

# 設定無線區域網路控制器中的有線訪客驗證和疑難排解

## 目錄

---

---

## 簡介

本文說明如何使用外部Web驗證在9800和IRCM中設定、驗證和疑難排解有線訪客存取。

## 必要條件

### 需求

思科建議您瞭解以下主題：

9800 WLC

AireOS WLC

行動通道

ISE

假設在設定有線訪客存取之前，已在兩個WLC之間建立行動通道。

此方面不在本組態範例範圍內。有關詳細說明，請參閱附件標題為[在9800上配置移動拓撲](#)的檔案

### 採用元件

9800 WLC版本17.12.1

5520 WLC版本8.10.185.0

ISE版本3.1.0.518

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。

## 在錨定到另一個catalyst 9800的catalyst 9800上配置有線訪客

### 網路圖表



網路拓撲

## 外部9800 WLC上的配置

### 配置Web引數對映

第1步：導航到配置>安全> Web身份驗證，選擇全局，驗證控制器的虛擬IP地址和信任點對映，並確保將型別設定為webauth。

Configuration > Security > Web Auth

**Edit Web Auth Parameter**

Parameter Map Name: global

Maximum HTTP connections: 100

Init-State Timeout(secs): 120

Type: webauth

Captive Bypass Portal:

Disable Success Window:

Disable Logout Window:

Disable Cisco Logo:

Sleeping Client Status:

Sleeping Client Timeout (minutes): 720

Virtual IPv4 Address: 192.0.2.1

Trustpoint: TP-self-signed-3...

Virtual IPv4 Hostname:

Virtual IPv6 Address: :::::X

Web Auth intercept HTTPs:

Enable HTTP server for Web Auth:

Disable HTTP secure server for Web Auth:

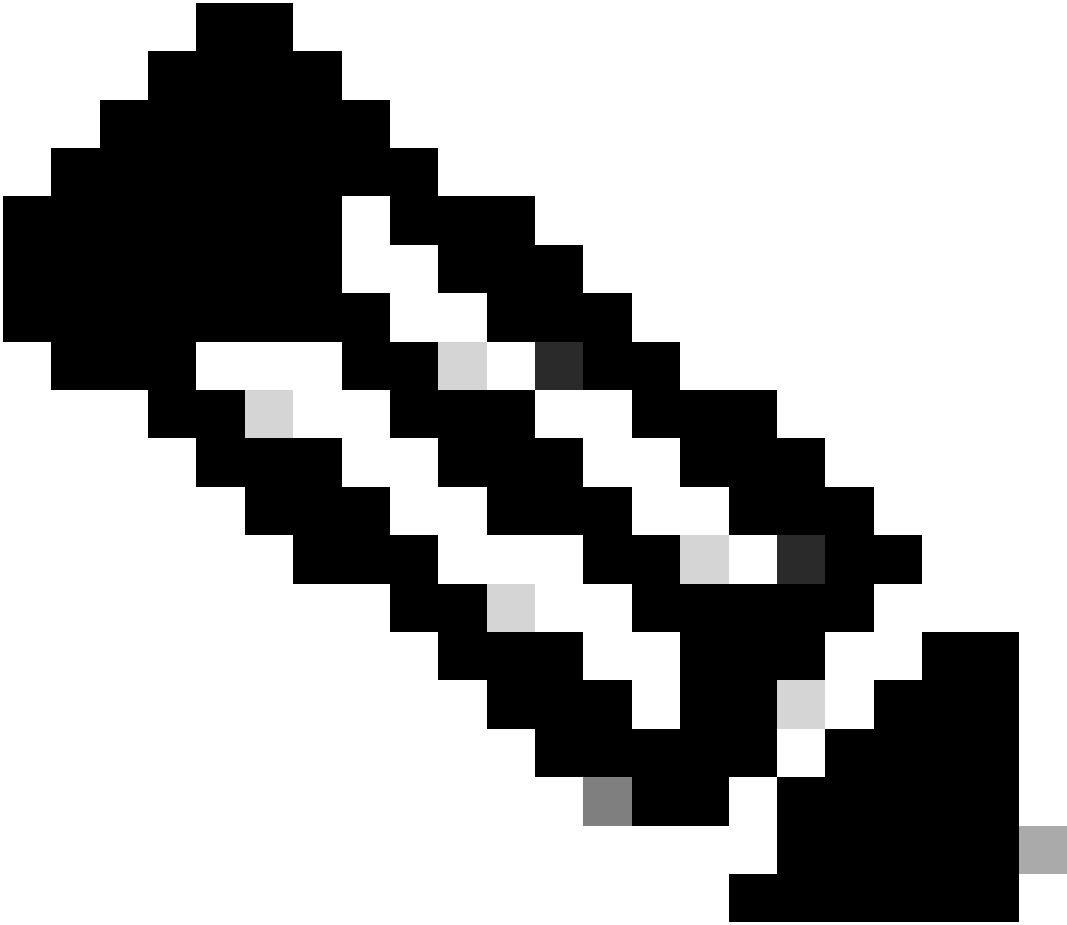
**Banner Configuration**

Banner Title:

Banner Type:  None  Banner Text

全局引數對映

---



附註：Web Auth intercept HTTPs是選用設定。如果需要HTTPS重新導向，則必須啟用Web Auth攔截HTTPS選項。但是，不建議使用此配置，因為它會增加CPU使用率。

---

第2步：在高級頁籤下，配置客戶端重定向的外部網頁URL。設定「Redirect URL for Login」和「Redirect On-Failure」；「Redirect On-Success」是選用的。設定後，重新導向URL的預覽會顯示在Web Auth設定檔上。

**i** Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	X::X::X::X

進階標籤

### CLI配置

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

附註：在此案例中，會使用全域引數對應。根據要求，選取新增來設定自訂Web引數對應，並在「進階」標籤下設定重新導向URL。信任點和虛擬IP設定從全局配置檔案繼承。

AAA設定：

步驟1：建立Radius伺服器：

導航到Configuration > Security > AAA，按一下Server/Group部分下的「Add」，然後在「Create AAA Radius Server」頁中輸入伺服器名稱、IP地址和共用金鑰。

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Name\*' and 'Server Address\*' fields are highlighted with a red box. The 'Key Type' dropdown is set to 'Clear Text'. The 'Key\*' and 'Confirm Key\*' fields are also highlighted with a red box. The 'Support for CoA' checkbox is checked and labeled 'ENABLED'. The 'Automate Tester' checkbox is unchecked. The 'Apply to Device' button is visible at the bottom right.

Radius伺服器配置

## CLI配置

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

第2步：建立RADIUS伺服器組：

在「伺服器群組」段落下選取「新增」以定義伺服器群組，並切換要包含在群組組態中的伺服器。

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

[Servers / Groups](#)   [AAA Method List](#)   [AAA Advanced](#)

[+ Add](#)   [× Delete](#)

**RADIUS**

[Servers](#)   [Server Groups](#)

### Create AAA Radius Server Group

Name\*  ! Name is required

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance  DISABLED

Source Interface VLAN ID

Available Servers      Assigned Servers

Radius伺服器組

## CLI配置

```

aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5

```

第3步：配置AAA方法清單：

導航到AAA Method List頁籤，選擇Authentication下的Add，定義Type為「login」且Group type為

「Group」的方法清單名稱，並在Assigned Server Group部分下對映配置的身份驗證伺服器組。

Configuration > Security > AAA Show Me How

+ AAA Wizard

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

+ Add × Delete

Quick Setup: AAA Authentication

Method List Name\* ISE-List

Type\* login ⓘ

Group Type group ⓘ

Fallback to local

Available Server Groups

- tacacs1
- undefined
- Radius-Group
- Test-group
- test-group
- undefined
- tacacs1

Assigned Server Groups

- ISE-Group

驗證方法清單

## CLI配置

```
aaa authentication login ISE-List group ISE-Group
```

## 配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略，在常規頁籤中命名您的新配置檔案，並使用狀態切換啟用它。

+ Add

× Delete

Clone

## Add Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile

## General

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

GuestLANPolicy

Description

Enter Description

Status

ENABLED 

Passive Client

 DISABLED

IP MAC Binding

ENABLED 

Encrypted Traffic Analytics

 DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

## WLAN Switching Policy

Central Switching

ENABLED 

Central Authentication

ENABLED 

Central DHCP

ENABLED 

Flex NAT/PAT

 DISABLED

策略配置檔案

第2步：在訪問策略頁籤下，在錨點控制器上完成vlan對映時分配隨機vlan。在本例中，配置了vlan 1



RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

**WLAN Local Profiling**

Global State of Device Classification Disabled ⓘ

Local Subscriber Policy Name  ⓘ

**VLAN**

VLAN/VLAN Group  ⓘ

Multicast VLAN

**WLAN ACL**

IPv4 ACL  ⓘ

IPv6 ACL  ⓘ

**URL Filters** ⓘ

Pre Auth  ⓘ

Post Auth  ⓘ

訪問策略頁籤

**第3步：在移動頁籤下，將錨點控制器切換到主(1)，並根據冗餘要求配置輔助和第三移動隧道**

**Mobility Anchors**

Export Anchor

Static IP Mobility  DISABLED

*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (3)	Selected (1)
Anchor IP	Anchor IP   Anchor Priority
<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">  10.106.40.1 <span style="float: right;">➔</span> </div> <div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">  10.76.118.75 <span style="float: right;">➔</span> </div> <div style="border: 1px solid gray; padding: 5px;">  10.76.118.74 <span style="float: right;">➔</span> </div>	<div style="border: 2px solid red; padding: 5px; margin-bottom: 5px;">  10.76.118.70 <input type="text" value="Primary (1)"/> ⓘ <span style="float: right;">➔</span> </div>

移動圖

### CLI配置

wireless profile policy GuestLANPolicy

```
mobility anchor 10.76.118.70 priority 1
no shutdown
```

## 設定訪客LAN設定檔

第1步：導航到配置>無線>訪客LAN，選擇增加，配置唯一的配置檔名稱，啟用有線VLAN，輸入有線訪客使用者的VLAN ID，並將配置檔案狀態切換為啟用。

General		Security	
Profile Name*	<input type="text" value="Guest-Profile"/>	Client Association Limit	<input type="text" value="2000"/>
Guest LAN ID*	<input type="text" value="1"/>	Wired VLAN Status	<input checked="" type="checkbox"/> ENABLE
mDNS Mode	<input type="text" value="Bridging"/>	Wired VLAN ID*	<input type="text" value="2024"/>
Status	<input checked="" type="checkbox"/> ENABLE		

訪客LAN配置檔案

第2步：在Security頁籤下，啟用Web Auth，對映Web Auth引數對映，然後從Authentication下拉選單中選擇Radius伺服器。

# Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



訪客LAN安全頁籤

## CLI配置

```
guest-lan profile-name Guest-Profile 1 wired-vlan 2024  
security web-auth authentication-list ISE-List  
security web-auth parameter-map global
```

## 訪客LAN對映

導航到Configuration > Wireless > Guest LAN。

在訪客LAN對映配置部分，選擇增加並對映策略配置檔案和訪客LAN配置檔案

## Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map: GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page    0 - 0 of 0 items

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

Save    Cancel

訪客LAN對映

## CLI配置

```
wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy
```

## 錨點9800 WLC上的組態

### 配置Web引數對映

第1步：導航到配置>安全> Web身份驗證，選擇全局，驗證控制器的虛擬IP地址和信任點對映，並確保將型別設定為webauth。

Configuration > Security > Web Auth

+ Add    × Delete

Parameter Map Name

- global
- Web-Filter

1    10

### Edit Web Auth Parameter

General    Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	XXXXXX:XX
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input checked="" type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text

全局引數對映

第2步：在高級頁籤下，配置客戶端重定向的外部網頁URL。設定「Redirect URL for Login」和「Redirect On-Failure」；「Redirect On-Success」是選用的。

設定後，重新導向URL的預覽會顯示在Web Auth設定檔上。

General **Advanced**

**i** Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

Redirect URL for login	http://10.127.196.171/w
Redirect On-Success	http://10.127.196.171/w
Redirect On-Failure	http://10.127.196.171/w
Redirect Append for AP MAC Address	
Redirect Append for Client MAC Address	
Redirect Append for WLAN SSID	
Portal IPV4 Address	10.127.196.171
Portal IPV6 Address	x::x::x::x

進階標籤

## CLI配置

```
parameter-map type webauth global
 type webauth
 virtual-ip ipv4 192.0.2.1
 redirect for-login http://10.127.196.171/webauth/login.html
 redirect on-success http://10.127.196.171/webauth/logout.html
 redirect on-failure http://10.127.196.171/webauth/failed.html
 redirect portal ipv4 10.127.196.171
 intercept-https-enable.
 trustpoint TP-self-signed-3915430211
 webauth-http-enable
```

AAA設定：

步驟1：建立Radius伺服器：

導航到Configuration > Security > AAA，按一下Server/Group部分下的Add，然後在「Create AAA Radius Server」頁上，輸入伺服器名稱、IP地址和共用金鑰。

The screenshot shows the 'Create AAA Radius Server' configuration page. The 'Name\*' field is empty. The 'Server Address\*' field contains 'IPv4/IPv6/Hostname'. The 'Key Type' dropdown is set to 'Clear Text'. The 'Key\*' and 'Confirm Key\*' fields are empty. The 'Auth Port' is 1812, 'Acct Port' is 1813, 'Server Timeout (seconds)' is 1-1000, and 'Retry Count' is 0-100. The 'Support for CoA' checkbox is checked and labeled 'ENABLED'. The 'CoA Server Key Type' dropdown is set to 'Clear Text'. The 'CoA Server Key' and 'Confirm CoA Server Key' fields are empty. The 'Automate Tester' checkbox is unchecked. The 'Apply to Device' button is visible at the bottom right.


