

使用9800控制器為接入點配置802.1X Supplicant客戶端

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[將LAP配置為802.1x請求方](#)

[如果AP已加入到WLC:](#)

[如果AP尚未加入WLC:](#)

[設定交換器](#)

[配置ISE伺服器](#)

[驗證](#)

[驗證驗證驗證型別](#)

[驗證交換機埠上的802.1x](#)

[疑難排解](#)

簡介

本檔案介紹如何將思科存取點(AP)設定為要在針對RADIUS伺服器的交換器連線埠上授權的802.1x要求者。

必要條件

需求

思科建議您瞭解以下主題：

- 無線Lan控制器(WLC)和LAP (輕量型存取點)。
- 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：

- WS-C3560CX、Cisco IOS® XE、15.2(3r)E2

- C9800-CL-K9,Cisco IOS® XE , 17.6.1
- ISE 3.0
- AIR-CAP3702
- AIR-AP3802

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。

背景資訊

在此設定中，接入點(AP)充當802.1x請求方，並由交換機針對ISE使用EAP方法EAP-FAST進行身份驗證。

在連線埠設定為802.1X驗證後，在連線到連線埠的裝置成功進行驗證之前，交換器不會允許802.1X流量以外的任何流量通過該連線埠。

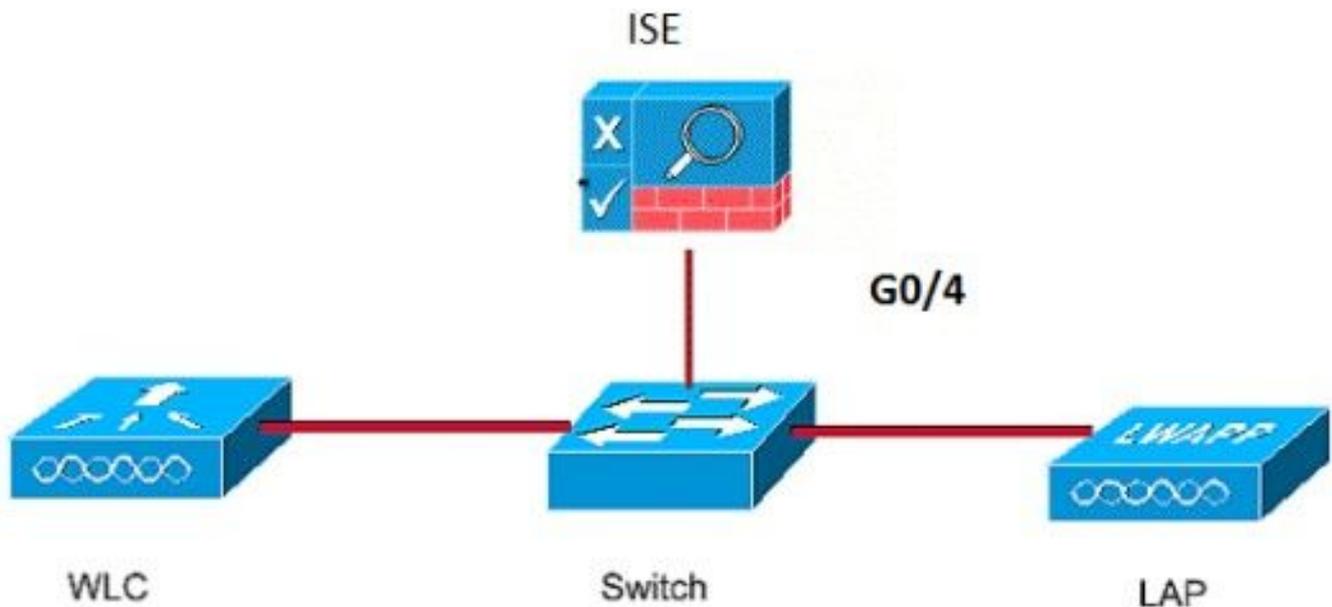
AP可以在加入WLC之前或加入WLC之後進行驗證，在這種情況下，您可以在LAP加入WLC之後在交換器上設定802.1X。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



