使用IBNS 2.0和介面模板標準化有線802.1X AP身份驗證

目錄

簡介

本文檔介紹使用IBNS 2.0介面模板的802.1X配置。

問題陳述

使用IEEE 802.1X實現埠安全是常見的最佳實踐。除了提高網路安全性外，它還通過允許在整個網路中實現標準化接入埠配置來簡化交換機部署。

本指南介紹如何將單個標準化交換機埠配置同時用於終端裝置和思科接入點(AP)。 雖然每個交換機埠最初都作為標準接入埠運行，並執行IEEE 802.1X身份驗證，但經過身份驗證的AP根據其部署方

案可能需要不同的運行模式。

特別是，在FlexConnect本地交換模式下運行的AP必須在中繼埠上運行，因為來自多個SSID的客戶端流量在本地進行橋接。因此，成功進行身份驗證後，交換機介面必須動態地從接入埠轉換到中繼埠。

連線基礎設施裝置而不是簡單終端裝置的接入埠通常要求介面配置不同於預設接入埠行為。

因此，在身份驗證過程中必須動態修改交換機介面配置。多年以來，人們已經使用多種方法來實現此行為，包括Auto SmartPorts和嵌入式事件管理器(EEM)小程式。目前，推薦的解決方案是IBNS 2.0 [1]與介面模板結合使用，它提供了一種可擴展的一致方法，用於在成功身份驗證後動態更改介面配置。

方針

要使設定正常工作，必須正確配置各種元件，即

- Radius伺服器（身分識別服務引擎）
- 交換器
- 存取點/無線LAN控制器

由於存在現有文檔（請參閱結尾處的參考資料），我們關注本文檔中的特定場景，並參考現有文檔作為支援材料。

需求

思科建議您瞭解以下主題：

- 無線Lan控制器(WLC)和輕量AP(LAP)
- 思科交換機和ISE上的802.1x
- 可擴充驗證通訊協定(EAP)
- 遠端驗證撥入使用者服務(RADIUS)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

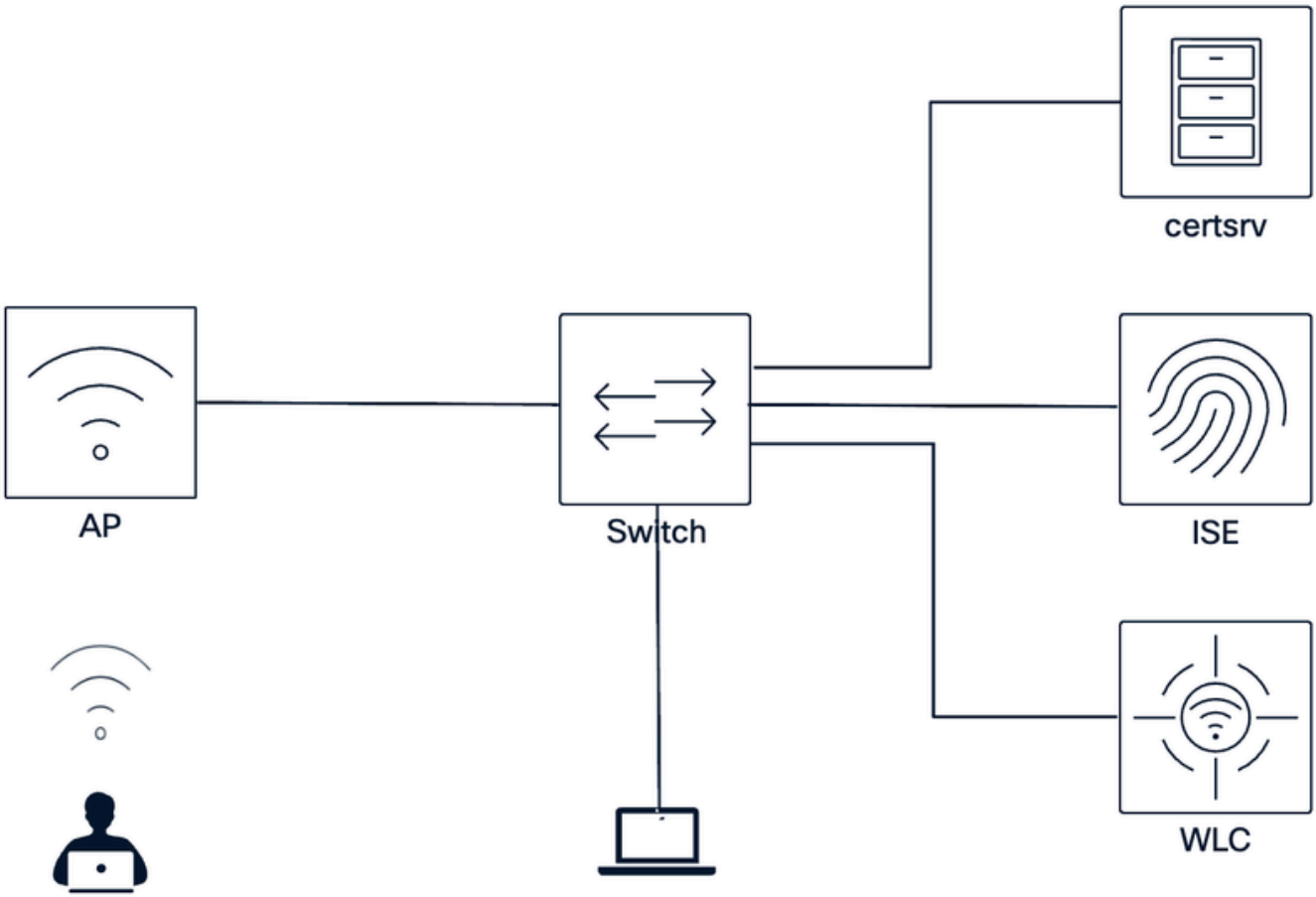
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C9800-40 WLC - IOS XE 26.1.1
- ISE版本3.5補丁1
- AP CW917x、CW916x