Radius伺服器配置

## CLI配置

```
radius server ISE-Auth  
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813  
key *****  
server name ISE-Auth
```

第2步：建立RADIUS伺服器組：

在「Server Groups」部分下選擇Add以定義伺服器組，並切換要包括在組配置中的伺服器。

Name*	ISE-Group
Group Type	RADIUS
MAC-Delimiter	none ▼
MAC-Filtering	none ▼
Dead-Time (mins)	5
Load Balance	<input type="checkbox"/> DISABLED
Source Interface VLAN ID	2081 ▼ 

Available Servers

Assigned Servers

	>	ISE-Auth
--	---	----------

錨點半徑組

### CLI配置

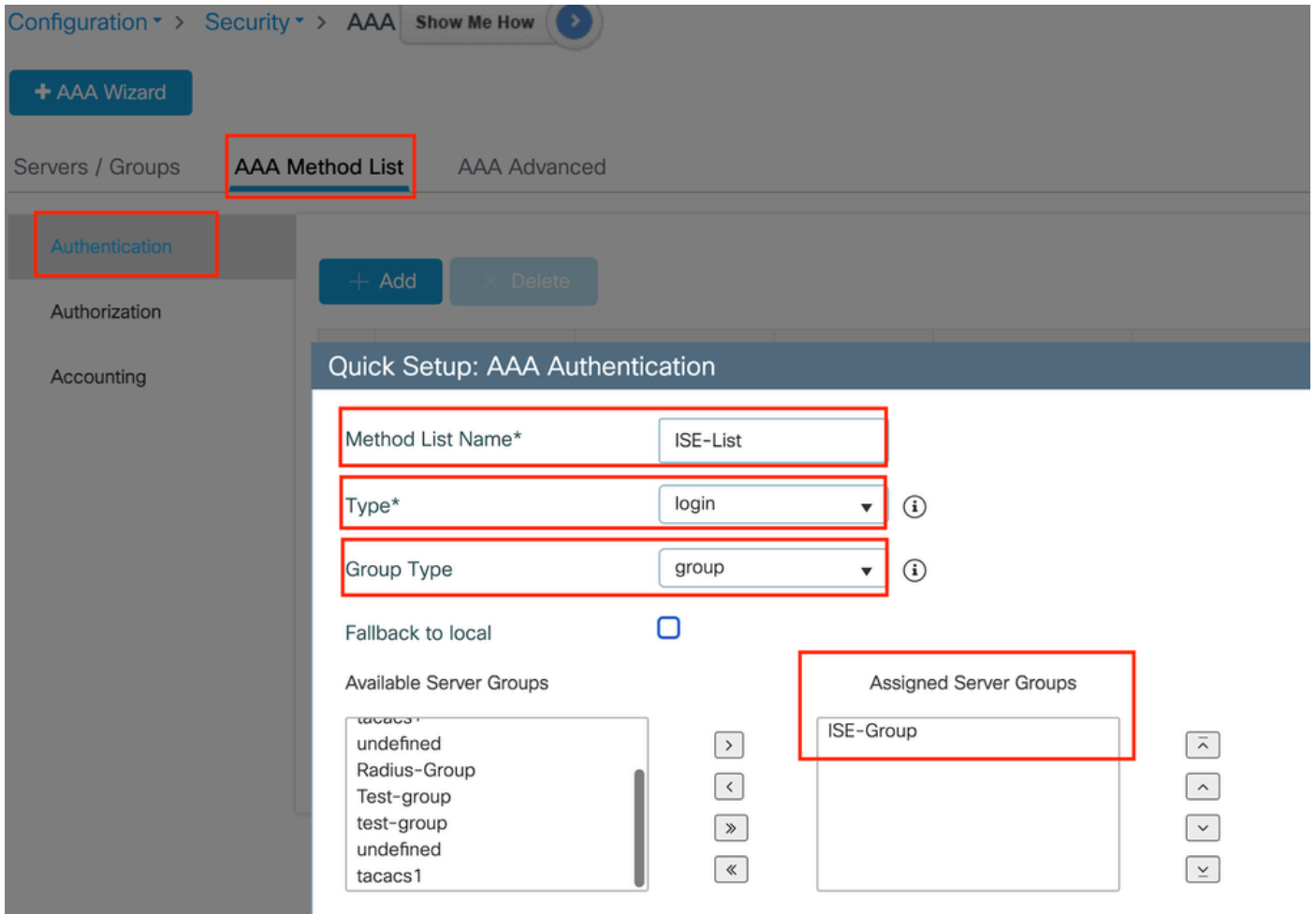
```

aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2081
deadtime 5

```

第3步：配置AAA方法清單：

導航到AAA Method List頁籤，選擇Authentication下的Add，使用「Type」作為「login」定義「Type」並將「Group type」作為「Group」定義「method list name」，然後在「Assigned Server Group」部分下對映配置的身份驗證伺服器組。



驗證方法清單

## CLI配置

```
aaa authentication login ISE-List group ISE-Group
```

## 配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略，使用與外部控制器上的名稱配置策略配置檔案並啟用配置檔案。



General

Access Policies

QOS and AVC

Mobility

Advanced

Name*	GuestLANPolicy
Description	Enter Description
Status	ENABLED <input checked="" type="checkbox"/>
Passive Client	<input type="checkbox"/> DISABLED
IP MAC Binding	ENABLED <input checked="" type="checkbox"/>
Encrypted Traffic Analytics	<input type="checkbox"/> DISABLED
CTS Policy	
Inline Tagging	<input type="checkbox"/>
SGACL Enforcement	<input type="checkbox"/>
Default SGT	2-65519

WLAN Switching Policy

Central Switching	ENABLED <input checked="" type="checkbox"/>
Central Authentication	ENABLED <input checked="" type="checkbox"/>
Central DHCP	ENABLED <input checked="" type="checkbox"/>
Flex NAT/PAT	<input type="checkbox"/> DISABLED

錨點策略配置檔案

第2步：在訪問策略下，從下拉選單中對映有線客戶端VLAN

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select

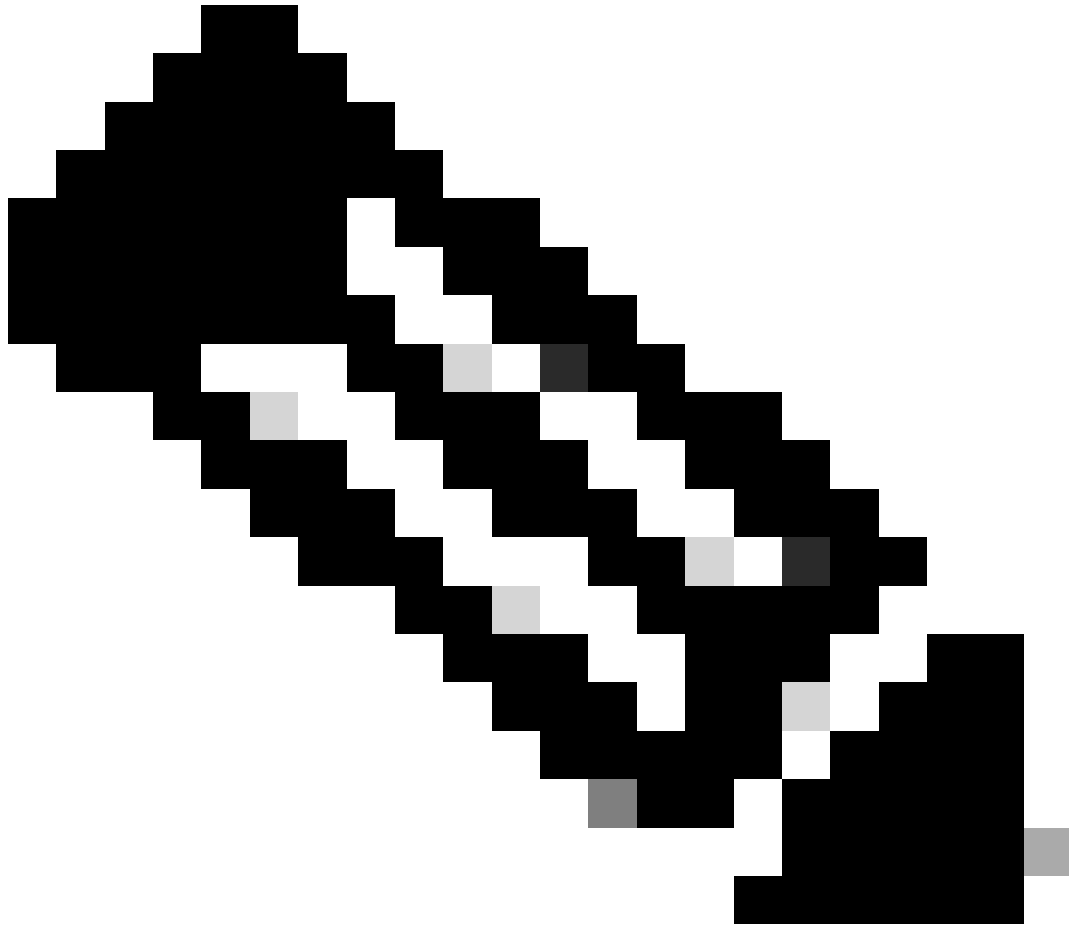


### VLAN

VLAN/VLAN Group

VLAN2024





注意：除VLAN外，其他控制器和錨點控制器上的策略配置檔案配置必須匹配。

---

第3步：在移動頁籤下，選中導出錨點覈取方塊。

**Mobility Anchors**

Export Anchor



Static IP Mobility



*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

Available (2)

Selected (0)

Anchor IP

Anchor IP

Anc

匯出錨點



注意：此組態會指定9800無線LAN控制器(WLC)為與指定原則設定檔關聯任何WLAN的錨點WLC。當外部9800 WLC將客戶端重定向到錨點WLC時，它提供有關分配給客戶端的WLAN和策略配置檔案的詳細資訊。這使錨點WLC能夠根據收到的資訊應用適當的本地策略配置檔案。

---

## CLI配置

```
wireless profile policy GuestLANPolicy
mobility anchor
vlan VLAN2024
no shutdown
```

## 設定訪客LAN設定檔

第1步：導航到配置>無線>訪客LAN，然後選擇增加建立和配置訪客LAN配置檔案。確定設定檔名

稱與外部控制器的名稱相符。請注意，必須在錨點控制器上停用有線VLAN。

Configuration > Wireless > Guest LAN

> Guest LAN Configuration

+ Add    × Delete

### Add Guest LAN Profile

**General**    Security

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	ENABLE <input checked="" type="checkbox"/>		

