

使用AireOS和下一代WLC配置ISE無線CWA和熱點流

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[配置統一5508 WLC](#)

[全域性配置](#)

[配置訪客的服務集識別符號\(SSID\):](#)

[設定重新導向ACL](#)

[HTTPS重新導向](#)

[主動故障轉移](#)

[強制網路旁路](#)

[配置融合3850 NGWC](#)

[全域性配置](#)

[SSID配置](#)

[重新導向 ACL 組態](#)

[命令列介面\(CLI\)配置](#)

[配置ISE](#)

[常見ISE配置任務](#)

[使用案例1：在每個使用者連線中使用訪客身份驗證的CWA](#)

[使用案例2：具有裝置註冊的CWA每天強制執行一次訪客身份驗證。](#)

[使用案例3:HostSpot門戶](#)

[驗證](#)

[使用案例1](#)

[使用案例2](#)

[使用案例3](#)

[AireOS中的FlexConnect本地交換](#)

[Foreign-Anchor方案](#)

[疑難排解](#)

[AireOS和融合接入WLC上常見的斷開狀態](#)

[AireOS WLC](#)

[NGWC](#)

[ISE](#)

[相關資訊](#)

簡介

本文說明如何使用Cisco AireOS和下一代無線LAN控制器在身份服務引擎中配置三個訪客案例。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco無線LAN控制器 (整合和融合存取)
- 身分識別服務引擎 (ISE)

採用元件

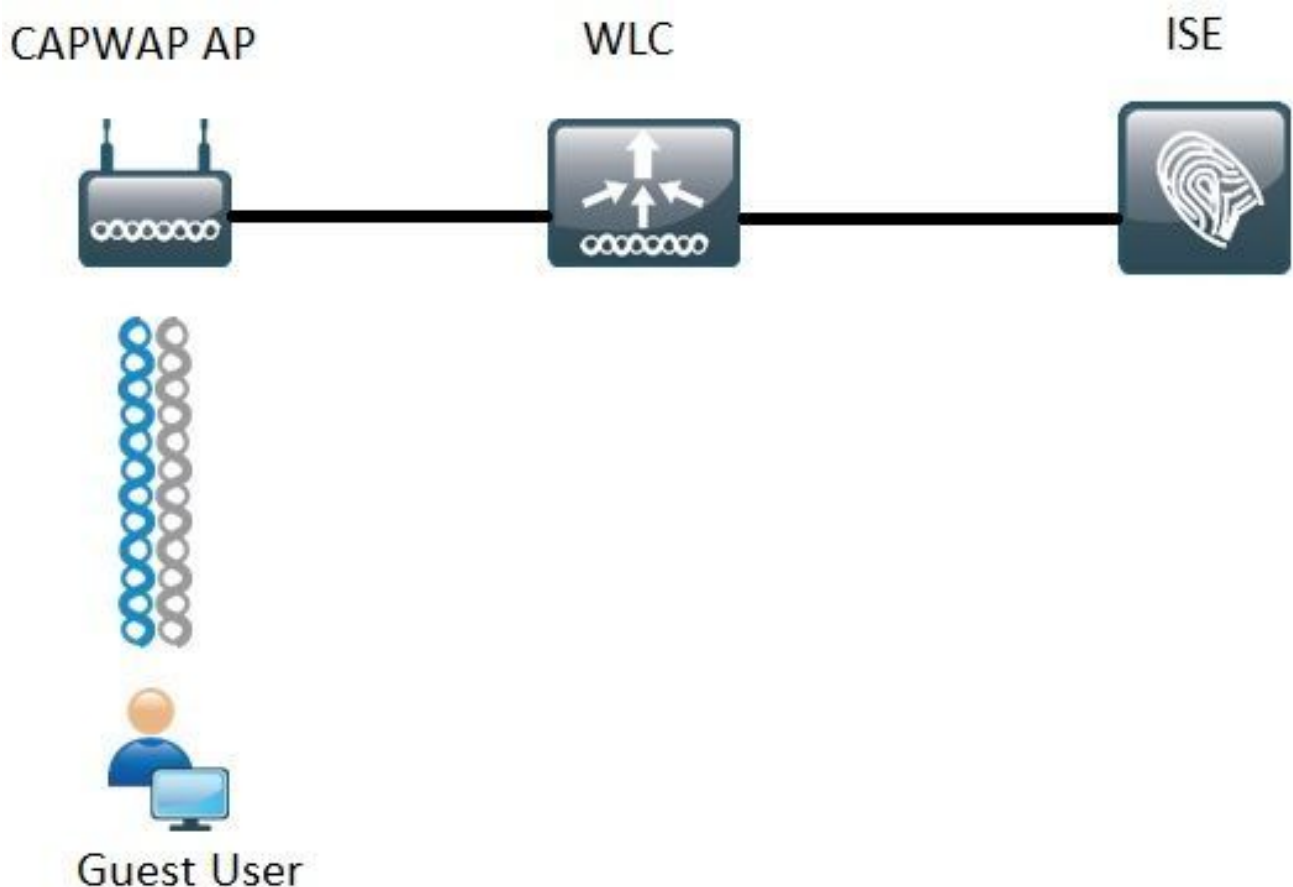
本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎版本2.1
- 採用8.0.121.0的Cisco無線LAN控制器5508
- 採用03.06.04.E的下一代無線控制器(NGWC)catalyst 3850(WS-C3850-24P)

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



本文檔中介紹的步驟描述了統一接入和融合接入WLC上的典型配置，以支援使用ISE的任何訪客流。

配置統一5508 WLC

無論在ISE中配置何種用例，從WLC的角度來看，它都以無線端點開始，該端點連線到啟用了MAC過濾的開放SSID（加AAA覆蓋和RADIUS NAC），該端點指向ISE作為身份驗證和記帳伺服器。這可確保ISE動態地將必要屬性推送到WLC，以便成功實施重定向到ISE的訪客門戶。

全域性配置

1. 將ISE全域性新增為身份驗證和記帳伺服器。

- 導覽至Security > AAA > Authentication，然後按一下New



- 輸入ISE伺服器IP和共用金鑰
- 確保「Server Status」和「Support for RFC 3676(Change of Authorization or CoA support)」都設定為「Enabled」。
- 在伺服器超時下，預設情況下AireOS WLC有2秒。取決於網路特性（延遲、不同位置的ISE和WLC），將伺服器超時至少增加到5秒可避免不必要的故障切換事件。
- 按一下「Apply」。
- 如果有多個要配置的策略服務節點(PSN)，請繼續建立其他伺服器條目。

注意：此特定配置示例包括2個ISE例項

- 導覽至Security > AAA > RADIUS > Accounting，然後按一下New
- 輸入ISE伺服器IP和共用金鑰
- 確保「伺服器狀態」設定為「已啟用」
- 如有必要，增加伺服器超時（預設值為2秒）。

2. 回退配置。

在統一環境中，一旦觸發伺服器超時，WLC將移至下一個配置的伺服器。WLAN中的下一行。如果沒有其它可用的專案，WLC會選擇全域伺服器清單中的下一個專案。當發生故障轉移後，在SSID（主、輔助）上配置多個伺服器時，WLC預設繼續將身份驗證和（或）記帳流量永久傳送至輔

助例項，即使主伺服器恢復聯機也是如此。

為了緩解此行為，啟用回退。導覽至**Security > AAA > RADIUS > Fallback**。預設行為為關閉。從伺服器關閉事件中恢復的唯一方法需要管理員干預（全域性退回伺服器的管理員狀態）。

要啟用回退，您有兩個選項：

- **被動** — 在被動模式下，如果伺服器沒有響應WLC身份驗證請求，WLC會將伺服器移動到非活動隊列並設定計時器（Interval in Sec選項）。計時器到期時，WLC會將伺服器移動到作用中佇列，而不論伺服器實際狀態如何。如果身份驗證請求導致超時事件（這意味著伺服器仍然處於關閉狀態），伺服器條目會再次移動到非活動隊列中，計時器再次啟動。如果伺服器成功作出響應，則它仍保留在活動隊列中。此處的可配置值範圍為180到3600秒。
- **Active** — 在主動模式下，當伺服器沒有響應WLC身份驗證請求時，WLC會將伺服器標籤為停機，然後將伺服器移動到非主動伺服器池，並定期開始傳送探測消息，直到該伺服器作出響應。如果伺服器回應，WLC會將失效伺服器移動到作用中池，並停止傳送探測訊息。

在此模式下，WLC要求您輸入使用者名稱和探測時間間隔（以秒為單位）（180到3600）。

注意：WLC探測不需要成功的身份驗證。無論哪種方式，成功或失敗的身份驗證都被視為伺服器響應，足以將伺服器提升到活動隊列。

設定訪客的服務組識別碼(SSID):

- 導覽至WLANs索引標籤，然後在Create New選項下按一下Go:



- 輸入配置檔名稱和SSID名稱。按一下「Apply」。
- 在General頁籤下，選擇要使用的介面或介面組（訪客VLAN）。



- 在**Security > Layer 2 > Layer 2 Security**下，選擇None並啟用Mac Filtering覈取方塊。



- 在AAA Servers頁籤下，將Authentication and Accounting servers設定為enabled，並選擇主伺服器 and 輔助伺服器。



- **臨時更新**：這是不向此流新增任何益處的可選配置。如果您偏好啟用WLC，WLC必須執行8.x或更高版本的代碼：

已禁用：功能已完全禁用。

啟用0間隔：每次客戶端的移動台控制塊(MSCB)條目(即IPv4或IPv6地址分配或更改，客戶端漫遊事件。)不會傳送其他定期更新。

啟用已配置的臨時間隔：在此模式下，WLC在客戶端的MSCB條目發生更改時向ISE傳送通知，並在已配置的間隔內傳送其他定期記帳通知(無論任何更改)。

- 在Advanced頁籤下的Enable **Allow AAA Override**下，在**NAC state**下，選擇**RADIUS NAC**。這可確保WLC應用來自ISE的任何屬性值對(AVP)。
- 導航到SSID general頁籤，將SSID狀態設定為**Enabled**

WLANs > Edit 'Guest'

General	Security	QoS	Policy-Mapping	Advanced
Profile Name	Guest			
Type	WLAN			
SSID	Guest			
Status	<input checked="" type="checkbox"/> Enabled			

- 應用更改。

設定重新導向ACL

此ACL由ISE引用，它確定重定向哪些流量以及允許哪些流量通過。

- 前往**Security**索引標籤 > **Access Control Lists**，然後按一下**New**
- 以下是ACL範例

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	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

此ACL必須允許通過TCP埠8443訪問DNS服務和ISE節點。底部有一個隱含的deny，表示其餘流量將重新導向到ISE的訪客門戶URL。

HTTPS重新導向

AireOS 8.0.x及更高版本支援此功能，但預設情況下會將其關閉。若要啟用HTTPS支援，請前往**WLC Management > HTTP-HTTPS > HTTPS Redirection**，並將其設定為**Enabled**，或在CLI中應用此命令：

```
(Cisco Controller) >config network web-auth https-redirect enable
```

啟用HTTPS重定向後的證書警告

啟用https-redirect後，使用者在重新導向期間可能會遇到憑證信任問題。即使控制器上存在有效的鏈結憑證，且此憑證是由第三方受信任的憑證授權機構簽署，也會發生這種情況。原因在於，WLC上安裝的憑證已核發給其虛擬介面主機名或IP位址。使用者端嘗試https://cisco.com時，瀏覽器預期憑證將核發到cisco.com。但是，WLC若要能夠擷取使用者端核發的GET，首先需要建立HTTPS作業階段，在SSL交握階段期間，WLC會出示其虛擬介面憑證。這會導致瀏覽器顯示警告

，因為在SSL交握期間顯示的憑證尚未核發給使用者端嘗試存取的原始網站(例如，cisco.com與WLC的虛擬介面主機名相對)。您可以在不同的瀏覽器中看到不同的證書錯誤消息，但所有消息都與同一問題有關。

