配置Catalyst 9800無線控制器AP授權清單

目錄

簡介

本檔案介紹如何設定Catalyst 9800無線LAN控制器存取點(AP)驗證原則。

背景資訊

若要授權存取點(AP)，需要使用9800無線LAN控制器的本機資料庫或外部遠端驗證撥入使用者服務(RADIUS)伺服器來授權AP的乙太網路MAC位址。

此功能可確保只有授權存取點(AP)才能加入Catalyst 9800無線LAN控制器。本文檔不介紹網狀（1500系列）AP的情況，這些接入點需要mac過濾器條目才能加入控制器，但不會跟蹤典型的AP授權流（請參閱參考資料）。

必要條件

需求

思科建議您瞭解以下主題：

- 9800 WLC
- 對無線控制器的命令列介面(CLI)訪問

採用元件

9800 WLC v16.12

AP 1810W

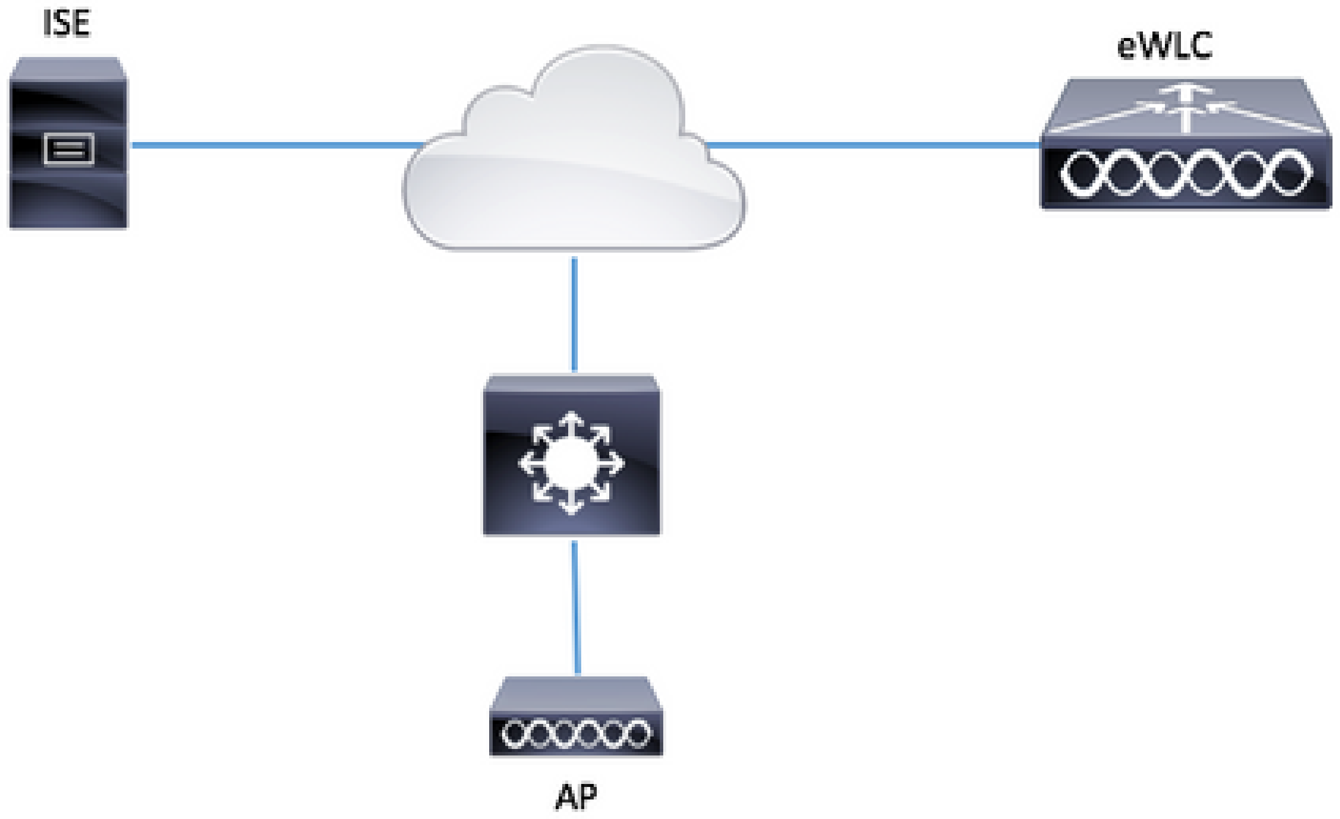
AP 1700

身分識別服務引擎(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



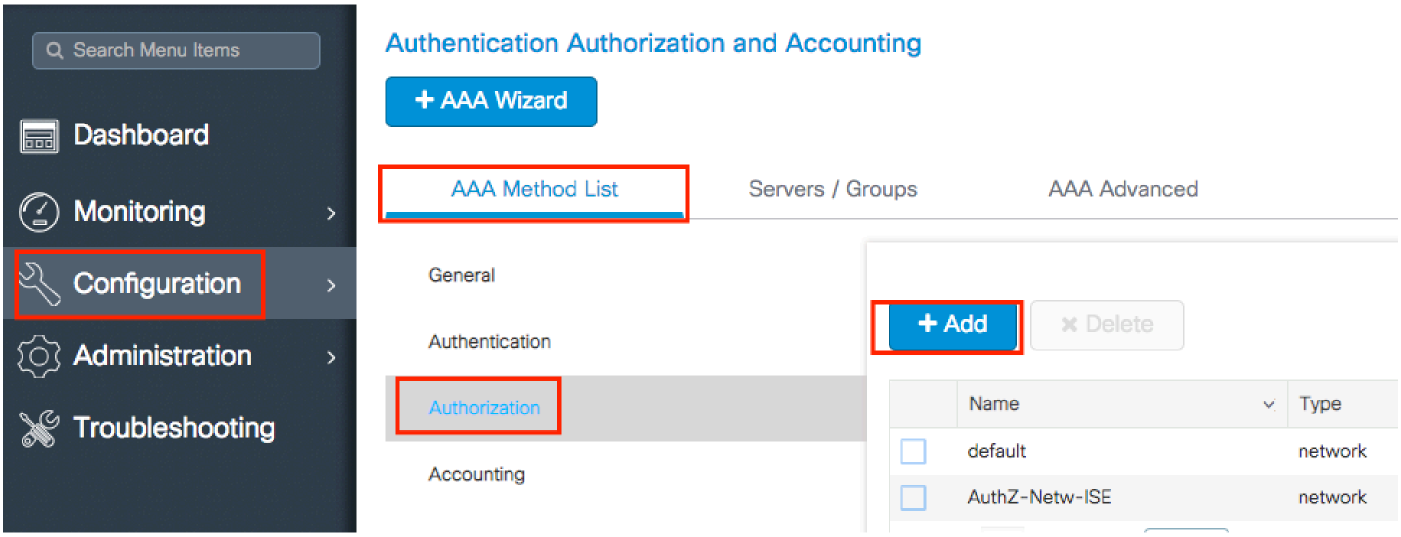
組態

MAC AP授權清單 — 本地

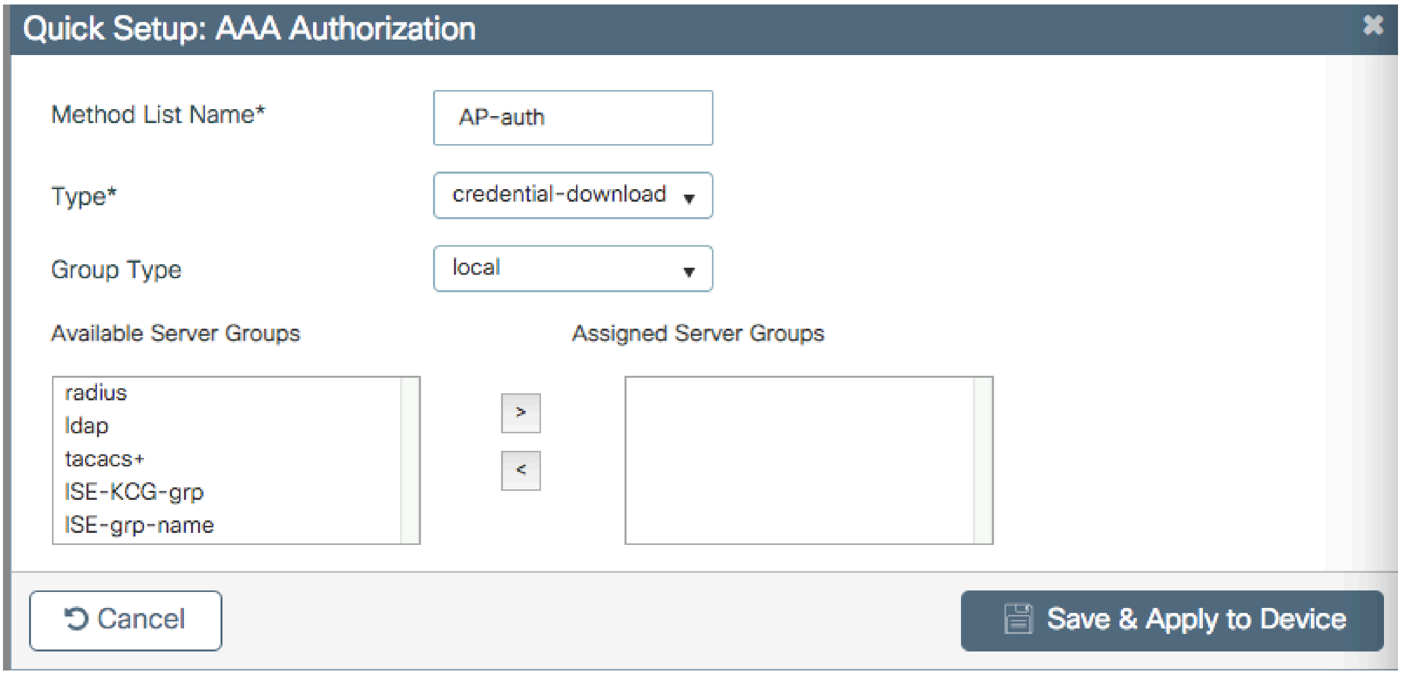
授權的AP的MAC位址儲存在9800 WLC本機。

步驟 1.建立本地授權憑證下載方法清單。

導覽至Configuration > Security > AAA > AAA Method List > Authorization > + Add



	Name	Type
□	default	network
□	AuthZ-Netw-ISE	network



Method List Name* AP-auth

Type* credential-download

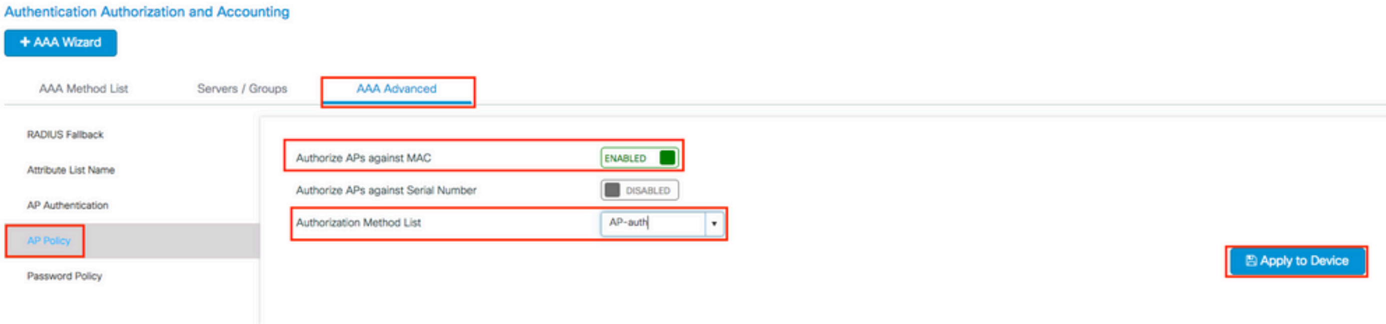
Group Type local

Available Server Groups: radius, ldap, tacacs+, ISE-KCG-grp, ISE-grp-name

Assigned Server Groups

步驟 2.啟用AP MAC授權。

導航至 Configuration > Security > AAA > AAA Advanced > AP Policy。 啟用根據MAC授權AP，並選擇步驟1中建立的Authorization Method List。