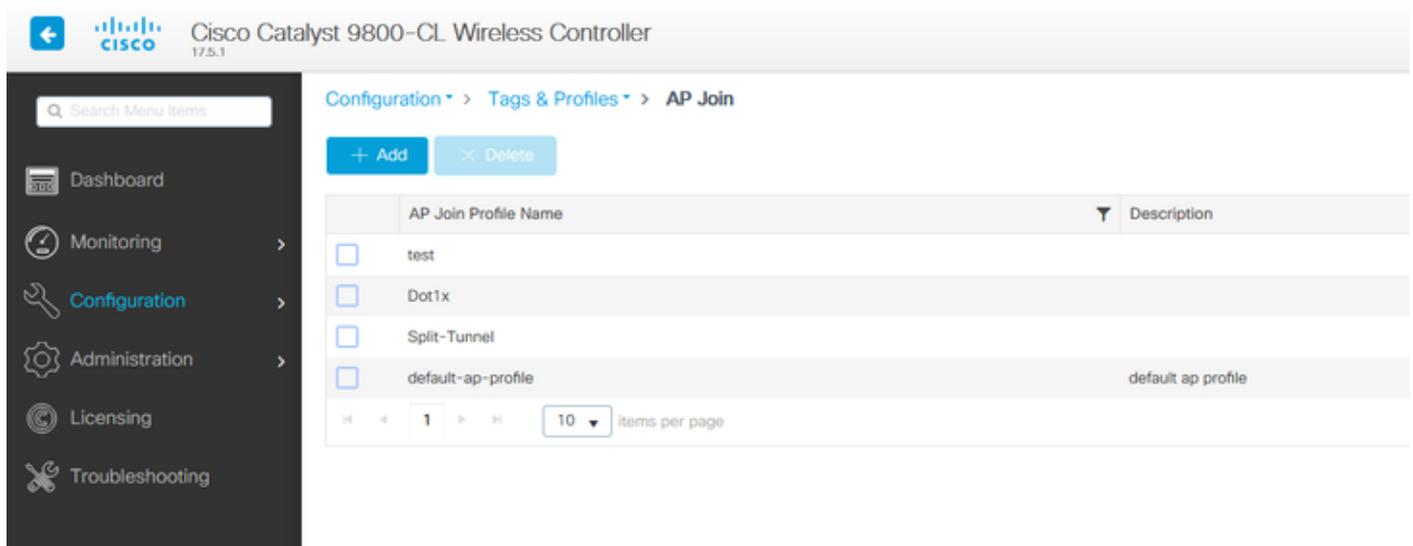
將LAP配置為802.1x請求方

如果AP已加入到WLC:

設定802.1x驗證型別和本地重要憑證(LSC)AP驗證型別：

步驟1.在AP Join Profile頁面上，導航至Configuration > Tags & Profiles > AP Join > On the AP Join Profile，點選Add以新增新加入配置檔案，或在點選AP加入配置檔名稱時編輯該加入配置檔案

。



步驟2.在AP Join Profile頁面中，從AP > General導航至AP EAP Auth Configuration部分。從EAP Type下拉選單中，選擇EAP型別作為EAP-FAST、EAP-TLS或EAP-PEAP，以配置dot1x身份驗證型別。

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type Unknown ▾

Injector Switch MAC 00:00:00:00:00:00

AP EAP Auth Configuration

EAP Type EAP-FAST ▾

AP Authorization Type

- EAP-FAST
- EAP-TLS
- EAP-PEAP

Client Statistics Reporting Interval

5 GHz (sec) 90

2.4 GHz (sec) 90

Extended Module

Enable

Mesh

Profile Name mesh-profile ▾ [Clear](#)

↶ Cancel 📄 Update & Apply to Device

步驟3.從AP Authorization Type下拉選單中，選擇型別為CAPWAP DTLS +或CAPWAP DTLS >按一下Update & Apply to Device。

