

使用ISE在WLC上配置FlexConnect AP的CWA

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[WLC配置](#)

[ISE 組態](#)

[建立授權配置檔案](#)

[建立驗證規則](#)

[建立授權規則](#)

[啟用IP續訂 \(可選\)](#)

[流量傳輸](#)

[驗證](#)

[相關資訊](#)

簡介

本文檔介紹如何在本地交換模式下使用WLC ISE上的FlexConnect AP配置中央Web身份驗證。

必要條件

需求

本文件沒有特定需求。

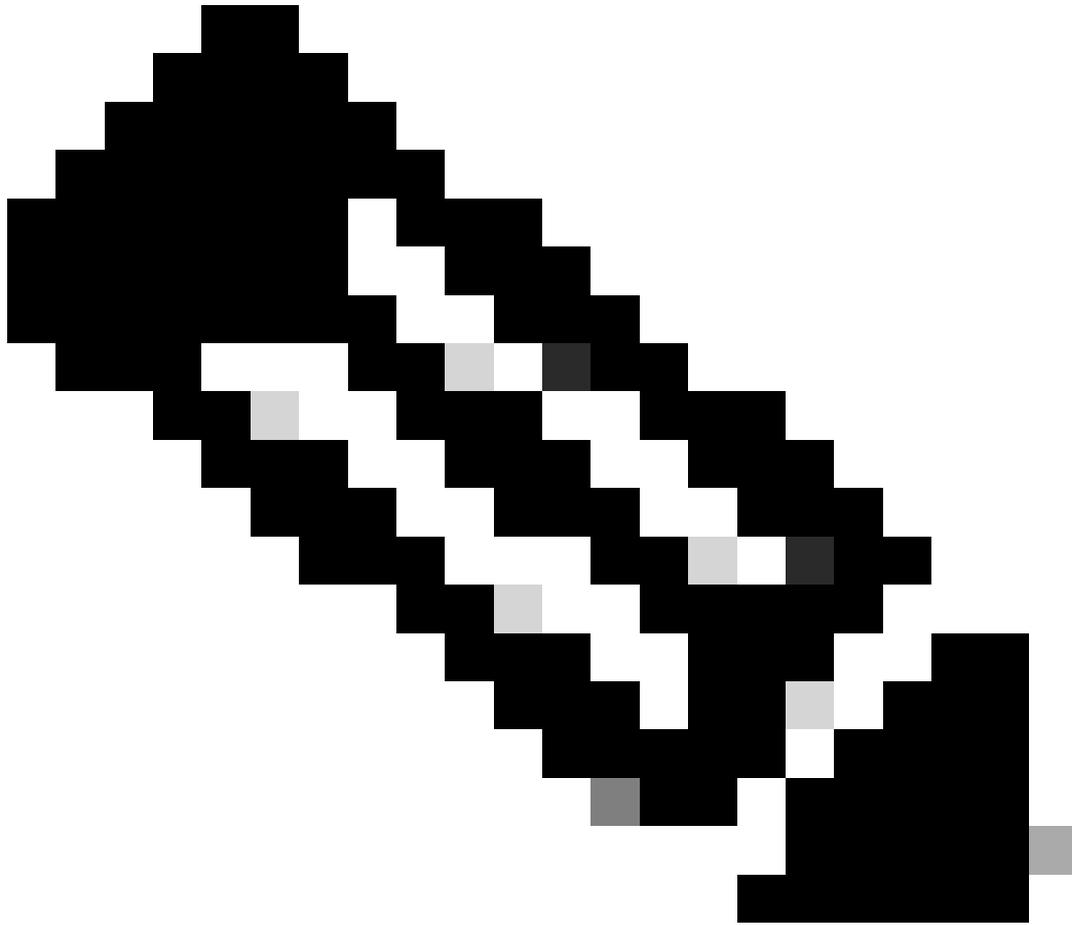
採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身份辨識服務引擎(ISE)，版本1.2.1
- 無線LAN控制器(WLC)軟體版本- 7.4.100.0
- 存取點(AP)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊



注意：此時，此方案不支援FlexAP上的本地身份驗證。

本系列的其他檔案

- [使用交換機和身份服務引擎的集中Web身份驗證配置示例](#)
- [WLC 和 ISE 的中央 Web 驗證的組態範例](#)

設定

在無線LAN控制器(WLC)上設定中央Web驗證的方法有多種。第一種方法是本地Web身份驗證，其中WLC將HTTP流量重定向到提示使用者進行身份驗證的內部或外部伺服器。然後，WLC會擷取憑證（在外部伺服器的情況下，會透過HTTP GET要求傳回）並執行RADIUS驗證。在訪客使用者的情況下，需要外部伺服器(例如身份服務引擎(ISE)或NAC訪客伺服器(NGS))，因為門戶提供裝置註冊和自助調配等功能。此程式包含下列步驟：

1. 使用者與Web身份驗證SSID關聯。
2. 使用者打開其瀏覽器。
3. 輸入URL後，WLC會立即重新導向到訪客入口網站（例如ISE或NGS）。
4. 使用者在門戶上進行身份驗證。
5. 訪客門戶使用輸入的憑據重定向回WLC。
6. WLC透過RADIUS驗證訪客使用者。
7. WLC重新導向回原始URL。