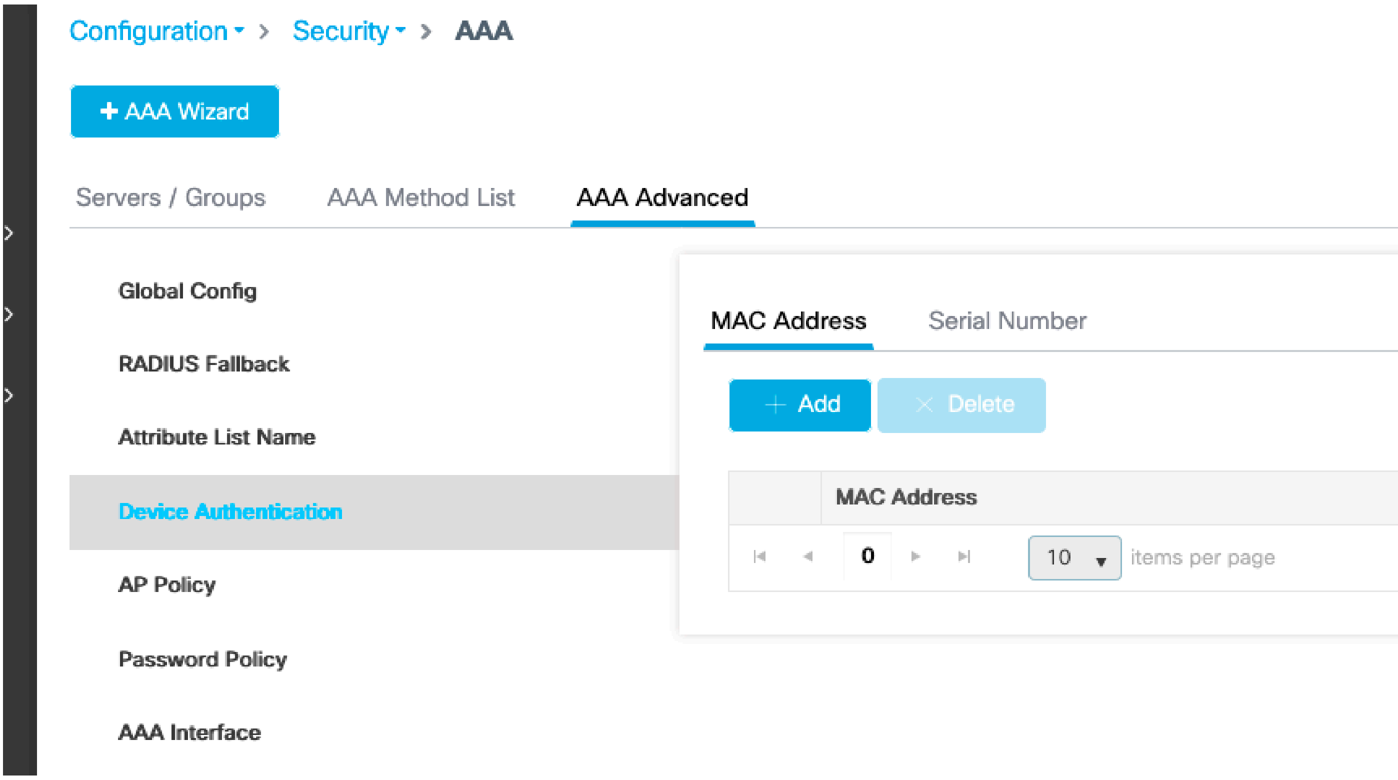
Authorize APs against MAC ENABLED

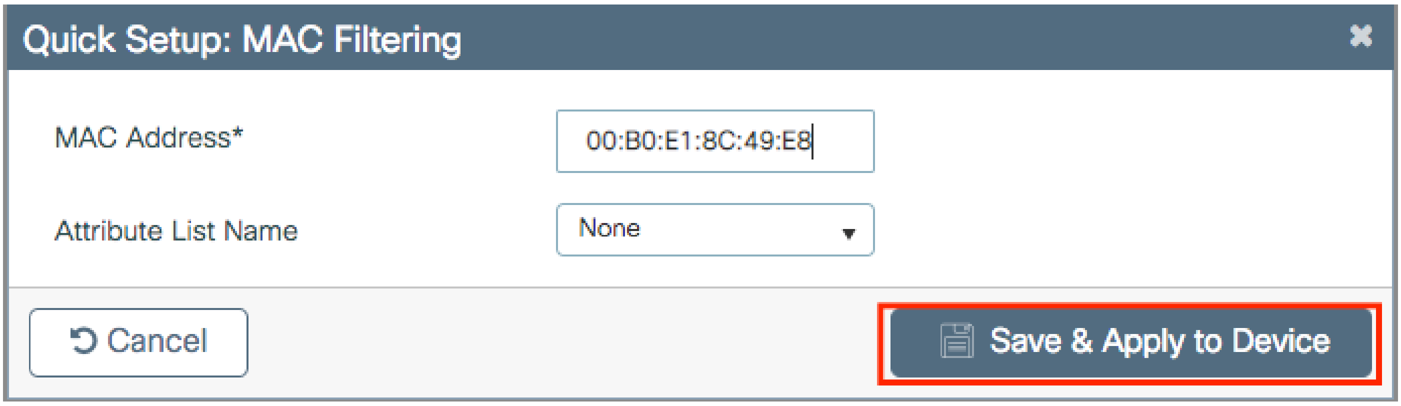
Authorize APs against Serial Number DISABLED

Authorization Method List AP-auth

步驟 3.新增AP乙太網mac地址。

導航至 Configuration > Security > AAA > AAA Advanced > Device Authentication > MAC Address > + Add





MAC Address*: 00:B0:E1:8C:49:E8

Attribute List Name: None

注意:AP乙太網MAC地址必須是 在16.12版的Web UI(xx:xx:xx:xx:xx:xx（或）xxxx.xxxx.xxxx（或）xx-xx-xx-xx-xx-xx)中輸入時，採用其中一種格式。在17.3版中，格式必須為xxxxxxxxxxx，不能使用任何分隔符。在任何版本中，CLI格式始終為xxxxxxxxxxxx（在16.12中，Web UI刪除配置中的分隔符）。思科錯誤ID CSCvv43870允許在CLI或Web UI的較新版本中使用任何格式。

CLI:

```
# config t
# aaa new-model
# aaa authorization credential-download <AP-auth> local
# ap auth-list authorize-mac
# ap auth-list method-list <AP-auth>

# username <aaaabbbbcccc> mac
```

MAC AP授權清單 — 外部RADIUS伺服器

9800 WLC組態

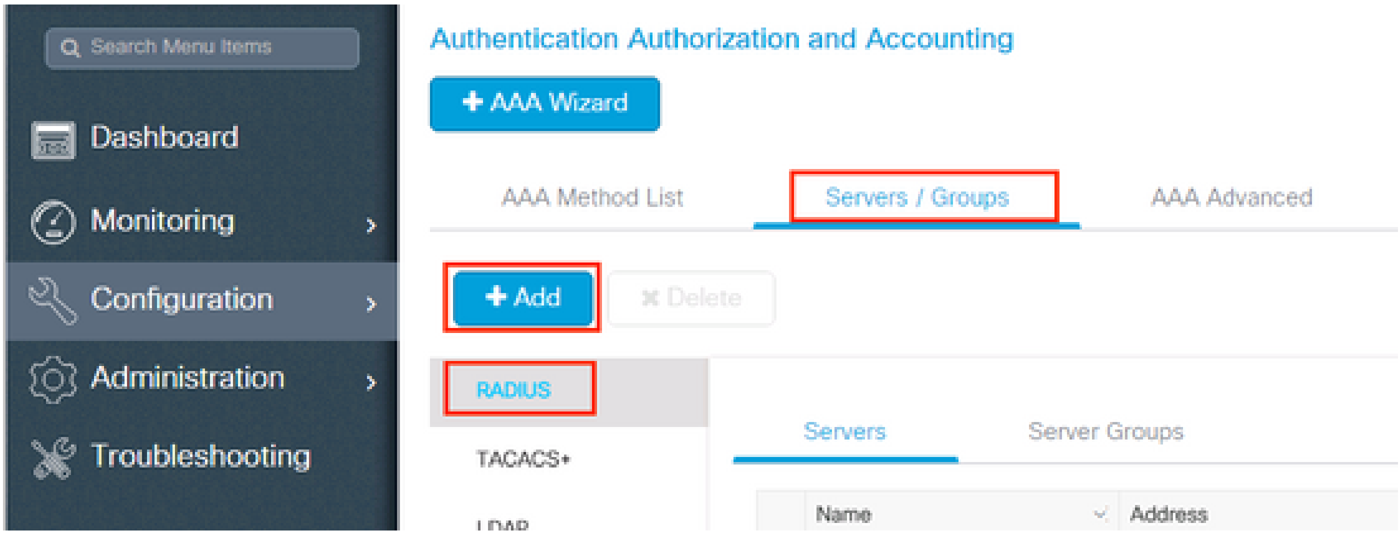
授權的AP的MAC地址儲存在外部RADIUS伺服器（在本例中為ISE）上。

在ISE上，您可以將AP的MAC地址註冊為使用者名稱/密碼或終端。各個步驟中會指導您選擇使用其中一種方法。

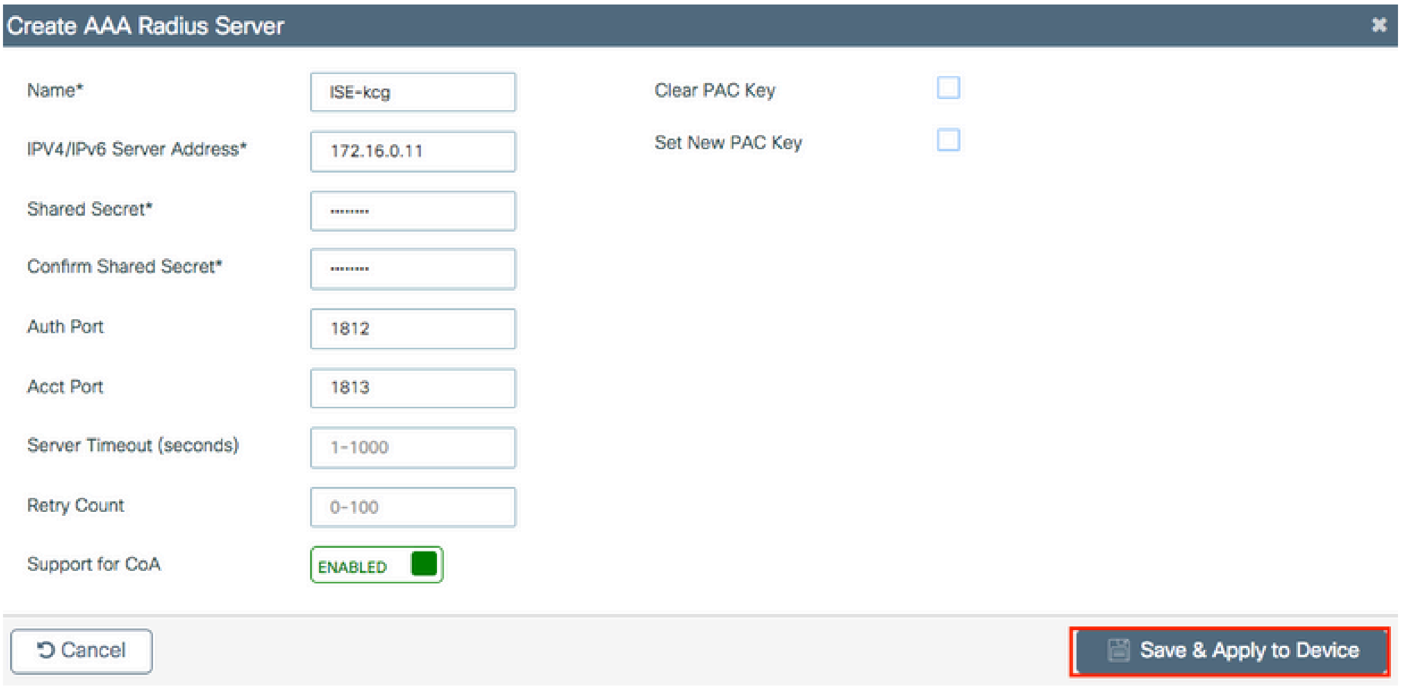
GUI:

步驟 1.宣告RADIUS伺服器

導覽至Configuration > Security > AAA > Servers / Groups > RADIUS > Servers > + Add，然後輸入RADIUS伺服器資訊。