訪客LAN配置檔案

第2步：在安全設定中，啟用Web Auth，然後配置Web Auth引數對映和身份驗證清單。

## Edit Guest LAN Profile

General

**Security**

Layer3

Web Auth

ENABLE



Web Auth Parameter Map

global



Authentication List

ISE-List



---

注意：除了有線VLAN狀態外，外部控制器和錨點控制器之間的訪客LAN配置檔案配置必須相同

---

## CLI配置

```
guest-lan profile-name Guest-Profile 1
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## 訪客LAN對映

第1步：導航到配置>無線>訪客LAN。在Guest LAN MAP configuration部分，選擇Add並將策略配置檔案對映到訪客LAN配置檔案。



## Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map : GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	
◀ ◻ ▶	10 items per page
0 - 0 of 0 items	

Profile Name: Guest-Profile

Policy Name: GuestLANPolicy

✓ Save    ↺ Cancel

訪客LAN對映

wireless guest-lan map GuestMap  
guest-lan Guest-Profile policy GuestLANPolicy

## 在Catalyst 9800上配置錨定到AireOS 5520控制器的有線訪客



網路拓撲

## 外部9800 WLC上的配置

## 配置Web引數對映

第1步：導航到配置>安全> Web身份驗證，然後選擇全局。驗證控制器的虛擬IP地址和信任點是否已正確對映到配置檔案上，並且型別設定為webauth。

General	Advanced
Parameter-map Name	global
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Captive Bypass Portal	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>
Sleeping Client Status	<input type="checkbox"/>
Sleeping Client Timeout (minutes)	720
Virtual IPv4 Address	192.0.2.1
Trustpoint	TP-self-signed-3...
Virtual IPv4 Hostname	
Virtual IPv6 Address	:::X::X::X
Web Auth intercept HTTPs	<input type="checkbox"/>
Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable HTTP secure server for Web Auth	<input type="checkbox"/>
<b>Banner Configuration</b>	
Banner Title	
Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

### Web引數對映

第2步：在高級頁籤下，指定客戶端必須重定向到的外部網頁URL。配置Redirect URL for Login和Redirect On-Failure。Redirect On-Success設定是可選配置。

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

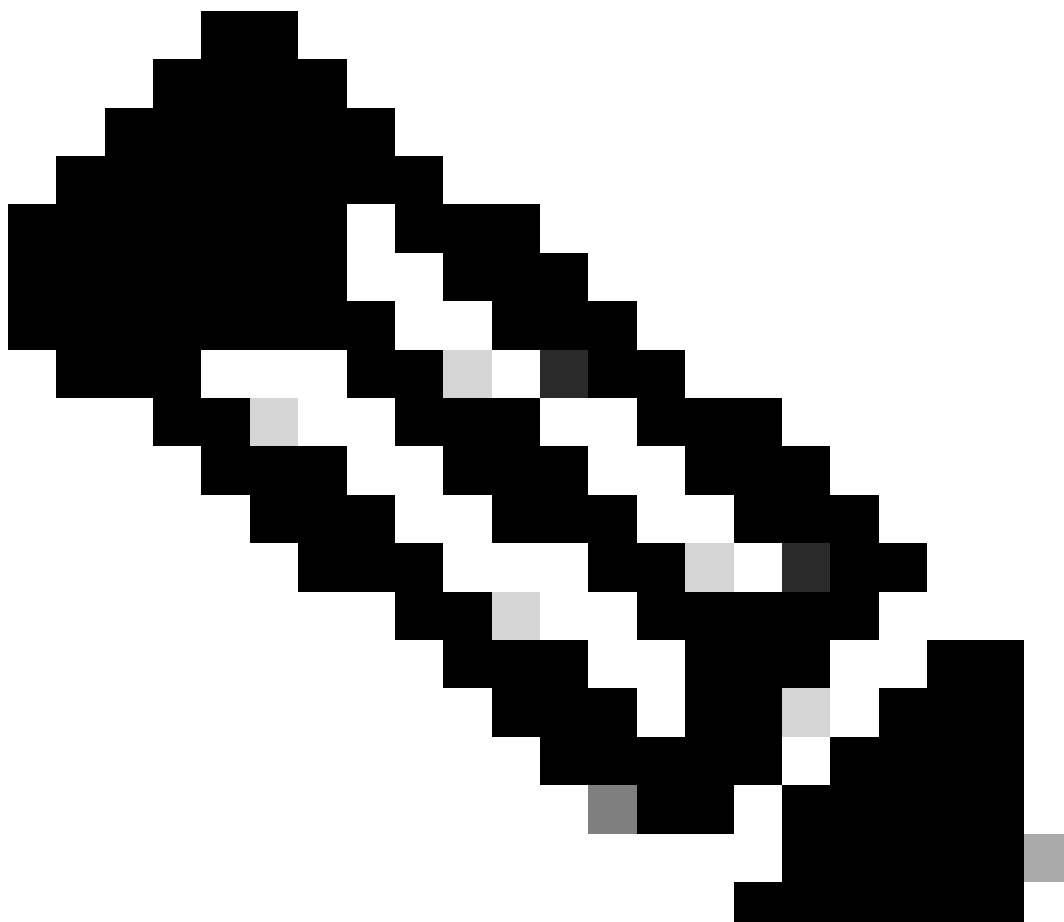
Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X:X:X:X"/>

進階標籤

### CLI配置

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```

---



注意：有關AAA配置，請參閱外部9800 WLC的「」部分中提供的配置詳細資訊。

---

## 配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略。選擇Add，並在General頁籤中為配置檔案提供一個名稱並啟用狀態切換。

General

Access Policies

QOS and AVC

Mobility

Advanced

Name\*

Guest

Description

Enter Description

Status

ENABLED

Passive Client

DISABLED

IP MAC Binding

ENABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Flex NAT/PAT

DISABLED

策略配置檔案

第2步：在訪問策略頁籤中，分配隨機VLAN。

General

**Access Policies**

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



### VLAN

VLAN/VLAN Group

1



Multicast VLAN

Enter Multicast VLAN

訪問策略

第3步：在移動性頁籤中，切換錨點控制器並將其優先順序設定為主(1)

### Mobility Anchors

Export Anchor



Static IP Mobility



*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

#### Available (1)



Anchor IP

 10.76.6.156 
---

#### Selected (1)

Anchor IP

Anchor Priority

 10.76.118.74	Primary (1) 
--	---

Mobility頁籤

---

注意：9800外部WLC的策略配置檔案必須與5520錨點WLC的訪客LAN配置檔案匹配，但vlan配置除外

---

## CLI配置

```
wireless profile policy Guest
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor 10.76.118.74 priority 1
no shutdown
```

## 設定訪客LAN設定檔

第1步：導航到配置>無線>訪客LAN，選擇增加。配置一個唯一的配置檔名稱並啟用Wired



VLAN，指定專用於有線訪客使用者的VLAN ID。最後，將配置檔案狀態切換為Enabled。

General Security

Profile Name*	Guest	Client Association Limit	2000
Guest LAN ID*	2	Wired VLAN Status	ENABLE <input checked="" type="checkbox"/>
mDNS Mode	Bridging ▼	Wired VLAN ID*	11
Status	ENABLE <input checked="" type="checkbox"/>		

訪客LAN策略

第2步：在安全頁籤下，啟用Web身份驗證，對映Web身份驗證引數對映，然後從身份驗證下拉選單中選擇RADIUS伺服器。

General Security

Layer3

Web Auth	ENABLE <input checked="" type="checkbox"/>
Web Auth Parameter Map	global ▼
Authentication List	ISE-List ▼

「安全」頁籤

---

注意：9800外部和5520錨點控制器的訪客LAN配置檔名稱必須相同

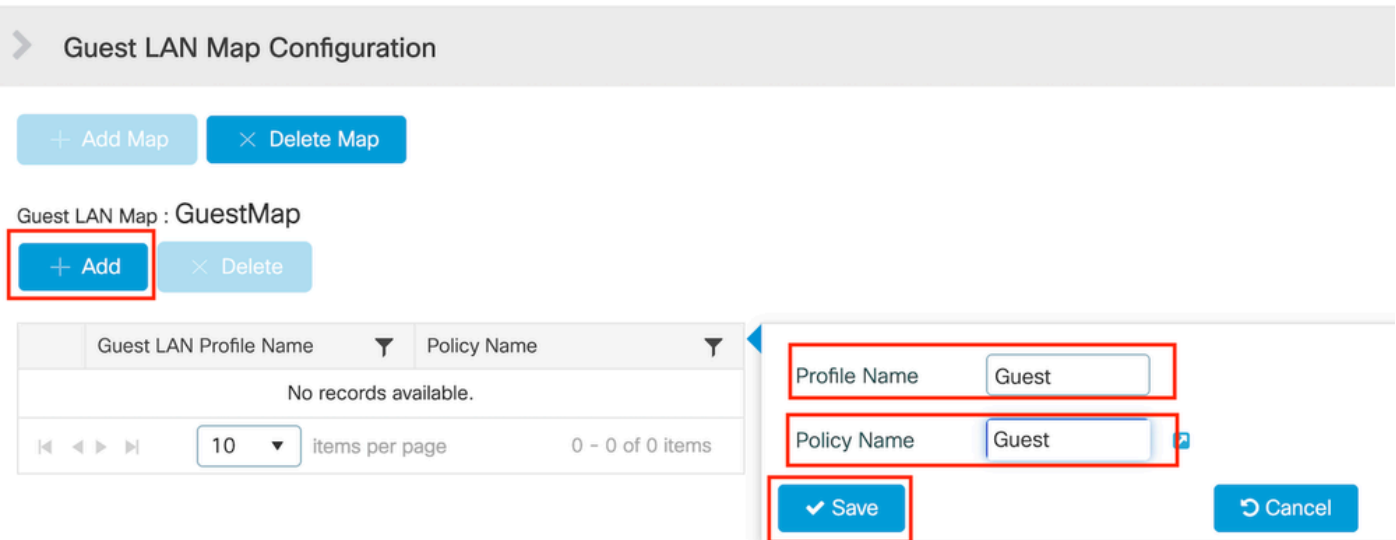
---

## CLI配置

```
guest-lan profile-name Guest 2 wired-vlan 11
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## 訪客LAN對映

第1步：導航到配置>無線>訪客LAN。在訪客LAN對映配置部分，選擇增加，並將策略配置檔案對映到訪客LAN配置檔案。



訪客LAN對映

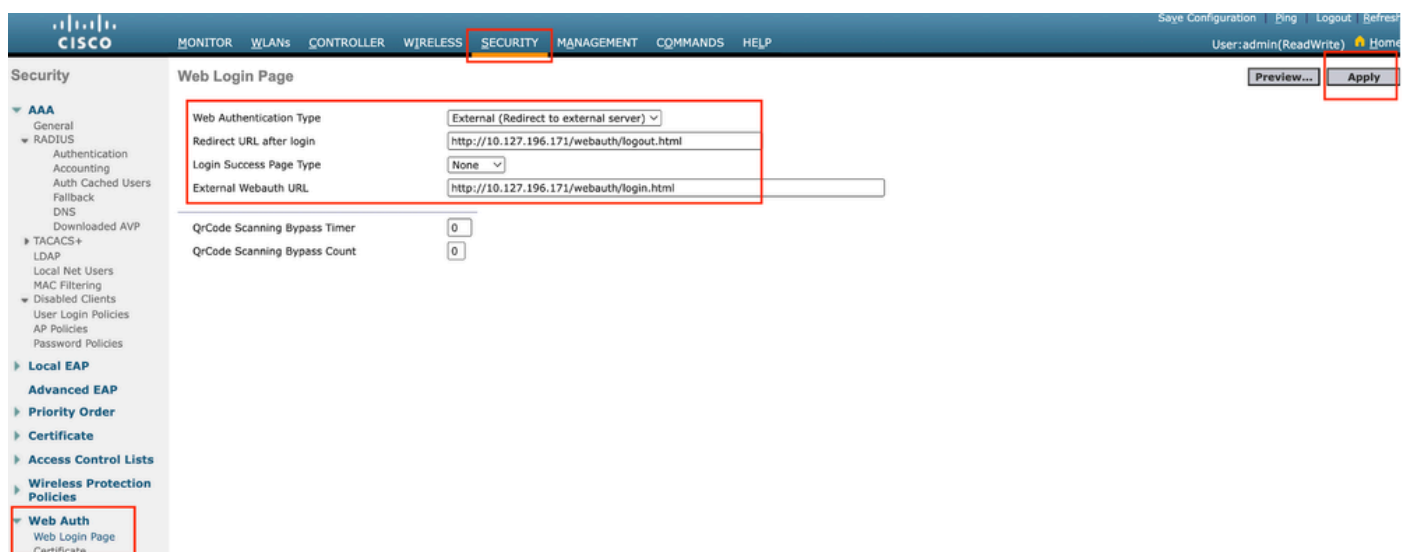
## CLI配置

```
wireless guest-lan map GuestMap
guest-lan Guest policy Guest
```

## 錨點5520 WLC上的組態

### 設定Web驗證

第1步：導航到安全> Web身份驗證> Web登入頁。將Web身份驗證型別設定為External ( 重定向到外部伺服器 )，並配置外部Web Auth URL。登入後重定向URL是可選的，並且如果客戶端在身份驗證成功之後需要重定向到專用頁，則可以配置此項。



Web身份驗證設定

AAA設定：

步驟1：配置RADIUS伺服器

導航到Security > Radius > Authentication > New。



Radius伺服器

第2步：在控制器上配置RADIUS伺服器IP和共用金鑰。將伺服器狀態切換為Enabled，並選中Network User覈取方塊。

## RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

伺服器配置

### 配置訪問控制清單

第1步：導航到安全>訪問控制清單，選擇新建。建立允許流量到達DNS和外部Web伺服器的預先驗

## 證ACL。

The screenshot shows the Cisco ISE Security page. The 'SECURITY' tab is highlighted in the top navigation bar. The left sidebar shows the 'Access Control Lists' menu item highlighted. The main content area is titled 'Access Control Lists > Edit' and shows the configuration for the 'Pre-Auth\_ACL' list. The 'General' section is expanded, showing the 'Access List Name' as 'Pre-Auth\_ACL' and 'Deny Counters' as '0'. Below this is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

允許流量進入Web伺服器的訪問清單

## 設定訪客LAN設定檔

第1步：導航到WLAN >，選擇Create New。

選擇Type作為Guest LAN，並配置與9800外部控制器的策略配置檔案相同的名稱。

The screenshot shows the Cisco ISE WLANs page. The 'WLANs' tab is highlighted in the top navigation bar. The 'Create New' button is highlighted in a red box. The page shows the 'Current Filter: None' and options to 'Change Filter' or 'Clear Filter'. Below the filter options is a table with columns for 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

建立訪客LAN

The screenshot shows the Cisco ISE WLANs > New page. The 'Type' dropdown is set to 'Guest LAN' and is highlighted in a red box. The 'Profile Name' field is set to 'Guest' and the 'ID' field is set to '2'. The 'Apply' button is highlighted in a red box. The top navigation bar shows the 'WLANs' tab highlighted.