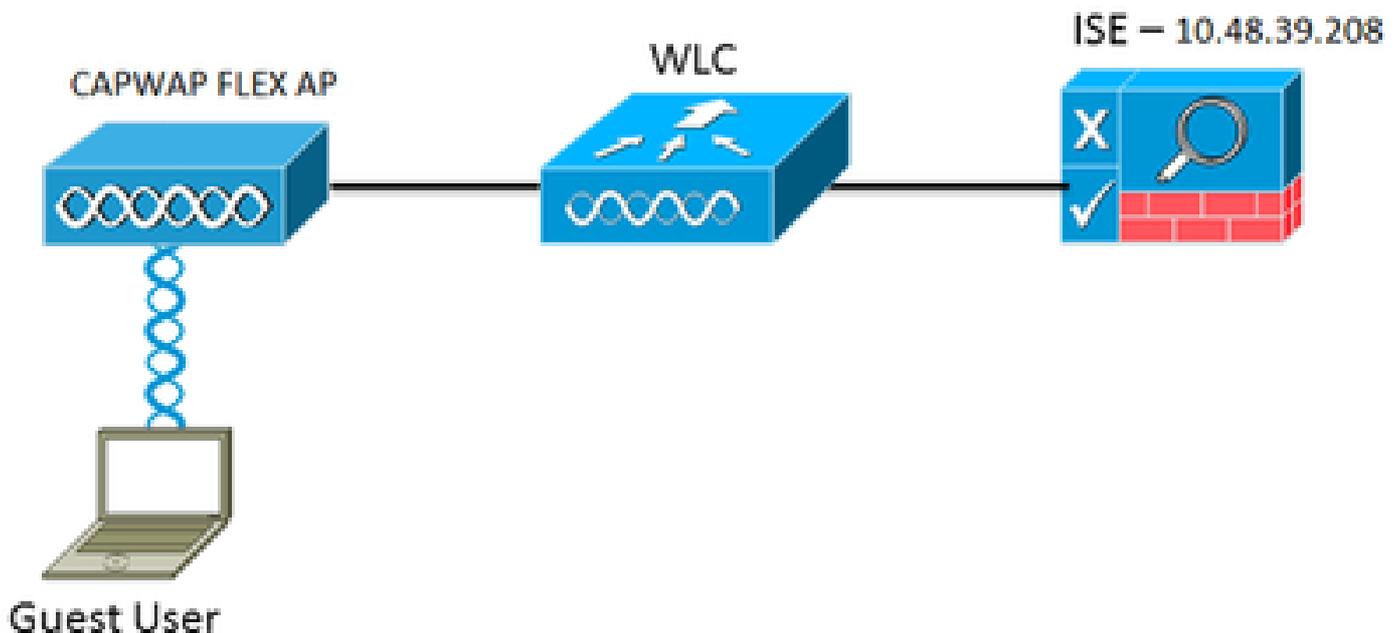
這個程式包含許多重新導向。新方法是使用中央Web驗證，該驗證可與ISE（1.1版以上）和WLC（7.2版以上）配合使用。此程式包含下列步驟：

1. 使用者與Web身份驗證SSID關聯。
2. 使用者打開其瀏覽器。
3. WLC會重新導向至訪客入口網站。
4. 使用者在門戶上進行身份驗證。
5. ISE傳送RADIUS授權更改（CoA - UDP埠1700）以向控制器指示使用者是有效的，並最終推送RADIUS屬性，例如訪問控制清單(ACL)。
6. 系統會提示使用者重試原始URL。

本節介紹在WLC和ISE上配置中央Web身份驗證的必要步驟。

網路圖表

此配置使用以下網路設定：



網路設定

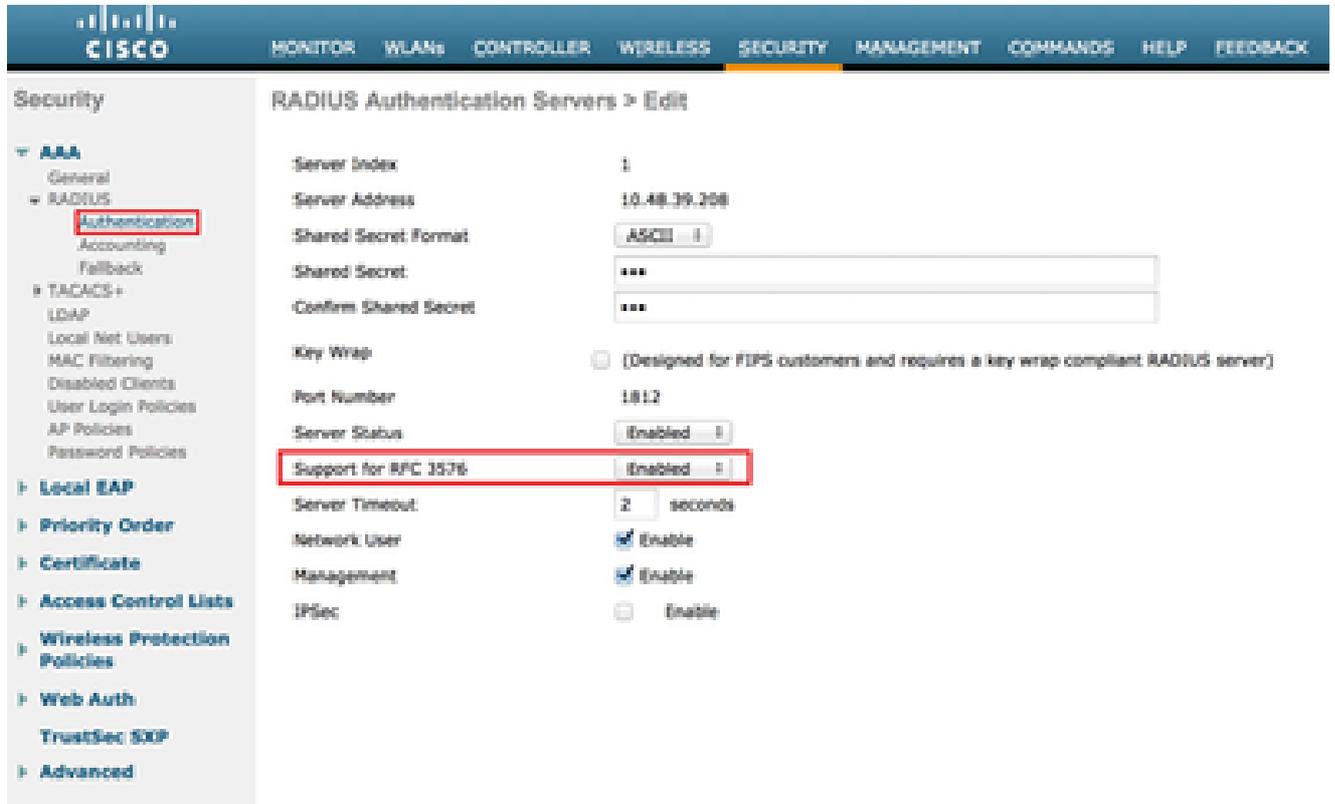
WLC配置

WLC的配置相當簡單。使用（與交換機上相同）技巧從ISE獲取動態身份驗證URL。（由於它使用CoA，因此需要建立會話，因為會話ID是URL的一部分。）SSID配置為使用MAC過濾，而ISE配置