如果您未來計畫使用中央 Web 驗證（或任何需要 CoA 的安全性類型），請確認「CoA 支援」已啟用。



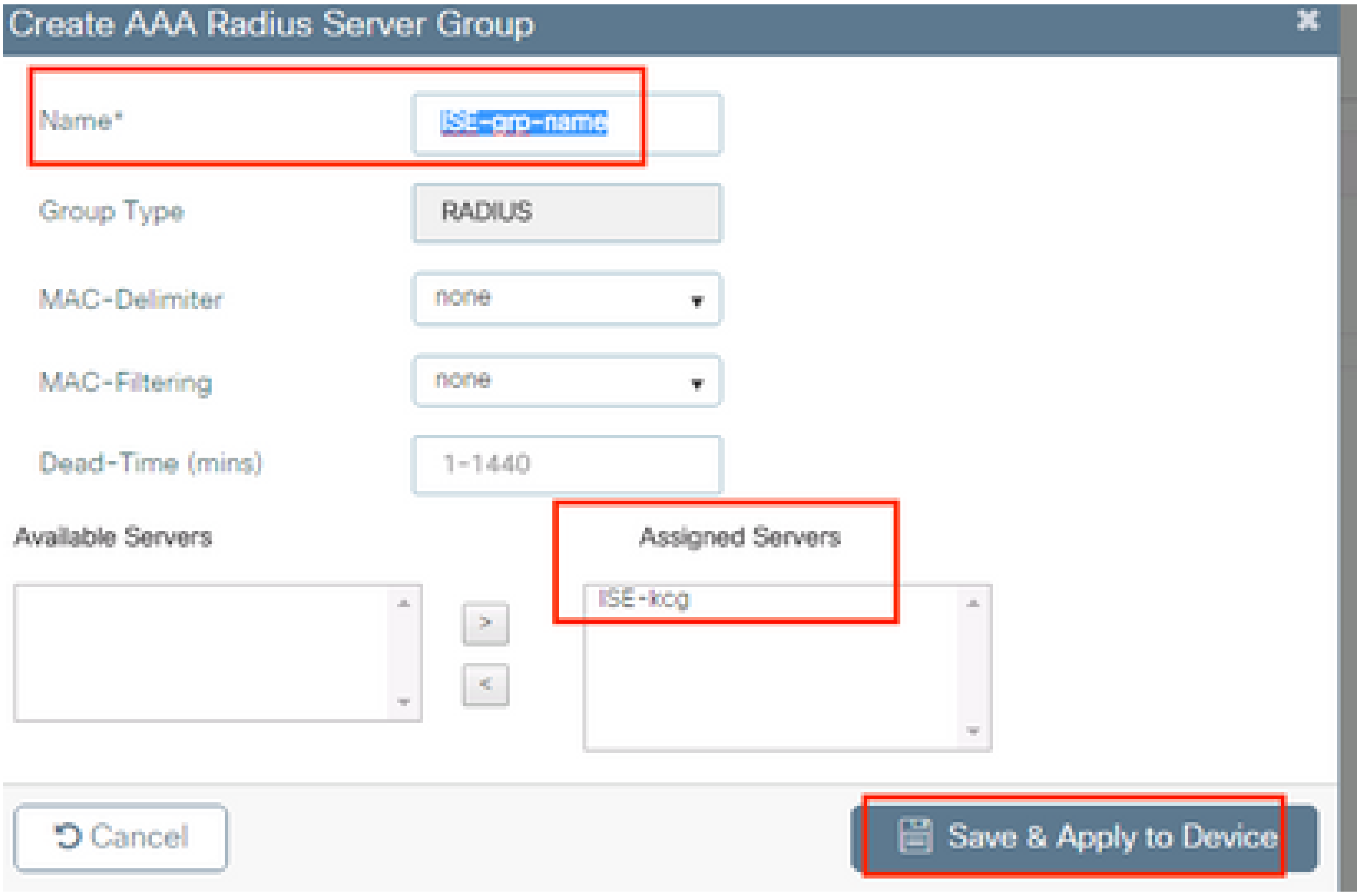
Create AAA Radius Server

Name*	ISE-kcg	Clear PAC Key	□
IPV4/IPv6 Server Address*	172.16.0.11	Set New PAC Key	□
Shared Secret*	....		
Confirm Shared Secret*	....		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		
Support for CoA	ENABLED		