主動故障轉移

AireOS WLC中預設啟用此功能。啟用主動故障切換後，WLC會將AAA伺服器標籤為無響應，並在RADIUS超時事件影響一個客戶端後，移動到下一個配置的AAA伺服器。

如果禁用此功能，則只有在至少3個客戶端會話發生RADIUS超時事件時，WLC才會故障切換到下一台伺服器。此功能可由此命令禁用（此命令不需要重新啟動）：

```
(Cisco Controller) >config radius aggressive-failover disable
```

驗證功能的當前狀態：

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

強制網路旁路

支援強制網路助理(CNA)機制以發現強制網路門戶並自動啟動登入頁面的終端通常在受控視窗中通過偽瀏覽器執行此操作，而其他終端則啟動完全可用的瀏覽器以觸發此功能。對於CNA啟動偽瀏覽器的終端，這可能會中斷流重定向至ISE強制網路門戶時。這通常影響Apple IOS裝置，在需要裝置註冊、VLAN DHCP釋放、合規性檢查的流中尤其有負面影響。

取決於使用的流量的複雜性，建議啟用強制旁路。在這種情況下，WLC會忽略CNA入口探索機制，且使用者端需要開啟瀏覽器以啟動重新導向程式。

驗證功能的狀態：

```
(Cisco Controller) >show network summary
```

```
Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

若要啟用此功能，請鍵入以下命令：

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

WLC會提醒使用者，只有重設系統（重新啟動）才能使變更生效。

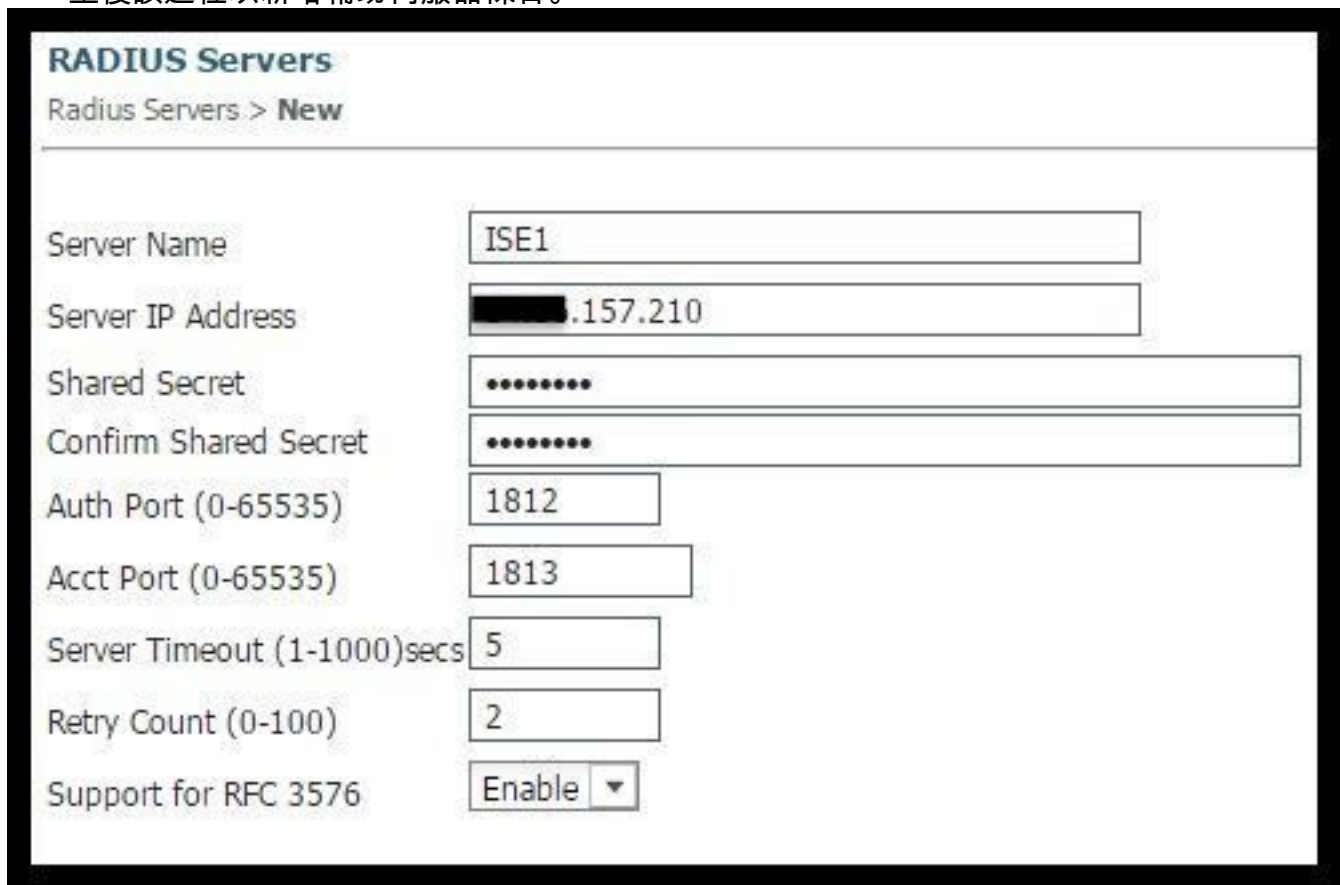
此時，**show network summary**會顯示功能已啟用，但要使更改生效，需要重新啟動WLC。

配置融合3850 NGWC

全域性配置

1. 將ISE全域性新增為身份驗證和記帳伺服器

- 導覽至**Configuration > Security > RADIUS > Servers**，然後按一下**New**
- 輸入反映您環境條件的ISE伺服器IP地址、共用金鑰、伺服器超時和重試計數。
- 確保啟用RFC 3570支援（CoA支援）。
- 重複該過程以新增輔助伺服器條目。



Field	Value
Server Name	ISE1
Server IP Address	[REDACTED].157.210
Shared Secret	*****
Confirm Shared Secret	*****
Auth Port (0-65535)	1812
Acct Port (0-65535)	1813
Server Timeout (1-1000)secs	5
Retry Count (0-100)	2
Support for RFC 3576	Enable

2. 建立ISE的伺服器組

- 導航到**Configuration > Security > Server Groups**，然後點選**New**
- 為組分配名稱並輸入**Dead-time**值（分鐘）。這是控制器將伺服器保持在非活動隊列中的時間，然後才會將其再次提升到活動伺服器清單。
- 從**Available Servers**清單中將它們新增到**Assigned Servers**列。

Radius Server Group
Radius Server Group > New

Name: ISE_Group

MAC-delimiter: colon

MAC-filtering: none

Dead-time (0-1440) in minutes: 10

Group Type: radius

Servers In This Group

Available Servers

Assigned Servers: ISE2, ISE1

3. 全局啟用Dot1x

- 導覽至Configuration > AAA > Method Lists > General，然後啟用Dot1x system Auth Control

General

Dot1x System Auth Control

Local Authentication: None

Local Authorization: None

4. 配置方法清單

- 導覽至Configuration > AAA > Method Lists > Authentication，然後建立一個新的方法清單。在本例中，它是Type Dot1x and Group ISE_Group（在上一步中建立的組）。然後按下Apply

Authentication
Authentication > New

Method List Name: ISE_Method

Type: dot1x login

Group Type: group local

Fallback to local:

Groups In This Method

Available Server Groups

Assigned Server Groups: ISE_Group

- 對記帳(Configuration > AAA > Method Lists > Accounting)和授權(Configuration > AAA >

Method Lists > Authorization)執行相同操作。他們一定像這樣

The screenshot shows the 'Accounting' configuration page. The 'Method List Name' is 'ISE_Method'. The 'Type' is 'identity', selected with a radio button. Below, there are two list boxes: 'Available Server Groups' (empty) and 'Assigned Server Groups' (containing 'ISE_Group'). Navigation arrows are between the lists.

The screenshot shows the 'Authorization' configuration page. The 'Method List Name' is 'ISE_Method'. The 'Type' is 'network', selected with a radio button. The 'Group Type' is 'group', selected with a radio button. Below, there are two list boxes: 'Available Server Groups' (empty) and 'Assigned Server Groups' (containing 'ISE_Group'). Navigation arrows are between the lists.

5. 建立授權MAC過濾器方法。

稍後從SSID設定呼叫此功能。

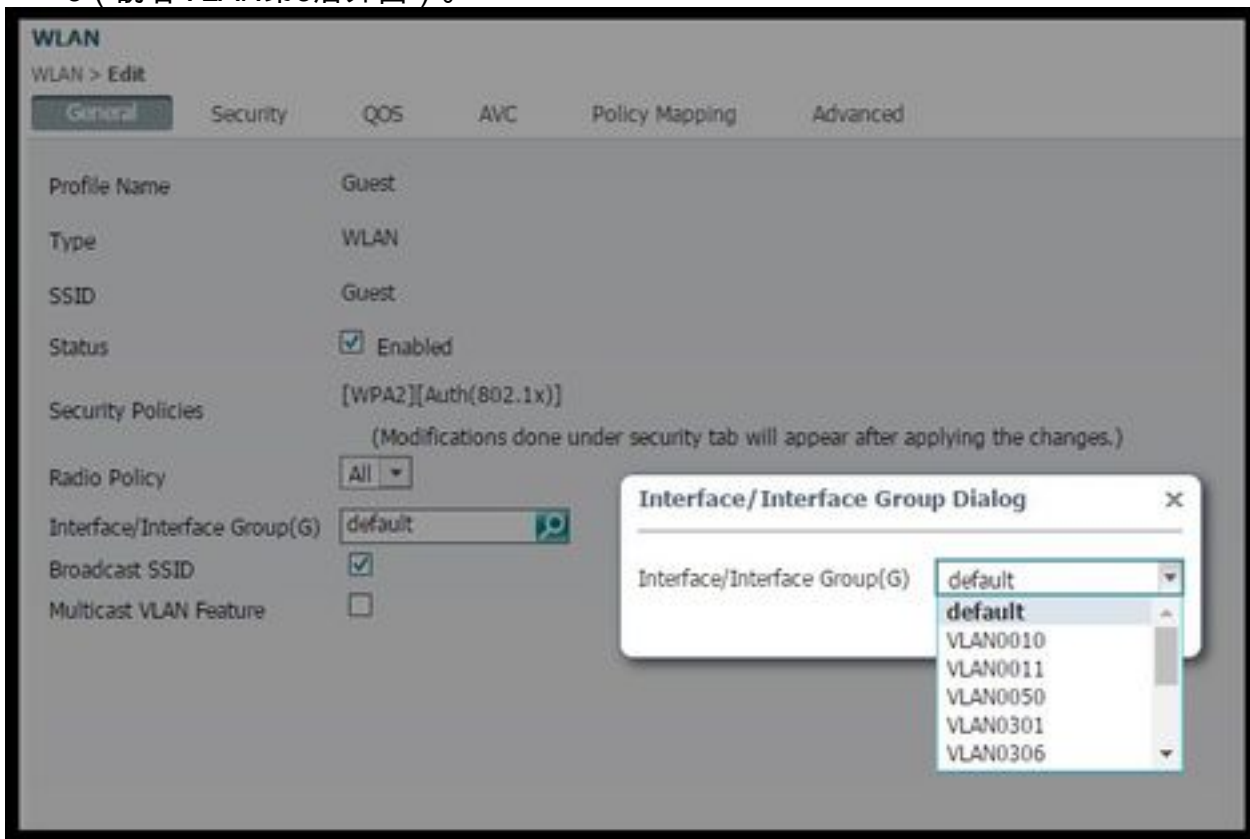
- 導覽至Configuration > AAA > Method Lists > Authorization，然後按一下New。
- 輸入方法清單名稱。選擇Type = Network和Group Type Group。
- 將ISE_Group新增到Assigned Server Groups欄位。

The screenshot shows the 'Authorization' configuration page for a new method list named 'MacFilterMethod'. The 'Type' is 'network', selected with a radio button. The 'Group Type' is 'group', selected with a radio button. Below, there are two list boxes: 'Available Server Groups' (empty) and 'Assigned Server Groups' (containing 'ISE_Group'). Navigation arrows are between the lists.

SSID配置

1. 建立訪客SSID

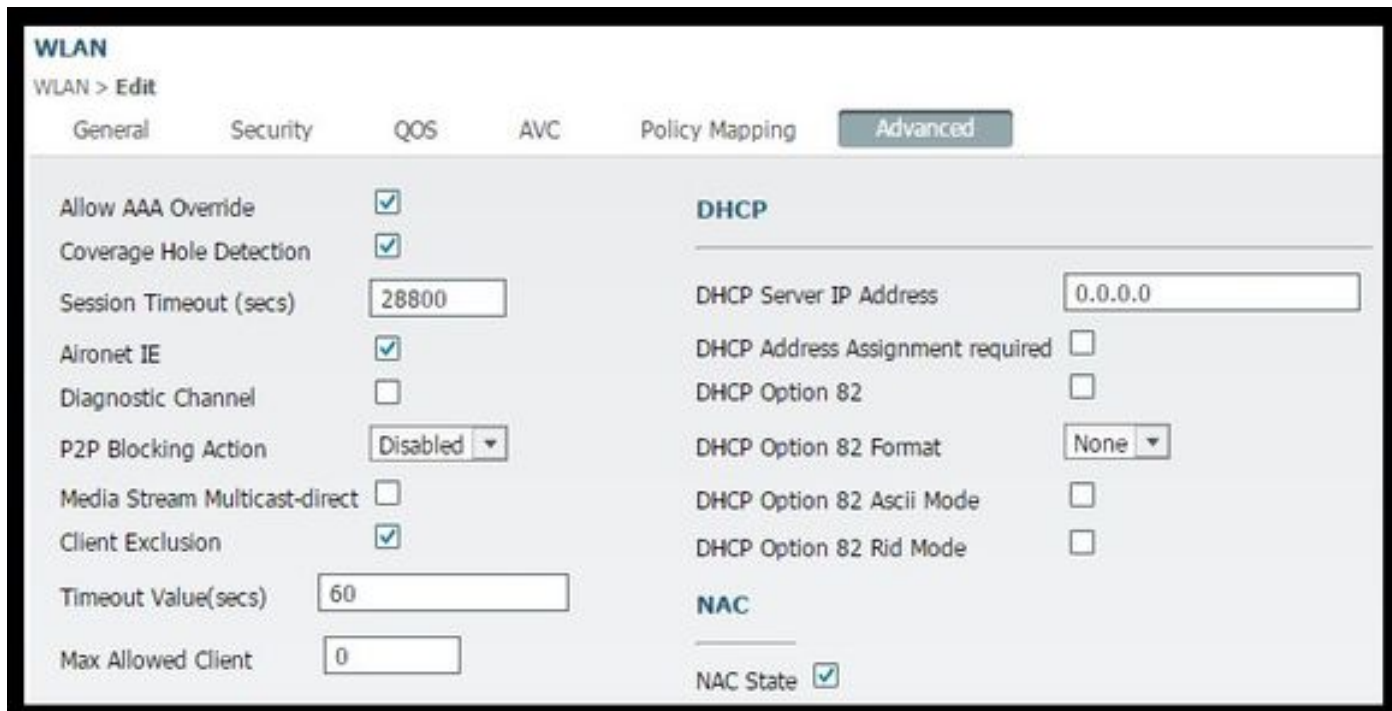
- 導覽至**Configuration > Wireless > WLANs**，然後按一下**New**
- 輸入WLAN ID、SSID和Profile Name，然後點選Apply。
- 進入Interface / Interface Group (介面/介面組) 下的SSID設定後，選擇Guest VLAN Layer 3 (訪客VLAN第3層介面)。



- 在**Security > Layer 2**下，選擇**None**，然後在**Mac Filtering**旁邊輸入先前設定的Mac Filter Method清單名稱(MacFilterMethod)。
- 在**Security > AAA Server**頁籤下，選擇正確的身份驗證和記帳方法清單(ISE_Method)。



- 在Advanced頁籤下，啟用Allow AAA Override and NAC state。必須根據每個部署要求調整其餘設定（會話超時、客戶端排除、支援Aironet擴展）。



WLAN
WLAN > Edit

General Security QOS AVC Policy Mapping **Advanced**

Allow AAA Override
 Coverage Hole Detection
 Session Timeout (secs)
 Aironet IE
 Diagnostic Channel
 P2P Blocking Action
 Media Stream Multicast-direct
 Client Exclusion
 Timeout Value(secs)
 Max Allowed Client

DHCP

DHCP Server IP Address
 DHCP Address Assignment required
 DHCP Option 82
 DHCP Option 82 Format
 DHCP Option 82 Ascii Mode
 DHCP Option 82 Rid Mode

NAC

NAC State

- 導航到「常規」頁籤，將「狀態」設定為「已啟用」。然後按下Apply。

重新導向 ACL 組態

此ACL稍後會由ISE在響應初始MAB請求的access-accept中引用。NGWC使用它來確定要重定向的流量以及必須允許通過的流量。

- 導覽至configuration > security > ACL > Access Control Lists，然後按一下Add New。
- 選擇擴展並輸入ACL名稱。
- 此圖顯示典型重新導向ACL的範例：



Access Control Lists
ACLs > ACL detail

Details :

Name: **Guest_Redirect**
 Type: **IPv4 Extended**

Add Sequence Remove

	Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
<input type="radio"/>	10	deny	icmp	any	any	-	-
<input type="radio"/>	20	deny	udp	any	any	-	eq 67
<input type="radio"/>	30	deny	udp	any	any	-	eq 68
<input type="radio"/>	40	deny	udp	any	any	-	eq 53
<input type="radio"/>	50	deny	tcp	any	[redacted].157.210	-	eq 8443
<input type="radio"/>	60	deny	tcp	any	[redacted].157.21	-	eq 8443
<input type="radio"/>	70	permit	tcp	any	any	-	eq 80
<input type="radio"/>	80	permit	tcp	any	any	-	eq 443

註：第10行是可選行。此內容通常新增到故障排除建議中。此ACL必須允許訪問DHCP、

DNS服務以及ISE伺服器埠TCP 8443 (拒絕ACE)。HTTP和HTTPS流量被重定向 (允許ACE)。

命令列介面(CLI)配置

前面步驟中討論的所有配置也可通過CLI應用。

802.1x全域性啟用

