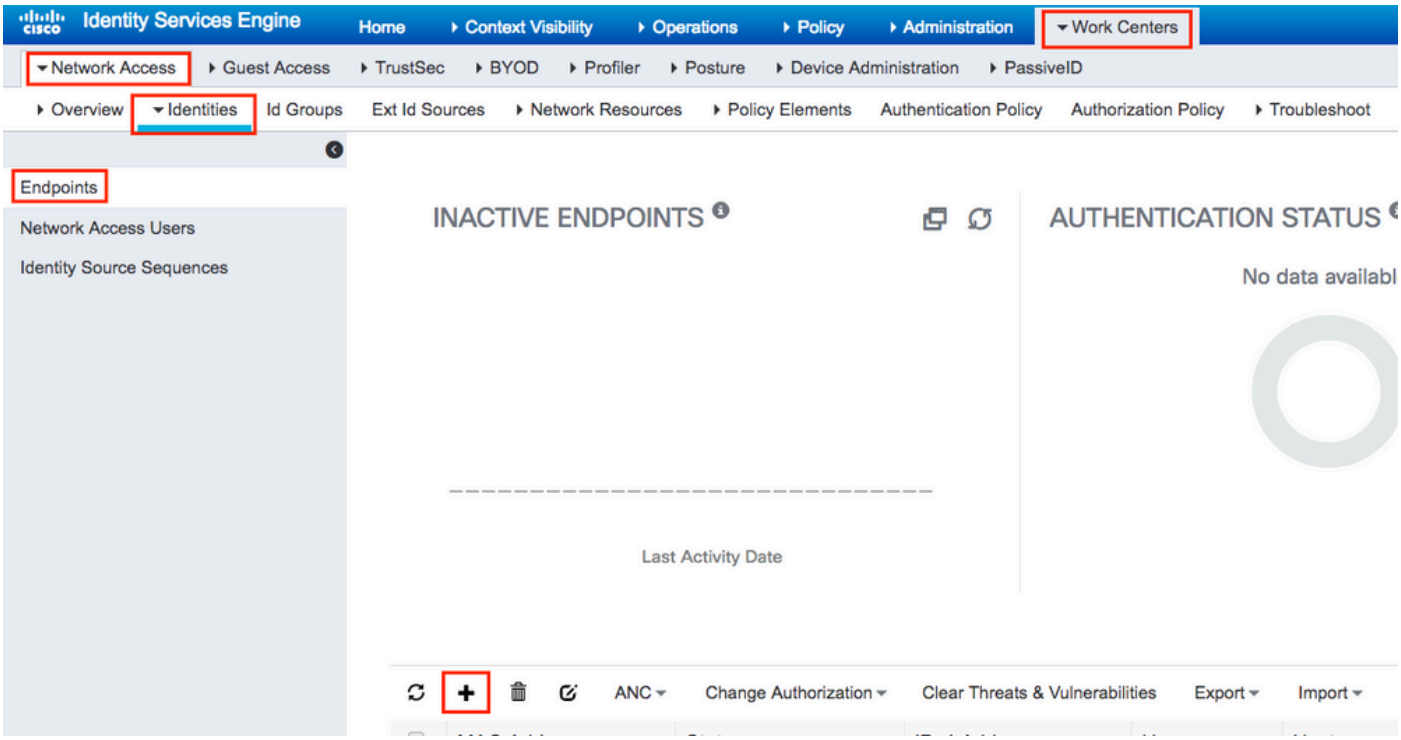
步驟 1.（選用）建立新的端點群組。

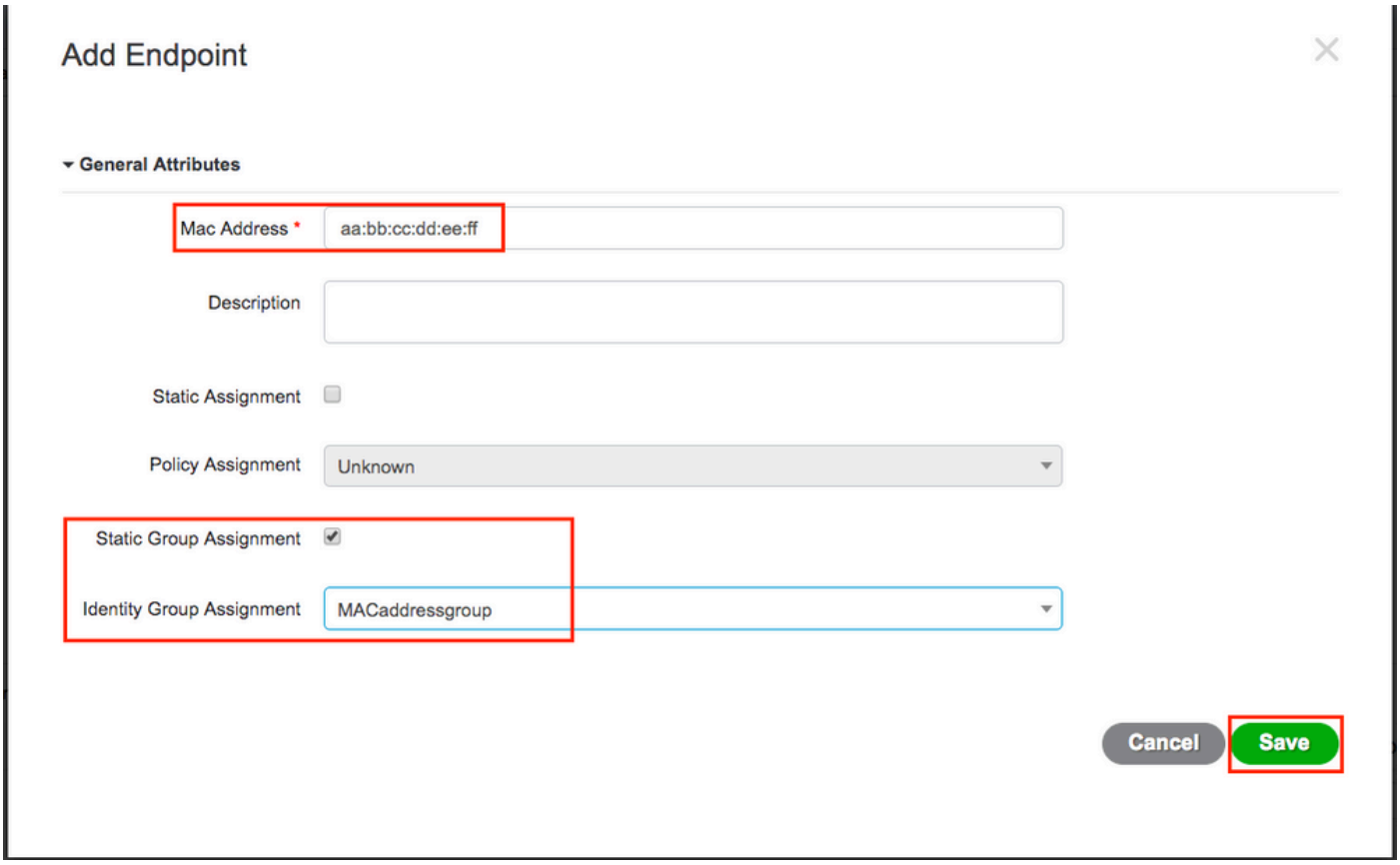
導航至Work Centers > Network Access > Id Groups > Endpoint Identity Groups > + Add。