步驟 2.將RADIUS伺服器新增到RADIUS群組

導覽至Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add

要使ISE將AP MAC地址作為使用者名稱進行身份驗證，請將MAC過濾保留為無。

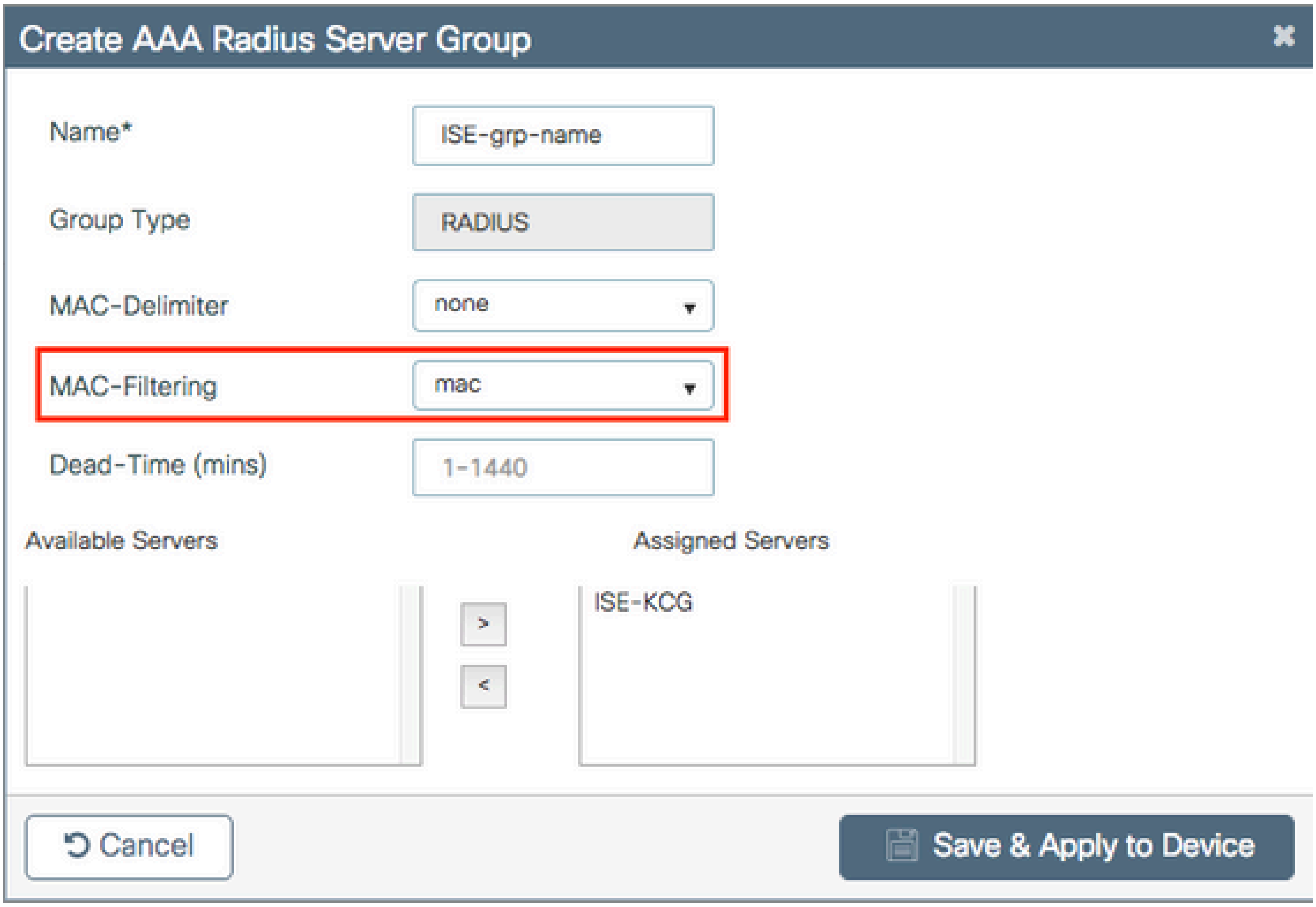


Create AAA Radius Server Group

Name*	ISE-grp-name
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	1-1440

Available Servers	Assigned Servers
	ISE-kcg

在終端將MAC過濾更改為MAC時讓ISE驗證AP MAC地址。



Create AAA Radius Server Group

Name*: ISE-grp-name

Group Type: RADIUS

MAC-Delimiter: none

MAC-Filtering: mac

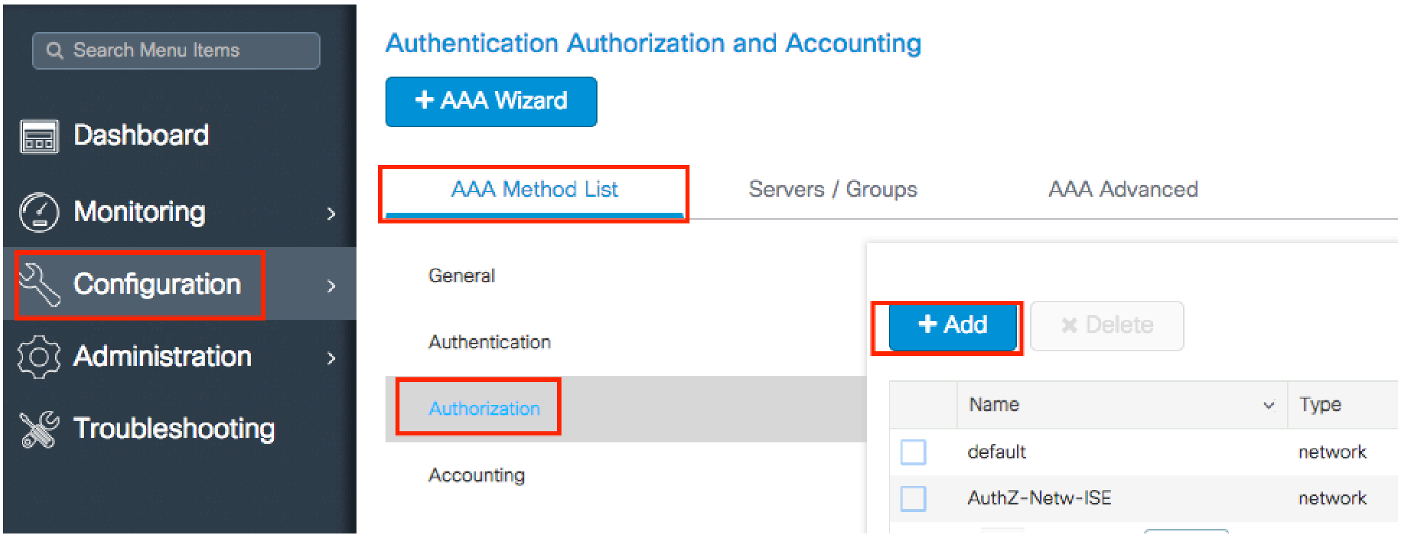
Dead-Time (mins): 1-1440

Available Servers

Assigned Servers: ISE-KCG

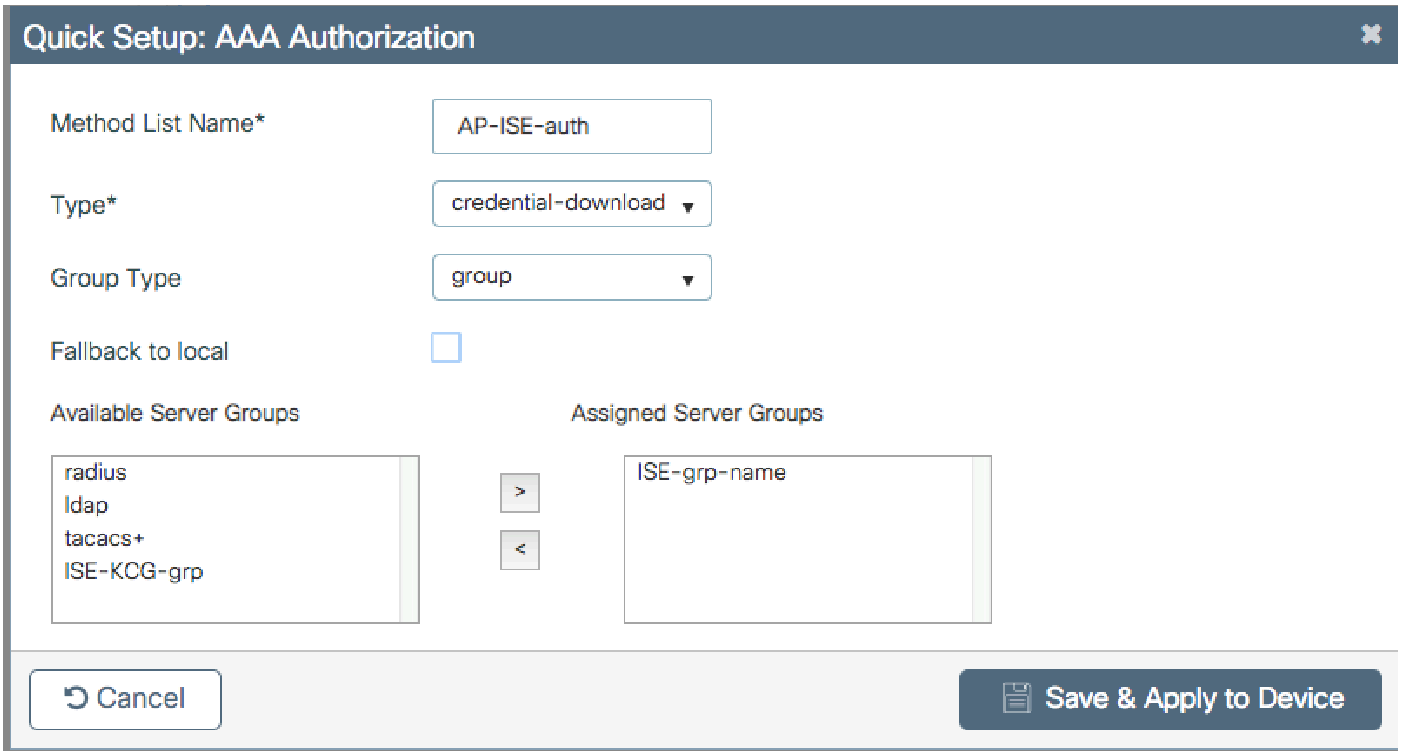
步驟 3.建立授權憑證下載方法清單。

導覽至Configuration > Security > AAA > AAA Method List > Authorization > + Add



Authentication Authorization and Accounting

	Name	Type
□	default	network
□	AuthZ-Netw-ISE	network



Quick Setup: AAA Authorization

Method List Name*: AP-ISE-auth

Type*: credential-download

Group Type: group

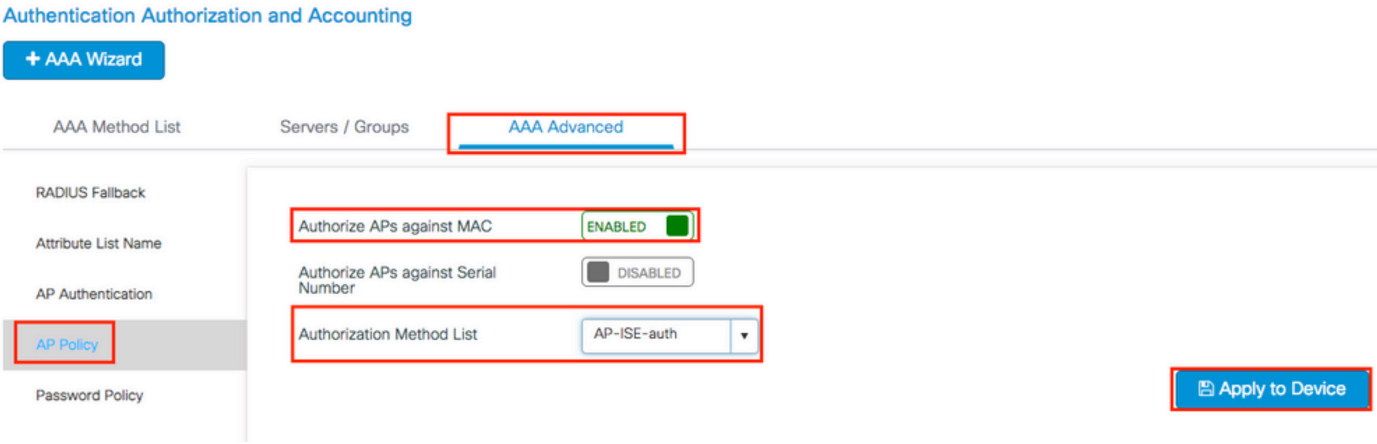
Fallback to local: □

Available Server Groups: radius, ldap, tacacs+, ISE-KCG-grp

Assigned Server Groups: ISE-grp-name

步驟 4.啟用AP MAC授權。

導航至 Configuration > Security > AAA > AAA Advanced > AP Policy。 啟用根據MAC授權AP，並選擇步驟3中建立的Authorization Method List。