```
dot1x system-auth-control
```

全域性AAA配置

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

Wlan配置

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
```

```
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

重新導向ACL範例

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

HTTP和HTTPS支援

```
3850#show run | inc http
ip http server
ip http secure-server
```

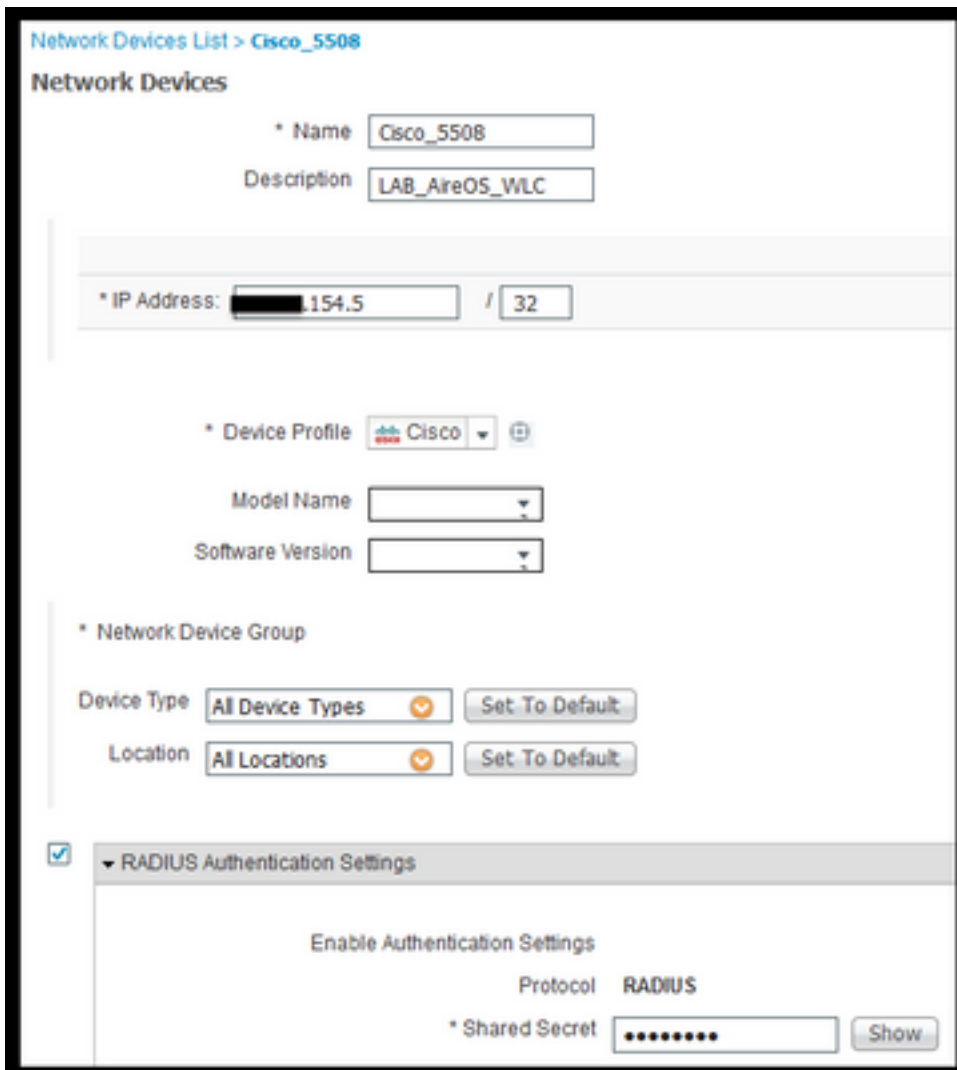
註： 如果套用ACL來限制透過HTTP對WLC的存取，則會影響重新導向。

配置ISE

本節介紹ISE上支援本文檔中討論的所有使用案例所需的配置。

常見ISE配置任務

1. 登入到ISE並導航到**Administration > Network Resources > Network Devices**，然後點選Add
2. 輸入與WLC關聯的**Name**和裝置的**IP地址**。
3. 選中**RADIUS身份驗證設定框**，並鍵入WLC端配置的**共用金鑰**。然後按一下Submit。

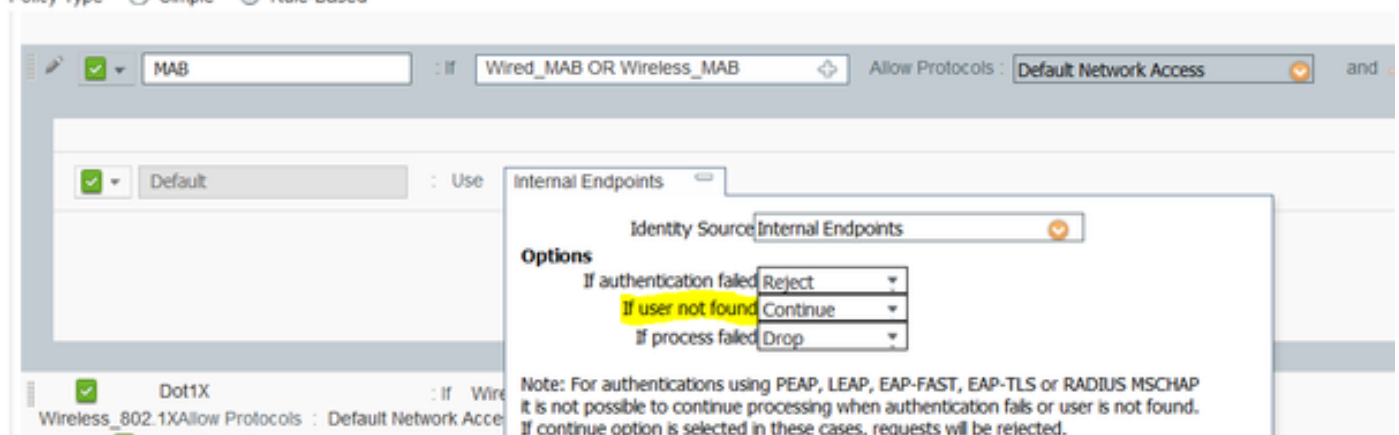


4. 導航到 Policy > Authentication，然後在 MAB 下按一下 Edit，並確保在 Use: Internal Endpoints 下，將 If user not found 選項設定為 Continue (預設情況下必須存在)。

Authentication Policy

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

Policy Type Simple Rule-Based



使用案例1：在每個使用者連線中使用訪客身份驗證的CWA

流量概覽

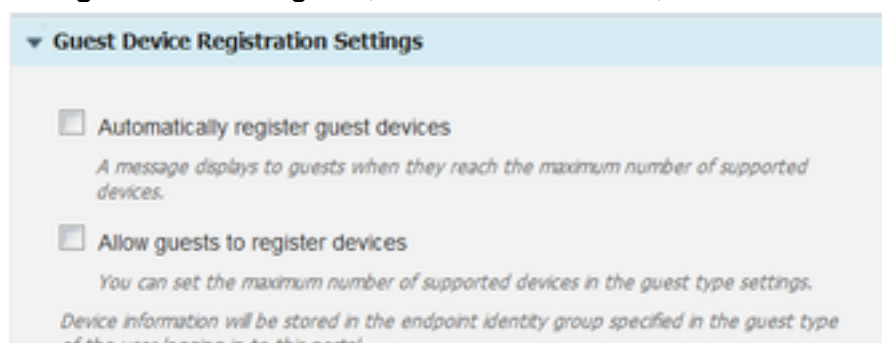
1. 無線使用者連線到訪客SSID。

2. WLC根據終端在ISE上的MAC地址作為AAA伺服器對終端進行身份驗證。
3. ISE使用兩個屬性值對(AVP)返回back和access-accept:url-redirect和url-redirect-acl。WLC將此AVP套用至終端作業階段後，站台會轉換為DHCP-Required，且一旦擷取IP位址，它就會保留在CENTRAL_WEB_AUTH中。在此步驟中，WLC準備開始重新導向使用者端的http/https流量。
4. 終端使用者開啟Web瀏覽器，在生成HTTP或HTTPS流量後，WLC會將使用者重定向到ISE訪客門戶。
5. 使用者進入Guest Portal後，會提示輸入訪客憑證（在此情況下由發起人建立）。
6. 憑證驗證後，ISE顯示AUP頁面，一旦使用者端接受，動態CoA型別Re-authenticate就會傳送到WLC。
7. WLC會重新處理MAC過濾驗證，而不向移動站發出解除驗證功能。這必須無縫到終端。
8. 發生重新身份驗證事件後，ISE會重新評估授權策略，這次終端被授予允許訪問許可權，因為之前有一個成功的訪客身份驗證事件。

每次使用者連線到SSID時，此過程都會自行重複。

組態

1. 導航到ISE並導航到工作中心(Work Centers)>訪客接入(Guest Access)>配置(Configure)>訪客門戶(Guest Portals)>選擇發起訪客門戶(Select Sponsored Guest Portal)（或建立新的門戶型別Sponsored-Guest）。
2. 在**Guest Device Registration** settings下，取消選中所有選項，然後按一下**Save**。



3. 定位至**Policy > Policy Elements > Results > Authorization > Authorization Profiles**。按一下「**Add**」。

4. 響應於初始Mac驗證略過(MAB)要求，此設定檔會以**Redirect-URL**和**Redirect-URL-ACL**向下推送到WLC。

- 選中Web重新導向(CWA、MDM、NSP、CPP)後，選擇Centralized Web Auth，然後在ACL欄位下輸入Redirect ACL名稱，然後在**Value**下選擇**Sponsored GuestPortal(default)**（或先前步驟中建立的任何其他特定入口）。

該配置檔案必須與此圖片中的配置檔案相似。然後按一下「**Save**」。

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

 Web Redirection (CWA, MDM, NSP, CPP)

 ACL

 Value
 Display Certificates Renewal Message

 Static IP/Host name/FQDN

頁面底部的屬性詳細資訊將屬性值對(AVP)推送到WLC

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5.定位至**Policy > Authorization**，然後插入新規則。此規則是用來觸發重新導向程式以回應來自WLC的初始MAC驗證要求的規則。(在本案例中稱為**Wireless_Guest_Redirect**)。

6.在**Conditions**下選擇**Select Existing Condition from Library**，然後在**condition name**下選擇**Compound condition**。選擇一個名為**Wireless_MAB**的預定義複合條件。

註：此條件包含從WLC發出的訪問請求中預期的2個Radius屬性(NAS-Port-Type= IEEE 802.11 <存在於所有無線請求中>和Service-Type = Call Check< (表示對mac身份驗證繞行的特定請求))

7.在結果下，選擇**Standard > CWA_Redirect** (在上一步中建立的授權配置檔案)。然後按一下「**Done**」和「**Save**」