訪客LAN配置檔案

第2步：在訪客LAN配置檔案上對映入口和出口介面。

在此案例中，輸入介面是無，因為輸入介面是來自外部控制器的EoIP通道。

Egress介面是有線客戶端物理連線的VLAN。

General Security QoS Advanced

Profile Name

Type Guest LAN

Status  Enabled

Security Policies **Web-Auth**  
(Modifications done under security tab will appear after applying the changes.)

Ingress Interface

Egress Interface

NAS-ID

訪客LAN配置檔案

第3步：在Security頁籤下，選擇第3層安全作為Web Authentication，並對映預身份驗證ACL。

## WLANs > Edit 'Guest'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security

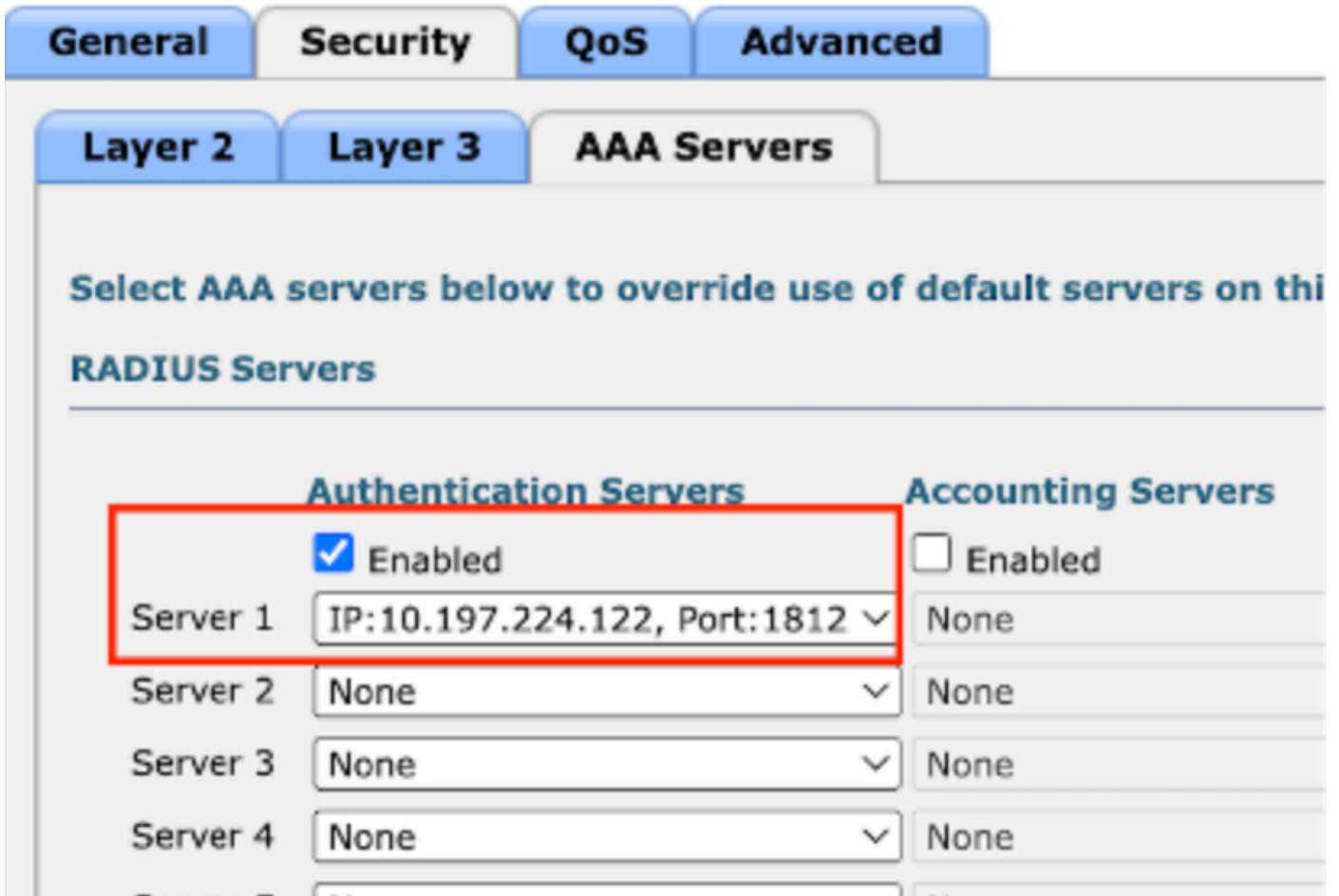
Preauthentication ACL IPv4  IPv6

Override Global Config<sup>20</sup>  Enable

訪客LAN安全頁籤

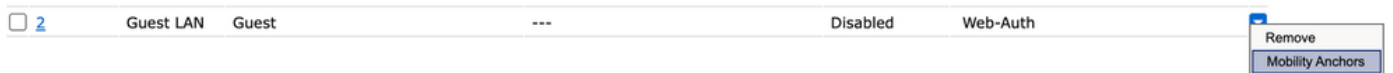
第4步：導航到安全> AAA伺服器。

選取下拉式清單，將RADIUS伺服器對應到訪客LAN設定檔。



將RADIUS伺服器對映到訪客LAN配置檔案

第5步：導航到WLAN。將滑鼠懸停在訪客LAN配置檔案的下拉圖示上，然後選擇移動錨點。



第6步：選擇Mobility Anchor Create為此訪客LAN配置檔案將控制器配置為導出錨點。



移動錨點建立

在AireOS 5520上配置錨定到Catalyst 9800的有線訪客





網路拓撲

## 外部5520 WLC上的設定

### 控制器介面配置

第1步：導航到Controller > Interfaces > New。配置介面名稱、VLAN ID並啟用訪客LAN。

有線訪客需要兩個動態介面。

首先，建立一個第2層動態介面並將其指定為Guest LAN。此介面可作為訪客LAN的輸入介面，有線使用者端可在此處進行實體連線。

**Controller**

- General
- Icons
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- ▶ Network Routes
- ▶ Fabric Configuration
- ▶ Redundancy
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ PMIPv6
- ▶ Tunneling
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced

### Interfaces > Edit

#### General Information

Interface Name	wired-guest
MAC Address	a0:e0:af:32:d9:ba

#### Configuration

Guest Lan	<input checked="" type="checkbox"/>
NAS-ID	none

#### Physical Information

Port Number	1
Backup Port	0
Active Port	1

#### Interface Address

VLAN Identifier	2020
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>

輸入介面

第2步：導航到Controller > Interfaces > New。配置介面名稱、VLAN ID。

第二個動態介面必須是控制器上的第3層介面，有線客戶端從此vlan子網接收IP地址。此介面可作為訪客LAN設定檔的輸出介面。

**Controller**

- General
- Icons
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- ▶ Network Routes
- ▶ Fabric Configuration
- ▶ Redundancy
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ PMIPv6
- ▶ Tunneling
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced
- Lawful Interception

**Interfaces > Edit**

**General Information**

Interface Name	vlan2024
MAC Address	a0:e0:af:32:d9:ba

**Configuration**

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	none

**Physical Information**

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

**Interface Address**

VLAN Identifier	2024
IP Address	10.105.211.85
Netmask	255.255.255.128
Gateway	10.105.211.1

輸出介面

## 交換機埠配置

有線訪客使用者連線到接入層交換機，這些指定埠必須配置有在控制器上啟用訪客LAN的VLAN

### 接入層交換機埠配置

```
interface gigabitEthernet <x/x/x>
```

說明有線訪客訪問

```
switchport access vlan 2020
```

```
switchport mode access
```

```
end
```

外部控制器上行鏈路埠配置

```
interface TenGigabitEthernet<x/x/x>
```

說明到外部WLC的中繼埠

```
switchport mode trunk
```

```
switchport trunk native vlan 2081
```

```
switchport trunk allowed vlan 2081,2020
```

```
end
```

錨點控制器上行鏈路埠配置

```
interface TenGigabitEthernet<x/x/x>
```

描述連線到錨點WLC的中繼埠

```
switchport mode trunk
```

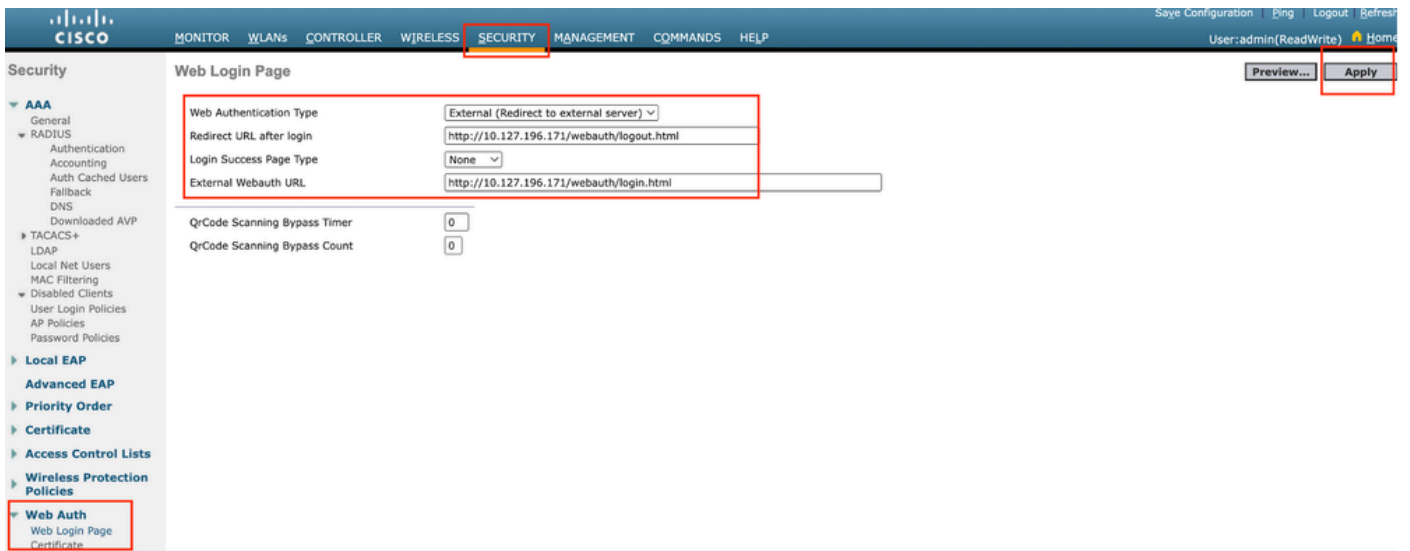
```
switchport trunk native vlan 2081
```

```
switchport trunk allowed vlan 2081,2024
```

```
end
```

## 設定Web驗證

第1步：導航到安全> Web身份驗證> Web登入頁。將Web身份驗證型別設定為External ( 重定向到外部伺服器 )，並配置外部Web Auth URL。登入後重定向URL是可選的，並且如果客戶端在身份驗證成功之後需要重定向到專用頁，則可以配置此項。



Web身份驗證設定

AAA設定：

步驟1：配置RADIUS伺服器

導航到Security > Radius > Authentication > New。



Radius伺服器

第2步：在控制器上配置RADIUS伺服器IP和共用金鑰。將伺服器狀態切換為Enabled，並選中Network User覈取方塊。

## RADIUS Authentication Servers > New

Server Index (Priority)	4 ▾
Server IP Address(Ipv4/Ipv6)	<input type="text"/>
Shared Secret Format	ASCII ▾
Shared Secret	<input type="text"/>
Confirm Shared Secret	<input type="text"/>
Apply Cisco ISE Default settings	<input type="checkbox"/>
Apply Cisco ACA Default settings	<input type="checkbox"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for CoA	Disabled ▾
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	5 seconds
Tunnel Proxy	<input type="checkbox"/> Enable
PAC Provisioning	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable
Cisco ACA	<input type="checkbox"/> Enable

伺服器配置

### 配置訪問控制清單

第1步：導航到安全>訪問控制清單，選擇新建。建立允許流量到達DNS和外部Web伺服器的預先驗

## 證ACL。

The screenshot shows the Cisco Meraki Security page. The 'SECURITY' tab is highlighted in the top navigation bar. On the left sidebar, 'Access Control Lists' is highlighted. The main content area is titled 'Access Control Lists > Edit' and shows the 'General' tab for an 'Access List Name' of 'Pre-Auth\_ACL' with 'Deny Counters' set to 0. Below this is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTP	Any	Any	0
4	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.127.196.171 / 255.255.255.255	TCP	Any	HTTPS	Any	Any	0
6	Permit	10.127.196.171 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Any	0

允許流量進入Web伺服器的訪問清單

## 設定訪客LAN設定檔

第1步：導航到WLAN > Create New > Go。

The screenshot shows the Cisco Meraki WLANs page. The 'WLANs' tab is highlighted in the top navigation bar. On the right side, the 'Create New' button is highlighted with a red box. Below the navigation bar, there is a 'Current Filter: None' section with links for '[Change Filter]' and '[Clear Filter]'. Below that, there is a table header with columns: 'WLAN ID', 'Type', 'Profile Name', 'WLAN SSID', 'Admin Status', and 'Security Policies'.