為返回Access-Accept消息，即使MAC地址未找到，它也會為所有使用者傳送重定向URL。

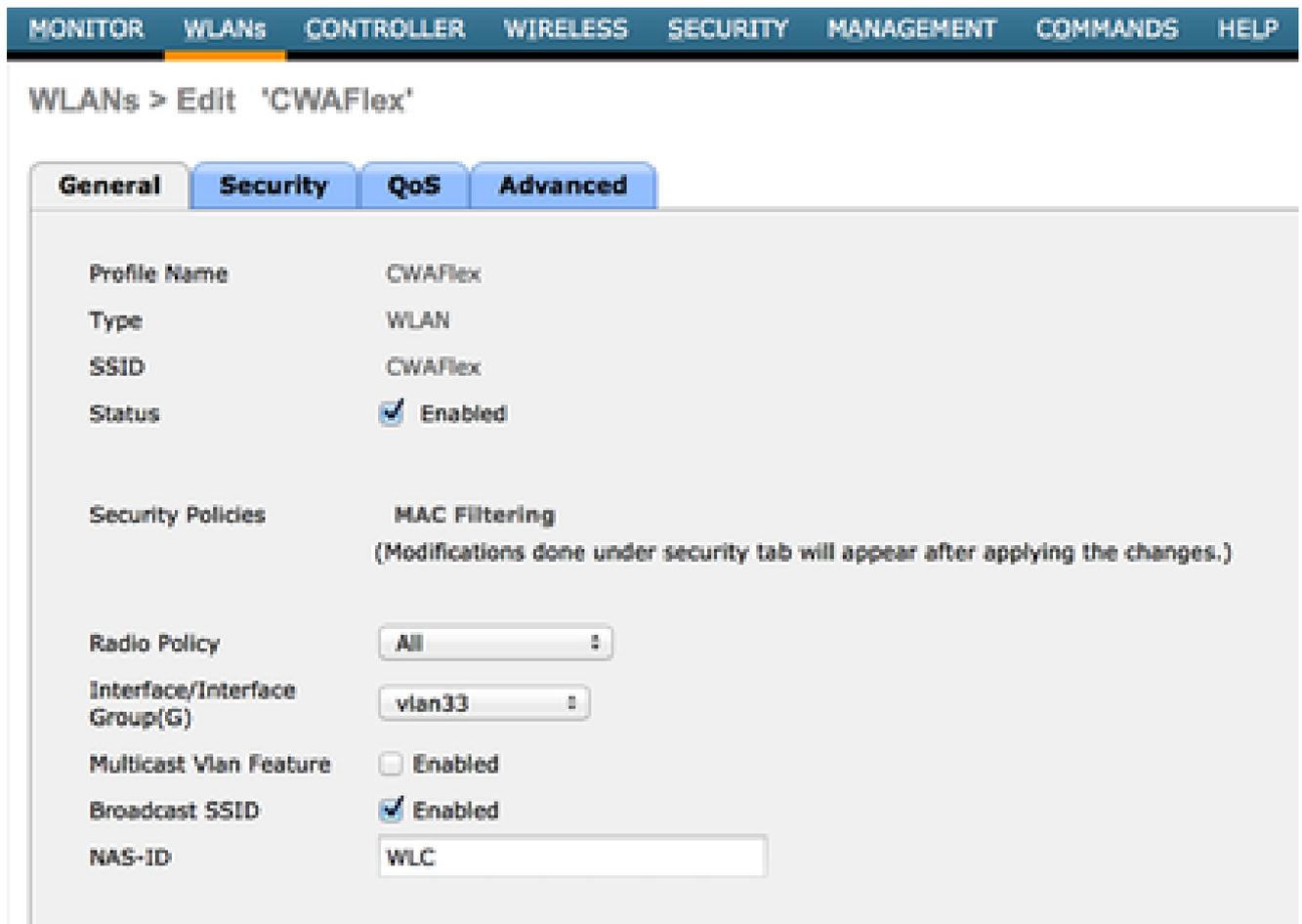
此外，必須啟用RADIUS網路認可控制(NAC)和AAA覆寫。RADIUS NAC允許ISE傳送CoA請求，指示使用者現在已透過身份驗證且能夠訪問網路。它還用於狀態評估，其中ISE根據狀態結果更改使用者配置檔案。

1. 確保RADIUS伺服器已啟用RFC3576 (CoA)，這是預設設定。



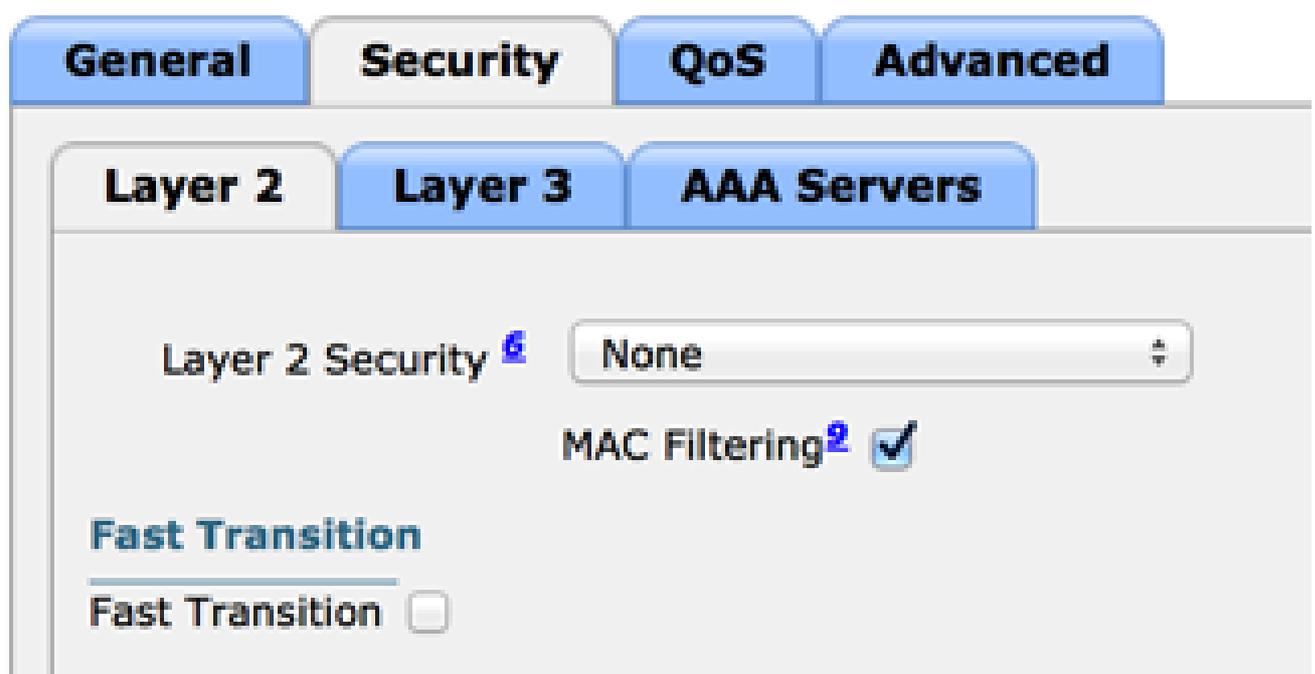
RADIUS伺服器有RFC3576

2. 建立一個新的 WLAN。本示例將建立一個名為CWAFlex的新WLAN並將其分配給vlan33。
(請注意，由於存取點處於本地交換模式，因此它不會產生太大效果。)