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





ISE 組態

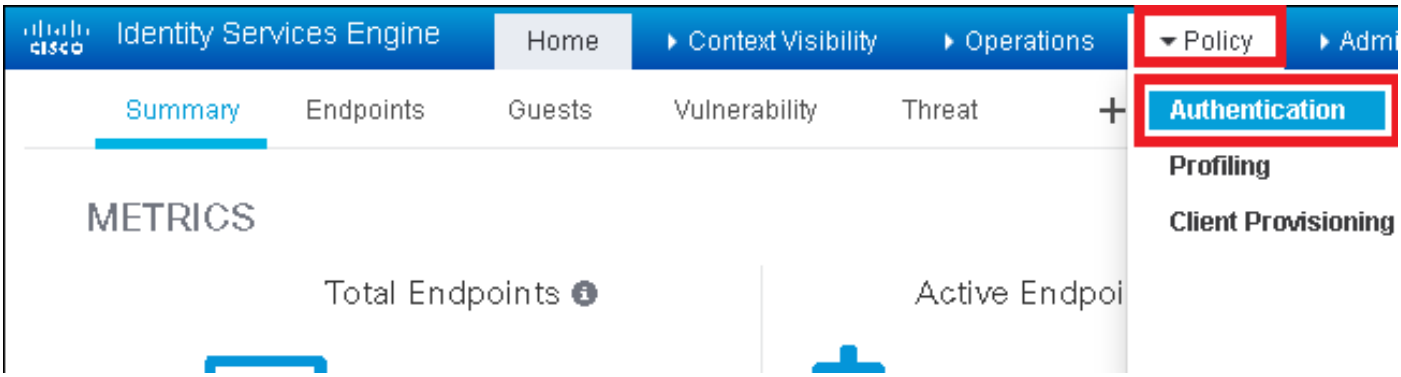
將 9800 WLC 新增至 ISE.