Authorize APs against MAC: ENABLED

Authorize APs against Serial Number: DISABLED

Authorization Method List: AP-ISE-auth

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 credential-download <AP-auth> group <radius-grp-name>
# ap auth-list authorize-mac
# ap auth-list method-list <AP-ISE-auth>
```

ISE配置

步驟 1.要將9800 WLC新增到ISE:

在ISE上宣告9800 WLC

選擇根據身份驗證使用所需步驟配置AP的MAC地址：

配置USE以將MAC地址作為終端進行身份驗證

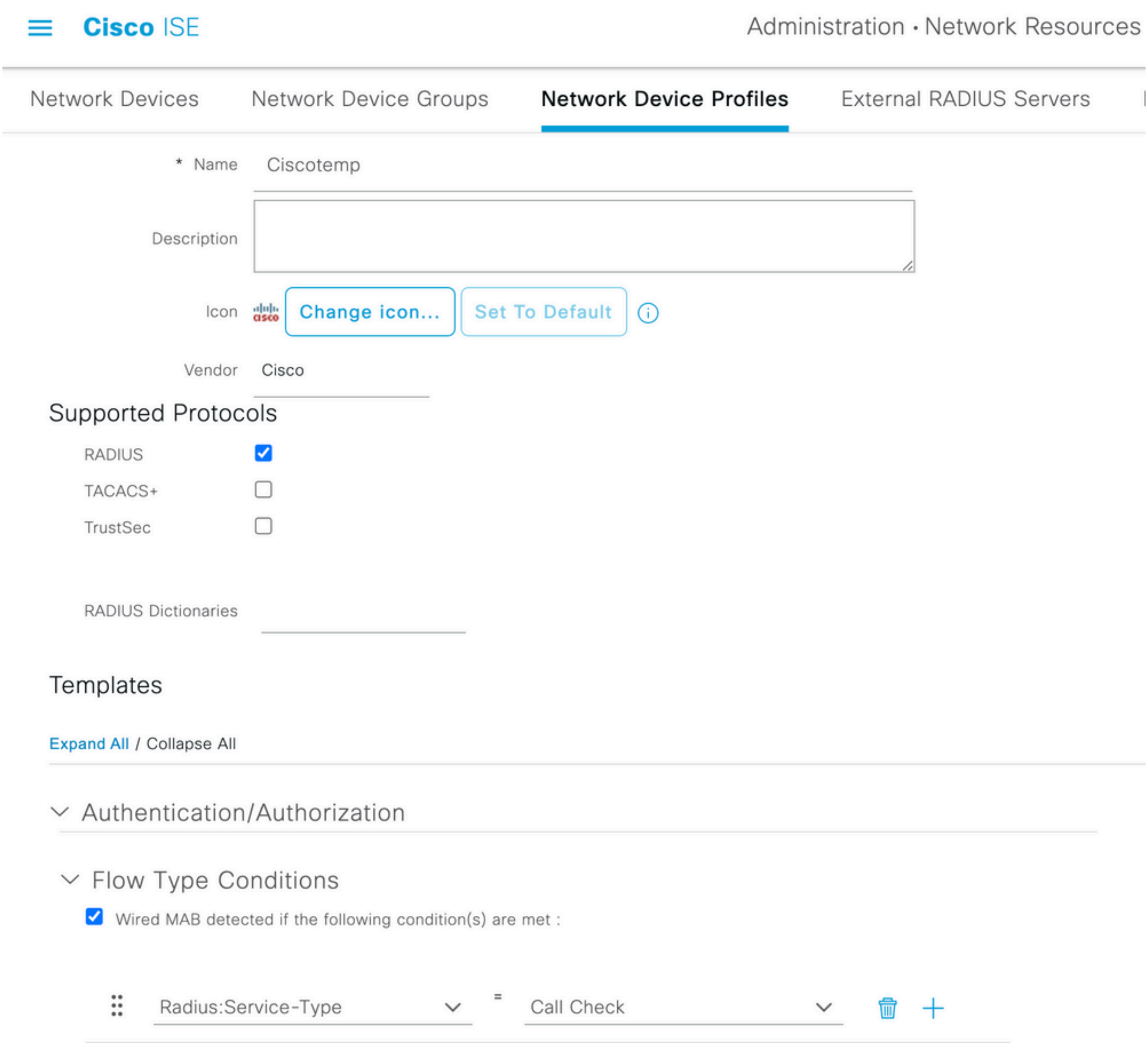
將ISE配置為以使用者名稱/密碼身份驗證MAC地址

配置ISE以將MAC地址作為終端進行身份驗證

步驟2.（可選）為接入點建立身份組

因為9800不會傳送具有AP授權的NAS-port-Type屬性Cisco錯誤IDCSCvy74904
)中，ISE無法將AP授權識別為MAB工作流，因此，如果AP的MAC地址位於終端清單中，則無法對AP進行身份驗證，除非您將MAB工作流修改為不要求ISE上的NAS-PORT-type屬性。

導航到Administrator > Network device profile，然後建立新的裝置配置檔案。為有線MAB啟用RADIUS並新增service-type=call-check。您可以從思科原始配置檔案中複製其餘部分，其理念是對於有線MAB沒有「nas埠型別」條件。



* Name: Ciscotemp

Description:

Icon

Vendor: Cisco

Supported Protocols

RADIUS ☑

TACACS+ □

TrustSec □

RADIUS Dictionaries

Templates

Expand All / Collapse All

Authentication/Authorization

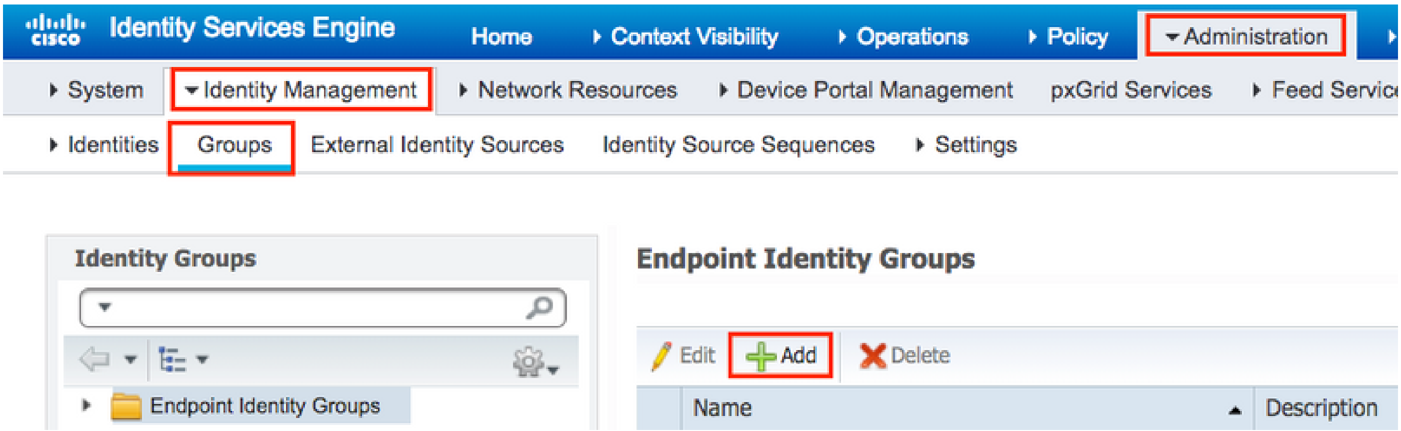
Flow Type Conditions

☑ Wired MAB detected if the following condition(s) are met :

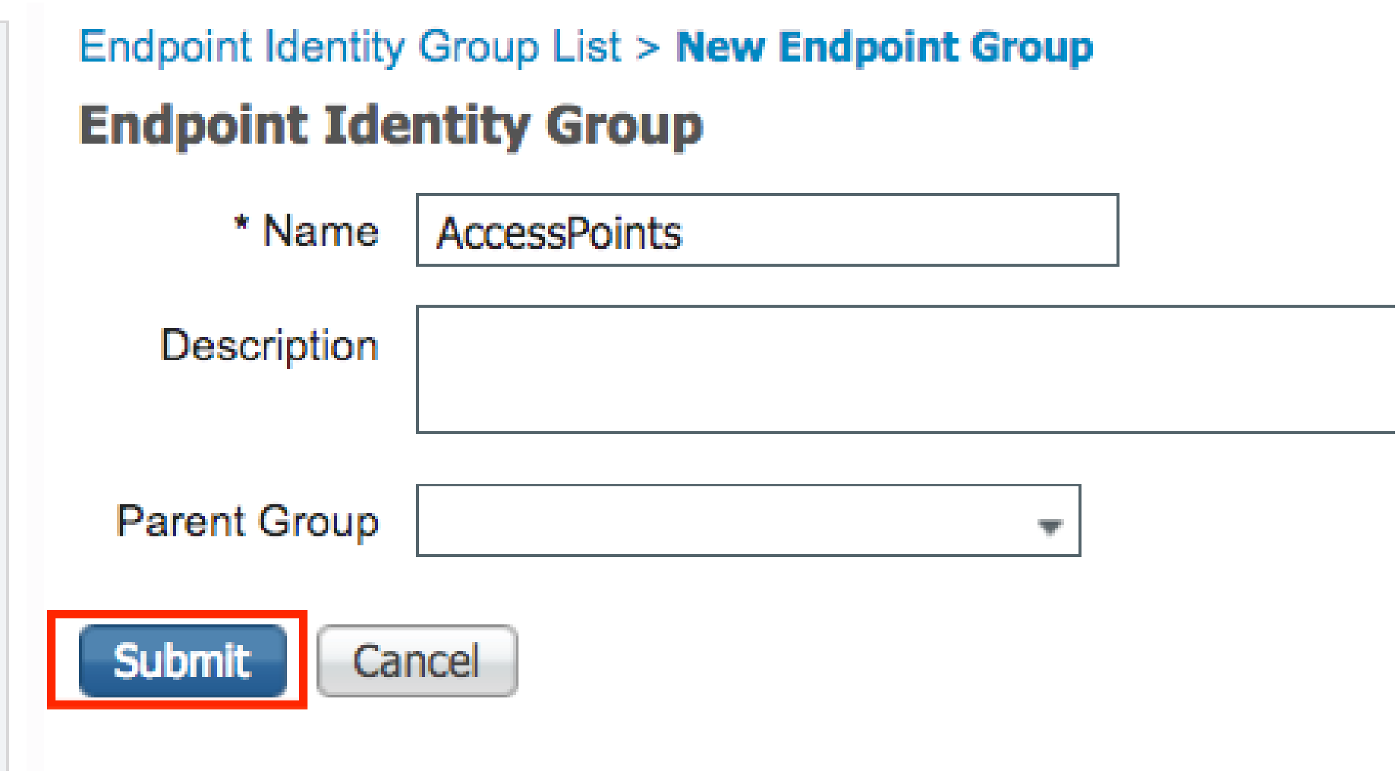
Radius:Service-Type = Call Check

返回9800的網路裝置條目，並將其配置檔案設定為新建立的裝置配置檔案。

導航到Administration > Identity Management > Groups > Endpoint Identity Groups > + Add。



選擇名稱，然後點選提交。



Endpoint Identity Group List > **New Endpoint Group**

Endpoint Identity Group

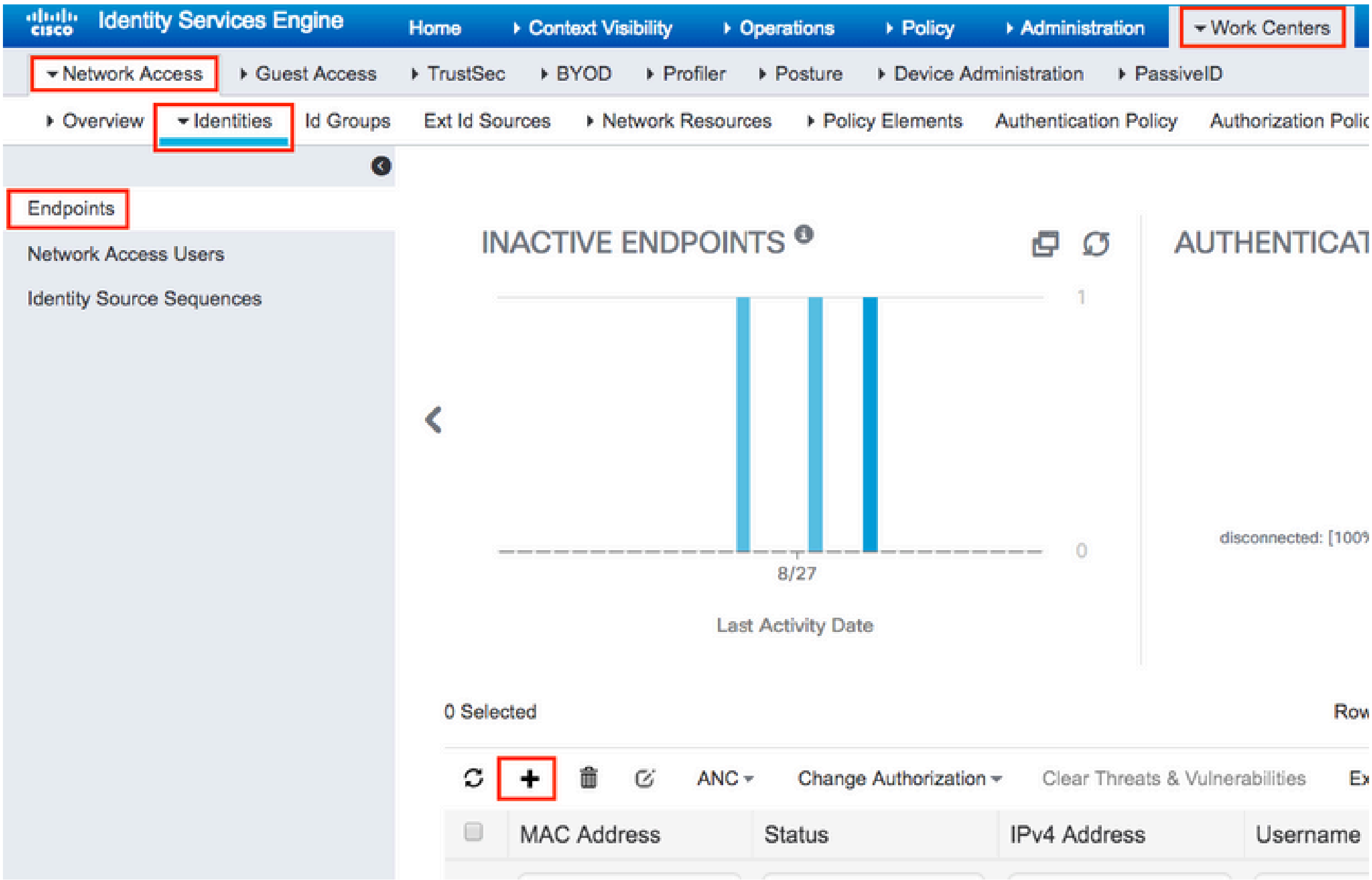
* Name: AccessPoints

Description:

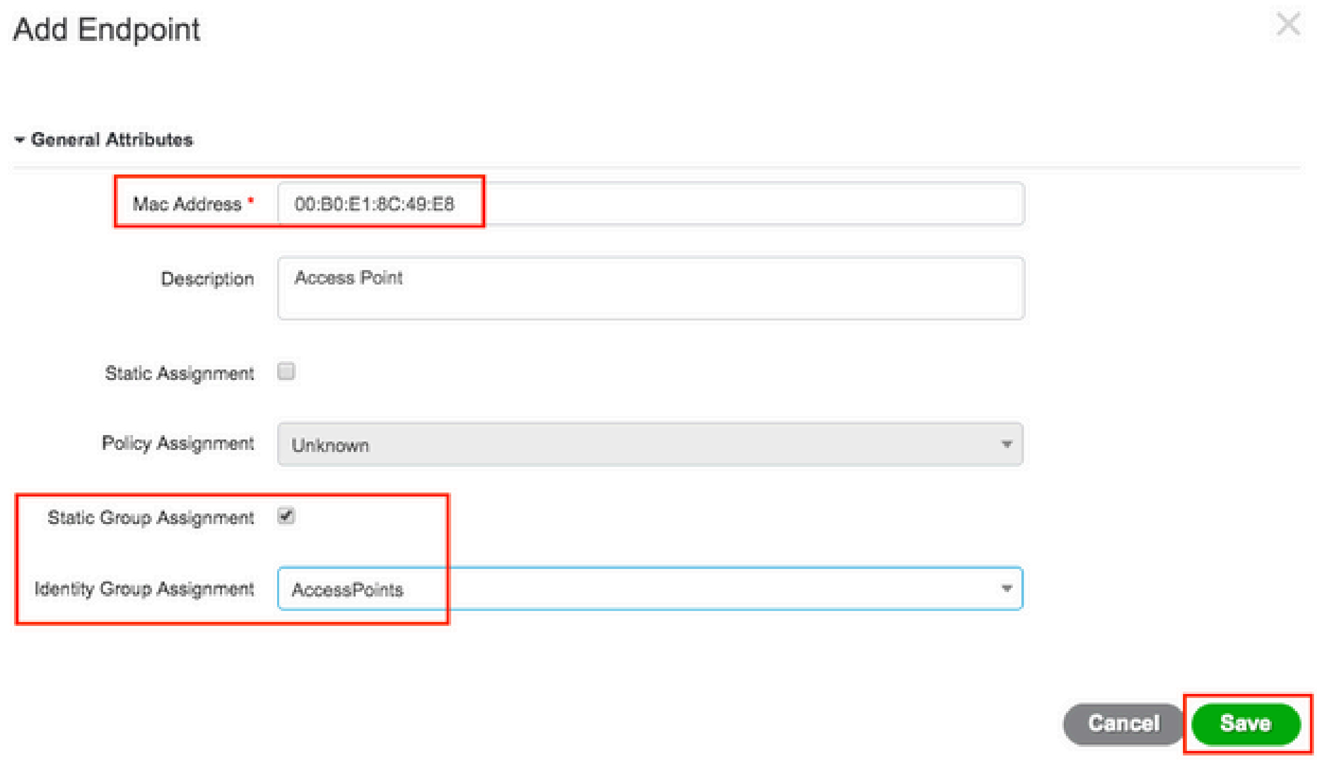
Parent Group:

步驟 3.將AP乙太網MAC地址新增到其終端身份組。

導航至工作中心>網路訪問>身份>終端> +



輸入所需資訊。



Add Endpoint

▾ General Attributes

Mac Address * 00:B0:E1:8C:49:E8

Description Access Point

Static Assignment □

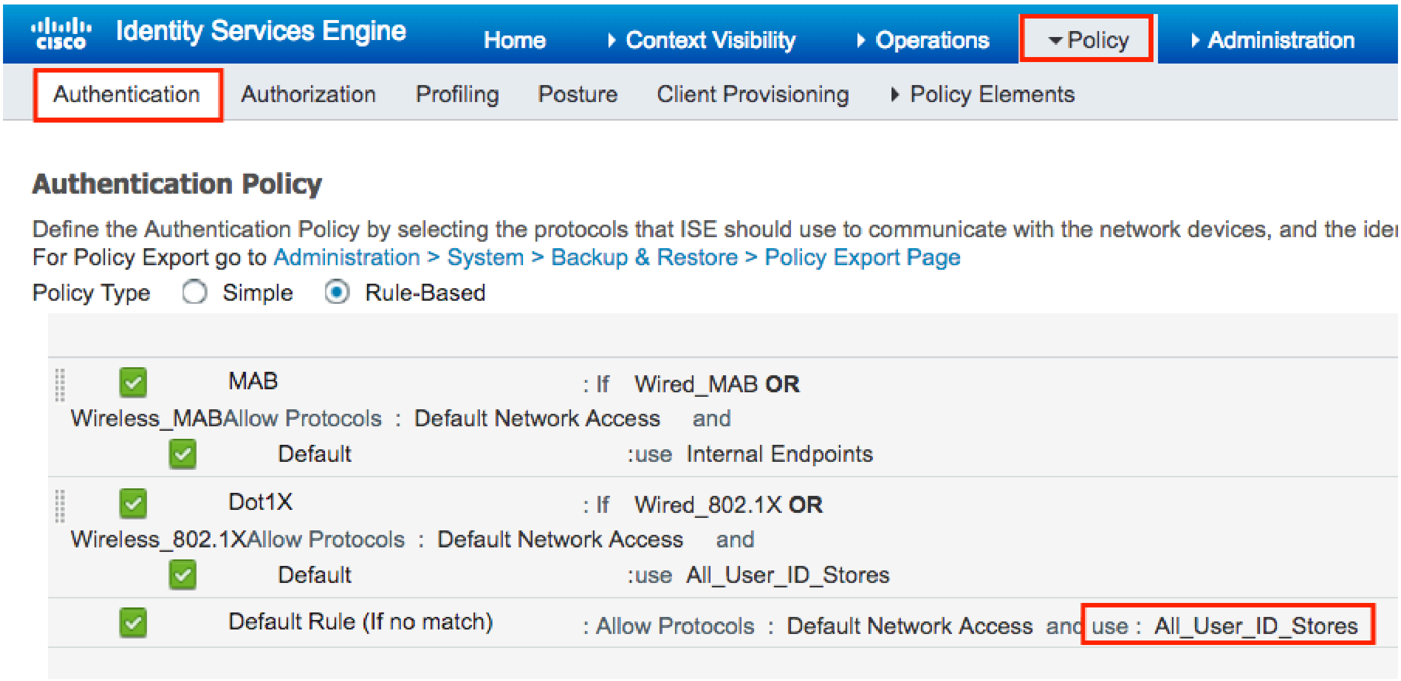
Policy Assignment Unknown

Static Group Assignment ☑

Identity Group Assignment AccessPoints

步驟 4.驗證預設身份驗證規則上使用的身份儲存是否包含內部終結點。

A.導航到Policy > Authentication，並注意Identity store。



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the ide
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

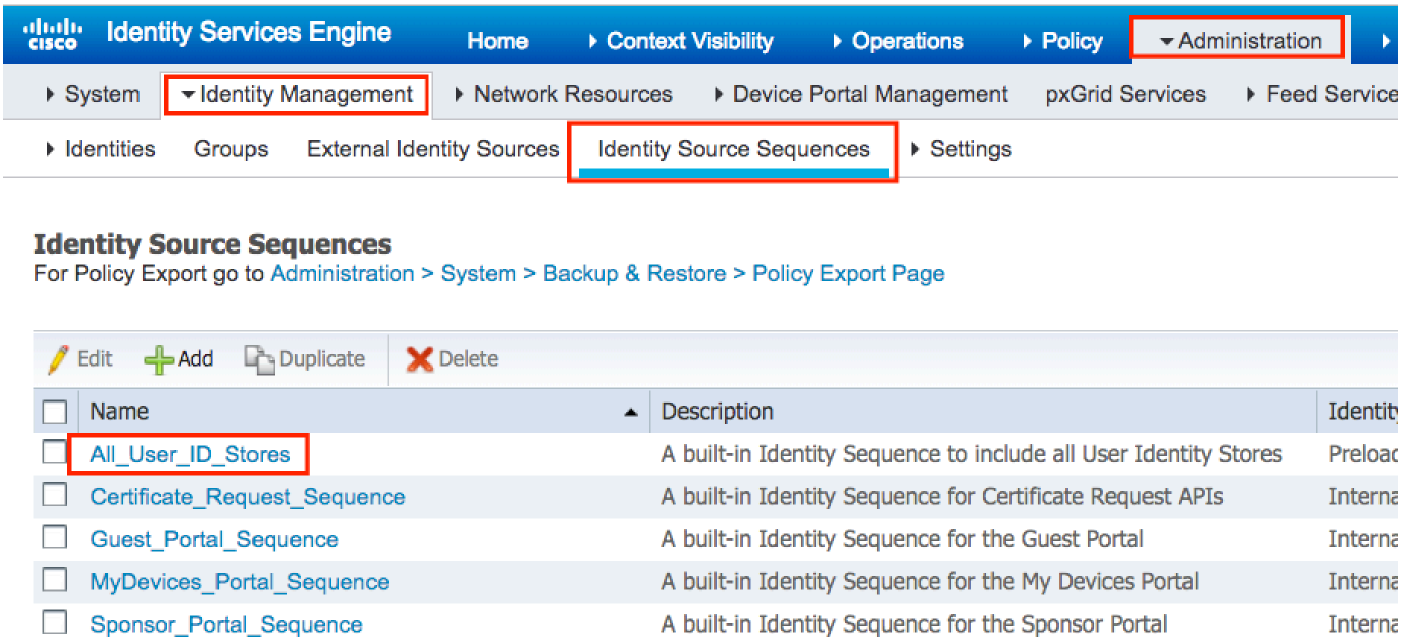
Policy Type ○ Simple ● Rule-Based

✓ MAB : If Wired_MAB **OR**
Wireless_MABAllow Protocols : Default Network Access and
✓ Default :use Internal Endpoints

✓ Dot1X : If Wired_802.1X **OR**
Wireless_802.1XAllow Protocols : Default Network Access and
✓ Default :use All_User_ID_Stores

✓ Default Rule (If no match) : Allow Protocols : Default Network Access and use : All_User_ID_Stores

B.導航到管理>身份管理>身份源序列>身份名稱。

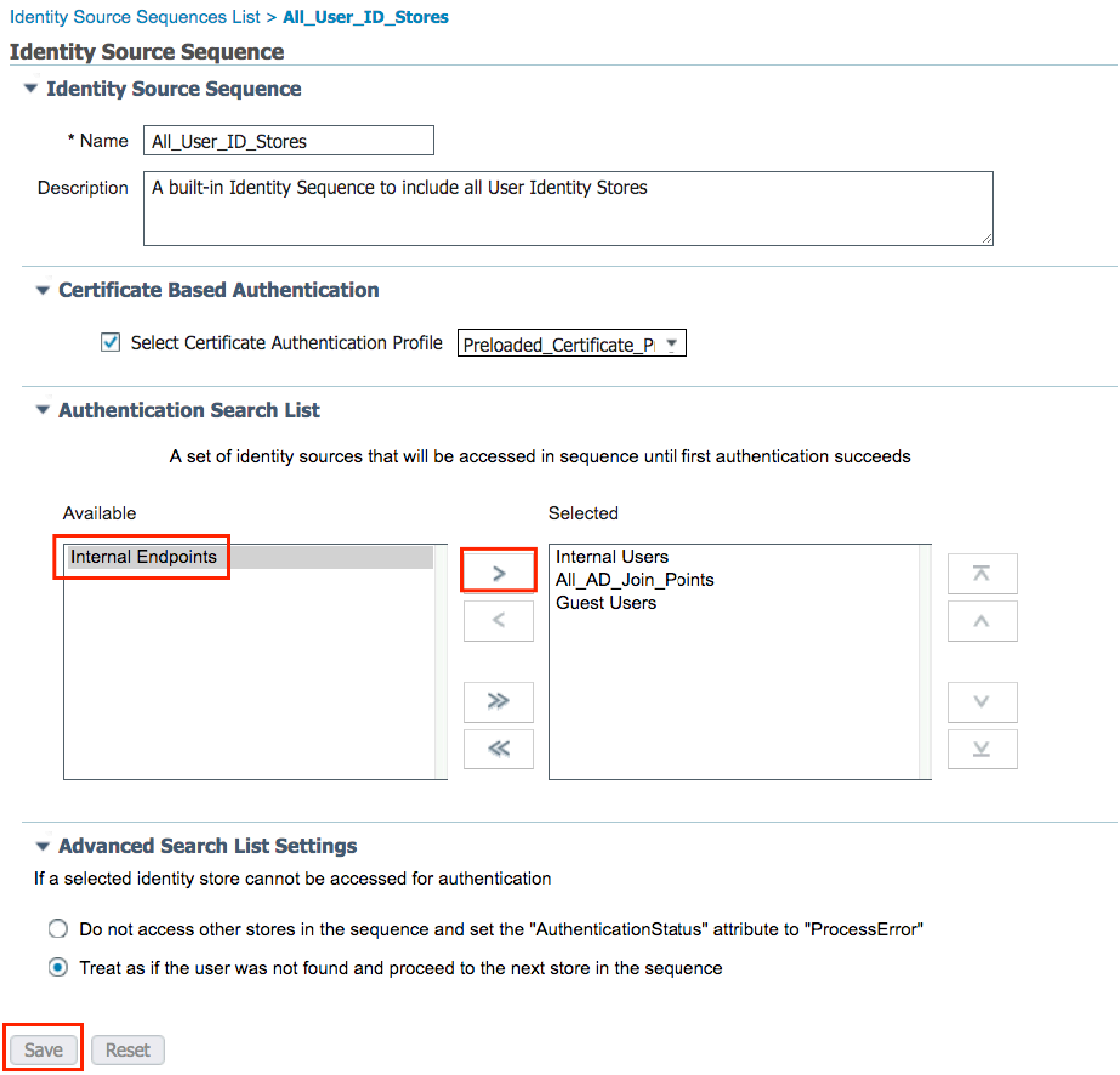


Identity Source Sequences

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

□	Name	Description	Identit