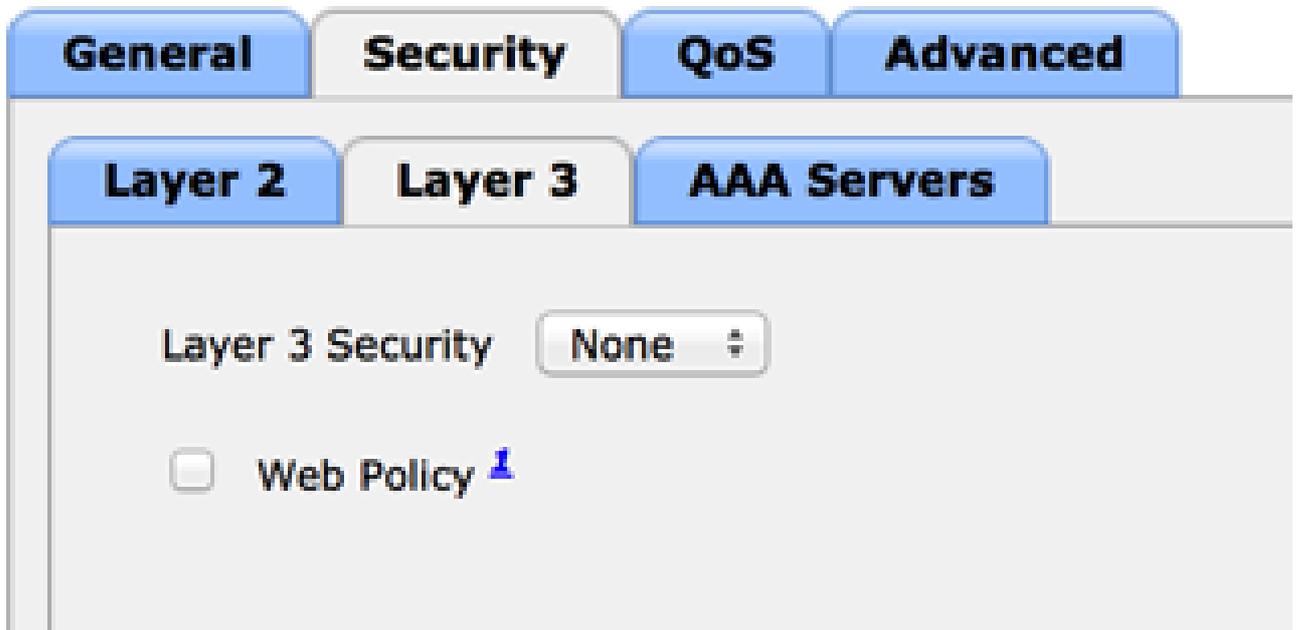
建立新的WLAN

3. 在Security頁籤上，啟用MAC Filtering as Layer 2 Security。



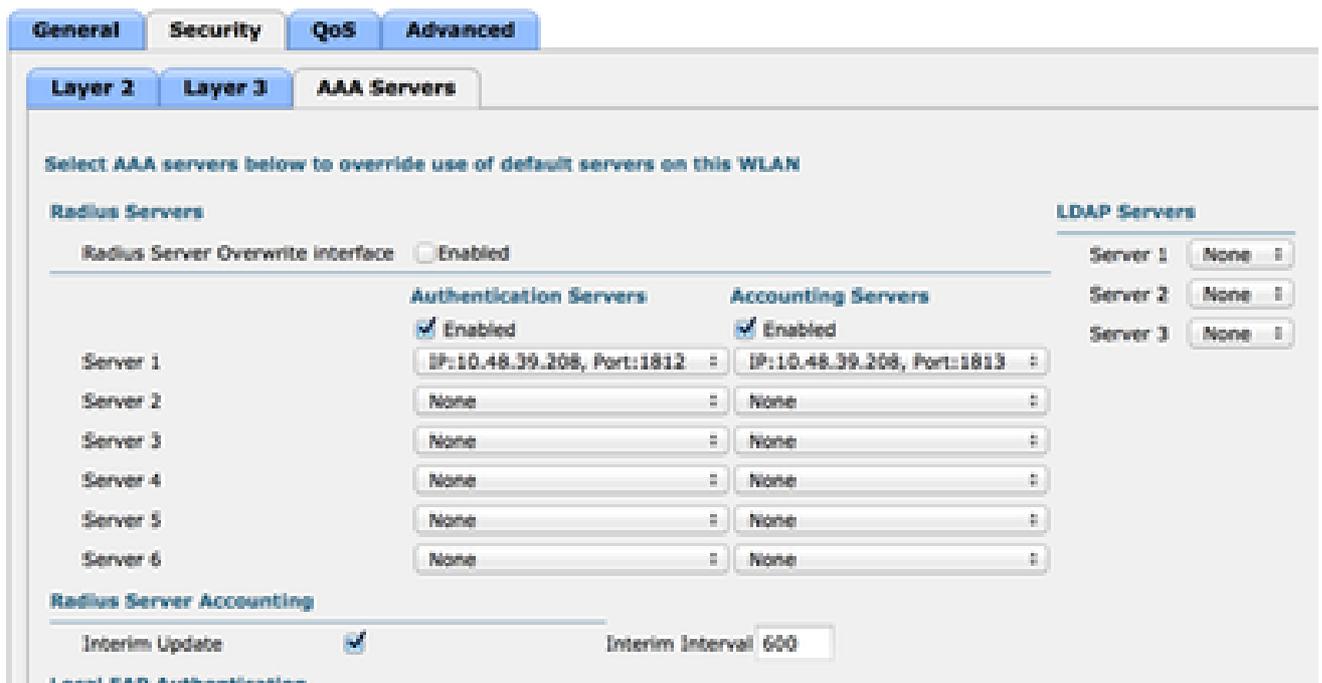
啟用MAC過濾

4. 在Layer 3頁籤上，確保停用安全性。（如果在第3層啟用了Web身份驗證，則會啟用本地Web身份驗證，而不是中央Web身份驗證。）



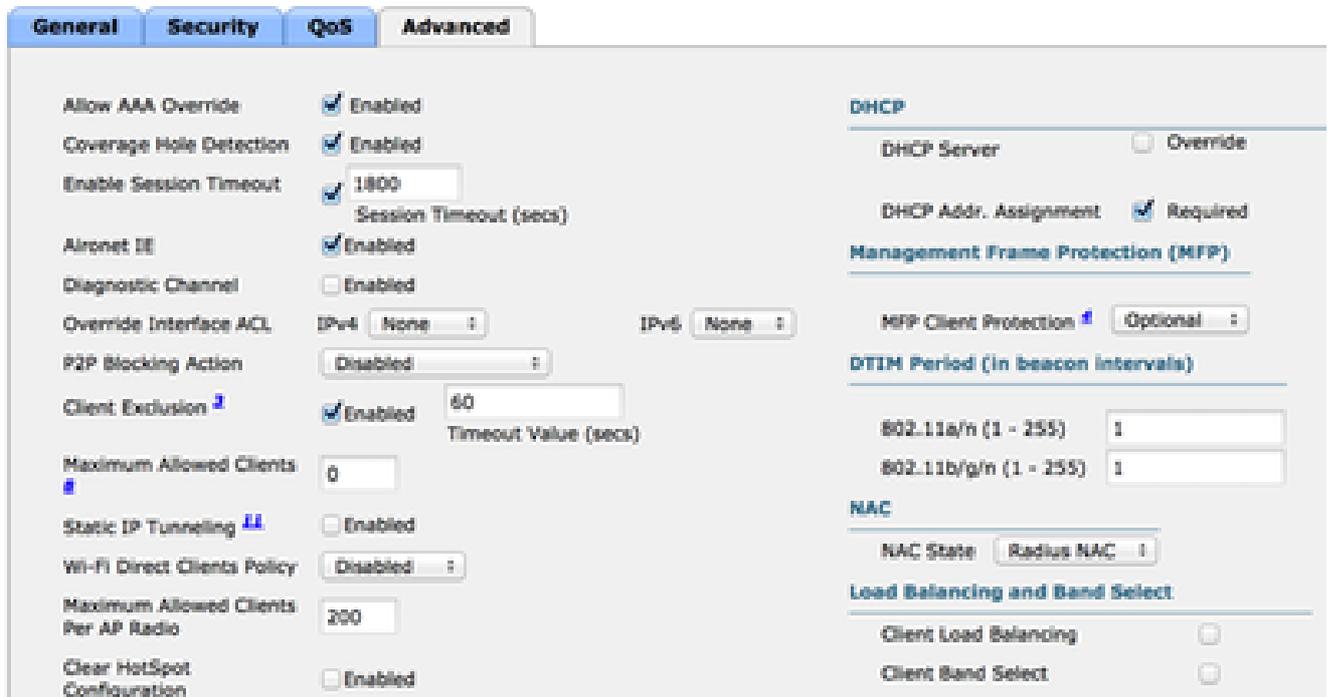
確保停用安全性

5. 在AAA Servers頁籤上，為WLAN選擇ISE伺服器作為RADIUS伺服器。或者，您可以為記賬選擇它，以便獲得有關ISE的更多詳細資訊。



選擇ISE伺服器

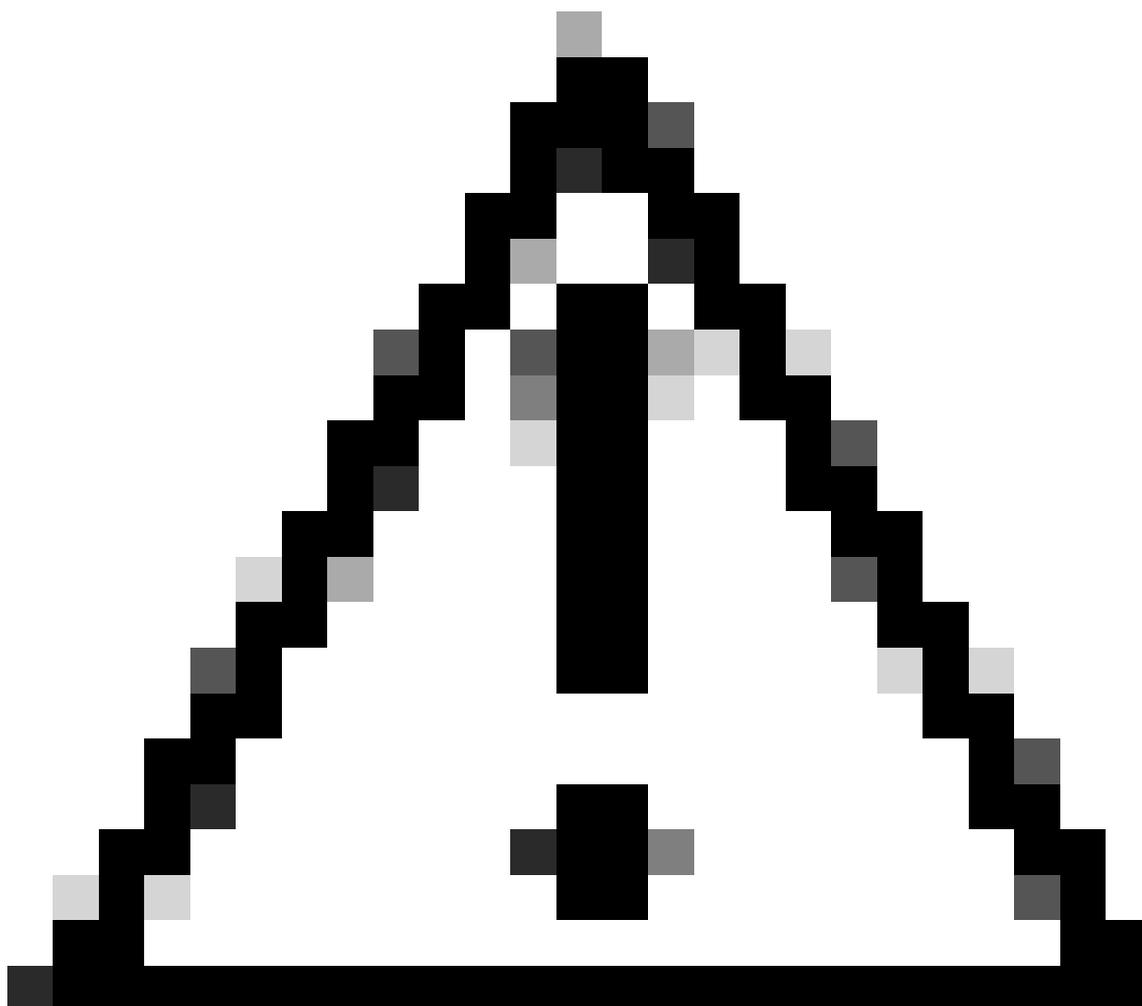
6. 在Advanced頁籤上，確保選中Allow AAA Override並為NAC State選擇Radius NAC。



確保選中「允許AAA覆蓋」

7. 建立重新導向ACL。

此ACL在ISE的Access-Accept消息中引用，並定義必須重定向哪些流量（由ACL拒絕）以及不能重定向哪些流量（由ACL允許）。基本上，需要允許DNS和與ISE之間的流量



注意：FlexConnect AP的一個問題是您必須建立與普通ACL分開的FlexConnect ACL。此問題已記錄在Cisco錯誤ID [CSCue68065](#)中，並在版本7.5中進行了修復。在WLC 7.5及更高版本中，僅需要FlexACL，不需要標準型ACL。WLC預期ISE返回的重定向ACL是普通ACL。但是，為確保它正常工作，您需要應用與FlexConnect ACL相同的ACL。（只有已註冊的思科使用者才能訪問內部思科工具和資訊。）

本示例顯示如何建立名為flexred的FlexConnect ACL：

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar shows a tree view under 'Wireless' with categories like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'RF Profiles', 'FlexConnect Groups', and 'FlexConnect ACLs'. The main content area is titled 'FlexConnect Access Control Lists' and shows a table with one entry: 'flexred'.