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。

配置還記錄在netascode.cisco.com資料模型中，用於交換和ISE，以便輕鬆複製設定。

組態

網路圖表



示例設定

出於我們的目的，我們將重點放在單個場景上，並提供配置片段和逐步指導。由於這一過程中存在各種不同的變體，因此我們指出這些變體並參考現有的文檔來實現此目的。

本指南中涉及的場景：

- 採用EAP-FAST驗證的AP有線Dot1X
- 通過C9800 WLC調配的Dot1X憑證
- AP在Flex Connect本地交換模式下

在此設計中，交換機埠最初使用帶MAB回退的通用閉合模式802.1X配置。在首次登入期間，AP可能沒有802.1X憑證，因此ISE可以通過MAB對AP進行授權，有限的訪問許可權足以到達WLC或Catalyst中心。調配憑證或憑證後，AP會執行有線802.1X驗證。然後ISE返回適用於AP_FLEX_TRUNK介面模板的授權結果，將埠轉換為所需的FlexConnect中繼配置。

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

表 1：概述中的其他變體和選項

AP 組態

要將有線Dot1x身份驗證與您的AP結合使用，您必須首先將憑證和/或證書根據選定的身份驗證方法滾出到AP。

Cisco Catalyst AP Dot1x請求方通常支援EAP-FAST、EAP-PEAP或EAP-TLS。此外，MAB也可以是一個選項，尤其是因為AP需要首先收集能夠執行EAP型別身份驗證的憑證或證書。

- MAB:

    - 無需進行接入點端設定
    - 管理硬體MAC地址需要工具
    - 很容易被偽裝
    - 允許通用埠配置

- EAP-FAST:
    - 基於使用者名稱/密碼
    - 易於推廣
    - 需要在ISE上啟用匿名帶內PAC調配

- EAP-PEAP:
    - 基於使用者名稱/密碼
    - 伺服器驗證需要證書
    - 需要相應地規劃證書續訂

- EAP-TLS:
    - 基於證書
    - 需要相應地規劃證書續訂

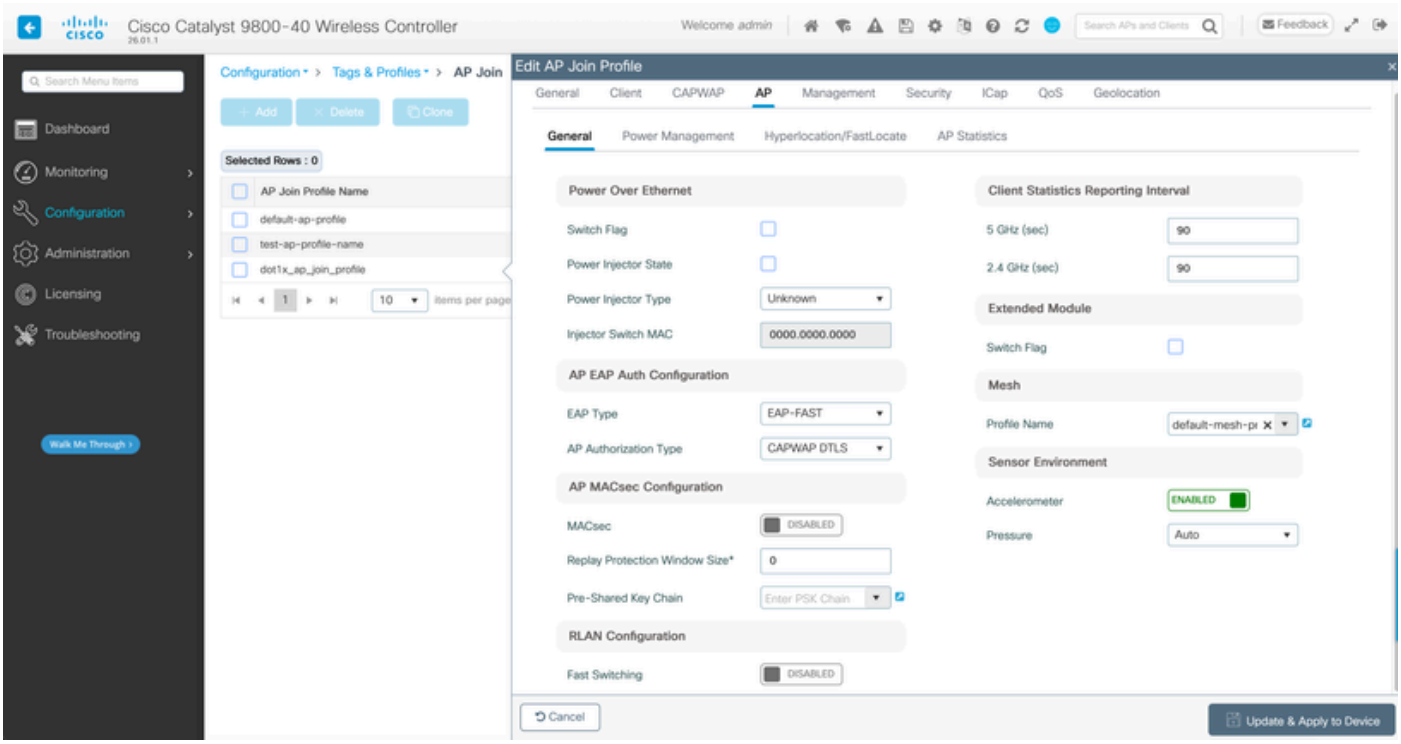
要配置AP有線Dot1X請求方，可通過以下介紹的無線區域網控制器或Catalyst Center實現此目的。在進入這些詳細資訊之前，必須預先選擇您要使用的身份驗證型別。