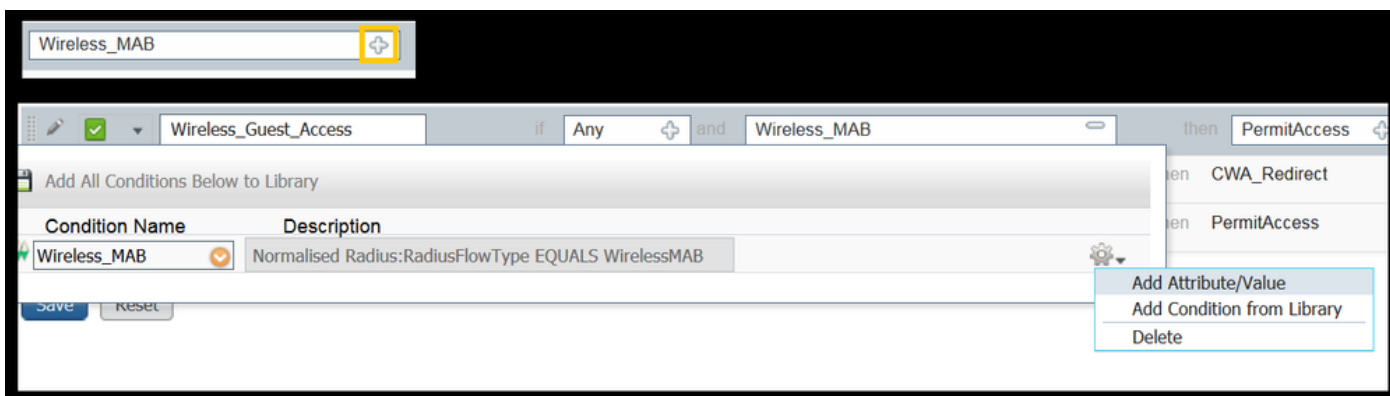
Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect

8.導航到**CWA_Redirect**規則的末尾，然後按一下**Edit**旁邊的箭頭。然後選擇**duplicate above**。

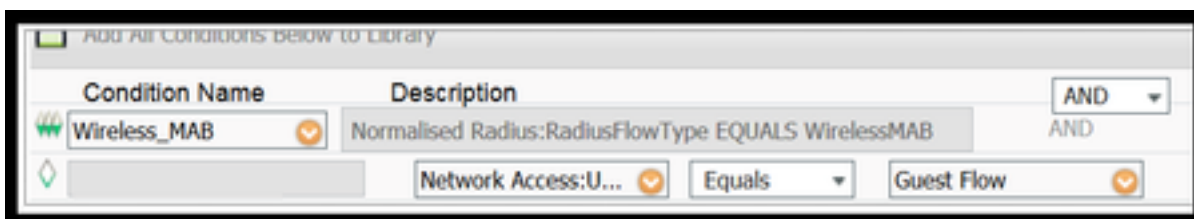
9.修改名稱，因為一旦會話在ISE的CoA (本例中為**Wireless_Guest_Access**) 上重新進行身份驗證，此策略即終端匹配。

10.在**Wireless_MAB**複合條件旁邊，按一下+符號展開條件，然後在**Wireless_MAB**條件結束時按一

下Add Attribute/Value。



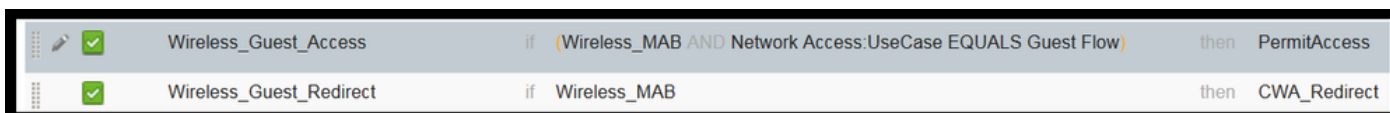
11.在「選擇屬性」下，選擇網路訪問>用例等於訪客流



12.在許可權下，選擇PermitAccess。然後按一下「Done」和「Save」



這兩個策略必須如下所示：



使用案例2：具有裝置註冊的CWA每天強制執行一次訪客身份驗證。

流量概覽

1. 無線使用者連線到訪客SSID。
2. WLC根據終端在ISE上的MAC地址作為AAA伺服器對終端進行身份驗證。
3. ISE使用兩個屬性值對(AVP) (url-redirect和url-redirect-acl) 返回back和access-accept。
4. WLC將此AVP套用至終端作業階段後，站台會轉換為DHCP-Required，且一旦擷取IP位址，它就會保留在CENTRAL_WEB_AUTH中。在此步驟中，WLC準備開始重新導向使用者端的http/https流量。
5. 終端使用者開啟Web瀏覽器，在生成HTTP或HTTPS流量後，WLC會將使用者重定向到ISE訪客門戶。
6. 使用者進入Guest Portal後，系統會提示他輸入發起人建立的憑據。
7. 憑證驗證後，ISE將此終端新增到特定（預配置的）終端身份組（裝置註冊）。
8. 顯示AUP頁面，一旦客戶端接受，就會出現動態CoA型別Re-authenticate。傳送到WLC。
9. WLC重新處理MAC過濾身份驗證，而不向移動站發出取消身份驗證。這必須無縫到終端。
10. 發生重新身份驗證事件後，ISE會重新評估授權策略。這一次，由於端點是正確端點身份組ISE的成員，ISE返回無限制的訪問接受。
11. 由於終結點已在步驟6中註冊，每次使用者返回時，都允許其在網路上，直到從ISE手動刪除

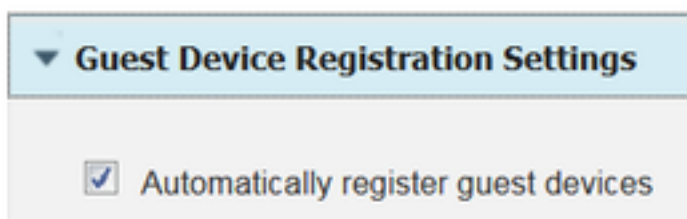
它，或者終端清除策略運行刷新符合條件的終結點。

在本實驗場景中，身份驗證每天執行一次。重新身份驗證觸發器是一個端點清除策略，它每天刪除已使用的端點身份組的所有端點。

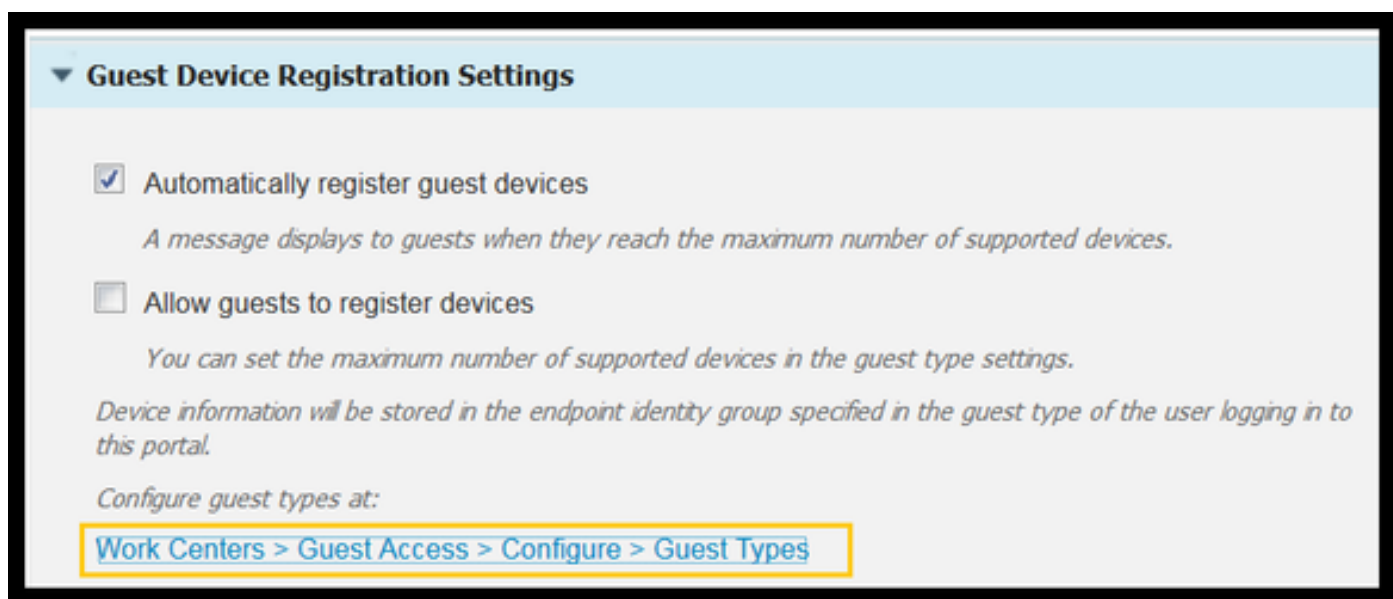
注意：可以根據自上次AUP接受以來經過的時間強制實施訪客身份驗證事件。如果您需要更頻繁地實施Guest Logon（例如每4小時），則可以選擇此選項。

組態

1. 在ISE上，導航至**工作中心>訪客接入>配置>訪客門戶**>選擇**發起訪客門戶**（或建立新的門戶型別Sponsored-Guest）。
2. 在**Guest Device Registration**設定下，驗證是否選中**Automatically register guest devices**選項。按一下「**Save**」。



3. 導航到**工作中心>訪客訪問>配置>訪客型別**，或只需按一下門戶中「訪客裝置註冊設定」下指定的快捷方式。



4. 發起人使用者建立訪客帳戶時，會為其分配訪客型別。每個單獨的訪客型別可以具有屬於不同終端身份組的註冊終結點。要分配裝置必須新增到的終端身份組，請選擇發起人用於這些訪客使用者的訪客型別(此使用案例基於每週（預設）)。

5. 進入訪客型別後，在**Login Options**下，從下拉選單**Endpoint Identity group for guest device registration**中選擇**Endpoint Group**

Maximum devices guests can register: (1-999)

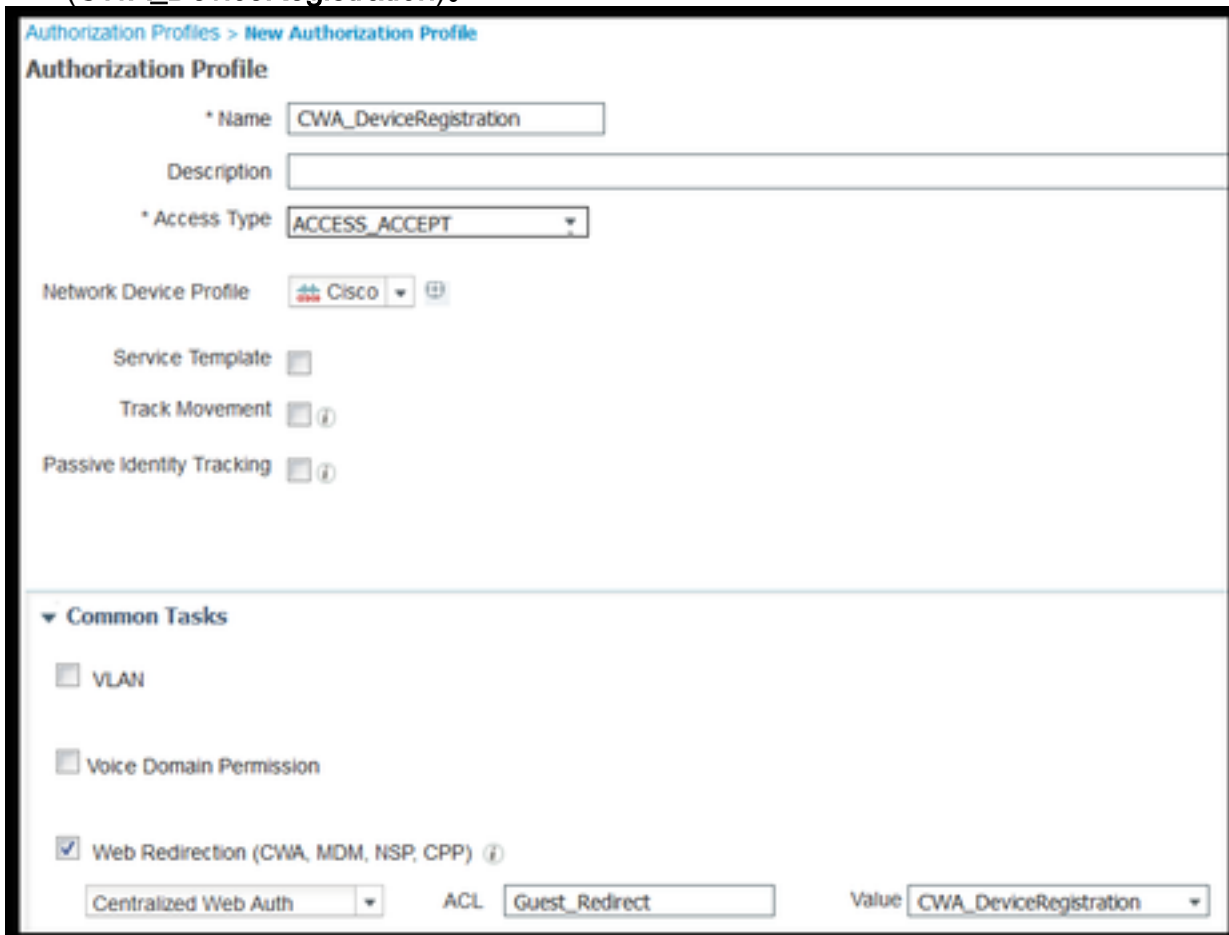
Endpoint identity group for guest device registration: ⓘ

6. 定位至**Policy > Policy Elements > Results > Authorization > Authorization Profiles**。按一下「

Add」。

7.響應於初始Mac驗證略過(MAB)請求，此設定檔會以Redirect-URL和Redirect-URL-ACL向下推送到WLC。

- 勾選完Web重新導向(CWA、MDM、NSP、CPP)後，選擇**Centralized Web Auth**，然後在**ACL**欄位下輸入重新導向ACL名稱，然後在**Value**下選擇為此流量建立的入口網站(CWA_DeviceRegistration)。



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: CWA_DeviceRegistration

Description: [Empty]

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template: [Unchecked]

Track Movement: [Unchecked]

Passive Identity Tracking: [Unchecked]

Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth: [Dropdown]

ACL: Guest_Redirect

Value: CWA_DeviceRegistration

8.定位至Policy > Authorization，然後插入一個新規則。此規則是用來觸發重新導向程式以回應來自WLC的初始MAC驗證要求的規則。(在本案例中稱為Wireless_Guest_Redirect)。