訪客LAN配置檔案

選擇Type as Guest LAN並配置配置檔名稱。必須在9800錨點控制器的原則設定檔和訪客LAN設定檔上設定相同的名稱。

## WLANs > New

Type

Guest LAN ▾

Profile Name

Guest-Profile

ID

3 ▾

訪客LAN配置檔案

第2步：在General頁籤下，在訪客LAN配置檔案上對映入口和出口介面。

輸入介面是有線使用者端實際連線的vlan。

輸出介面是客戶端請求的IP地址的VLAN子網。

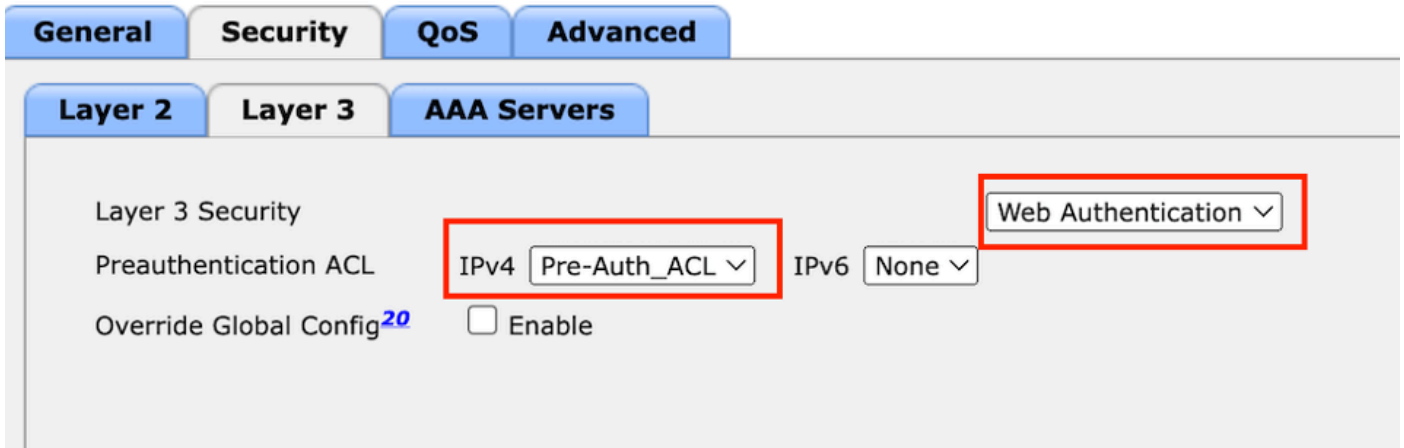
General	Security	QoS	Advanced
Profile Name	Guest-Profile		
Type	Guest LAN		
Status	<input checked="" type="checkbox"/> Enabled		
Security Policies	<b>Web-Auth</b> (Modifications done under security tab will appear after applying th		
Ingress Interface	wired-guest ▾		
Egress Interface	vlan2024 ▾		
NAS-ID	none		

訪客LAN配置檔案

第3步：導航到安全>第3層。

選擇Layer 3 Security作為Web Authentication，並對映預身份驗證ACL。

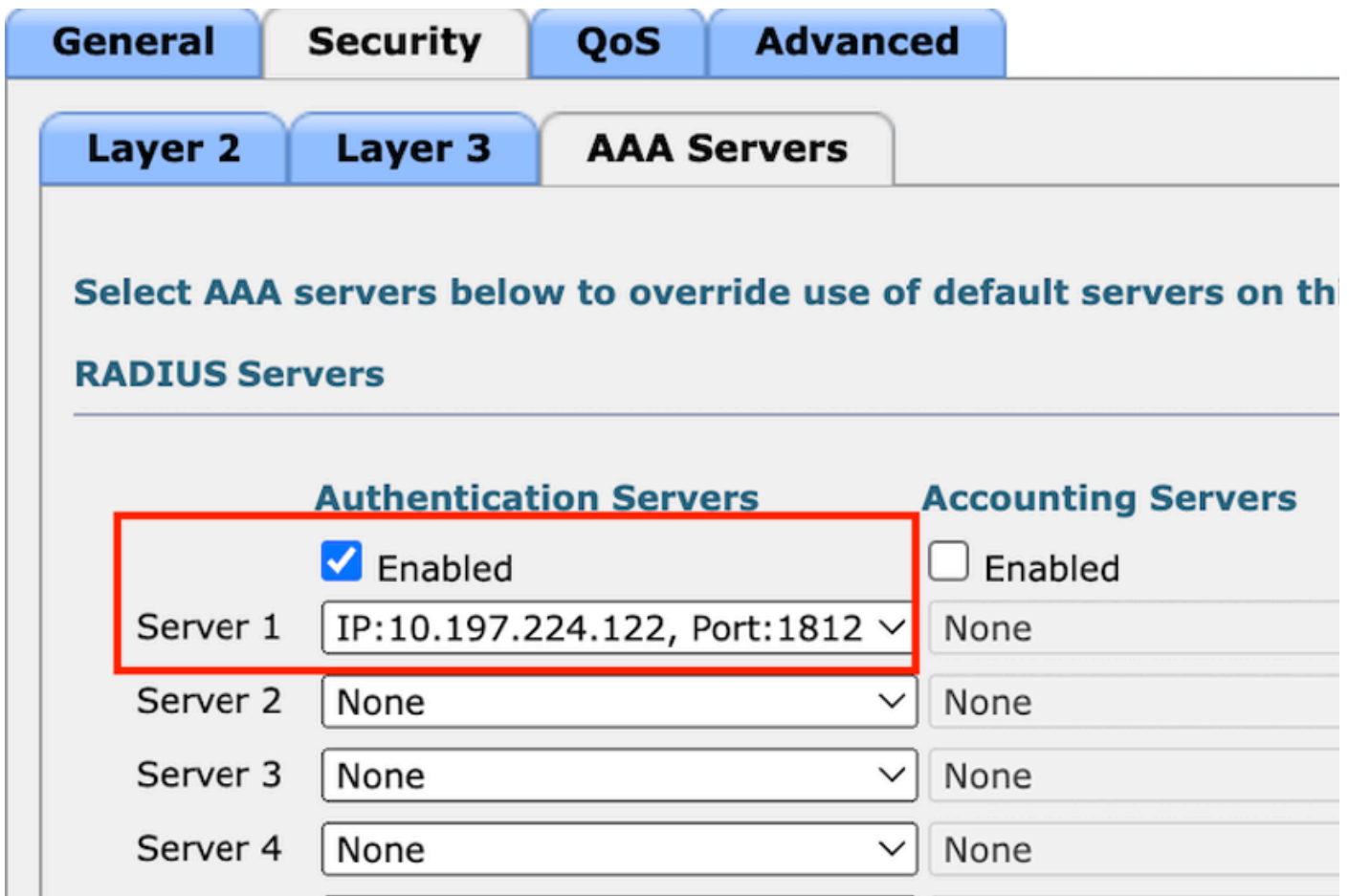




第3層安全頁籤

步驟4：

在AAA servers頁籤下，對映RADIUS伺服器 and Enabled 覆取方塊。



將RADIUS伺服器對應到訪客LAN設定檔

第5步：導航到WLAN頁面，將滑鼠懸停在訪客LAN配置檔案的下拉圖示上，然後選擇移動錨點。



行動錨點

第6步：將移動錨點從下拉選單對映到訪客LAN配置檔案。

## Mobility Anchors

WLAN SSID Guest-Profile

Switch IP Address (Anchor) Data Path Co

**Mobility Anchor Create**

Switch IP Address (Anchor)

Foot Notes

將移動錨點對映到訪客LAN

## 錨點9800 WLC上的組態

### 配置Web引數對映

第1步：導航到配置>安全> Web身份驗證，然後選擇全局。驗證控制器的虛擬IP地址和信任點是否已正確對映到配置檔案上，並且型別設定為webauth。

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-3... ▼
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth ▼	Virtual IPv6 Address	:::XX::X
Captive Bypass Portal	<input type="checkbox"/>	Web Auth intercept HTTPs	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>	Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>	Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>	Banner Configuration	
Sleeping Client Status	<input type="checkbox"/>	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	<input checked="" type="radio"/> None <input type="radio"/> Banner Text <input type="radio"/> Read From File

Web引數對映

第2步：在高級頁籤下，指定客戶端必須重定向到的外部網頁URL。配置Redirect URL for Login和

Redirect On-Failure。Redirect On-Success設定是可選配置。

General Advanced

Preview of the Redirect URL:

http://10.127.196.171/webauth/login.html?switch\_url=https://192.0.2.1/login.html&redirect=<website-name>

### Redirect to external server

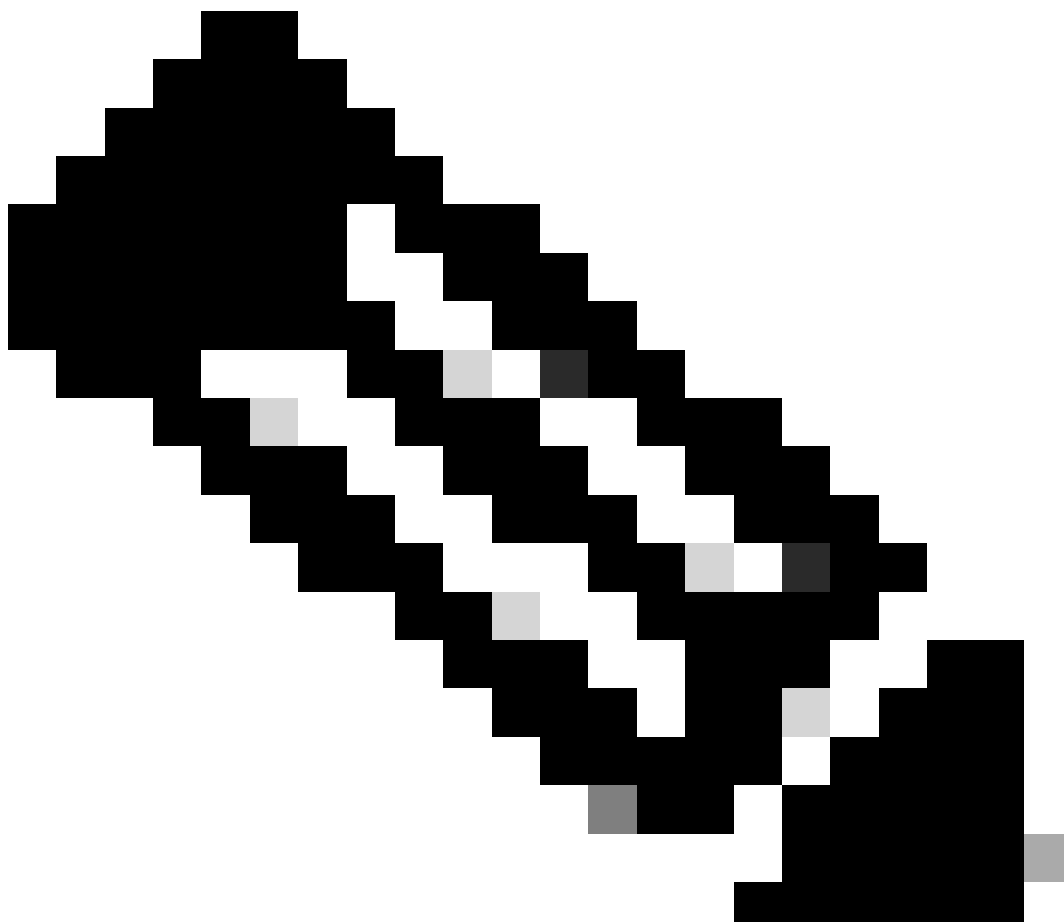
Redirect URL for login	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Success	<input type="text" value="http://10.127.196.171/w"/>
Redirect On-Failure	<input type="text" value="http://10.127.196.171/w"/>
Redirect Append for AP MAC Address	<input type="text"/>
Redirect Append for Client MAC Address	<input type="text"/>
Redirect Append for WLAN SSID	<input type="text"/>
Portal IPV4 Address	<input type="text" value="10.127.196.171"/>
Portal IPV6 Address	<input type="text" value="X::X::X"/>