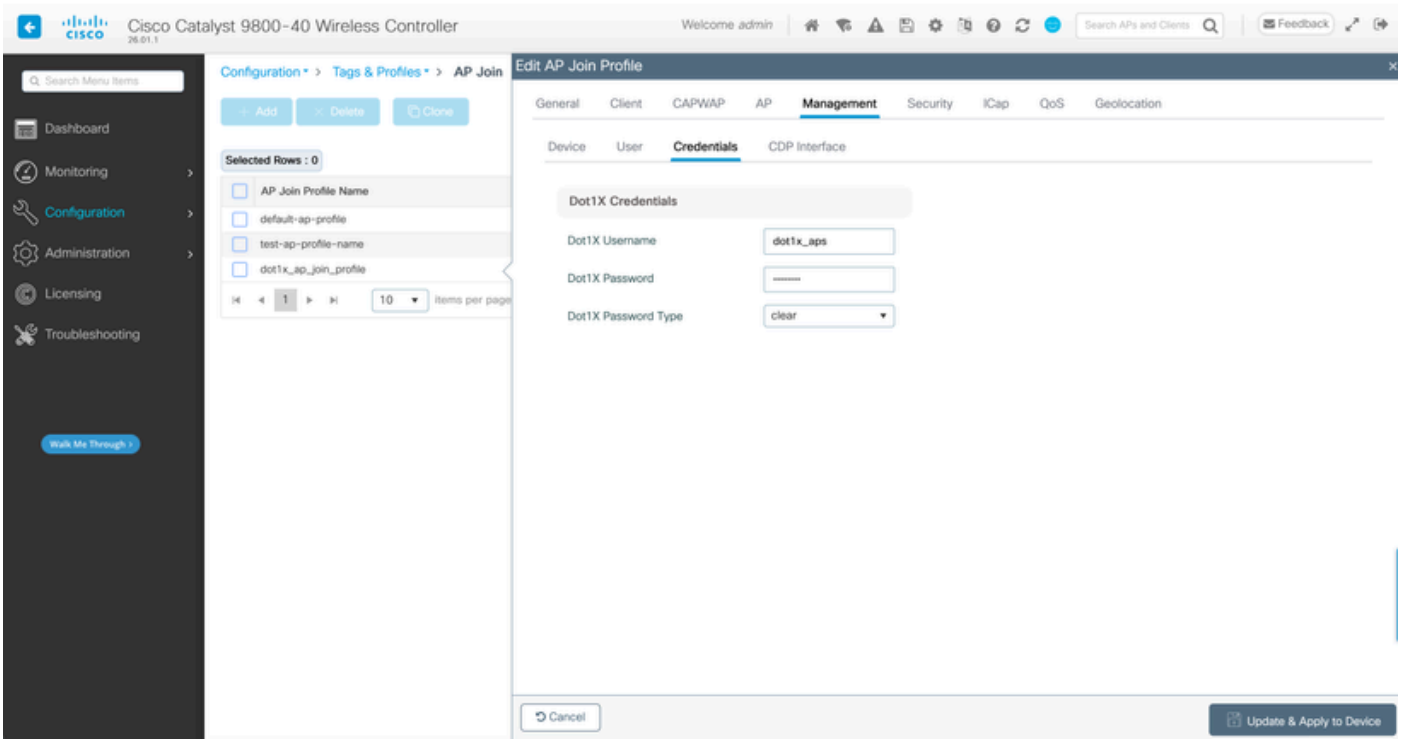
通過Cisco 9800無線LAN控制器設定有線Dot1X

如果您選擇了基於證書的身份驗證(EAP-PEAP或EAP-TLS[1])，則需要確定下一步如何通過SCEP [2]或EST [3]頒發本地重要AP證書(LSC)的方法。

在我們的場景中使用EAP-FAST時，只需生成一個AP加入配置檔案（在其中輸入Dot1X使用者和密碼），將該加入配置檔案繫結到站點標籤並將其分配給AP。

GUI配置





CLI組態

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

通過Catalyst中心即插即用設定有線Dot1X

要使PnP [4]正常工作，需要將Catalyst Center與ISE整合。由於需要證書才能從AP端對使用ISE的EAP身份驗證進行伺服器驗證，因此部分需要此驗證。對於裝置端憑證，AP會收到由Catalyst Center CA頒發的憑證，該憑證預設為自己的內建，或是由各個CA的SubCA/SCEP設定。

通過PnP的設定過程允許在裝置加入WLC之前調配證書和/或憑證。

交換器組態

除了身份驗證是一種安全機制，它也是一種標準化交換機埠配置的方法。因此，這些部分描述了實現此目標所需的要素。這是一個配置示例，必須檢查並調整以適應您的設定。一般情況下，此組態會允許Dot1x和回退MAB正確處理停用Radius案例、重新驗證等。

全域Radius屬性：

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Radius伺服器組：

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
!
!
aaa group server radius client-radius-group
 server name client-radius-server01
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

AAA Config:

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

IBNS2.0類對映和服務模板：

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
```

```
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

IBNS 2.0服務策略：

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
  10 authenticate using mab priority 20
 70 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
!
```

介面模板：

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

介面組態：

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

全域性必填：