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

AP EAP Auth Configuration

EAP Type

AP Authorization Type

- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

Extended Module

Enable

Mesh

Profile Name [Clear](#)

配置802.1x使用者名稱和密碼：

步驟1.從Management > Credentials > Enter Dot1x username and password details >選擇適當的802.1x密碼型別>按一下Update & Apply to Device

Edit AP Join Profile ×

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

Dot1x Credentials

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

如果AP尚未加入WLC:

您必須通過控制檯連線到LAP，才能設定憑據並使用以下CLI命令：(對於Cheetah OS和Cisco IOS® AP)

CLI:

```
LAP# debug capwap console cli  
LAP# capwap ap dot1x username
```

清除AP上的Dot1x認證 (如果需要)

對於Cisco IOS® AP，重新載入AP之後：

CLI:

```
LAP# clear capwap ap dot1x
```

對於Cisco COS AP，重新載入AP之後：

CLI:

```
LAP# capwap ap dot1x disable
```

設定交換器

在交換機上全域性啟用dot1x並將ISE伺服器新增到交換機。

CLI:

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

配置AP交換機埠

CLI:

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

如果AP處於Flex Connect模式，即本地交換，則必須在交換機介面上進行額外配置，以允許埠上有多個MAC地址，因為客戶端流量在AP級別釋放：

```
authentication host-mode multi-host
```

注意：意味著讀者要注意。註釋包含有用的建議或文檔未涵蓋的材料的引用。

注意：多主機模式對第一個MAC地址進行身份驗證，然後允許無限數量的其他MAC地址。如果已連線的AP已配置為本地交換模式，請在交換機埠上啟用主機模式。這允許使用者端的流量通過交換器連線埠。如果您需要安全的流量路徑，請在WLAN上啟用dot1x以保護客戶端資料

配置ISE伺服器

步驟1. 將交換機新增為ISE伺服器上的網路裝置。導覽至Administration > Network Resources > Network Devices > Click Add > Enter Device name , IP address , enable RADIUS Authentication Settings , Specify Shared Secret Value , COA port (或保留為預設值) > Submit。

The screenshot displays the Cisco ISE Administration interface for configuring a new network device. The breadcrumb navigation is Administration > Network Resources > Network Devices > New Network Device. The 'RADIUS Authentication Settings' section is expanded and highlighted with a red box. The configuration includes:

- Device Name: MySwitch
- IP Address: 10.48.39.100 / 32
- Device Profile: Cisco
- Location: All Locations (Set To Default)
- Is IPSEC Device: (Set To Default)
- Device Type: All Device Types (Set To Default)
- RADIUS Authentication Settings
 - Protocol: RADIUS
 - Shared Secret: (masked) (Show)
 - Use Second Shared Secret:
 - CoA Port: 1700 (Set To Default)
 - RADIUS DTLS Settings: (Info icon)
 - DTLS Required:
 - Shared Secret: radius/dtls (Info icon)

步驟2. 將AP憑證新增到ISE。導航到Administration > Identity Management > Identities > Users，然後點選Add按鈕以新增使用者。您需要在此處輸入在WLC的AP加入配置檔案中配置的憑據。請注意，使用者在此置入預設組，但可根據要求進行調整。

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users
Latest Manual Network Scan Res...

Network Access User

Name dot1x

Status Enabled

Email

Passwords

Password Type: Internal Users

Password Re-Enter Password

Login Password

Generate Password

Enable Password

User Information

Account Options

Account Disable Policy

User Groups

ALL_ACCOUNTS (default)

步驟3.在ISE上，配置身份驗證策略和授權策略。轉至Policy > Policy Sets，選擇要配置的策略集和右側的藍色箭頭。在這種情況下，會使用預設策略集，但可以根據要求自定義該策略集。