進階標籤

### CLI配置

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
redirect for-login http://10.127.196.171/webauth/login.html
redirect on-success http://10.127.196.171/webauth/logout.html
redirect on-failure http://10.127.196.171/webauth/failed.html
redirect portal ipv4 10.127.196.171
trustpoint TP-self-signed-3010594951
webauth-http-enable
```

---



注意：有關AAA配置，請參閱外部9800 WLC的「在Catalyst 9800上配置錨定到其他Catalyst 9800的有線訪客」部分中提供的配置詳細資訊。

---

## 配置策略配置檔案

第1步：導航到配置>標籤和配置檔案>策略。使用與外部控制器的訪客LAN配置檔案相同的名稱配置策略配置檔案。

Name*	<input type="text" value="Guest-Profile"/>	WLAN Switching Policy	
Description	<input type="text" value="Enter Description"/>	Central Switching	<input checked="" type="checkbox" value="ENABLED"/>
Status	<input checked="" type="checkbox" value="ENABLED"/>	Central Authentication	<input checked="" type="checkbox" value="ENABLED"/>
Passive Client	<input type="checkbox" value="DISABLED"/>	Central DHCP	<input checked="" type="checkbox" value="ENABLED"/>
IP MAC Binding	<input checked="" type="checkbox" value="ENABLED"/>	Flex NAT/PAT	<input type="checkbox" value="DISABLED"/>
Encrypted Traffic Analytics	<input type="checkbox" value="DISABLED"/>		
CTS Policy			
Inline Tagging	<input type="checkbox"/>		
SGACL Enforcement	<input type="checkbox"/>		
Default SGT	<input type="text" value="2-65519"/>		

策略配置檔案

第2步：在Access Policies頁籤下，從下拉選單中對映有線客戶端VLAN

General

**Access Policies**

QOS and AVC

Mobility

Advanced

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

### WLAN Local Profiling

Global State of Device  
Classification

Disabled ⓘ

Local Subscriber Policy Name

Search or Select



### VLAN

VLAN/VLAN Group

VLAN2024



Multicast VLAN

Enter Multicast VLAN

訪問策略

第3步：在移動頁籤下，選中導出錨點覈取方塊。

## Mobility Anchors

Export Anchor



Static IP Mobility



*Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients.*

Drag and Drop/double click/click on the arrow to add/remove Anchors

移動性頁籤

## CLI配置

```
wireless profile policy Guest-Profile
no accounting-interim
exclusionlist timeout 180
no flex umbrella dhcp-dns-option
mobility anchor
vlan VLAN2024
no shutdown
```

## 設定訪客LAN設定檔

第1步：導航到配置>無線>訪客LAN，選擇增加配置訪客LAN配置檔案並停用有線VLAN狀態。

錨點上的訪客LAN配置檔名稱必須與外部WLC上的訪客LAN配置檔案相同。

Profile Name*	Guest-Profile	Client Association Limit	2000
Guest LAN ID*	1	Wired VLAN Status	<input type="checkbox"/> DISABLE
mDNS Mode	Bridging		
Status	<input checked="" type="checkbox"/> ENABLE		

訪客LAN配置檔案

第2步：在安全頁籤下，啟用Web身份驗證。從下拉選單中選擇Web身份驗證引數對映和身份驗證清單

## Edit Guest LAN Profile

### Layer3

Web Auth	<input checked="" type="checkbox"/> ENABLE
Web Auth Parameter Map	global
Authentication List	ISE-List

訪客LAN安全頁籤

### CLI配置

```
guest-lan profile-name Guest-Profile 1
```



```
security web-auth authentication-list ISE-List
security web-auth parameter-map global
```

## 訪客LAN對映

第1步：導航到配置>無線>訪客LAN。在訪客LAN對映配置部分，選擇增加，並將策略配置檔案對映到訪客LAN配置檔案。

### > Guest LAN Map Configuration

Guest LAN Map Configuration

+ Add Map    × Delete Map

Guest LAN Map: GuestMap

+ Add    × Delete

Guest LAN Profile Name	Policy Name
No records available.	

10 items per page    0 - 0 of 0 items

Profile Name: Guest-Profile

Policy Name: Guest-Profile

Save    Cancel

訪客LAN對映

## 驗證

### 驗證控制器配置

```
#show guest-lan summary
```

```
GLAN  GLAN Profile Name      Status
-----
1      Guest-Profile             UP
2      Guest                     UP
```

```
#show guest-lan id 1
```

```
<#root>
```

```
Guest-LAN Profile Name      : Guest
=====
Guest-LAN ID                : 2
Wired-Vlan                  :
11
Status                       :
```

Enabled

Number of Active Clients : 0  
Max Associated Clients : 2000  
Security  
    WebAuth :

Enabled

    Webauth Parameter Map : global  
    Webauth Authentication List :

ISE-List

    Webauth Authorization List : Not configured  
mDNS Gateway Status : Bridge

#show parameter-map type webauth global

<#root>

Parameter Map Name : global  
Type :

webauth

Redirect:  
    For Login :

http://10.127.196.171/webauth/login.html

    On Success :

http://10.127.196.171/webauth/logout.html

    On Failure :

http://10.127.196.171/webauth/failed.html

    Portal ipv4 :

10.127.196.171

        Virtual-ipv4 :

192.0.2.1

#show parameter-map type webauth name <profile name> ( 如果使用自定義web引數配置檔案 )

#show wireless guest-lan-map summary

GLAN Profile Name	Policy Name
Guest	Guest

#show無線移動性摘要

IP	Public Ip	MAC Address
10.76.118.70	10.76.118.70	f4bd.9e59.314b

#show ip http伺服器狀態

HTTP server status: Enabled  
HTTP server port: 80  
HTTP server active supplementary listener ports: 21111  
HTTP server authentication method: local

HTTP secure server capability: Present  
HTTP secure server status: Enabled  
HTTP secure server port: 443  
HTTP secure server trustpoint: TP-self-signed-3010594951

>show guest-lan summary

Number of Guest LANs..... 1

GLAN ID	GLAN Profile Name	Status	Interface Name
2	Guest	Enabled	wired-vlan-11

>show guest-lan 2

Guest LAN Identifier..... 2  
Profile Name..... Guest  
Status..... Enabled  
Interface..... wired-vlan-11

Radius Servers  
Authentication..... 10.197.224.122 1812 \*  
Web Based Authentication..... Enabled  
Web Authentication Timeout..... 300  
IPv4 ACL..... Pre-Auth\_ACL

Mobility Anchor List

GLAN ID	IP Address	Status
2	10.76.118.74	Up

>show custom-web all

```
Radius Authentication Method..... PAP
Cisco Logo..... Enabled
CustomLogo..... None
Custom Title..... None
Custom Message..... None
Custom Redirect URL..... http://10.127.196.171/webauth/logout.html
Web Authentication Login Success Page Mode..... None
Web Authentication Type..... External
Logout-popup..... Enabled
External Web Authentication URL..... http://10.127.196.171/webauth/login.html
QR Code Scanning Bypass Timer..... 0
QR Code Scanning Bypass Count..... 0
```

>show custom-web guest-lan 2

```
Guest LAN Status..... Enabled
Web Security Policy..... Web Based Authentication
WebAuth Type..... External
Global Status..... Enabled
```

### 驗證客戶端策略狀態

關於外國，

#show無線客戶端摘要

在客戶端成功關聯後，外部控制器上的客戶端策略管理器狀態為RUN。

<#root>

MAC Address	AP Name	Type ID	State	Protocol Method
a0ce.c8c3.a9b5	N/A			

GLAN 1

Run

802.3

Web Auth

Export Foreign

>show client detail a0ce.c8c3.a9b5

<#root>

```
Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username ..... N/A
Client Webauth Username ..... N/A
Client State..... Associated
User Authenticated by ..... None
Client User Group.....
Client NAC OOB State..... Access
guest-lan..... 1
Wireless LAN Profile Name..... Guest-Profile
Mobility State.....
```

**Export Foreign**

Mobility Anchor IP Address.....

10.76.118.70

Security Policy Completed.....

**Yes**

Policy Manager State.....

**RUN**

Pre-auth IPv4 ACL Name..... Pre-Auth\_ACL

EAP Type..... Unknown

Interface.....

**wired-guest-egress**

VLAN..... 2024

Quarantine VLAN..... 0

在錨點上，

必須在錨點控制器上監視客戶端狀態轉換。

客戶端策略管理器狀態為Web Auth pending ( Web身份驗證掛起 )。

<#root>

MAC Address	AP Name	Type ID	State	Protocol Meth
a0ce.c8c3.a9b5	10.76.6.156			

**GLAN 1**

Webauth Pending

802.3

Web Auth

**Export Anchor**

一旦客戶端進行身份驗證，策略管理器狀態將轉換為RUN狀態。

MAC Address	AP Name	Type ID	State	Protocol	Method
a0ce.c8c3.a9b5	10.76.6.156	GLAN 1	Run	802.3	Web

#show無線客戶端mac-address a0ce.c8c3.a9b5 detail

<#root>

Client MAC Address : a0ce.c8c3.a9b5  
Client MAC Type : Universally Administered Address  
Client DUID: NA  
Client IPv4 Address :

10.105.211.69

Client State : Associated  
Policy Profile : Guest-Profile  
Flex Profile : N/A  
Guest Lan:  
GLAN Id: 1  
GLAN Name: Guest-Profile

Mobility:

Foreign IP Address :

10.76.118.74

Point of Attachment : 0xA0000003  
Point of Presence : 0  
Move Count : 1  
Mobility Role :

Export Anchor

Mobility Roam Type :

L3 Requested

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 35 seconds

VLAN : VLAN2024

Session Manager:

Point of Attachment : mobility\_a0000003  
IIF ID : 0xA0000003  
Authorized : FALSE  
Session timeout : 28800  
Common Session ID: 4a764c0a0000008ea0285466  
Acct Session ID : 0x00000000  
Auth Method Status List  
Method : Web Auth

```
Webauth State      :
Login
Webauth Method     :
Webauth
Server Policies:
  Resultant Policies:
    URL Redirect ACL :
WA-v4-int-10.127.196.171
    Preauth ACL      :
WA-sec-10.127.196.171
    VLAN Name        : VLAN2024
    VLAN             :
2024
    Absolute-Timer   : 28800
```

客戶端在成功Web身份驗證後進入RUN狀態。

```
show wireless client mac-address a0ce.c8c3.a9b5 detail
```

```
<#root>
```

```
Client MAC Address : a0ce.c8c3.a9b5
Client MAC Type    : Universally Administered Address
Client DUID: NA
Client IPv4 Address :
10.105.211.69
Client Username    :
testuser
```

```
Client State : Associated
Policy Profile : Guest-Profile
Flex Profile  : N/A
Guest Lan:
  GLAN Id: 1
  GLAN Name: Guest-Profile
Wireless LAN Network Name (SSID) : N/A
BSSID : N/A
Connected For : 81 seconds
Protocol : 802.3
```

```
Policy Manager State:
```

```
Run
```

```
Last Policy Manager State :
```

**Webauth Pending**

Client Entry Create Time : 81 seconds  
VLAN : VLAN2024

Last Tried Aaa Server Details:  
Server IP :

10.197.224.122

**Auth Method Status List**

Method : Web Auth  
Webauth State : Authz  
Webauth Method : Webauth

**Resultant Policies:**

URL Redirect ACL :

**IP-Adm-V4-LOGOUT-ACL**

VLAN Name : VLAN2024  
VLAN :

2024

Absolute-Timer : 28800

>show client detail a0 : ce : c8 : c3 : a9 : b5

<#root>

Client MAC Address..... a0:ce:c8:c3:a9:b5  
Client Username ..... N/A  
Client Webauth Username ..... N/A  
Client State..... Associated  
Wireless LAN Profile Name..... Guest  
WLAN Profile check for roaming..... Disabled  
Hotspot (802.11u)..... Not Supported  
Connected For ..... 90 secs  
IP Address..... 10.105.211.75  
Gateway Address..... 10.105.211.1  
Netmask..... 255.255.255.128  
Mobility State.....

**Export Anchor**

Mobility Foreign IP Address.....

10.76.118.70

Security Policy Completed..... No  
Policy Manager State.....

**WEBAUTH\_REQD**

Pre-auth IPv4 ACL Name.....

**Pre-Auth\_ACLPre-auth**

IPv4 ACL Applied Status..... Yes  
Pre-auth IPv4 ACL Applied Status.....



Yes

在身份驗證客戶端轉換到RUN狀態之後。

<#root>

```
show client detail a0:ce:c8:c3:a9:b5
Client MAC Address..... a0:ce:c8:c3:a9:b5
Client Username .....
testuser
Client Webauth Username .....
testuser
Client State.....
Associated
User Authenticated by .....
RADIUS Server
Client User Group..... testuser
Client NAC OOB State..... Access
Connected For ..... 37 secs
IP Address.....
10.105.211.75
Gateway Address..... 10.105.211.1
Netmask..... 255.255.255.128
Mobility State.....
Export Anchor
Mobility Foreign IP Address..... 10.76.118.70
Security Policy Completed..... Yes
Policy Manager State.....
RUN
Pre-auth IPv4 ACL Name..... Pre-Auth_ACL
Pre-auth IPv4 ACL Applied Status..... Yes
EAP Type..... Unknown
Interface.....
wired-vlan-11
VLAN.....
11
Quarantine VLAN..... 0
```

疑難排解

## AireOS控制器調試

### 啟用客戶端調試

```
>debug client <H.H.H>
```

### 驗證是否已啟用除錯

```
>show debugging
```

若要停用除錯，請執行下列動作

```
debug disable-all
```

## 9800放射性痕跡

啟用無線電活動跟蹤以在CLI中為指定的MAC地址生成客戶端調試跟蹤。

啟用放射性追蹤的步驟：

確定所有條件式偵錯都已停用。