```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
```

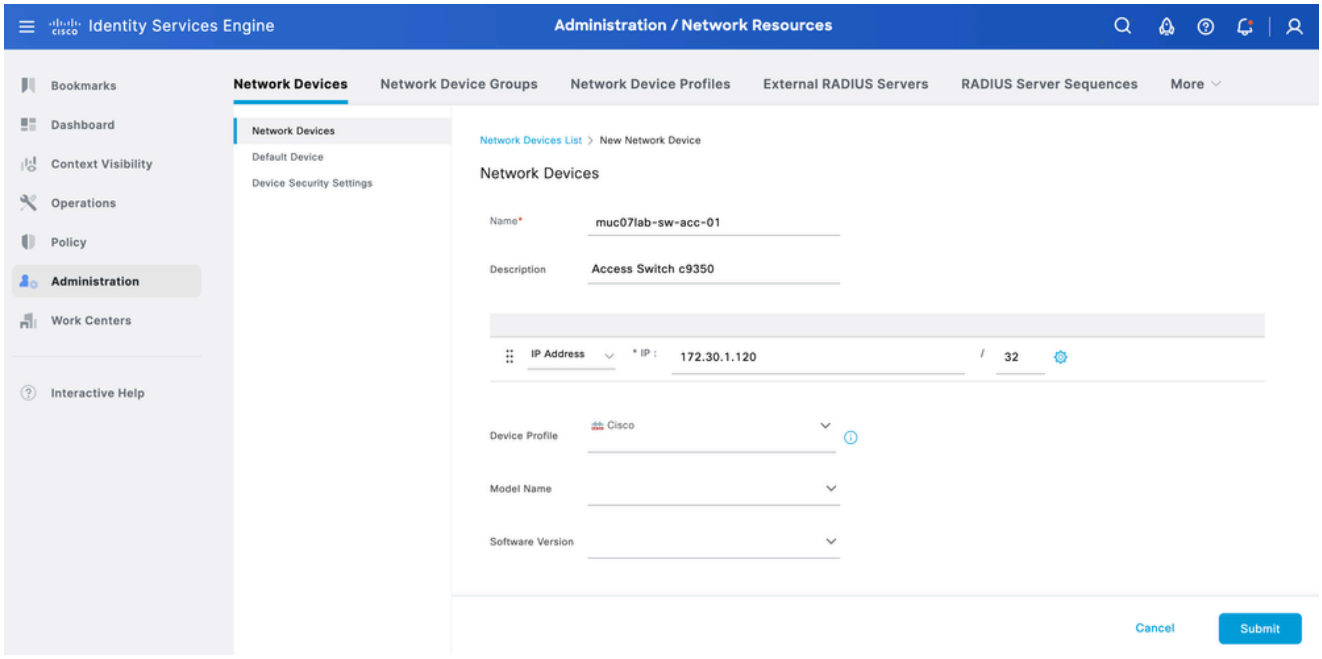
!

附註：使用CW9178時，AP在身份驗證期間提供兩個MAC地址。為了防止交換器連線埠進入err-disabled狀態，一開始必須將連線埠設定為主機模式多重驗證。在802.1X身份驗證成功後，建議將埠配置動態更改為主機模式多主機。

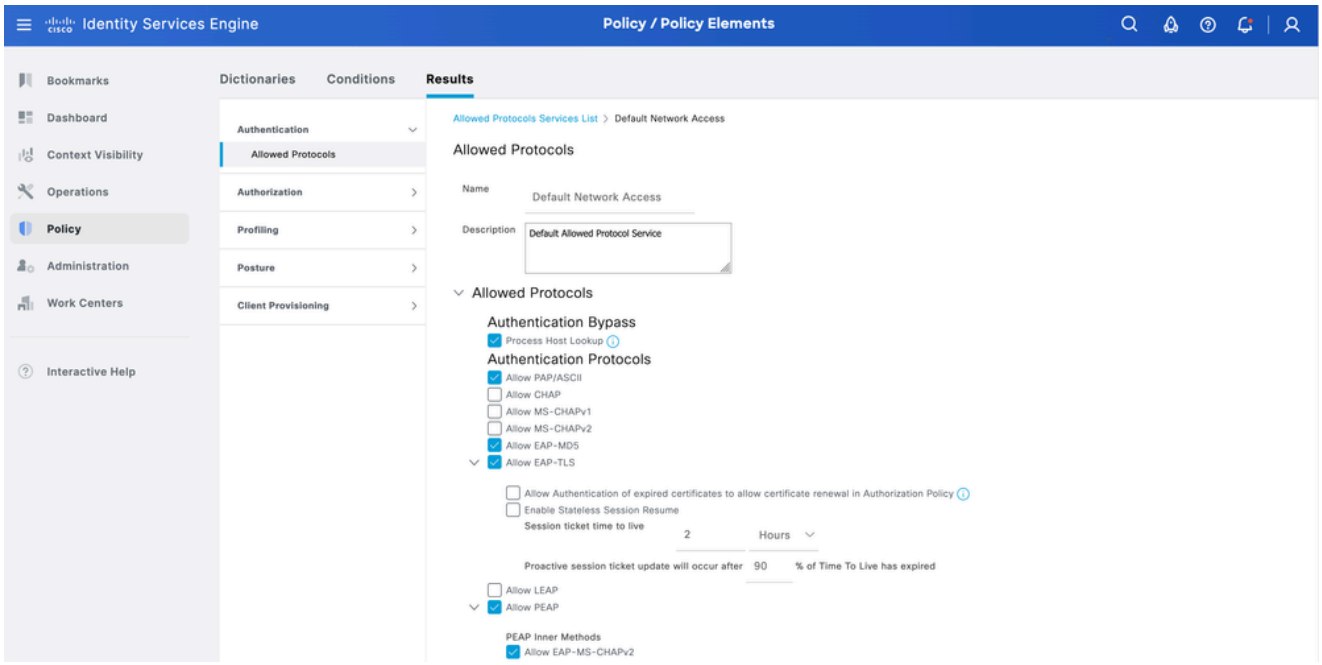
身份服務引擎配置

最後，還需要將RADIUS伺服器配置為允許身份驗證。對於有線Dot1x，有一個廣泛的指南[5],因此我們只關注本例中的相關部分。

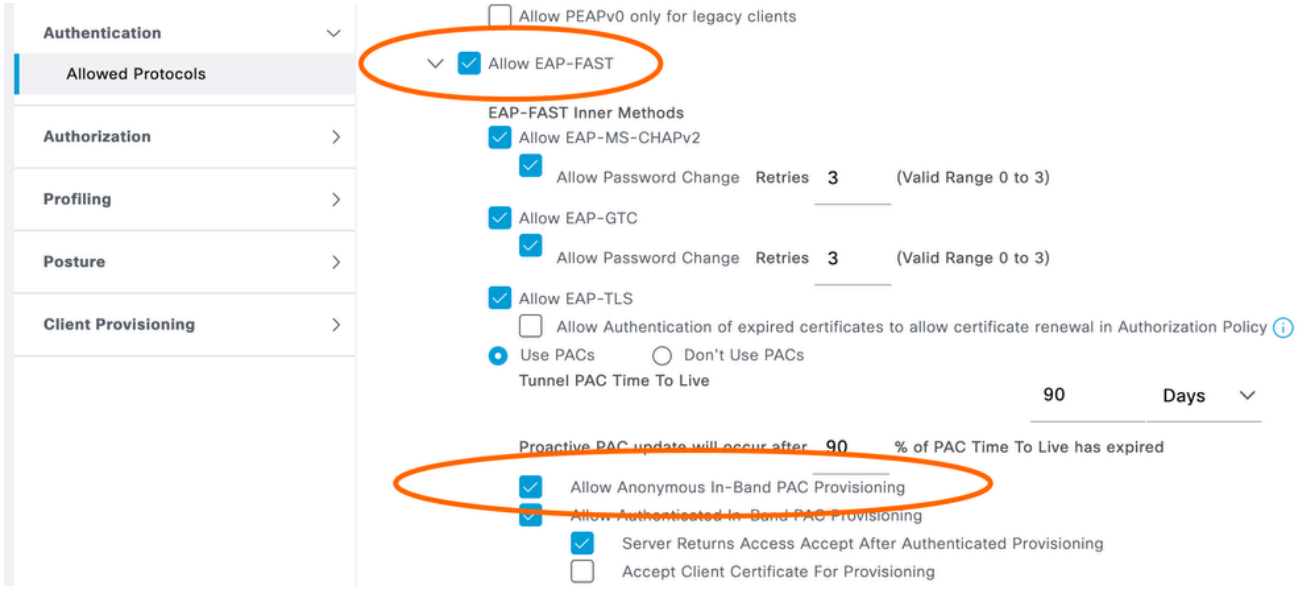
1. 將交換器新增為網路存取裝置：
   >管理>網路資源>網路裝置>新增



2. 啟用您正在使用的EAP協定：
   >策略>策略元素>結果>身份驗證>允許的協定



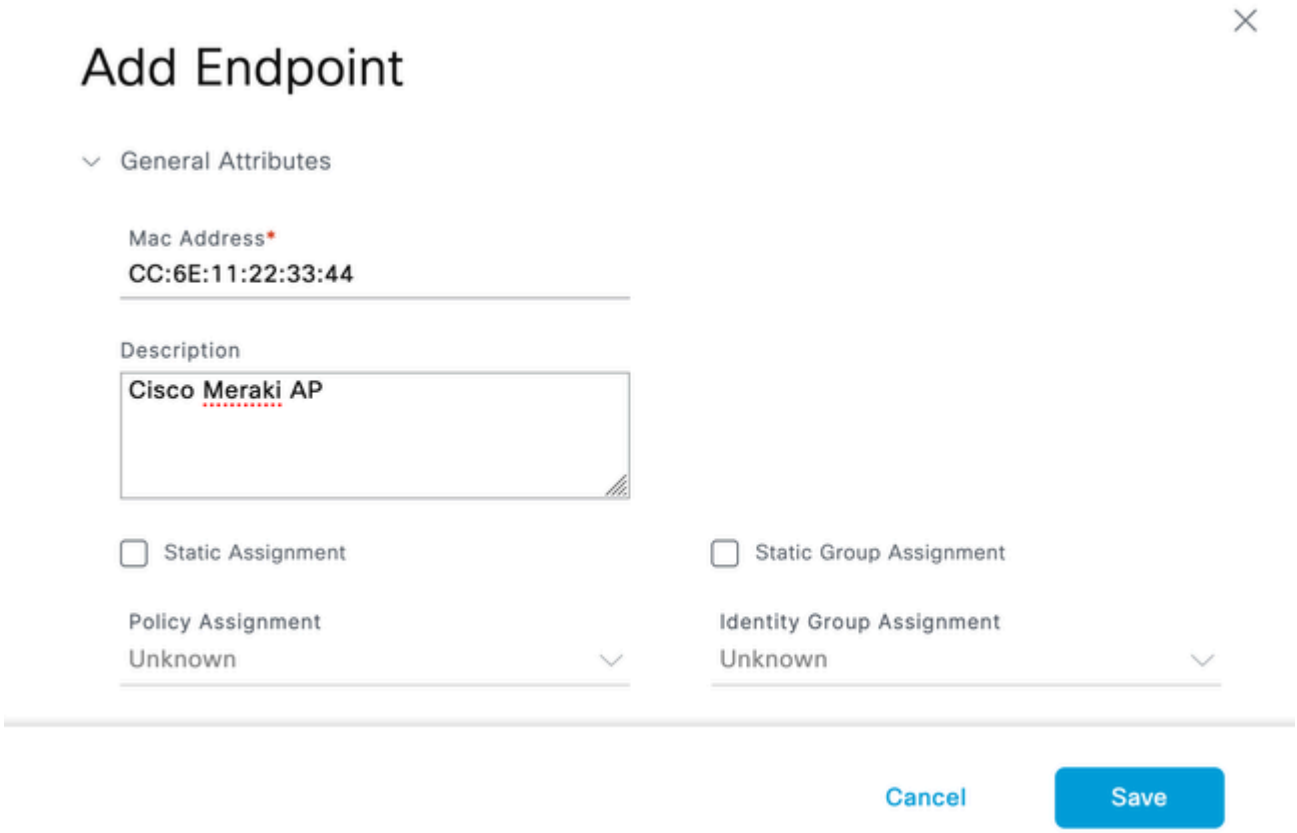