Cisco ISE Policy - Policy Sets

Evaluation Mode 60 Days

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	6		

Reset Save

然後配置身份驗證策略和授權策略。此處顯示的策略是在ISE伺服器上建立的預設策略，但可以根據需要進行調整和自定義。

在此示例中，配置可以轉換為：「如果使用有線802.1X並在ISE伺服器上知道使用者，則我們允許訪問身份驗證成功的使用者」。然後AP將獲得針對ISE伺服器的授權。

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
<input checked="" type="checkbox"/>	MAB	Wired_MAB Wireless_MAB	Internal Endpoints	0	
<input checked="" type="checkbox"/>	Dot1X	Wired_802.1X Wireless_802.1X	All_User_ID_Stores	6	
<input checked="" type="checkbox"/>	Default		All_User_ID_Stores	0	

Authorization Policy (12)		Results				
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	Select from list	6	⚙️
●	Default		DenyAccess x	Select from list	0	⚙️

步驟4.確保在允許的「預設網路訪問」協定中允許EAP-FAST。導航至Policy > Policy Elements > Authentication > Results > Allowed Protocols > Default Network Access> Enable EAP-TLS > Save。

The screenshot shows the Cisco ISE interface for configuring the 'Default Network Access' policy element. The 'Results' tab is active, and the 'Allowed Protocols' section is expanded. Under 'Authentication Protocols', the 'Allow EAP-TLS' checkbox is checked and highlighted with a red arrow. Other protocols like PAP, CHAP, and PEAP are also listed with their respective checkboxes.

驗證

使用本節內容，確認您的組態是否正常運作。

驗證驗證驗證型別

show命令顯示AP配置檔案的身份驗證資訊：

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

範例：

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
```

```
...
Dot1x EAP Method      : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE     : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

驗證交換機埠上的802.1x

show命令會顯示交換器連線埠上802.1x的驗證狀態：

CLI:

```
Switch# show dot1x all
```

輸出示例：

```
Sysauthcontrol          Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                        = AUTHENTICATOR
QuietPeriod                = 60
ServerTimeout              = 0
SuppTimeout                = 30
ReAuthMax                  = 2
MaxReq                      = 2
TxPeriod                    = 30
```

驗證連線埠是否已通過驗證

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

輸出示例：

```
Dot1x Info for GigabitEthernet0/8
-----
PAE                        = AUTHENTICATOR
QuietPeriod                = 60
ServerTimeout              = 0
SuppTimeout                = 30
ReAuthMax                  = 2
MaxReq                      = 2
TxPeriod                    = 30

Dot1x Authenticator Client List
-----
EAP Method                  = FAST
Supplicant                  = f4db.e67e.dd16
Session ID                  = 0A30279E00000BB7411A6BC4
  Auth SM State              = AUTHENTICATED
  Auth BEND SM State         = IDLE
ED
Auth BEND SM State = IDLE
```

在 CLI 上：

Switch#show authentication sessions

輸出示例：

```
Interface    MAC Address    Method  Domain  Status Fg Session ID
Gi0/8       f4db.e67e.dd16 dot1x   DATA   Auth    0A30279E00000BB7411A6BC4
```

在ISE中，選擇Operations > Radius Livelogs，並確認身份驗證成功並且推送了正確的授權配置檔案。

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	✓	🔒		dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access			nschyns-SW-...	FastEther
Nov 28, 2022 08:33:34.4...	✓	🔒		dot1x	A4:53:0E:37:A1:...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess		nschyns-SW-...	FastEther

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. 輸入ping命令以檢查是否可從交換機訪問ISE伺服器。
2. 確保將交換機配置為ISE伺服器上的AAA客戶端。
3. 確保交換機和ISE伺服器之間的共用金鑰相同。
4. 檢查ISE伺服器上是否啟用了EAP-FAST。
5. 檢查802.1x憑證是否為LAP配置且在ISE伺服器上相同。

注意：使用者名稱和密碼區分大小寫。

6. 如果驗證失敗，請在交換器上輸入以下命令：**debug dot1x**和**debug authentication**。

請注意，基於Cisco IOS的接入點(802.11ac wave 1)不支援TLS版本1.1和1.2。如果您的ISE或RADIUS伺服器配置為僅允許802.1X內部的TLS 1.2，則可能導致問題。

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）。