9.在Conditions下，選擇Select Existing Condition from Library，然後在condition name下，選擇Compound condition。選擇一個名為Wireless_MAB的預定義複合條件。

10.在「結果」下，選擇Standard > CWA_DeviceRegistration (在上一步中建立的授權配置檔案)。然後按一下「Done」和「Save」

Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

11.複製上述策略，修改其名稱，因為這是終端從重新身份驗證事件(稱為Wireless_Guest_Access)返回後觸發的策略。

12.在身份組詳細資訊框中，選擇終端身份組，然後選擇在「訪客型別」(GuestEndpoints)下引用的組。

13.在「結果」下，選擇PermitAccess。按一下「Done」，然後「Save」變更內容。

✓	Wireless_Guest_Access	if GuestEndpoints AND Wireless_MAB	then PermitAccess
✓	Wireless_Guest_Redirect	if Wireless_MAB	then CWA_DeviceRegistration

14. 建立並清除策略，以便每天清除訪客終端組。

- 導航到**管理>身份管理>設定>端點清除**
- 在**Purge**規則下，如果經過時間超過30天，預設情況下必須有一個觸發訪客終結點刪除的規則。
- 修改GuestEndpoints的現有策略或建立新策略（如果已刪除預設值）。請注意，清除策略在定義的時間裡每天運行。


在這種情況下，條件為已用天數小於1天的GuestEndpoints的成員

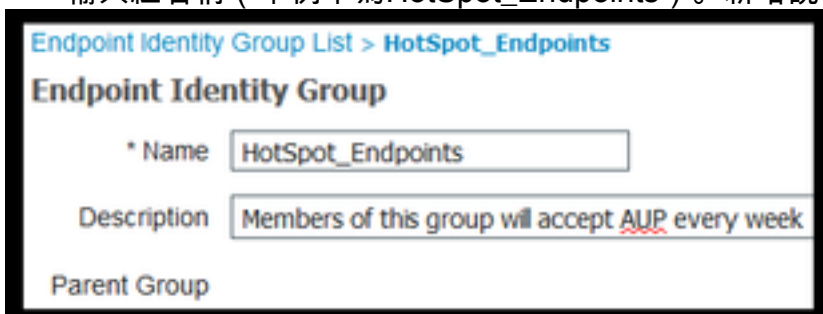
使用案例3:HostSpot門戶

流量概覽

1. 無線使用者連線到訪客SSID。
2. WLC使用ISE作為AAA伺服器，根據終端的MAC地址對終端進行身份驗證。
3. ISE返回具有兩個屬性值對(AVP)的access-accept:url-redirect和url-redirect-acl。
4. WLC將此AVP套用至終端作業階段後，站台會轉換為DHCP-Required，且一旦擷取IP位址，它就會保留在CENTRAL_WEB_AUTH中。在此步驟中，WLC準備重新導向使用者端的http/https流量。
5. 終端使用者開啟Web瀏覽器，在生成HTTP或HTTPS流量後，WLC會將使用者重定向到ISE熱點門戶。
6. 進入門戶後，系統會提示使用者接受可接受的使用策略。
7. ISE將終端MAC地址（終端ID）新增到已配置的終端身份組中。
8. 處理請求的策略服務節點(PSN)向WLC發出動態CoA型別Admin-Reset。
9. WLC處理完傳入CoA後，會向使用者端發出解除驗證碼（連線會因為使用者端傳回所需的時間而丟失）。
10. 客戶端重新連線後，會建立新的會話，因此ISE端沒有會話連續性。這意味著身份驗證作為一個新執行緒處理。
11. 由於終端已新增到已配置的終端身份組中，並且存在用於檢查終端是否屬於該組的授權策略，因此新身份驗證與此策略匹配。結果是完全訪問訪客網路。
12. 使用者不得再次接受AUP，除非終端身份對象由於終端清除策略從ISE資料庫中清除。

組態

1. 建立新的終端身份組以便在註冊時將這些裝置移動到。導航到**工作中心(Work Centers)>訪客訪問(Guest Access)>身份組(Identity Groups)>終端身份組(Endpoint Identity Groups)**，然後按一下  **Add**。
- 輸入組名稱（本例中為HotSpot_Endpoints）。新增說明，無需父組。



Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

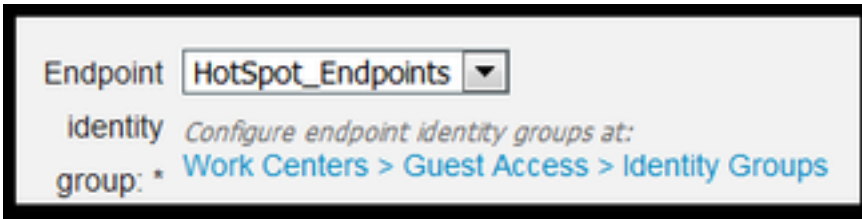
* Name

Description

Parent Group

2.定位至**工作中心>訪客訪問>配置>訪客門戶>選擇熱點門戶(預設)**。

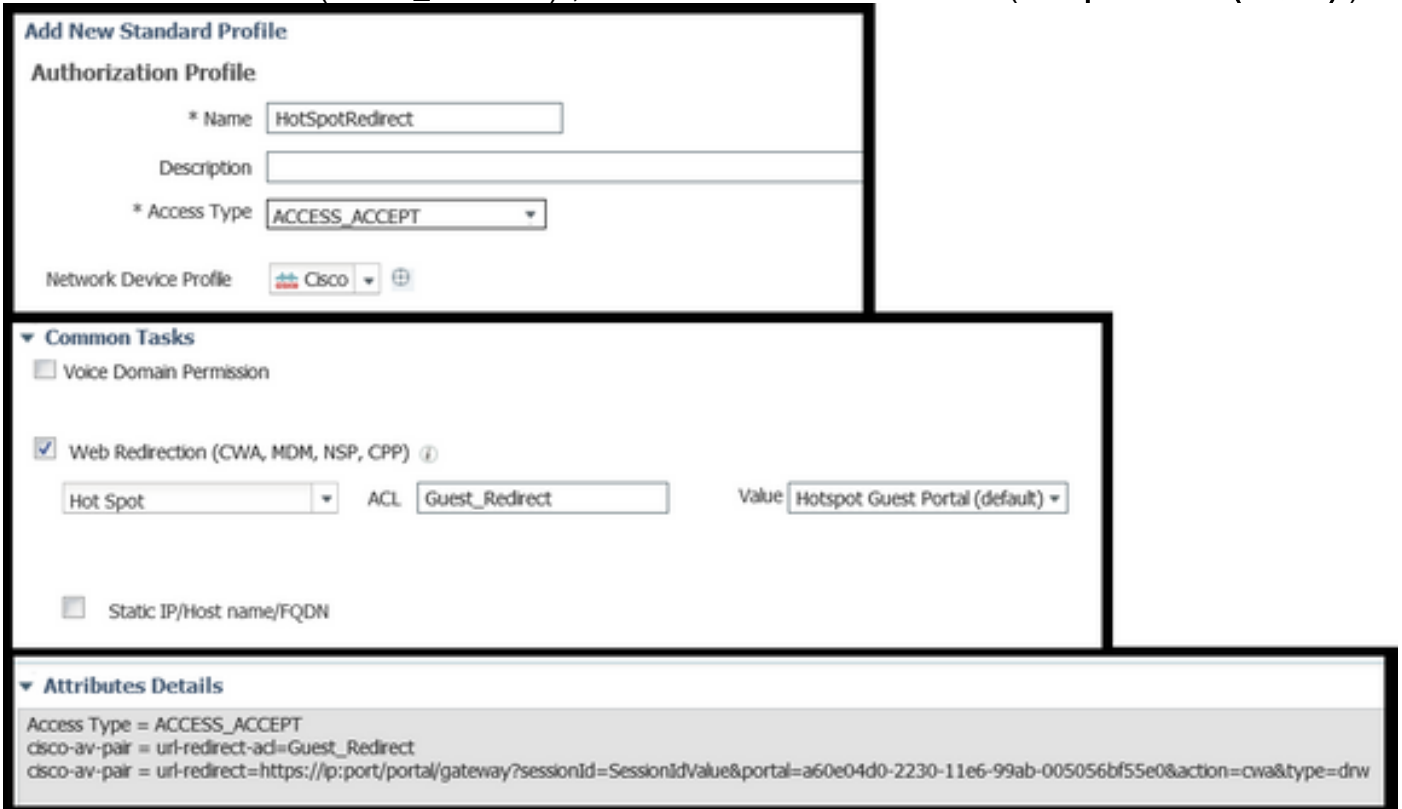
3.展開「門戶設定」，然後在「終端身份組」下選擇「終端身份組」下的HostSpot_Endpoints組。這會將註冊的裝置傳送到指定的組。



4.儲存更改。

5.建立在WLC發起的MAB身份驗證時呼叫HotSpot門戶的授權配置檔案。

- 導航到**Policy > Policy elements > Results > authorization > Authorization Profiles**並建立一個 (HotSpotRedirect)。
- 勾選**Web重新導向(CWA、MDM、NSP、CPP)**後，選擇**Hot Spot**，然後在ACL欄位中輸入Redirect ACL名稱(Guest_Redirect)，並作為值選擇正確的入口網站(Hotspot Portal (預設))。



6.建立授權策略，在WLC發出初始MAB請求時觸發HotSpotRedirect結果。

- 導航到**Policy > Authorization**並插入新規則。此規則是用來觸發重新導向程式以回應來自WLC的初始MAC驗證要求的規則。(在本案例中稱為Wireless_HotSpot_Redirect)。
- 在**Conditions**下選擇**Select Existing Condition from Library**，然後在**condition name**下選擇**Compound condition**
- 在「結果」下，選擇**Standard > HotSpotRedirect** (在上一步中建立的授權配置檔案)。然後按一下「Done」和「Save」

7.建立第二個授權策略。

- 複製上述策略，修改其名稱，因為這是終端從重新身份驗證事件（稱為 Wireless_HotSpot_Access）返回後觸發的策略。
- 在身份組詳細資訊框中，選擇端點身份組，然後選擇之前建立的組(HotSpot_Endpoints)。
- 在「結果」(Results)下，選擇PermitAccess。按一下「Done」，然後「Save」變更內容。

✓	Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