□	All_User_ID_Stores	A built-in Identity Sequence to include all User Identity Stores	Preload
□	Certificate_Request_Sequence	A built-in Identity Sequence for Certificate Request APIs	Interna
□	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Interna
□	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Interna
□	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Interna

C.確保內部終結點屬於它，如果不是，則新增它。



Identity Source Sequences List > **All_User_ID_Stores**

Identity Source Sequence

Identity Source Sequence

* Name: All_User_ID_Stores

Description: A built-in Identity Sequence to include all User Identity Stores

Certificate Based Authentication

☑ Select Certificate Authentication Profile: Preloaded_Certificate_P

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available: Internal Endpoints

Selected: Internal Users, All_AD_Join_Points, Guest Users

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

● Treat as if the user was not found and proceed to the next store in the sequence

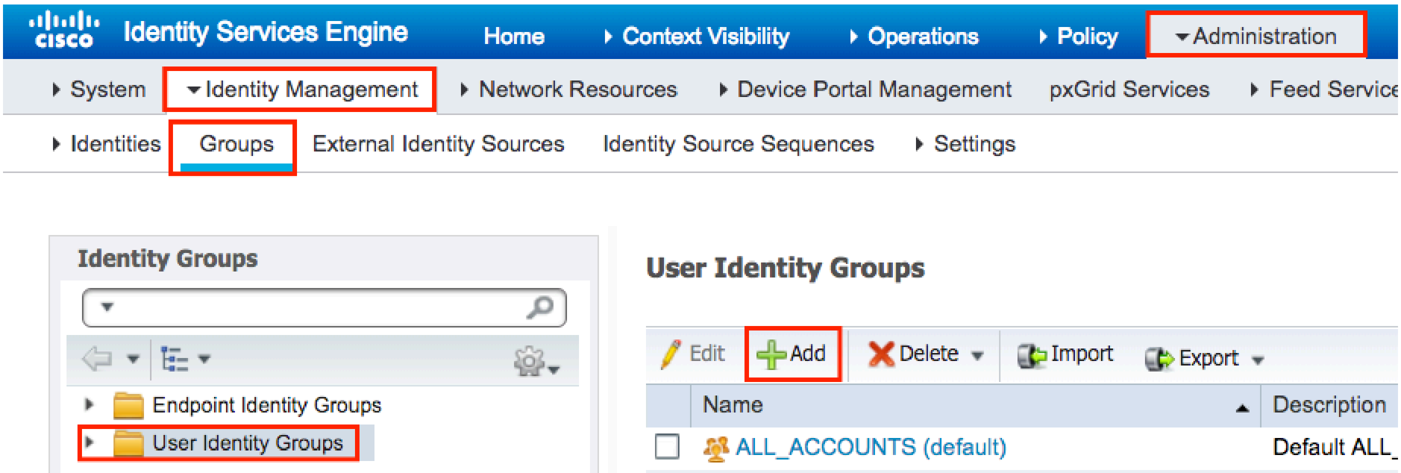
將ISE配置為以使用者名稱/密碼身份驗證MAC地址

不建議使用此方法，因為它需要較低的密碼策略以允許與使用者名稱相同的密碼。

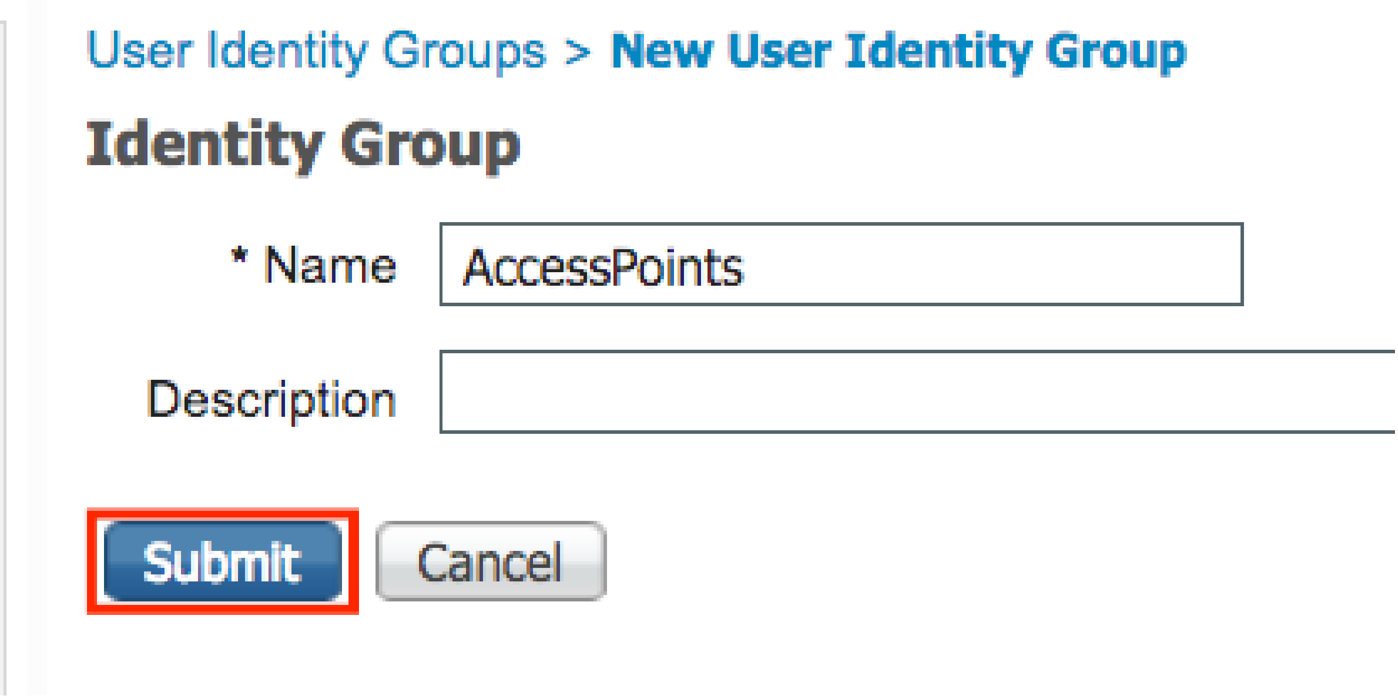
但是，如果無法修改網路裝置配置檔案，則此解決方案可以作為一種解決方法

步驟2.（可選）為接入點建立身份組

導航到Administration > Identity Management > Groups > User Identity Groups > + Add。



選擇名稱，然後點選提交。


User Identity Groups > New User Identity Group

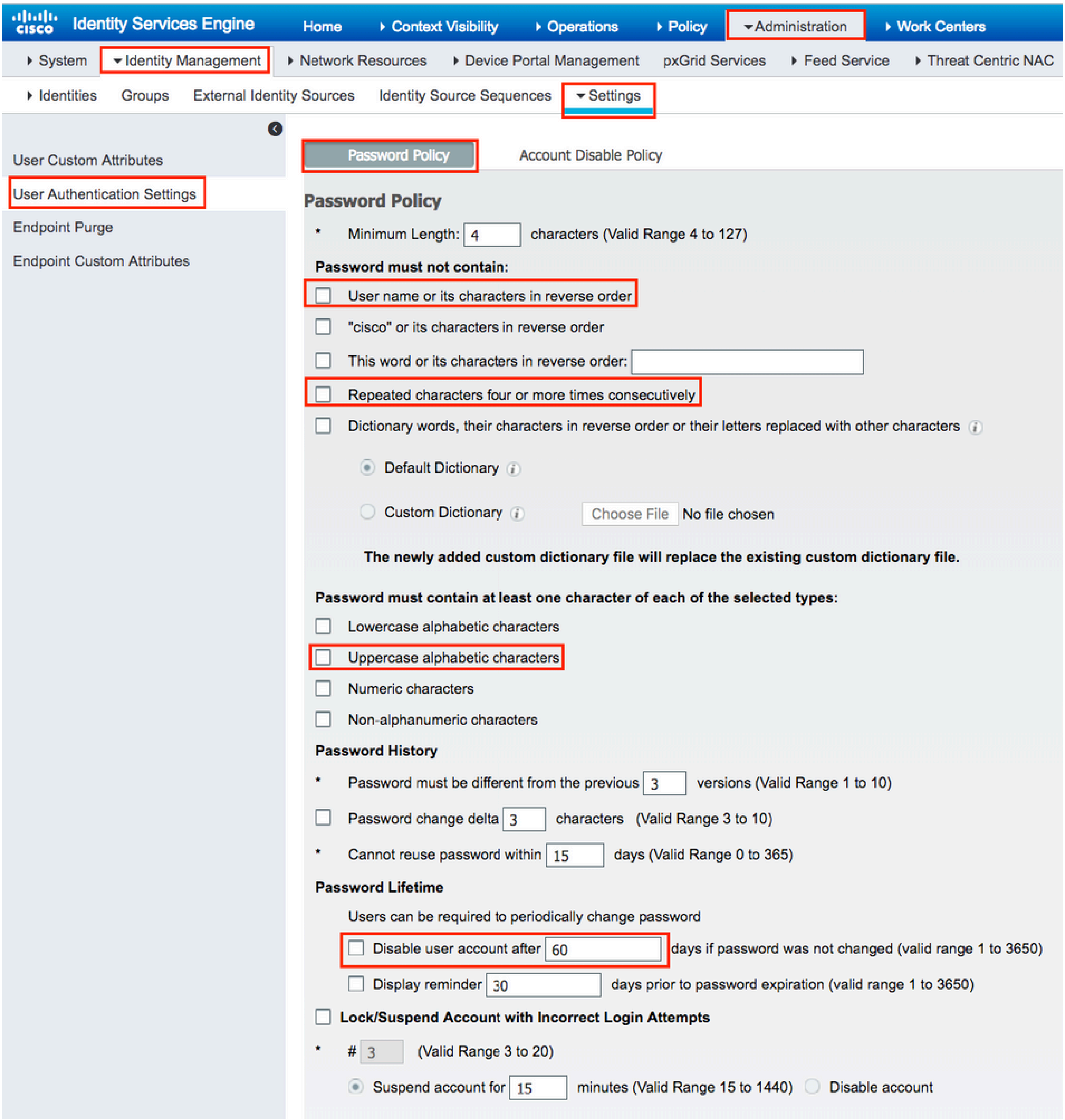
Identity Group

* Name: AccessPoints

Description:

步驟 3.驗證您當前的密碼策略是否允許您將mac地址新增為使用者名稱和密碼。

導航到Administration > Identity Management > Settings > User Authentication Settings > Password Policy，並確保至少禁用以下選項：



Password Policy

* Minimum Length: 4 characters (Valid Range 4 to 127)

Password must not contain:

□ User name or its characters in reverse order

□ "cisco" or its characters in reverse order

□ This word or its characters in reverse order:

□ Repeated characters four or more times consecutively

□ Dictionary words, their characters in reverse order or their letters replaced with other characters

● Default Dictionary

○ Custom Dictionary Choose File No file chosen

The newly added custom dictionary file will replace the existing custom dictionary file.

Password must contain at least one character of each of the selected types:

□ Lowercase alphabetic characters

□ Uppercase alphabetic characters

□ Numeric characters

□ Non-alphanumeric characters

Password History

* Password must be different from the previous 3 versions (Valid Range 1 to 10)

□ Password change delta 3 characters (Valid Range 3 to 10)

* Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

Users can be required to periodically change password

□ Disable user account after 60 days if password was not changed (valid range 1 to 3650)