建立名為Flexred的FlexConnect ACL

- a. 建立規則以允許DNS流量以及發往ISE的流量並拒絕其餘流量。

The screenshot shows the 'Access Control Lists > Edit' page for the 'flexred' ACL. The 'General' tab is active, showing the 'Access List Name' as 'flexred'. Below is a table of rules:

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	10.48.39.208 / 255.255.255.255	Any	Any	Any	Any
2	Permit	10.48.39.208 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any
5	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

允許DNS流量

如果您希望獲得最大安全性，則只能允許埠8443指向ISE。（如果做姿勢，您必須增加典型的安全狀態埠，例如8905,8906,8909,8910。）

- b. (僅限於7.5之前的版本中由於Cisco bug [IDCSCue68065](#)而出現的代碼)選擇Security > Access Control Lists以建立具有相同名稱的相同ACL。

Security

- AAA
 - General
 - RADIUS
 - Authentication
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
 - Access Control Lists**
 - CPU Access Control Lists
 - FlexConnect ACLs

Access Control Lists

Enable Counters

Name	Type
flexred	IPv4

建立相同的ACL

c. 準備特定的FlexConnect AP。請注意，對於較大的部署，通常使用FlexConnect組，出於可擴充性的原因，不會針對每個AP執行這些專案。

1. 按一下Wireless，然後選擇特定的存取點。
2. 按一下FlexConnect頁籤，然後按一下External Webauthentication ACLs。(7.4之前的版本將此選項命名為Web policies。)

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
- Mesh
- RF Profiles
- FlexConnect Group**
 - FlexConnect ACLs
 - 802.11a/n

All APs > Details for FlexAP1

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

VLAN Support

Native VLAN ID: 33 [VLAN Mappings](#)

FlexConnect Group Name: Not Configured

PreAuthentication Access Control Lists

- External WebAuthentication ACLs**
- Local Split ACLs
- Central DMCP Processing

點選FlexConnect頁籤

3. 將ACL(在本示例中為flexred)增加到Web策略區域。這會將ACL預先推送到存取點。它尚未應用，但ACL內容已指定給AP，以便其在需要時應用。

The screenshot shows the Cisco Wireless Management interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, and COMMANDS. The left sidebar shows the 'Wireless' menu with options like Access Points, Radios, Advanced, Mesh, RF Profiles, FlexConnect Groups, 802.11a/n, 802.11b/g/n, Media Stream, Application Visibility And Control, Country, Timers, and Netflow. The main content area is titled 'All APs > FlexAP1 > ACL Mappings'. It displays the AP Name as 'FlexAP1' and the Base Radio MAC as '00:1c:f9:c2:42:30'. Under 'WLAN ACL Mapping', there is a form with 'WLAN Id' set to 0 and 'WebAuth ACL' set to 'flexred'. An 'Add' button is visible. Below this is a table with columns 'WLAN Id', 'WLAN Profile Name', and 'WebAuth ACL'. Under 'WebPolicies', there is a form with 'WebPolicy ACL' set to 'flexred' and an 'Add' button. At the bottom, under 'WebPolicy Access Control Lists', there is a list with 'flexred' and a blue plus icon.

將ACL增加到Web策略區域

WLC配置現已完成。

ISE 組態

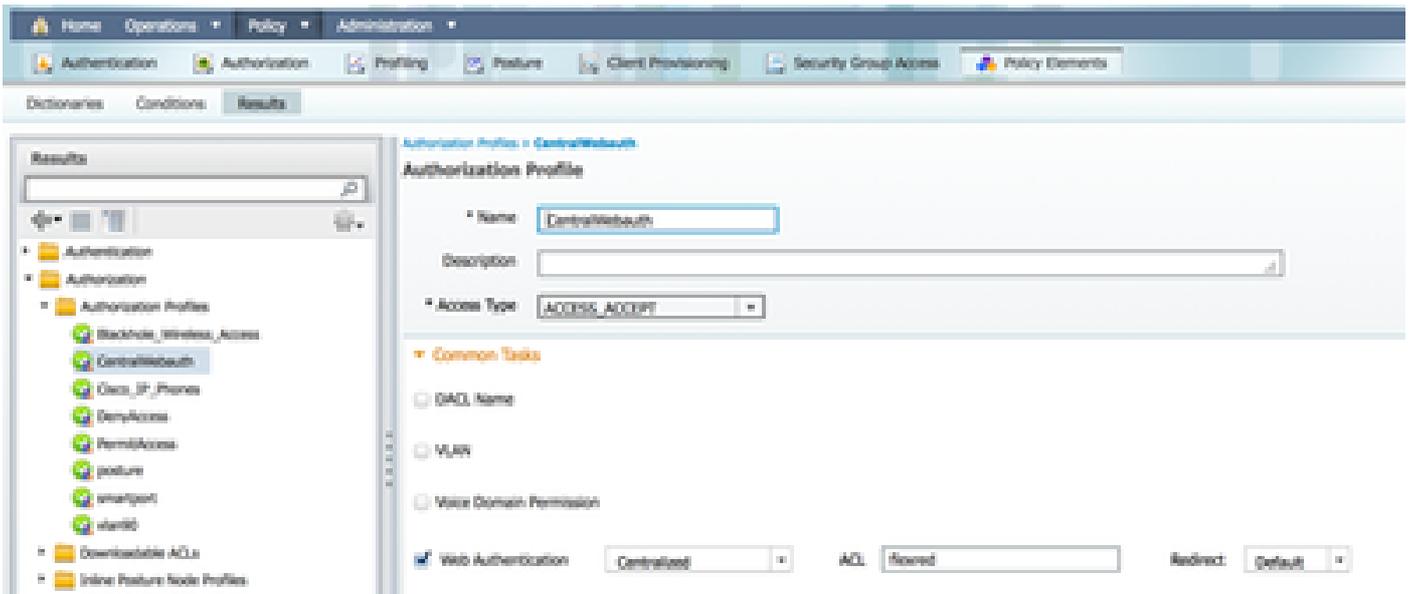
建立授權配置檔案

完成以下步驟以建立授權配置檔案：

1. 按一下Policy，然後按一下Policy Elements。
2. 按一下Results。
3. 展開Authorization，然後按一下Authorization profile。
4. 按一下Add按鈕為中央webauth建立新的授權配置檔案。
5. 在「名稱」欄位中，輸入設定檔的名稱。此範例使用CentralWebauth。