✓	Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

8.配置清除策略，清除經過時間大於5天的終結點。

- 導航到**管理>身份管理>設定>終端清除**，然後在「清除」規則下建立一個新規則。
- 在Identity Group Details框中，選擇Endpoint Identity Group > HotSpot_Endpoints
- 在conditions下，按一下Create New Condition(Advanced Option)。
- 在「選擇屬性」下選擇「ENDPOINTPURGE : ElapsedDays GREATER 5 days」

✓	HotSpot_Endpoints_PurgeRule	if HotSpot_Endpoints AND ENDPOINTPURGE:ElapsedDays GREATER THAN 5
---	-----------------------------	---

驗證

使用案例1

1. 使用者連線到訪客SSID。
2. 他開啟瀏覽器，一生成HTTP流量，就會顯示訪客門戶。
3. 訪客使用者驗證並接受AUP後，將顯示成功頁面。
4. 重新驗證的CoA被傳送（對客戶端透明）。
5. 端點作業階段會透過對網路的完整存取進行重新驗證。
6. 任何後續的訪客連線都必須通過訪客身份驗證，然後才能訪問網路。

CISCO Sponsored Guest Portal

Sign On
Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)



Sponsored Guest Portal

Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Sponsored Guest Portal

Success

You now have Internet access through this network.

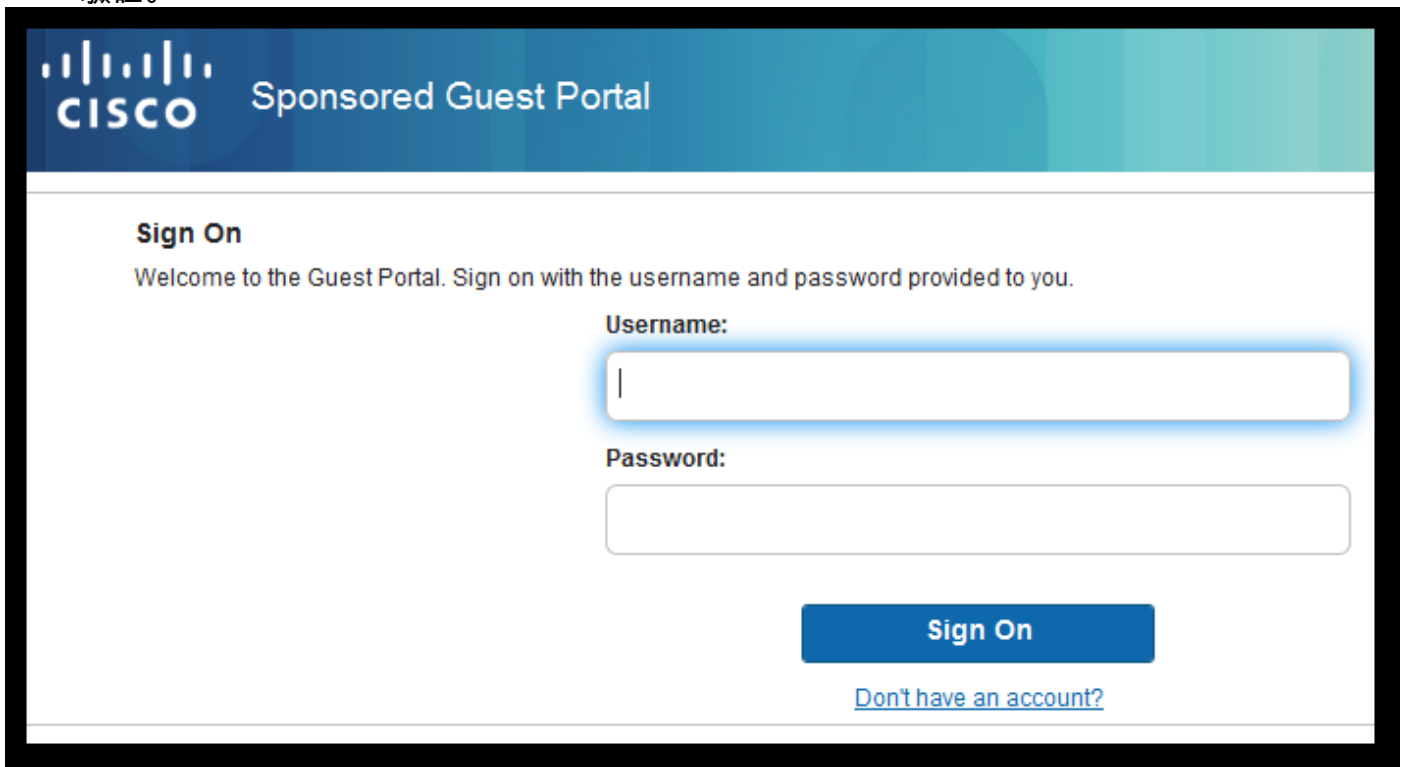
來自ISE RADIUS即時日誌的流量：

1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
	68:7F:74:72:18:2E					← CoA Event
1001	68:7F:74:72:18:2E					← Guest Authentication Event
68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

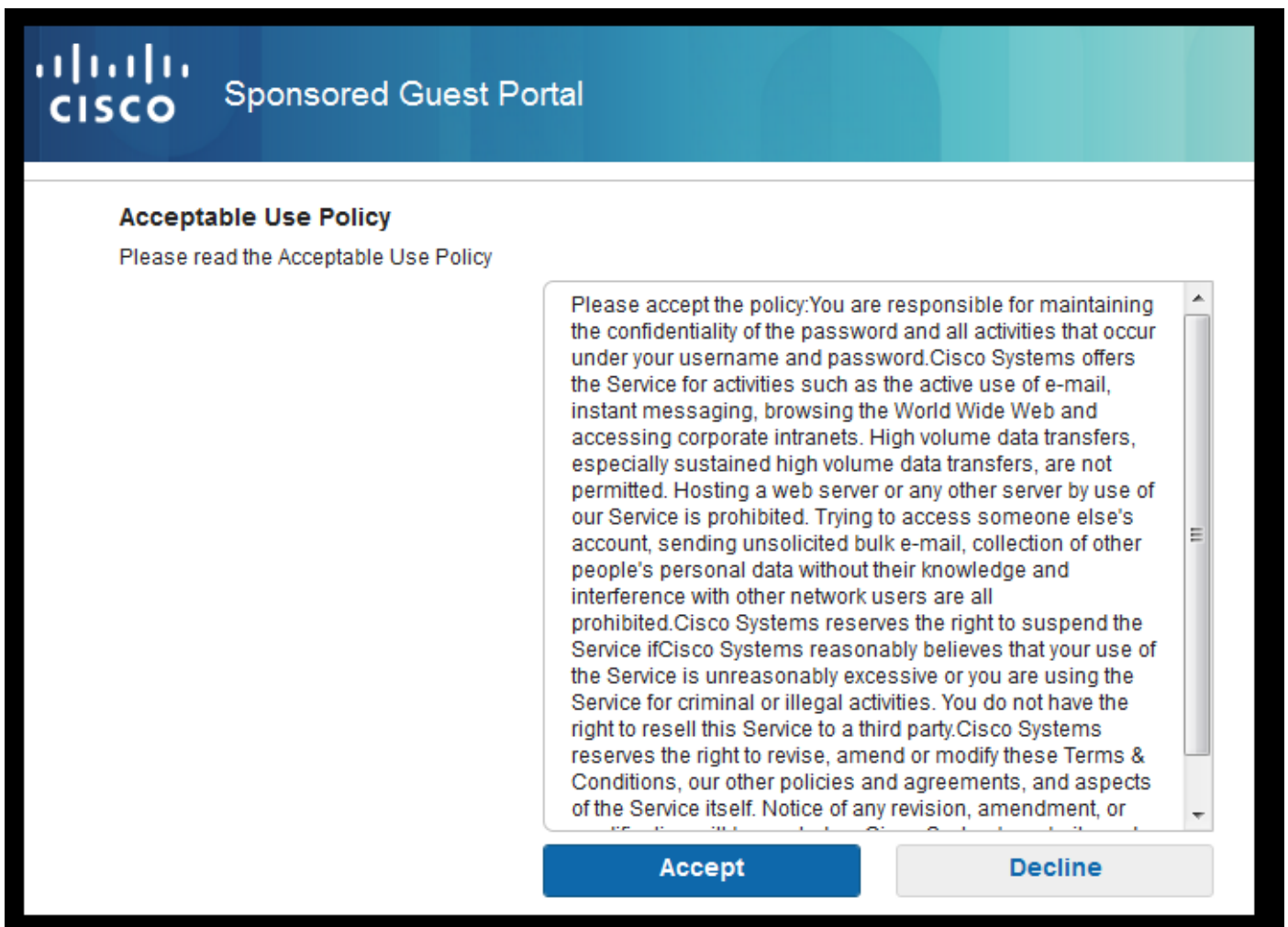
使用案例2

1. 使用者連線到訪客SSID。
2. 他開啟瀏覽器，一生成HTTP流量，就會顯示訪客門戶。
3. 訪客使用者驗證並接受AUP後，裝置即被註冊。

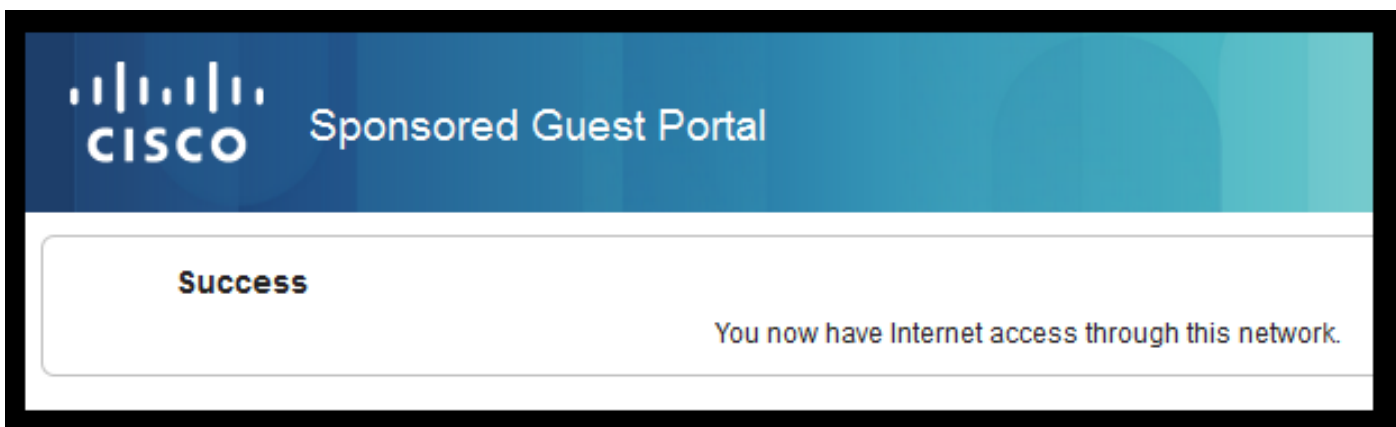
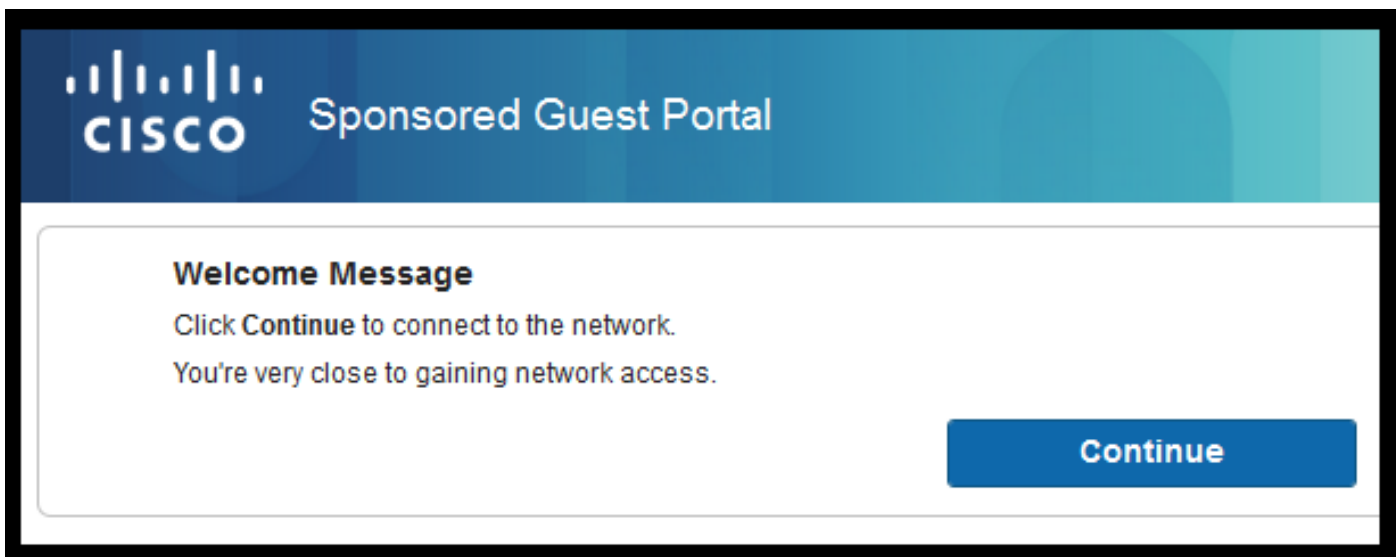
- 顯示成功頁面，並傳送Re-authenticate CoA (對客戶端透明)。
- 端點作業階段會透過對網路的完整存取進行重新驗證。
- 只要終端仍位於已配置的終端身份組中，就允許任何後續的Guest連線而不強制實施訪客身份驗證。



The screenshot shows the 'Sign On' section of the Cisco Sponsored Guest Portal. At the top left is the Cisco logo and the text 'Sponsored Guest Portal'. Below this, the heading 'Sign On' is followed by the instruction: 'Welcome to the Guest Portal. Sign on with the username and password provided to you.' There are two input fields: 'Username:' and 'Password:'. The 'Username:' field is currently empty and has a blue highlight. Below the input fields is a blue 'Sign On' button. At the bottom right, there is a blue link that says 'Don't have an account?'.



The screenshot shows the 'Acceptable Use Policy' section of the Cisco Sponsored Guest Portal. At the top left is the Cisco logo and the text 'Sponsored Guest Portal'. Below this, the heading 'Acceptable Use Policy' is followed by the instruction: 'Please read the Acceptable Use Policy'. A large text box contains the policy text: 'Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or...'. At the bottom of the text box are two buttons: a blue 'Accept' button and a grey 'Decline' button.



來自ISE RADIUS即時日誌的流量：

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	
■		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	GuestEndpoints
■		hfr592	68.7F:74.72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
■			68.7F:74.72:...		
■		hfr592	68.7F:74.72:...		GuestType_Contractor (default)