閱讀此連結中的說明：向ISE宣告WLC。

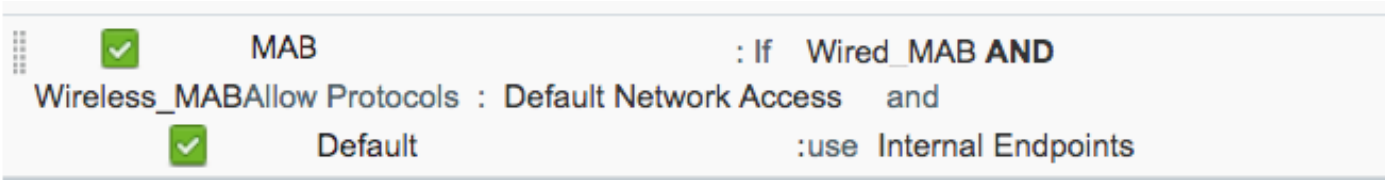
建立驗證規則

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：

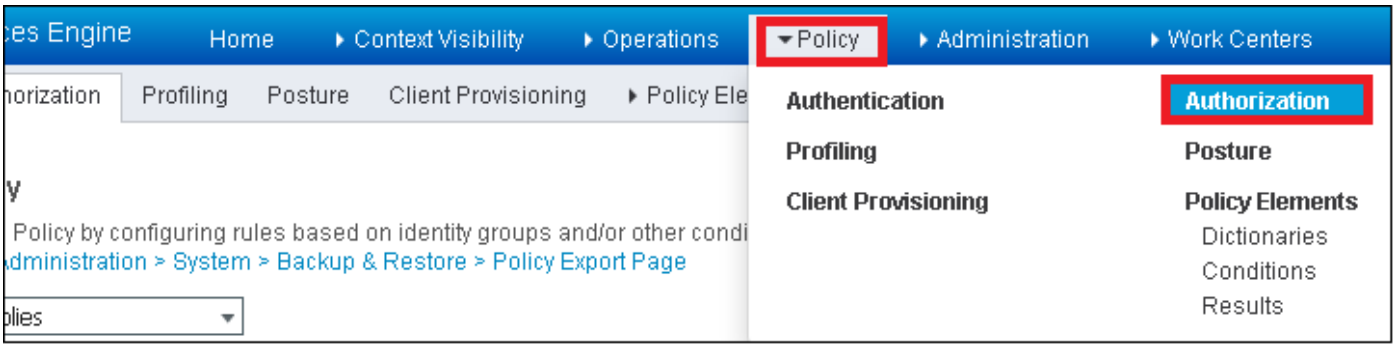


如果沒有，則可以在按一下時新增新的Insert new row above。

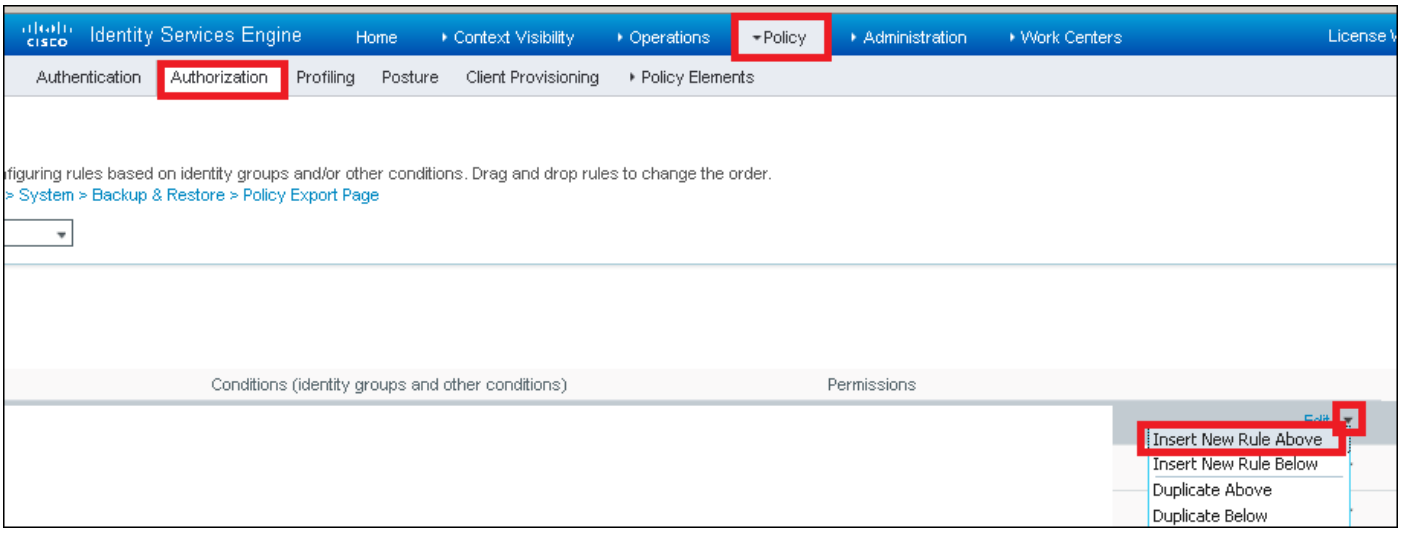
授權規則建立

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。

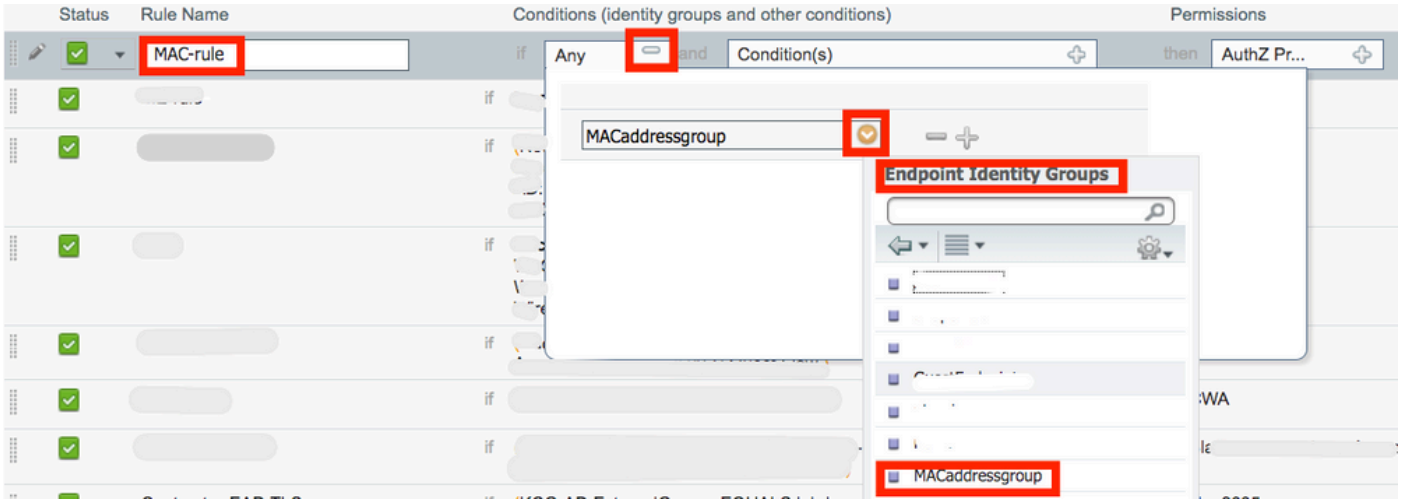


步驟 2.插入新規則，如下圖所示。

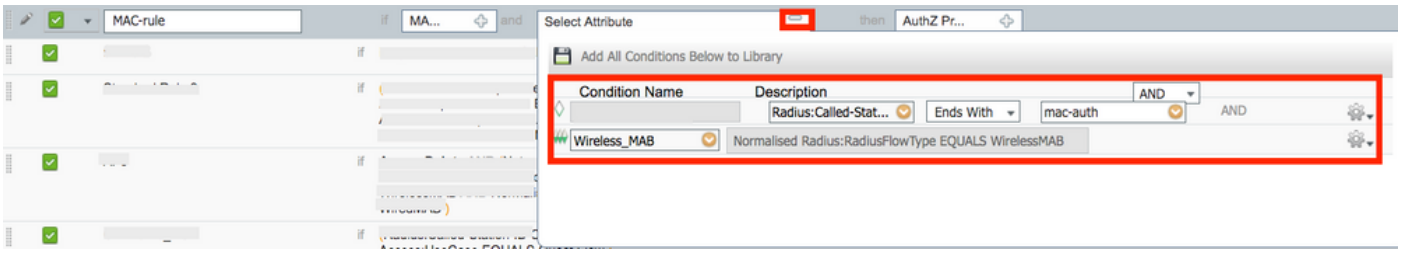


步驟 3.輸入值。

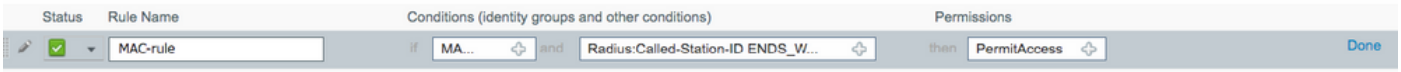
首先，選擇規則的名稱以及儲存端點的身份組(**MACaddressgroup**)，如下圖所示。



然後，選擇執行授權流程的其他條件以屬於此規則。在本示例中，如果授權進程使用無線MAB，並且其被叫站ID（SSID的名稱）以如下圖所mac-auth示，則授權進程會到達此規則。



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



驗證

您可以使用這些命令驗證當前配置：

```
# 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 general
# 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提供永遠線上的追蹤功能。這可確保所有與客戶端連線相關的錯誤、警告和通知級別消息均持續記錄，並且您可以在發生事故或故障情況後檢視其日誌。

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。

若要檢視9800 WLC在預設情況下蒐集的追蹤，可以透過SSH/Telnet連線到9800 WLC並讀取以下步驟（確保將作業階段記錄到文字檔中）。

步驟 1.請檢查控制器的當前時間，以便您可以跟蹤從問題發生時開始的日誌。

```
# 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中收集系統日誌。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.驗證是否已啟用任何調試條件。

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop

IOSXE Packet Tracing Configs:


Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

註：如果您看到列出了任何條件，則表示遇到啟用條件（mac地址、IP地址等）的所有進程的跟蹤將記錄到調試級別。這將增加日誌量。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地址未作為步驟3中的條件列出，請收集特定MAC地址的always-on通知級別跟蹤。

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

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(always-on)跟蹤未為您提供足夠的資訊來確定所調查問題的觸發因素，則可以啟用條件調試並捕獲無線活動(RA)跟蹤，該跟蹤為與指定條件（本例中為客戶端mac地址）互動的所有進程提供調試級別跟蹤。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>}
```

附註： 若要一次監控多個使用者端，請對每個mac位址執行debug wireless mac 命令。

注意:您看不到終端會話上客戶端活動的輸出，因為所有內容都在內部緩衝，供以後檢視。

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器時間開啟之前重現問題，則停止調試。

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

監控時間過後或偵錯無線功能停止後，9800 WLC會產生具有以下名稱的本地檔案

： 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。 您可以將複製到ra trace .log外部伺服器，或者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.
```

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。您無需再次調試客戶端，因為您只需進一步詳細檢視已收集和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 r
```

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，而且非常大。聯絡Cisco TAC以幫助分析這些跟蹤。

您可以將複製到ra-internal-FILENAME.txt外部伺服器，或者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後始終刪除調試條件。

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）。