6. 從Access Type下拉選單中選擇ACCESS_ACCEPT。
7. 選中Web Authentication 覈取方塊，並從下拉選單中選擇Centralized Web Auth。
8. 在ACL欄位中，輸入WLC上用於定義將重新導向之流量的ACL名稱。此範例使用flexred。
9. 從Redirect 下拉選單中選擇Default。

Redirect屬性定義ISE看到預設Web門戶還是ISE管理員建立的自定義Web門戶。例如，本示例中的flexred ACL會觸發從客戶端到任何位置的HTTP流量重定向。



ACL會觸發從客戶端到任意位置的HTTP流量重定向

建立驗證規則

完成以下步驟，以使用身份驗證配置檔案建立身份驗證規則：

1. 在Policy選單下，按一下Authentication。

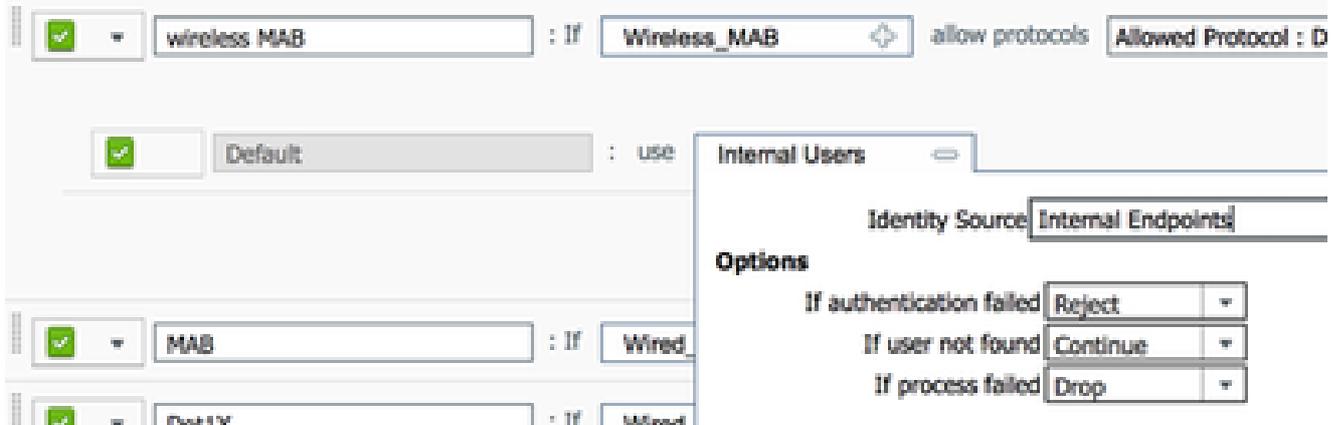
下圖展示了如何配置身份驗證策略規則的示例。在本示例中，配置了一個在檢測到MAC過濾時觸發的規則。



如何配置策略規則

2. 輸入驗證規則的名稱。本示例使用Wireless mab。
3. 在If條件欄位中選取加號(+)圖示。

4. 選擇Compound condition，然後選擇Wireless_MAB。
5. 選擇Default network access作為允許的協定。
6. 點選位於和.....旁邊的箭頭以進一步展開規則。
7. 點選Identity Source欄位中的+圖示，然後選擇Internal endpoints。
8. 從If user not found下拉選單中選擇Continue。



按一下繼續

此選項允許透過webauth對裝置進行身份驗證，即使其MAC地址未知。Dot1x使用者端仍可透過其認證進行驗證，且不得與此組態相關。

建立授權規則

現在，在授權策略中可配置若干規則。連線PC後，會進行mac過濾；假設MAC地址未知，則返回webauth和ACL。此MAC未知規則在下圖中顯示，並在本部分中進行配置。

<input checked="" type="checkbox"/>	2nd AUTH	if Network Access:UseCase EQUALS Guest Flow	then vlan34
<input checked="" type="checkbox"/>	IS-a-GUEST	if IdentityGroup:Name EQUALS Guest	then PermitAccess
<input checked="" type="checkbox"/>	MAC not known	if Network Access:AuthenticationStatus EQUALS UnknownUser	then CentralWebauth

MAC未知

完成以下步驟以建立授權規則：

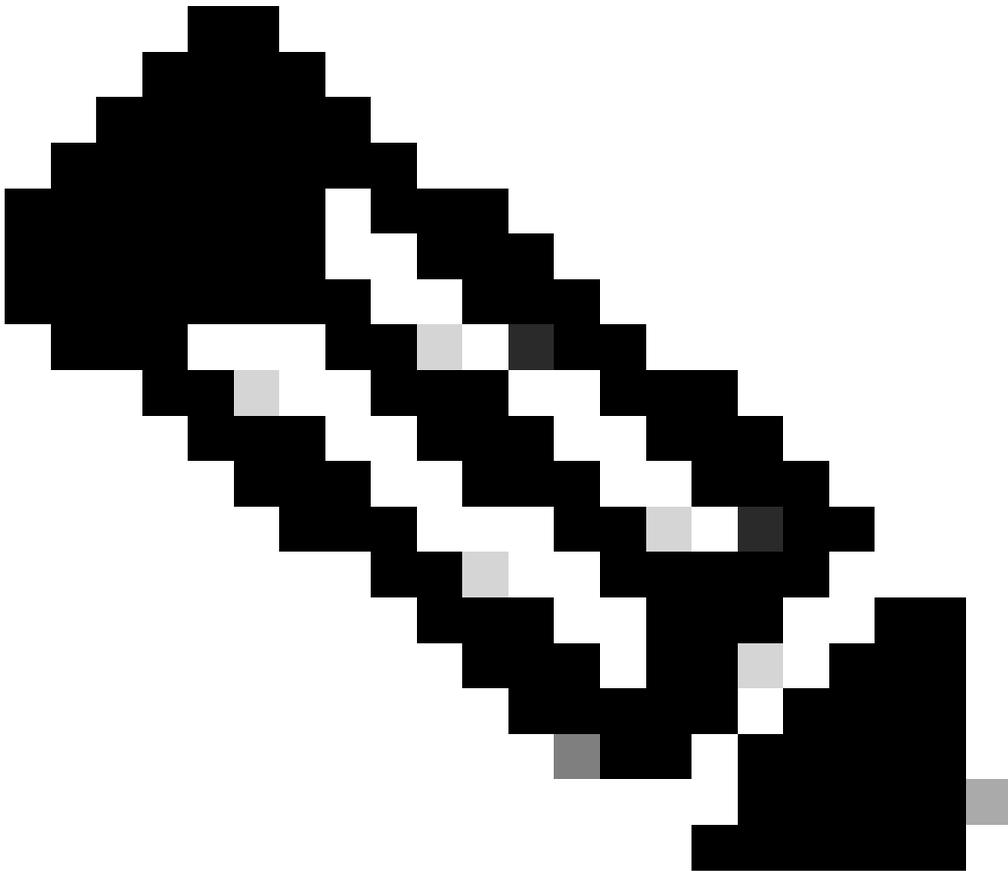
1. 建立新規則，然後輸入名稱。本示例使用MAC not known。
2. 在條件欄位中按一下加號(+)圖示，然後選擇建立新條件。
3. 展開表達式下拉選單。
4. 選擇Network access，然後展開它。
5. 按一下AuthenticationStatus，然後選擇Equals運算子。