□ Display reminder 30 days prior to password expiration (valid range 1 to 3650)

□ **Lock/Suspend Account with Incorrect Login Attempts**

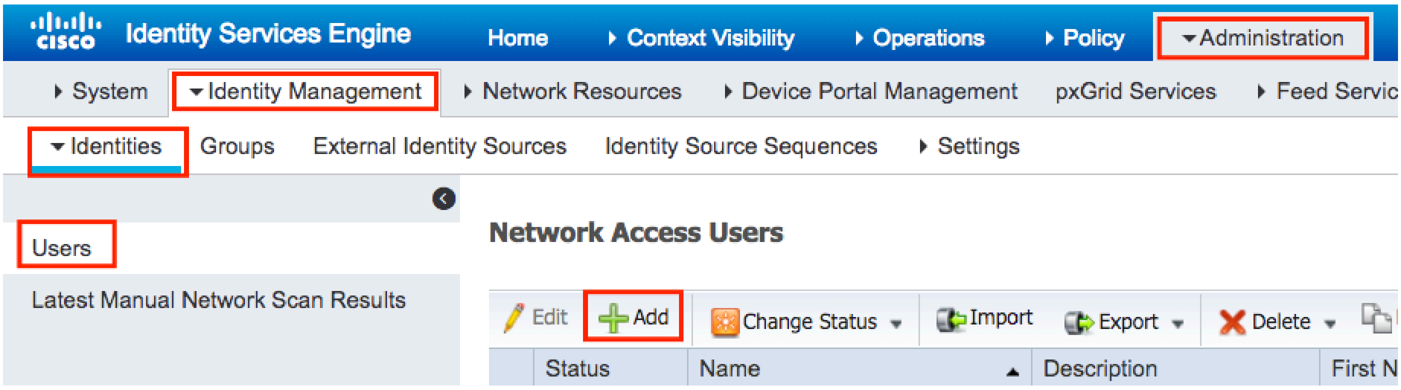
* # 3 (Valid Range 3 to 20)

● Suspend account for 15 minutes (Valid Range 15 to 1440) ○ Disable account

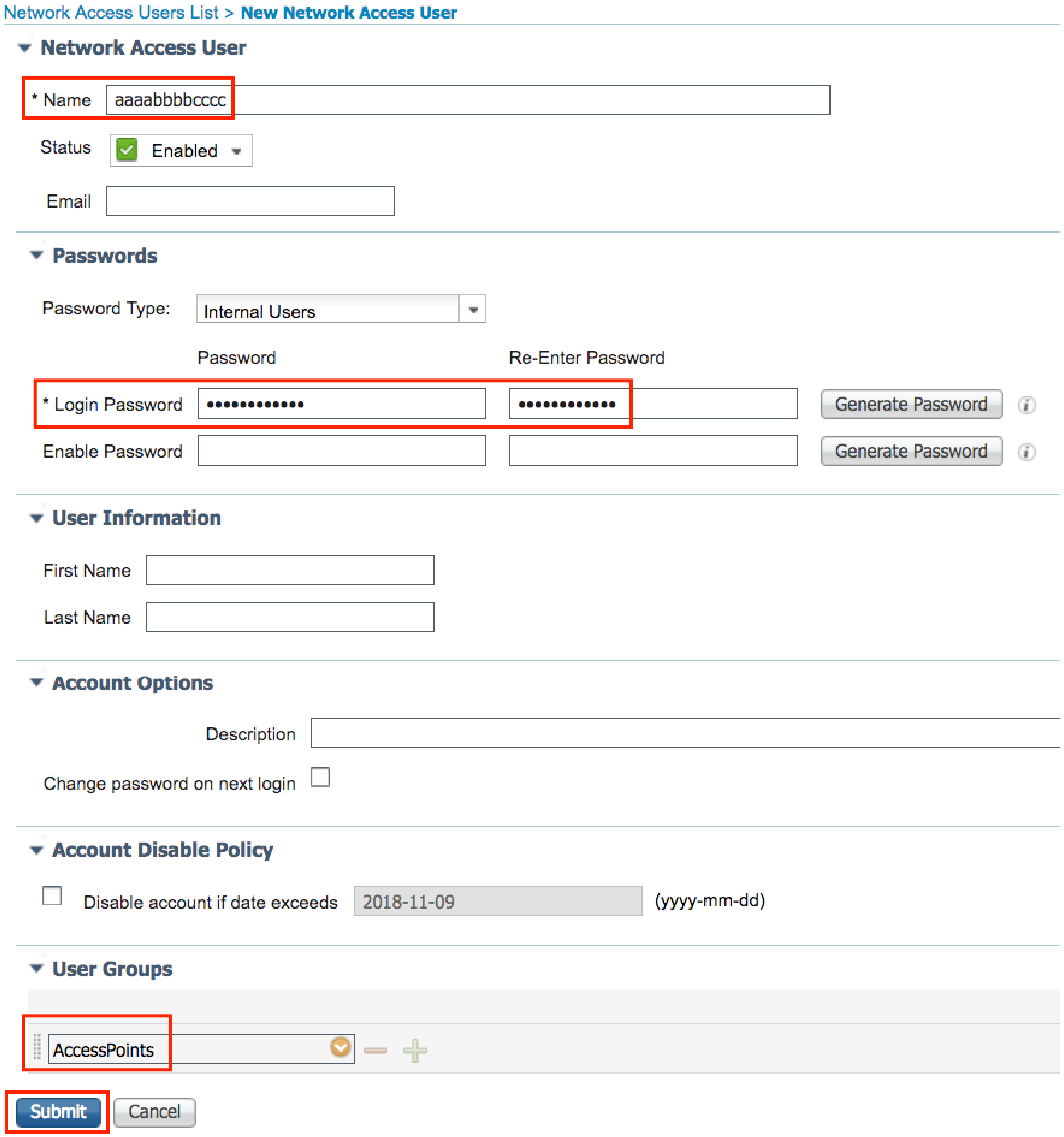
注意:如果密碼未更改，則還可以禁用在XX天后禁用使用者帳戶選項。由於這是mac地址，因此密碼從不更改。

步驟 4.新增AP乙太網mac地址。

導航到管理>身份管理>身份>使用者> +新增


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Servic
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Users
Latest Manual Network Scan Results
Network Access Users
Edit
Add
Change Status
Import
Export
Delete
Status
Name
Description
First N

輸入所需資訊。



Network Access Users List > New Network Access User

Network Access User

* Name aaaabbbbcccc

Status ☑ Enabled

Email

Passwords

Password Type: Internal Users

	Password	Re-Enter Password
* Login Password	•••••••••••••	•••••••••••••
Enable Password		

User Information

First Name

Last Name

Account Options

Description

Change password on next login □

Account Disable Policy

□ Disable account if date exceeds 2018-11-09 (yyyy-mm-dd)

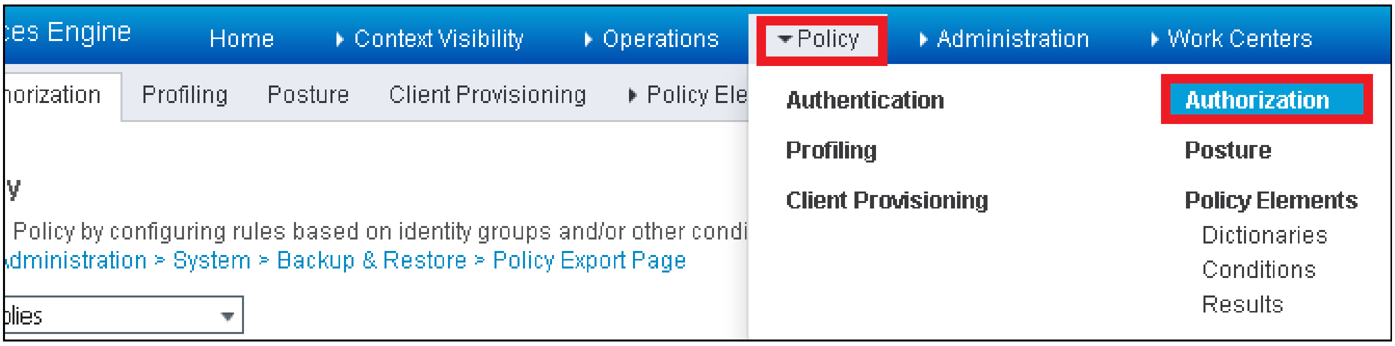
User Groups

AccessPoints

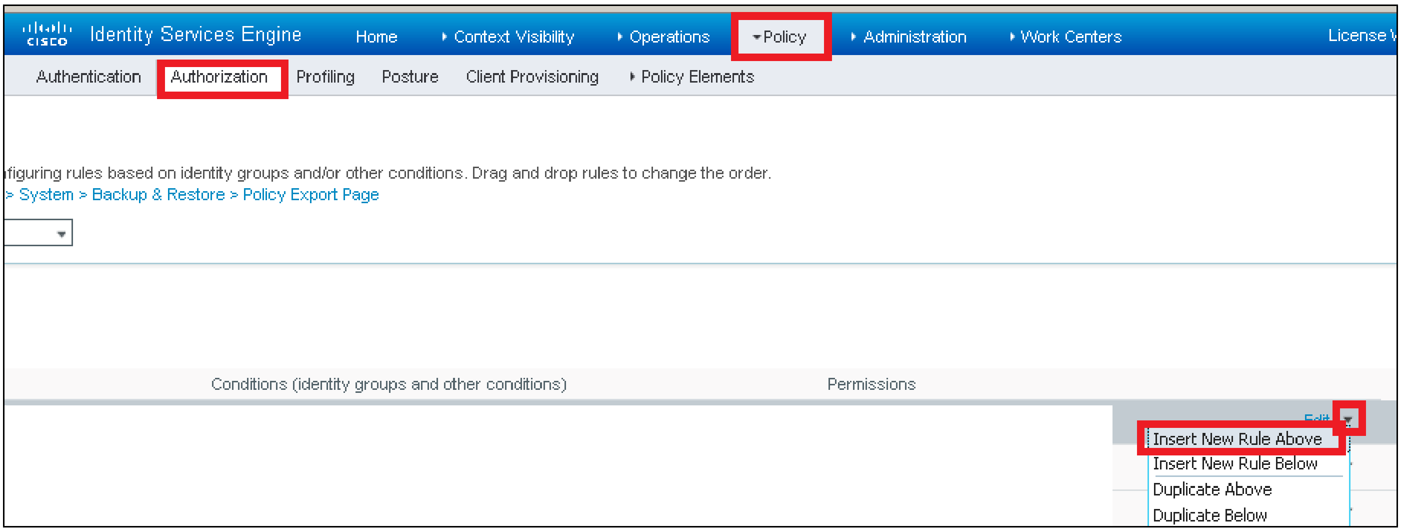
註: Name 和Login Password欄位必須是AP的乙太網MAC地址，全部為小寫且無分隔符。

對AP進行身份驗證的授權策略

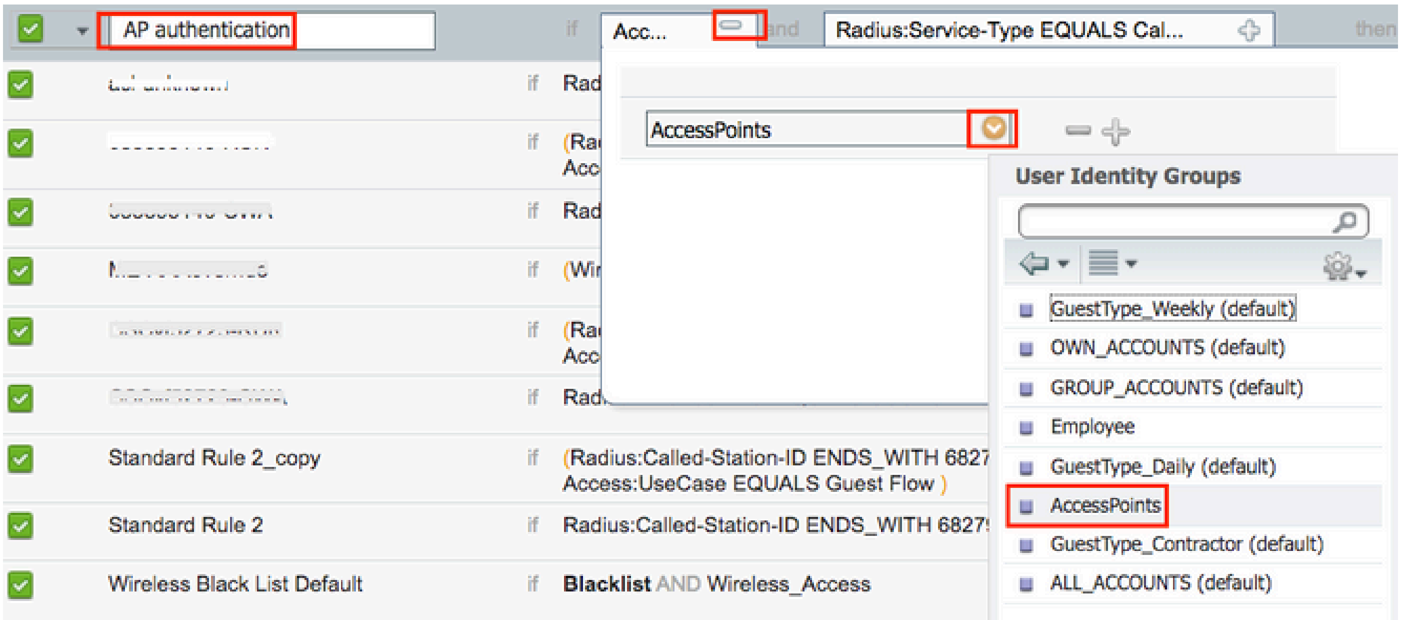
導覽至Policy > Authorization，如下圖所示。



插入新規則，如下圖所示。

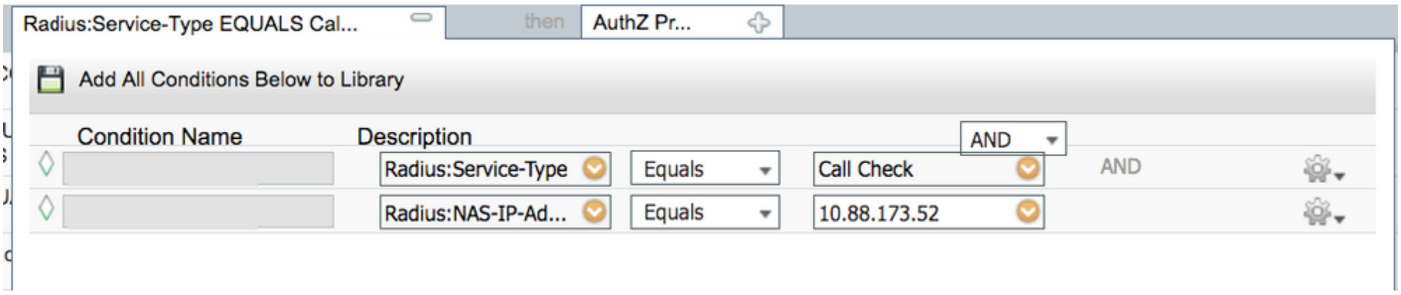


首先，為規則選擇一個名稱，然後為儲存接入點的身份組(AccessPoints)選擇一個名稱。 如果您決定將MAC地址作為使用者名稱密碼進行身份驗證，請選擇User Identity Groups；如果您選擇將AP MAC地址作為端點進行身份驗證，請選擇Endpoint Identity Groups。



AP authentication	if	Acc... and Radius:Service-Type EQUALS Cal...
[redacted]	if	Rad
[redacted]	if	(Ra Acc
[redacted]	if	Rad
[redacted]	if	(Wi
[redacted]	if	(Ra Acc
[redacted]	if	Rad
Standard Rule 2_copy	if	(Radius:Called-Station-ID ENDS_WITH 6827 Access:UseCase EQUALS Guest Flow)
Standard Rule 2	if	Radius:Called-Station-ID ENDS_WITH 6827
Wireless Black List Default	if	Blacklist AND Wireless_Access

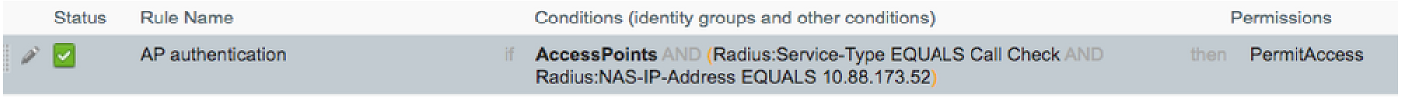
接著，選取讓授權程序符合此規則的其他條件。在本示例中，如果授權進程使用服務型別呼叫檢查，並且身份驗證請求來自IP地址10.88.173.52，則授權進程會命中此規則。


Radius:Service-Type EQUALS Cal... then AuthZ Pr...

Add All Conditions Below to Library

Condition Name	Description			AND	
	Radius:Service-Type	Equals	Call Check	AND	
	Radius:NAS-IP-Ad...	Equals	10.88.173.52		

最後，選擇分配給符合該規則的客戶端的授權配置檔案，單擊Donee並儲存它，如下圖所示。



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	AP authentication	if	AccessPoints AND (Radius:Service-Type EQUALS Call Check AND Radius:NAS-IP-Address EQUALS 10.88.173.52)	then	PermitAccess

注意:已加入控制器的AP不會失去關聯。但是，如果在啟用授權清單後，這些控制器與控制器失去通訊並嘗試重新加入，則它們會執行驗證程式。如果沒有在本地或RADIUS伺服器中列出其MAC位址，則它們無法重新加入控制器。

驗證

驗證9800 WLC是否已啟用ap驗證清單