■		68.7F:74.72:1...	68.7F:74.72:...	CWA_DeviceRegistration	Profiled

Accounting Start

 Subsequent MAB request(no redirect to guest portal)

 Re-Authentication Event

 CoA Reauth Event

 Guest Authentication and Device Registration

 Initial MAB request

使用案例3

1. 使用者連線到訪客SSID。
2. 他開啟瀏覽器，一生成HTTP流量，就會顯示AUP頁面。
3. 訪客使用者接受AUP後，裝置即被註冊。
4. 將顯示成功頁面，並傳送管理重置CoA (對客戶端透明)。
5. 端點重新連線，具有對網路的完全訪問許可權。
6. 只要終端保持在已配置的終端身份組中，就允許任何後續突風連線而不強制執行AUP接受 (除非另外配置)。



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

AireOS中的FlexConnect本地交換

配置FlexConnect本地交換時，網路管理員需要確保：

- 重新導向ACL設定為FlexConnect ACL。
- 重定向ACL已作為策略應用，或者通過AP本身在FlexConnect頁籤 > External WebAuthentication ACLs > Policies > 選擇重定向ACL並按一下Apply

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

[Local Split ACLs](#)

[Central DHCP Processing](#)

[Layer2 ACLs](#)

Policies

Policy ACL **Add**

Policy Access Control Lists

CWA_Redirect

或者通過將策略ACL新增到FlexConnect組所屬的(Wireless > FlexConnect Groups > 選擇正確的組 > ACL Mapping > Policies 選擇重定向ACL並按一下Add)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL **Add**

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

新增策略ACL會觸發WLC將配置的ACL向下推送到FlexConnect組的AP成員。如果未能如此，會導致Web重新導向問題。

Foreign-Anchor方案

在自動錨點（外部錨點）場景中，必須突出顯示以下事實：

- 需要在外部和錨點WLC上定義重新導向ACL。即使只在錨點上強制執行。
- 第2層驗證一律由外部WLC處理。這在設計階段（也用於故障排除）非常重要，因為所有RADIUS身份驗證和記帳流量都發生在ISE和外部WLC之間。
- 重新導向AVP套用至使用者端作業階段後，外部WLC會透過行動切換訊息更新錨點中的使用者端作業階段。
- 此時，錨點WLC開始使用預先設定的重新導向ACL強制重新導向。
- 必須在錨點WLC SSID上完全關閉記帳，以避免來自錨點和外部的指向ISE的記帳更新（引用相同的身份驗證事件）。
- Foreign-Anchor方案不支援基於URL的ACL。

疑難排解

AireOS和融合接入WLC上常見的斷開狀態

1. 客戶端無法加入訪客SSID

show client detailed xx:xx:xx:xx:xx:xx」顯示客戶端停滯在START中。通常，這表示WLC無法套用AAA伺服器傳回的屬性。

驗證ISE推送的重定向ACL名稱是否與WLC上預定義ACL的名稱完全匹配。

相同原則適用於您已設定ISE以推送到WLC的任何其他屬性（VLAN ID、介面名稱、Airespace-ACL）。然後使用者端必須轉換為DHCP，然後轉換為CENTRAL_WEB_AUTH。

2. 重定向AVP已應用於客戶端會話，但重定向不起作用

驗證使用者端的原則管理員狀態是CENTRAL_WEB_AUTH，且有效的IP位址與為SSID設定的動態介面對齊，並且重新導向ACL和URL-Redirect屬性已套用到使用者端的作業階段。

重新導向ACL

在AireOS WLC中，重新導向ACL必須明確允許不得重新導向的流量，例如兩個方向的TCP連線埠8443上的DNS和ISE，而隱含的deny ip any any會觸發其餘流量重新導向。

在融合接入中，邏輯正好相反。允許ACE觸發重定向時，拒絕ACE繞過重定向。這就是建議明確允許TCP埠80和443的原因。

驗證通過埠8443從訪客VLAN訪問ISE。如果從配置角度看一切都好，則最簡單的前進方法是捕獲客戶端無線介面卡後面的捕獲並驗證重定向中斷的位置。

- 是否發生DNS解析？
- 針對請求的頁面是否完成了TCP 3次握手？
- 使用者端啟動GET後，WLC是否傳回重新導向動作？
- 與ISE通過8443的TCP三次握手是否已完成？

3. 在ISE在訪客流結束時推送VLAN更改後，客戶端無法訪問網路

一旦客戶端在流開始時抓取了IP地址（Pre Redirect狀態），如果發生Guest身份驗證（CoA後重新進行身份驗證）後推下VLAN更改，在訪客流中強制DHCP釋放/續約的唯一方法（無狀態代理）就是通過流動裝置中無法工作的Java小程式。

這會使客戶端在VLAN X中保持黑洞，IP地址為VLAN Y。 規劃解決方案時必須考慮這一點。

4. ISE在重定向期間在訪客客戶端瀏覽器中顯示「HTTP 500內部錯誤，找不到Radius會話」消息

這通常是ISE上會話丟失的指標（會話已終止）。發生此情況的最常見原因是已部署外部錨點時，在錨點WLC上設定了計量。 修復錨點上的此禁用記帳，並保留外部控制代碼身份驗證和記帳。

5. 在ISE的熱點門戶接受AUP後，客戶端斷開連線並保持斷開連線或連線到不同的SSID。

由於此流程中涉及的授權動態變更(CoA)（CoA管理員重設）會導致WLC向無線站發出deauth，因此熱點中可能會出現這種情況。大多數無線端點在解除驗證後沒有任何問題返回到SSID，但在某些情況下，客戶端會連線到另一個首選SSID以響應解除驗證事件。從ISE或WLC無法進行任何操作來阻止此情況，因為要由無線客戶端來貼上原始SSID，或者連線到另一個可用（首選）SSID。

在這種情況下，無線使用者必須手動連線回HotSpot SSID。

AireOS WLC