3. 在我們的場景中，正如我們使用EAP-FAST一樣，請記住「匿名帶內PAC調配」必須啟用：



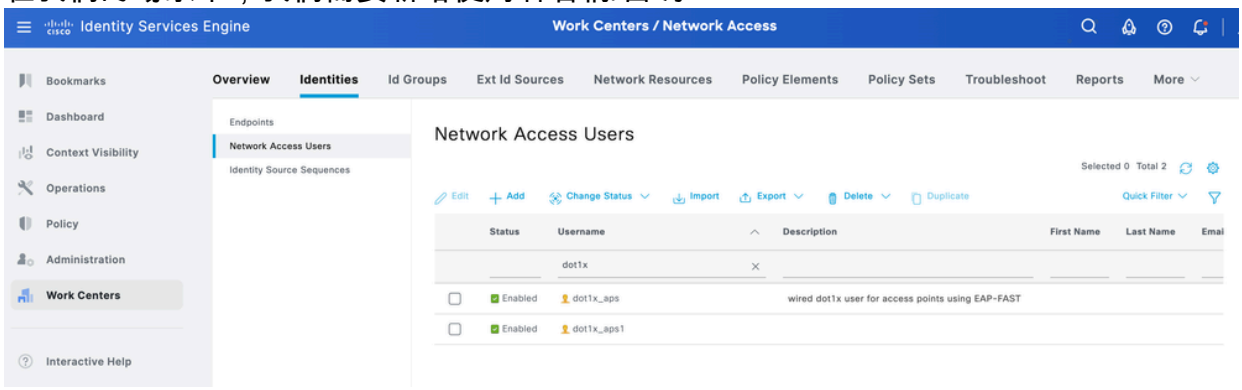
4. 新增標識

>工作中心>網路訪問>身份

a. 為了成功操作，該過程通常包括兩個步驟。最初AP沒有憑證，因此無法響應EAP身份驗證。因此，交換機埠必須首先使用MAB對AP進行身份驗證。這可以基於通用授權策略、基於位置的策略或裝置分析。無論使用哪種策略，初始MAB驗證都必須成功允許AP通過CAPWAP從WLC或通過即插即用(PnP)從Cisco Catalyst Center獲取其憑證。

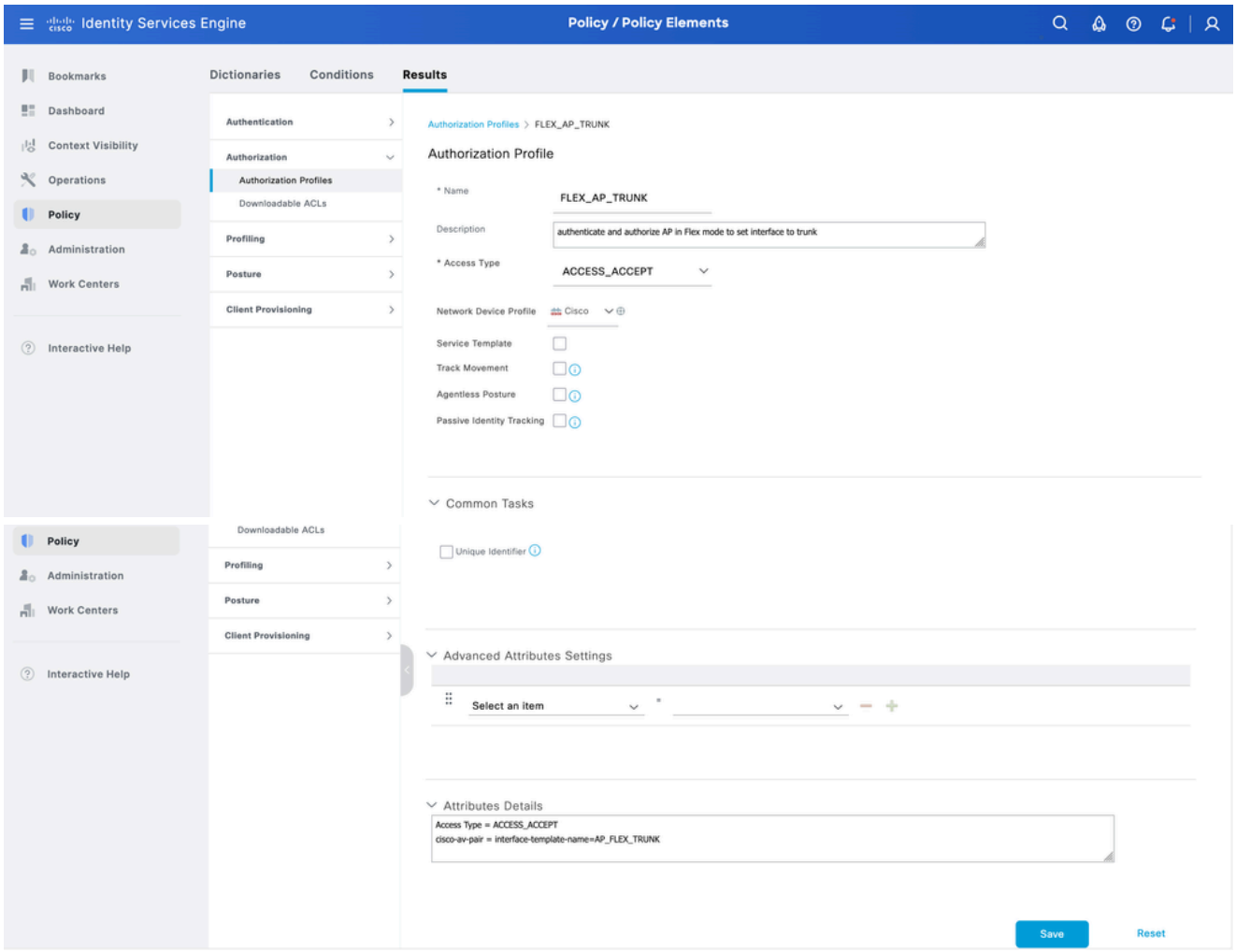


b. AP收集憑證/證書後，AP有線Dot1X請求方將響應EAPoL，Dot1X是啟用AP進行完全訪問的身份驗證的後續方法。
在我們的場景中，我們需要新增使用者名稱/密碼：



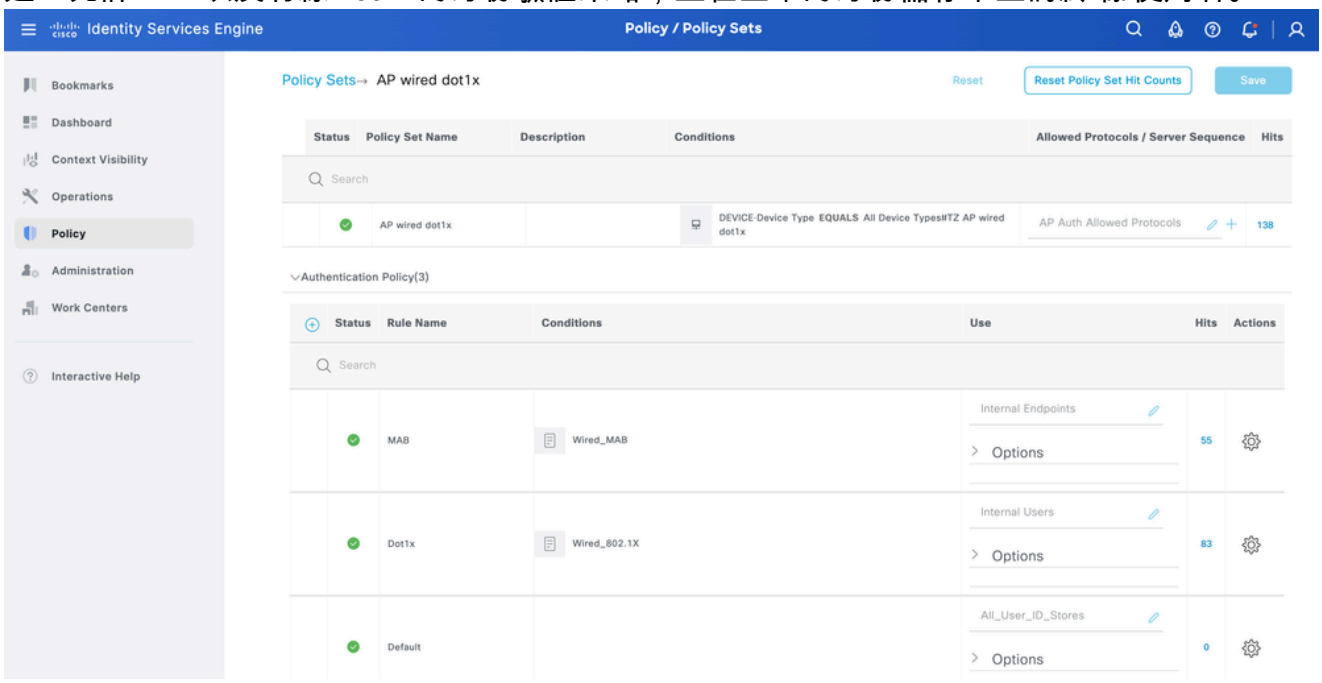
5. 建立授權設定檔