```
clear platform condition all
```

為指定的MAC地址啟用調試。

```
debug wireless mac <H.H.H> monitor-time <Time in seconds>
```

重現問題後，請停用調試以停止RA跟蹤收集。

```
no debug wireless mac <H.H.H>
```

一旦RA跟蹤停止，調試檔案將在控制器的bootflash中生成。

```
show bootflash: | include ra_trace
```

```
2728          179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

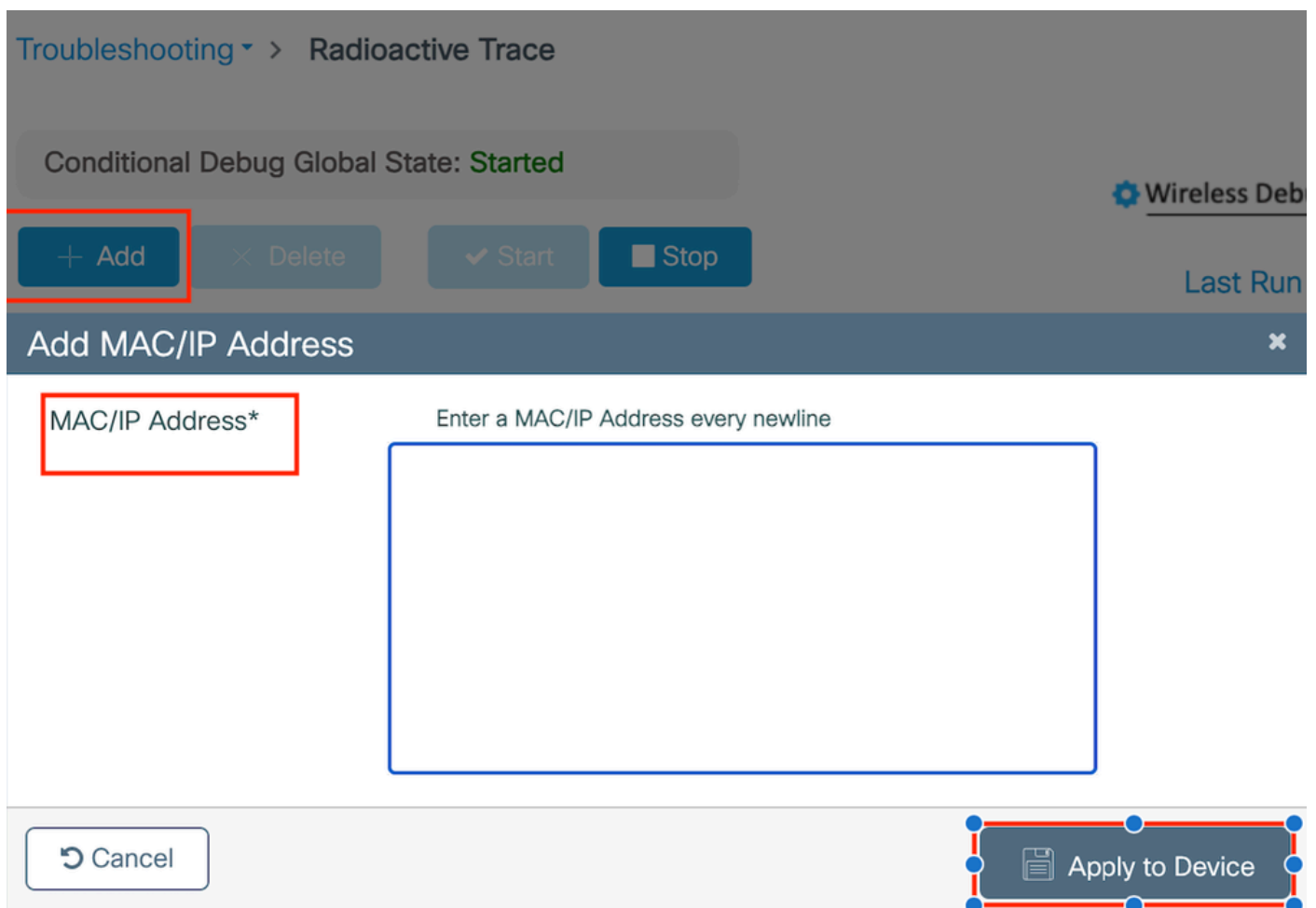
將檔案複製到外部伺服器。

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

顯示調試日誌：

```
more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

在GUI中啟用RA跟蹤，



在WebUI上啟用RA追蹤

### 內嵌式封包擷取

導航到故障排除>資料包捕獲。輸入捕獲名稱並指定客戶端的MAC地址作為內部過濾器MAC。將緩衝區大小設定為100，並選擇上行鏈路介面來監控傳入和傳出的資料包。

+ Add    × Delete

### Create Packet Capture

Capture Name\*    TestPCap

Filter\*    any

Monitor Control Plane

Inner Filter Protocol  DHCP

Inner Filter MAC

Buffer Size (MB)\*    100

Limit by\*    Duration    3600    secs ~ 1.00 hour

Available (12)    Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0

內嵌式封包擷取

注意：選擇「監控控制流量」選項以檢視重定向到系統CPU並重新注入資料平面的流量。

導航到故障排除>資料包捕獲，選擇開始捕獲資料包。

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	<input type="button" value="Start"/>

開始資料包捕獲

## CLI配置

```
monitor capture TestPCap inner mac <H.H.H>  
monitor capture TestPCap buffer size 100  
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both  
monitor capture TestPCap start
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

Packet Size to capture: 0 (no limit)

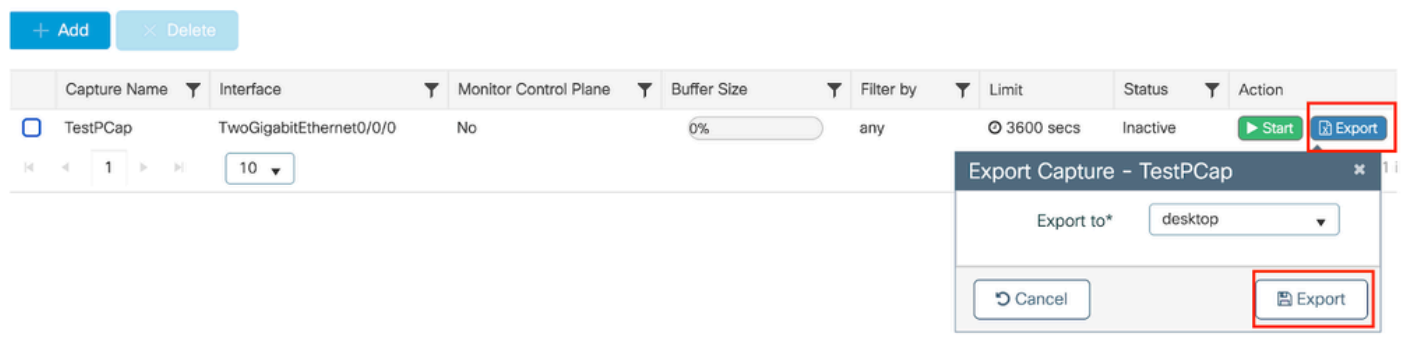
Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

將資料包捕獲導出到外部TFTP伺服器。

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```

導航到故障排除>資料包捕獲，選擇導出以將捕獲檔案下載到本地電腦上。



下載EPC

工作日誌片段

AireOS外部控制器客戶端調試日誌

從有線客戶端接收的有線資料包

\*apfReceiveTask: May 27 12:00:55.127: a0:ce:c8:c3:a9:b5 Wired Guest packet from 10.105.211.69 on mobi

## 外部控制器建立匯出錨點要求

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Attempting anchor export for mobile a0:ce:c8:c3:  
\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 mmAnchorExportSend: Building ExportForeignLradM  
\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 SGT Payload built in Export Anchor Req 0

外部控制器向錨點控制器傳送導出錨點請求。

\*apfReceiveTask: May 27 12:00:56.083: a0:ce:c8:c3:a9:b5 Export Anchor request sent to 10.76.118.70

## 錨點控制器為客戶端傳送錨點請求的確認

\*Dot1x\_NW\_MsgTask\_5: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Recvd Exp Anchor Ack for mobile a0:ce:c8:c3:

外部控制器上客戶端的移動角色已更新為導出外部。

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) mobility role update requ  
Peer = 10.76.118.70, Old Anchor = 10.76.118.70, New Anchor = 10.76.118.70

客戶端轉換到RUN狀態。

\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP\_REQD (7) State Update from Mobilit  
\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Stopping deletion of Mobile Station: (callerId:  
\*apfReceiveTask: May 27 12:00:56.091: a0:ce:c8:c3:a9:b5 Moving client to run state

## 9800放射性示蹤劑

使用者端與控制器關聯。

2024/07/15 04:10:29.087608331 {wncd\_x\_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b

關聯後移動性發現正在進行中。

```
2024/07/15 04:10:29.091585813 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5  
2024/07/15 04:10:29.091605761 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5
```

處理移動性發現後，客戶端漫遊型別是請求的L3更新。

```
2024/07/15 04:10:29.091664605 {wncd_x_R0-0}{1}: [mm-transition] [17765]: (info): MAC: a0ce.c8c3.a9b5 MM  
2024/07/15 04:10:29.091693445 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Roam t
```

外部控制器正在將導出錨點請求傳送到錨點WLC。

```
2024/07/15 04:10:32.093245394 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex  
2024/07/15 04:10:32.093253788 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Fo  
2024/07/15 04:10:32.093274405 {mobilityd_R0-0}{1}: [mm-client] [18316]: (info): MAC: a0ce.c8c3.a9b5 For
```

從錨點控制器接收導出錨點響應，並從使用者配置檔案應用vlan。

```
2024/07/15 04:10:32.106775213 {mobilityd_R0-0}{1}: [mm-transition] [18316]: (info): MAC: a0ce.c8c3.a9b5  
2024/07/15 04:10:32.106811183 {mobilityd_R0-0}{1}: [mm-client] [18316]: (debug): MAC: a0ce.c8c3.a9b5 Ex  
2024/07/15 04:10:32.107183692 {wncd_x_R0-0}{1}: [epm-misc] [17765]: (info): [a0ce.c8c3.a9b5:Tw0/0/0] An  
2024/07/15 04:10:32.107247304 {wncd_x_R0-0}{1}: [svm] [17765]: (info): [a0ce.c8c3.a9b5] Applied User Pr  
2024/07/15 04:10:32.107250258 {wncd_x_R0-0}{1}: [aaa-attr-inf] [17765]: (info): Applied User Profile:
```

處理導出錨點請求後，客戶端移動角色將更新為導出外部。

```
2024/07/15 04:10:32.107490972 {wncd_x_R0-0}{1}: [mm-client] [17765]: (debug): MAC: a0ce.c8c3.a9b5 Proce  
2024/07/15 04:10:32.107502336 {wncd_x_R0-0}{1}: [mm-client] [17765]: (info): MAC: a0ce.c8c3.a9b5 Mobili  
2024/07/15 04:10:32.107533732 {wncd_x_R0-0}{1}: [sanet-shim-translate] [17765]: (info): Anchor Vlan: 20  
2024/07/15 04:10:32.107592251 {wncd_x_R0-0}{1}: [mm-client] [17765]: (note): MAC: a0ce.c8c3.a9b5 Mobili
```

客戶端轉換到IP學習狀態。

```
2024/07/15 04:10:32.108210365 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b5  
2024/07/15 04:10:32.108293096 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: a0ce.c8c3.a9b5
```



在IP獲知後，客戶端在外部WLC上進入RUN狀態。

```
2024/07/15 04:10:32.108521618 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: a0ce.c8c3.a9b
```

### AireOS錨點控制器客戶端調試日誌

從外部控制器接收匯出錨點要求。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Anchor Export Request Recvd for mobile a0:c  
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv: Extracting mmPayloadExpo  
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv Ssid=Guest useProfileNa
```

本地橋接VLAN應用於客戶端。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Updated local bridging VLAN to 11 while app  
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 Applying Interface(wired-vlan-11) policy on  
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 After applying Interface(wired-vlan-11) pol
```

移動角色更新為「導出錨點」，客戶端狀態轉換為「關聯」。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5 0.0.0.0 START (0) mobility role update requ  
Peer = 10.76.118.70, Old Anchor = 0.0.0.0, New Anchor = 10.76.118.74  
Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5  
add client MAC a0:ce:c8:c3:a9:b5 IP 10.76.1  
*Dot1x_NW_MsgTask_5: May 28 10:46:27.831: a0:ce:c8:c3:a9:b5  
Sent message to add a0:ce:c8:c3:a9:b5 on me  
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 mmAnchorExportRcv (mm_listen.c:7933) Changi
```

移動已完成，客戶端狀態已關聯，移動角色為導出錨點。

```
*Dot1x_NW_MsgTask_5: May 28 10:46:27.832: a0:ce:c8:c3:a9:b5 0.0.0.0 DHCP_REQD (7) State Update from Mob
```

使用者端IP位址是在控制器上得知的，且狀態已從所需的DHCP轉換至所需的Web驗證。