```
(Cisco Controller) >debug client
```

Debug client sets設定為DEBUG客戶端狀態機器更改中涉及的一組元件。

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

```
Debug Flags Enabled:
```

```
dhcp packet enabled.  
dot11 mobile enabled.  
dot11 state enabled  
dot1x events enabled.  
dot1x states enabled.  
mobility client handoff enabled.  
pem events enabled.  
pem state enabled.  
802.11r event debug enabled.  
802.11w event debug enabled.  
CCKM client debug enabled.
```

調試AAA元件

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

這可能會影響資源，具體取決於通過MAB或Dot1X SSID連線的使用者數量。 DEBUG級別的這些元件記錄WLC和ISE之間的AAA事務，並在螢幕上列印RADIUS資料包。

如果您認為ISE無法提供預期屬性，或者WLC無法正確處理這些屬性，則這一點非常關鍵。

Web-Auth redirect

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

這麼做可驗證WLC是否成功觸發重新導向。以下是重新導向在偵錯中必須具有的樣子：

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430

*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is
HTTP/1.1 200 OK
Location:
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44
212-2da2-11e6-a5e2-0050
```

NGWC

Debug client sets設定為DEBUG客戶端狀態機器更改中涉及的一組元件。

```
3850#debug client mac-address <client MAC>
```

此元件在螢幕上列印RADIUS資料包（身份驗證和記帳）。當您需要驗證ISE是否提供正確的AVP以及驗證CoA是否正確傳送和處理時，這非常方便。

```
3850#debug radius
```

這將涉及無線客戶端的所有AAA轉換（身份驗證、授權和記帳）。這對於驗證WLC正確解析AVP並將其應用於客戶端會話至關重要。

```
3850#debug aaa wireless all
```

懷疑NGWC上的重新導向問題時，可以啟用此功能。

```
3850#debug epm plugin redirect all
```

```
3850#debug ip http transactions
```

```
3850#debug ip http url
```

ISE

RADIUS即時日誌

驗證是否已在ISE中正確處理初始MAB請求，以及ISE是否回推預期屬性。導覽至**Operations > RADIUS > Live logs**，然後使用Endpoint ID下的客戶端MAC過濾輸出。找到身份驗證事件後，按一下詳細資訊，然後驗證作為接受的一部分推送的結果。

Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

tcpdump

如需深入瞭解ISE和WLC之間的RADIUS封包交換，可使用此功能。通過這種方式，您可以證明ISE在access-accept中傳送正確的屬性，而無需在WLC端啟用調試。要使用TCDump啟動捕獲，請導航至操作>故障排除>診斷工具 >常規工具> TCPDump。

以下是通過TCPDump捕獲的正確流的示例

Source	Destination	Protocol	Length	Info
154.5	157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
157.13	154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
154.5	157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
157.13	154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
157.13	154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
154.5	157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
154.5	157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
157.13	154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

以下是響應初始MAB請求而傳送的AVP (上述螢幕截圖中的第二個資料包)。

```

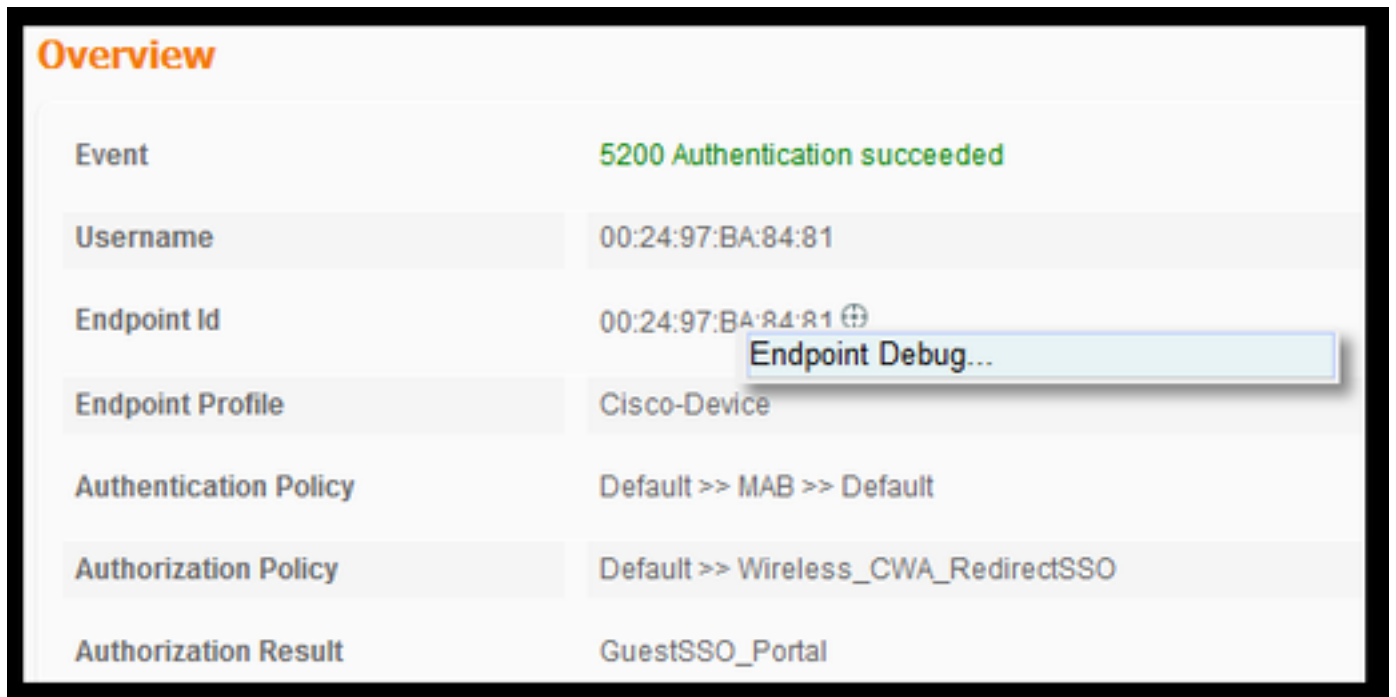
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: fleaaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=189 t=Cisco-AVPair(1): url-
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a0500000aa05565e1c9&portal
    
```


=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622
AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)

終端調試：

如果您需要深入瞭解涉及策略決策、門戶選擇、訪客身份驗證的ISE流程，CoA處理此問題的最簡單方法是啟用**Endpoint Debug**，而不是將完整元件設定為調試級別。

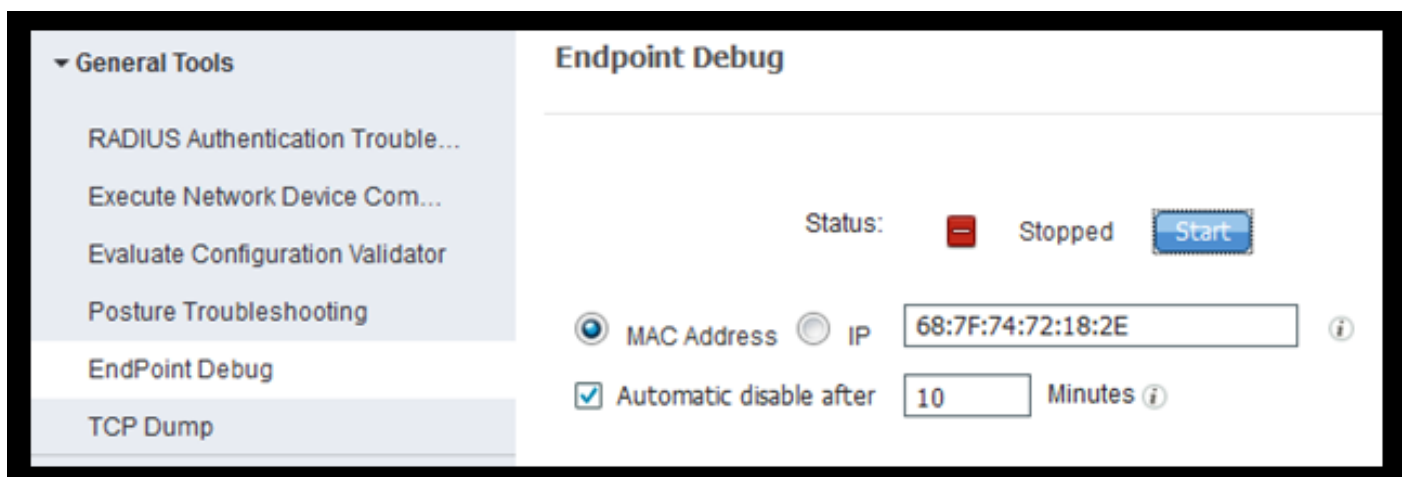
要啟用此功能，請導航到**操作>故障排除>診斷工具>常規工具 > EndPoint調試**。



Overview

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ Endpoint Debug...
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

進入終端調試頁面後，輸入終端MAC地址，並在準備重新建立問題時按一下開始。



Endpoint Debug

General Tools

- RADIUS Authentication Trouble...
- Execute Network Device Com...
- Evaluate Configuration Validator
- Posture Troubleshooting
- EndPoint Debug
- TCP Dump


Status: Stopped Start


MAC Address IP ⓘ


Automatic disable after Minutes ⓘ

調試停止後，按一下標識終端ID的連結以下載調試輸出。

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

相關資訊

[TAC建議的AireOS版本](#)

[思科無線控制器組態設定指南8.0版。](#)

[思科身份服務引擎管理員指南2.1版](#)

[帶身份服務引擎的通用NGWC無線配置](#)

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）。