授權配置檔案使用所需的av配對進行響應。在我們動態修改switchport時，需要配置介面模板：
>策略>策略元素>結果>授權>授權配置檔案

名稱:FLEX_AP_TRUNK
訪問型別：ACCESS_ACCEPT
介面模板：AP_FLEX_TRUNK

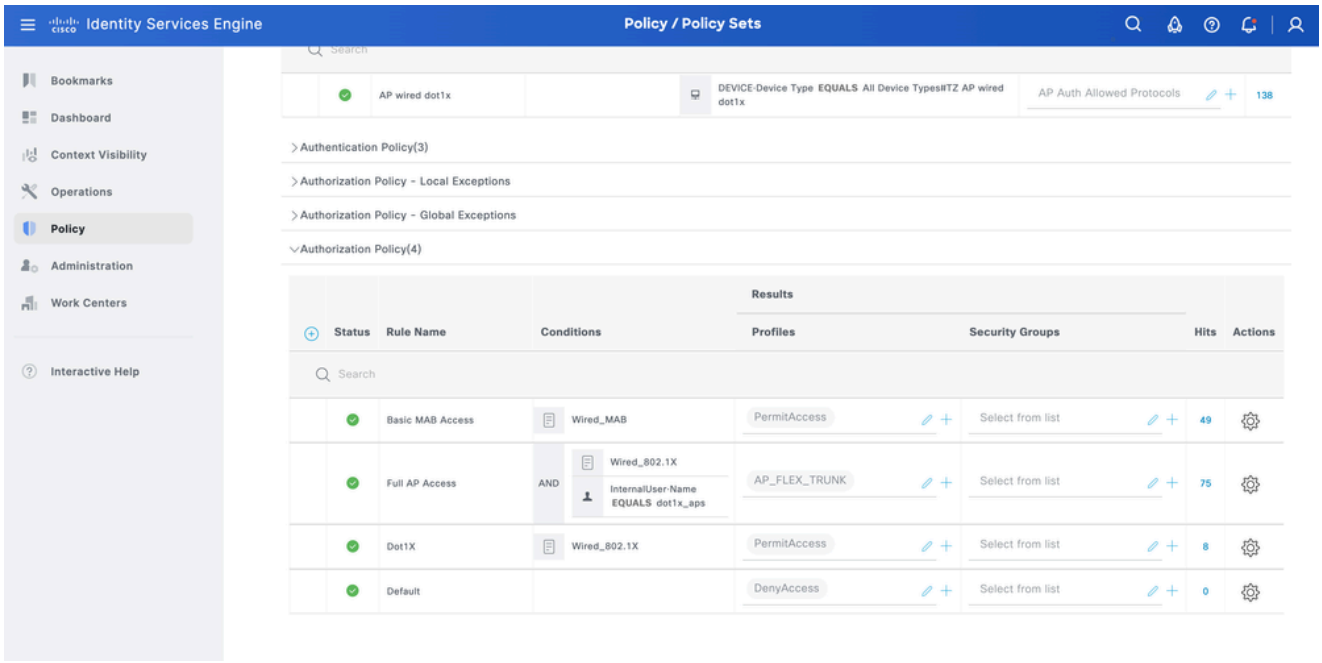


6. 建立授權策略

建立允許MAB以及有線Dot1X的身份驗證策略，並在正確的身份儲存中查詢終端/使用者。



根據您對MAB的需要，輸入有限的訪問授權結果，並輸入完整的AP訪問，包括引用的Dot1x介面模板av配對：



驗證

此配置到位後，將AP連線到交換機。作為前提條件，我們預期接入VLAN中的預設網路設定（在本例中帶有選項43的DHCP池指向WLC，並且AP可以與WLC進行CAPWAP通訊）是可能的。

AP命令

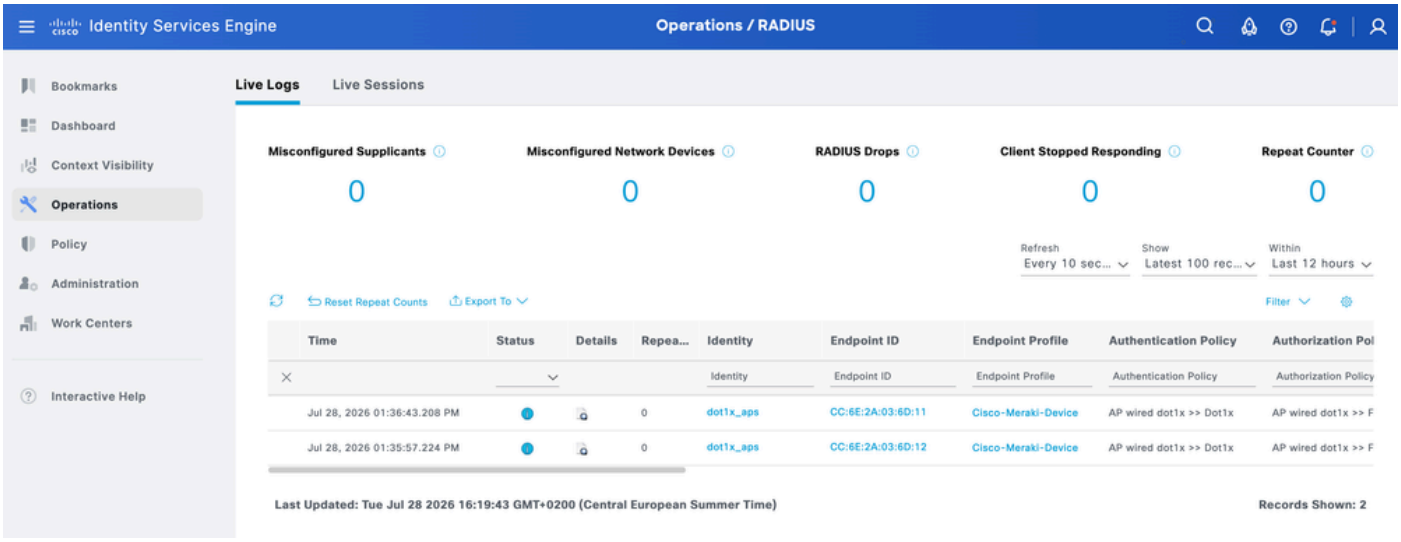
```
show ap authentication status
show crypto
show crypto pki trustpool