```
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 Static IP client associated to interface wired-vlan  
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 dtlArpSetType: Changing ARP Type from 0 ---> 1 for  
*dtlArpTask: May 28 10:46:58.356: a0:ce:c8:c3:a9:b5 10.105.211.75 DHCP_REQD (7) Change state to WEBAUTH
```

Webauth URL是透過增加外部重定向URL和控制器虛擬IP地址來形成的。

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Preparing redirect URL according to configure
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Web-auth type External, using URL:http://10.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added switch_url, redirect URL is now http://
```

已將客戶端MAC地址和WLAN增加到URL。

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added client_mac , redirect URL is now http://
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- Added wlan, redirect URL is now http://10.127
```

剖析主機10.105.211.1的HTTP GET後的最終URL

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser host is 10.105.211.1
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- parser path is /auth/discovery
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5-added redirect=, URL is now http://10.127.196.
```

重定向URL傳送到200 OK響應資料包中的客戶端。

```
*webauthRedirect: May 28 10:46:58.500: a0:ce:c8:c3:a9:b5- 200 send_data =HTTP/1.1 200 OK
Location:http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&client_mac=a0
```

客戶端與重定向url主機建立TCP連線。一旦使用者端在入口端提交登入使用者名稱和密碼，控制器就會將radius要求傳送到radius伺服器

控制器收到Access-Accept後，客戶端關閉TCP會話並進入RUN狀態。

```
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Sending the packet to v4 host 10.197.224.122:18
*aaaQueueReader: May 28 10:46:59:077: a0:ce:c8:c3:a9:b5 Successful transmission of Authentication Packe
*aaaQueueReader: May 28 10:46:59:077: AVP[01] User-Name.....testuser
*aaaQueueReader: May 28 10:46:59:077: AVP[03] Calling-Station-Id.....a0-ce-c8
*aaaQueueReader: May 28 10:46:59:077: AVP[04] Nas-Port.....0x000000
*aaaQueueReader: May 28 10:46:59:077: AVP[05] Nas-Ip-Address.....0x0a4c76
*aaaQueueReader: May 28 10:46:59:077: AVP[06] NAS-Identifier.....POD1586-
*aaaQueueReader: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 radiusServerFallbackPassiveStateUpdate: RADIUS
*radiusTransportThread: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Access-Accept received from RADIUS serv
```

\*Dot1x\_NW\_MsgTask\_5: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Processing Access-Accept for mobile a0:ce:c

\*apfReceiveTask: May 28 10:46:59:500: a0:ce:c8:c3:a9:b5 Moving client to run state

## 9800錨點控制器放射性跟蹤

來自外部控制器的客戶端移動通告消息。

2024/07/15 15:10:20.614677358 {mobilityd\_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Re

當客戶端正在關聯時，從外部控制器接收導出錨點請求，該客戶端的導出錨點響應由錨點控制器傳送，可在外部控制器RA跟蹤上驗證。

2024/07/15 15:10:22.615246594 {mobilityd\_R0-0}{1}: [mm-transition] [15259]: (info): MAC: a0ce.c8c3.a9b5

客戶端已移至關聯狀態，移動角色已轉換為導出錨點。

2024/07/15 15:10:22.616156811 {wncd\_x\_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 15:10:22.627358367 {wncd\_x\_R0-0}{1}: [mm-client] [14709]: (note): MAC: a0ce.c8c3.a9b5 Mobili

2024/07/15 15:10:22.627462963 {wncd\_x\_R0-0}{1}: [dot11] [14709]: (note): MAC: a0ce.c8c3.a9b5 Client da

2024/07/15 15:10:22.627490485 {mobilityd\_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Ex

2024/07/15 15:10:22.627494963 {mobilityd\_R0-0}{1}: [mm-client] [15259]: (debug): MAC: a0ce.c8c3.a9b5 Fo

IP學習完成，客戶端IP透過ARP學習。

2024/07/15 15:10:22.628124206 {wncd\_x\_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5

2024/07/15 15:10:23.627064171 {wncd\_x\_R0-0}{1}: [sisf-packet] [14709]: (info): RX: ARP from interface m

2024/07/15 15:10:24.469704913 {wncd\_x\_R0-0}{1}: [client-iplearn] [14709]: (note): MAC: a0ce.c8c3.a9b5

2024/07/15 15:10:24.470527056 {wncd\_x\_R0-0}{1}: [client-iplearn] [14709]: (info): MAC: a0ce.c8c3.a9b5

2024/07/15 15:10:24.470587596 {wncd\_x\_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5

2024/07/15 15:10:24.470613094 {wncd\_x\_R0-0}{1}: [client-orch-sm] [14709]: (debug): MAC: a0ce.c8c3.a9b5

客戶端策略狀態為web auth pending。

```
2024/07/15 15:10:24.470748350 {wncd_x_R0-0}{1}: [client-auth] [14709]: (info): MAC: a0ce.c8c3.a9b5 Cli
```

TCP握手被控制器偽裝。當客戶端傳送HTTP GET時，會傳送200 OK響應幀，其中包含重定向URL。

使用者端必須與重新導向URL建立TCP交握並載入頁面。

```
2024/07/15 15:11:37.579177010 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579190912 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579226658 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:37.579230650 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123072893 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:11:47.123082753 {wncd_x_R0-0}{1}: [webauth-httpd] [14709]: (info): mobility_a0000001[a0ce
```

使用者端在Web入口頁面上提交登入認證時，會向RADIUS伺服器傳送存取要求封包以進行驗證。

```
2024/07/15 15:12:04.281076844 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Send Access-Request t
2024/07/15 15:12:04.281087672 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator e3 01
2024/07/15 15:12:04.281093278 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Calling-Station-Id
2024/07/15 15:12:04.281097034 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
2024/07/15 15:12:04.281148298 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Cisco AVpair
```

從RADIUS伺服器收到Access-Accept，webauth成功。

```
2024/07/15 15:12:04.683597101 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: Received from id 1812
2024/07/15 15:12:04.683607762 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: authenticator 52 3e
2024/07/15 15:12:04.683614780 {wncd_x_R0-0}{1}: [radius] [14709]: (info): RADIUS: User-Name
```

身份驗證成功，客戶端策略狀態為RUN。

```
2024/07/15 15:12:04.683901842 {wncd_x_R0-0}{1}: [webauth-state] [14709]: (info): mobility_a0000001[a0ce
2024/07/15 15:12:04.690643388 {wncd_x_R0-0}{1}: [errmsg] [14709]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/15 15:12:04.690726966 {wncd_x_R0-0}{1}: [aaa-attr-inf] [14709]: (info): [ Applied attribute :bs
2024/07/15 15:12:04.691064276 {wncd_x_R0-0}{1}: [client-orch-state] [14709]: (note): MAC: a0ce.c8c3.a9b
```

嵌入式資料包捕獲分析

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)

```

> Frame 806: 863 bytes on wire (6904 bits), 863 bytes captured (6904 bits)
> Ethernet II, Src: Cisco_59:31:4b (f4:bd:9e:59:31:4b), Dst: Cisco_34:90:cb (6c:5e:3b:34:90:cb)
> Internet Protocol Version 4, Src: 10.76.118.70, Dst: 10.76.6.156
> User Datagram Protocol, Src Port: 16667, Dst Port: 16667
> Control And Provisioning of Wireless Access Points - Data
> Ethernet II, Src: Cisco_34:90:d4 (6c:5e:3b:34:90:d4), Dst: CeLink_c3:a9:b5 (a0:ce:c8:c3:a9:b5)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4095
> Internet Protocol Version 4, Src: 10.105.211.1, Dst: 10.105.211.69
> Transmission Control Protocol, Src Port: 80, Dst Port: 54351, Seq: 1, Ack: 108, Len: 743
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Location: http://10.127.196.171/webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://10.105.211.1/auth/discovery?architecture=9\r\n
    Content-Type: text/html\r\n
  < Content-Length: 527\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.000000000 seconds]
    [Request in frame: 804]
    [Request URI: http://10.105.211.1/auth/discovery?architecture=9]
    File Data: 527 bytes

```

使用者端已重新導向至入口網站頁面

收到重定向URL後，會話關閉。

No.	Time	Source	Destination	Length	Protocol	Info
804	15:10:24.826953	10.105.211.69	10.105.211.1		HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
805	15:10:24.826953	10.105.211.1	10.105.211.69		TCP	80 → 54351 [ACK] Seq=1 Ack=108 Win=65152 Len=0 TSval=2124108437 TSecr=2231352500
806	15:10:24.826953	10.105.211.1	10.105.211.69		HTTP	HTTP/1.1 200 OK (text/html)
807	15:10:24.826953	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=108 Ack=744 Win=131008 Len=0 TSval=2231352500 TSecr=2124108437
812	15:10:24.835955	10.105.211.69	10.105.211.1		TCP	54351 → 80 [FIN, ACK] Seq=108 Ack=744 Win=131072 Len=0 TSval=2231352510 TSecr=2124108437
813	15:10:24.836947	10.105.211.1	10.105.211.69		TCP	80 → 54351 [FIN, ACK] Seq=744 Ack=109 Win=65152 Len=0 TSval=2124108447 TSecr=2231352510
814	15:10:24.836947	10.105.211.69	10.105.211.1		TCP	54351 → 80 [ACK] Seq=109 Ack=745 Win=131072 Len=0 TSval=2231352510 TSecr=2124108447

收到重新導向URL後，TCP作業階段關閉

客戶端發起到重定向URL主機的TCP 3次握手，並傳送HTTP GET請求。

頁面載入後，登入憑證會提交到入口網站，控制器會向radius伺服器傳送存取要求，以驗證使用者端。

身份驗證成功後，與Web伺服器的TCP會話關閉，並在控制器上將客戶端策略管理器狀態轉換為RUN。

No.	Time	Source	Destination	Length	Protocol	Info
2348	15:11:38.598968	10.105.211.69	10.127.196.171		TCP	54381 → 80 [SYN, ECE, CW] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=2678067533 TSecr=0
2349	15:11:38.599959	10.127.196.171	10.105.211.69		TCP	80 → 54381 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
2350	15:11:38.599959	10.105.211.69	10.127.196.171		TCP	54381 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
2351	15:11:38.600966	10.105.211.69	10.127.196.171		HTTP	GET /webauth/login.html?switch_url=https://192.0.2.1/login.html&redirect=http://3.3.3.3/
2352	15:11:38.602965	10.127.196.171	10.105.211.69		HTTP	[TCP Previous segment not captured] Continuation
2354	15:11:38.602965	10.127.196.171	10.105.211.69		TCP	[TCP Out-of-Order] 80 → 54381 [ACK] Seq=1 Ack=485 Win=2097408 Len=1380
2355	15:11:38.603957	10.105.211.69	10.127.196.171		TCP	[TCP Dup ACK 2350#1] 54381 → 80 [ACK] Seq=485 Ack=1 Win=262144 Len=0 SLE=1381 SRE=1737
2356	15:11:38.603957	10.105.211.69	10.127.196.171		TCP	54381 → 80 [ACK] Seq=485 Ack=1737 Win=260352 Len=0
2358	15:11:38.615965	10.105.211.69	10.127.196.171		HTTP	GET /webauth/yourlogo.jpg HTTP/1.1
2359	15:11:38.616957	10.127.196.171	10.105.211.69		HTTP	HTTP/1.1 304 Not Modified
2360	15:11:38.616957	10.105.211.69	10.127.196.171		TCP	54381 → 80 [ACK] Seq=1113 Ack=1880 Win=261952 Len=0
2362	15:11:38.621961	10.105.211.69	10.127.196.171		HTTP	GET /webauth/aup.html HTTP/1.1
2363	15:11:38.623960	10.127.196.171	10.105.211.69		HTTP	HTTP/1.1 304 Not Modified
2364	15:11:38.623960	10.105.211.69	10.127.196.171		TCP	54381 → 80 [ACK] Seq=1706 Ack=2023 Win=261952 Len=0
2747	15:12:04.280976	10.76.118.70	10.197.224.122		RADIUS	Access-Request id=0
2751	15:12:04.682963	10.197.224.122	10.76.118.70		RADIUS	Access-Accept id=0
2836	15:12:09.729957	10.105.211.69	10.127.196.171		HTTP	GET /webauth/logout.html HTTP/1.1
2837	15:12:09.731956	10.127.196.171	10.105.211.69		HTTP	HTTP/1.1 304 Not Modified
2838	15:12:09.731956	10.105.211.69	10.127.196.171		TCP	54381 → 80 [ACK] Seq=2186 Ack=2166 Win=261952 Len=0
4496	15:13:07.964946	10.105.211.69	10.127.196.171		TCP	54381 → 80 [FIN, ACK] Seq=2186 Ack=2166 Win=262144 Len=0
4497	15:13:07.964946	10.127.196.171	10.105.211.69		TCP	80 → 54381 [FIN, ACK] Seq=2166 Ack=2187 Win=2097408 Len=0
4498	15:13:07.965938	10.105.211.69	10.127.196.171		TCP	54381 → 80 [ACK] Seq=2187 Ack=2167 Win=262144 Len=0

客戶端向門戶頁面傳送HTTP GET請求並成功完成身份驗證

Radius存取要求封包



## 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）。