```
<#root>

# show ap auth-list
```

```
Authorize APs against MAC : Disabled
Authorize APs against Serial Num : Enabled
Authorization Method List : <auth-list-name>
```

驗證radius設定：

```
<#root>

#

show run aaa
```

疑難排解

WLC 9800提供永遠線上的追蹤功能。這可確保持續記錄所有與AP連線相關的錯誤、警告和通知級別消息，並且您可在發生事件或故障情況後檢視其日誌。

註：生成的日誌數量從幾小時到幾天不等。

若要檢視9800 WLC在預設情況下蒐集的追蹤軌跡，您可以透過這些步驟，透過SSH/Telnet連線至9800 WLC（請確保將作業階段記錄到文字檔中）。

步驟 1.檢查控制器當前時間，這樣您就可以跟蹤問題發生時之前的日誌。

```
# 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。如此可快速檢視系統健全狀況和錯誤（如有）。

```
# 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 Trace 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。如此可能會增加記錄量。因此，建議您在未主動偵錯時清除所有條件。

步驟 4.假設在步驟3中未將待測試的mac地址列為條件，收集特定無線電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

如果全天候運作的追蹤未提供充足資訊，使您在調查之下無法判斷問題的觸發原因，則您可啟用條件式偵錯並擷取無線電主動式 (RA) 追蹤，如此可將偵錯層級追蹤提供給所有與指定條件（在此案例中為用戶端 MAC 位址）互動的所有程序。

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。

此指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：若要同時監控多個用戶端，請針對每個 MAC 位址執行 debug wireless mac <aaaa.bbbb.cccc> 指令。

附註：您沒有看到終端作業階段的用戶端活動輸出內容，因為每項內容皆在內部緩衝，稍後才可檢視。

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>
```

當監控時間結束或偵錯無線停止後，9800 WLC 會產生本機檔案，名稱如下：

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。　您可將 ra_trace.log 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

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，因為我們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 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。請聯絡 Cisco TAC 協助剖析此類追蹤。

您可將 ra-internal-FILENAME.txt 複製到外部伺服器，或將輸出內容直接顯示於螢幕上。

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。

參考資料

將網狀無線接入點連線到9800 WLC

關於此翻譯