```

交換機命令

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
Interface MAC Address Method Domain Status Fg Session ID
-----------------------------------------------------------------------------------------
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



縮寫詞清單

縮寫	擴展
AAA	驗證、授權及記帳
AP	存取器
AuthC	驗證
AuthZ	Authorization
CA	證書頒發機構
CISP	使用者端資訊訊號通訊協定
Dot1x	IEEE 802.1X
EAP	可擴充驗證通訊協定
EST	通過安全傳輸註冊
快速	透過安全通道進行彈性驗證
IBNS	基於身份的網路服務
ISE	身分識別服務引擎
MAB	MAC身份驗證繞行
NAD	網路存取裝置
PEAP	受保護的可擴展身份驗證協定
SCEP	簡單憑證註冊通訊協定
TLS	傳輸層安全

WLC	無線LAN控制器

參考資料

[1]在AP上為PEAP或使用LSC的EAP-TLS配置802.1X

[2]為9800 WLC上的本地重要憑證布建設定SCEP

[3]思科無線EST內部部署指南

[4]安全AP自註冊 — 增強型網路安全簡介

[5] ISE安全有線訪問規範部署指南

[6] LSC配置指南部分

[7]配置9800控制器用於接入點的802.1X請求方

[8]使用Dot1x保護Flexconnect AP交換機埠

[9] Cisco Catalyst 9800系列無線控制器軟體配置指南，Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Center使用手冊，版本3.2.x — 為Cisco IOS XE裝置的AP配置檔案配置管理設定

[12]使用IBNS 2.0和介面模板進行預設交換機埠配置

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）。