6. 在右側欄位中選擇UnknownUser。
7. 在「General Authorization」頁面上，在單字右側的欄位中選擇CentralWebauth([Authorization Profile](#))，然後。

即使使用者 (或MAC) 未知，此步驟仍允許ISE繼續。

現在會顯示「登入」頁面給未知的使用者。但是，一旦他們輸入其憑證，他們就會再次在ISE上看到身份驗證請求；因此，另一個規則必須配置滿足使用者為訪客使用者的條件。在本示例中，如果UseridentityGroup等於使用Guestis，並且假設所有訪客都屬於此組。

8. 按一下位於MAC not known規則末尾的「操作」按鈕，然後選擇在上方插入新規則。



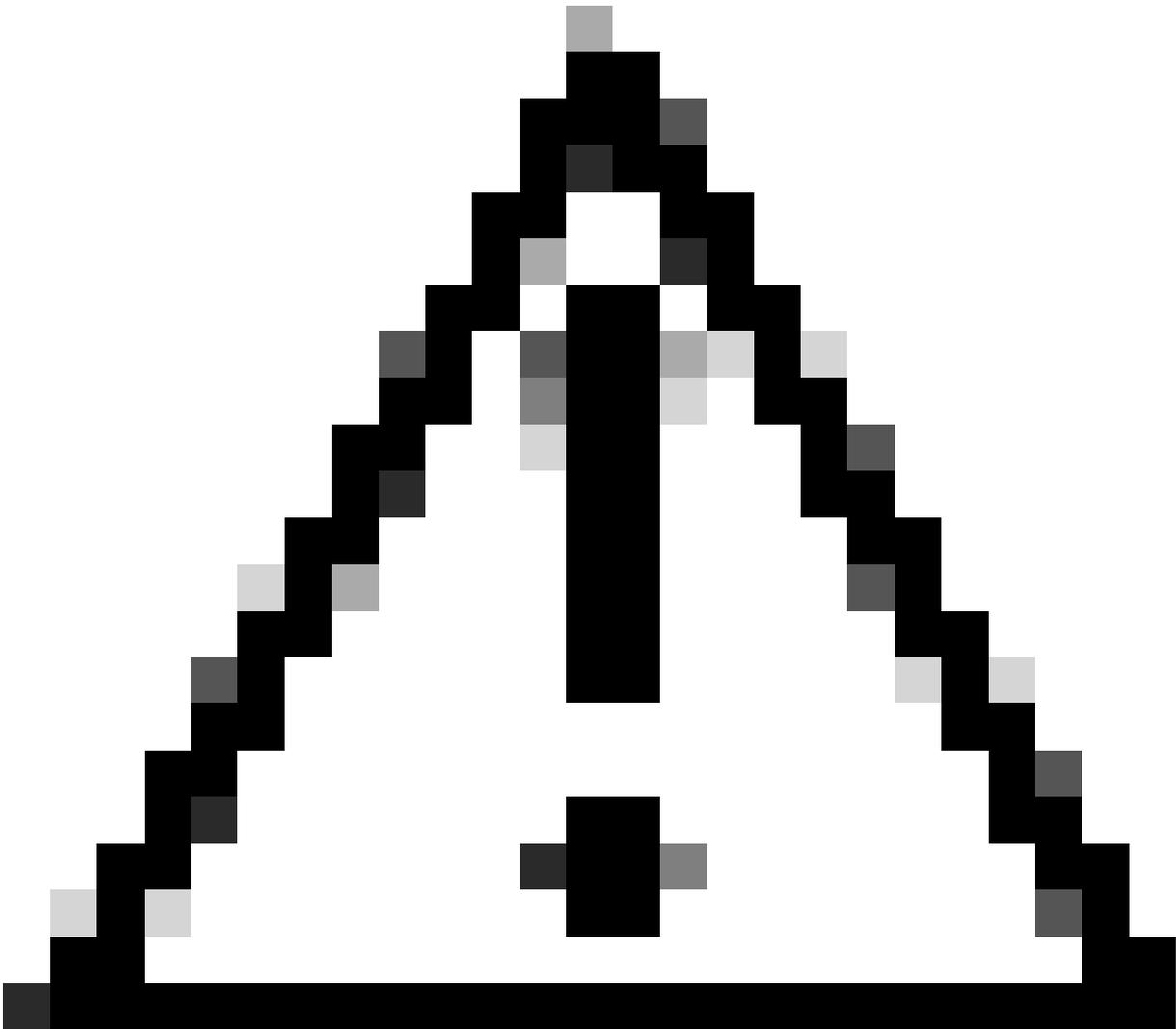
注意：此新規則必須位於MAC未知規則之前，這一點非常重要。

9. 在「name」欄位中輸入second AUTH。
10. 選取辨識群組作為條件。本示例選擇Guest。
11. 在「條件」欄位中，按一下加號(+)圖示，然後選擇建立新條件。

12. 選擇Network Access，然後按一下UseCase。
13. 選擇Equals作為運算子。
14. 選擇GuestFlow作為正確的運算元。這意味著您將捕獲剛剛登入網頁並在授權更改（規則的訪客流部分）後返回的使用者，並且僅當這些使用者屬於訪客身份組時。
15. 在授權頁面上，點選加號(+)圖示(位於tothen旁邊)為您的規則選擇結果。

在本範例中，已指派預先設定的設定檔(vlan34)；本檔案沒有顯示此組態。

您可以選擇Permit Access 選項或建立自定義配置檔案以返回您喜歡的VLAN或屬性。



注意：在ISE版本1.3中，根據Web身份驗證的型別，無法再遇到訪客流使用案例。然後，授權規則必須包含訪客使用者組作為唯一可能的條件。

啟用IP續訂 (可選)

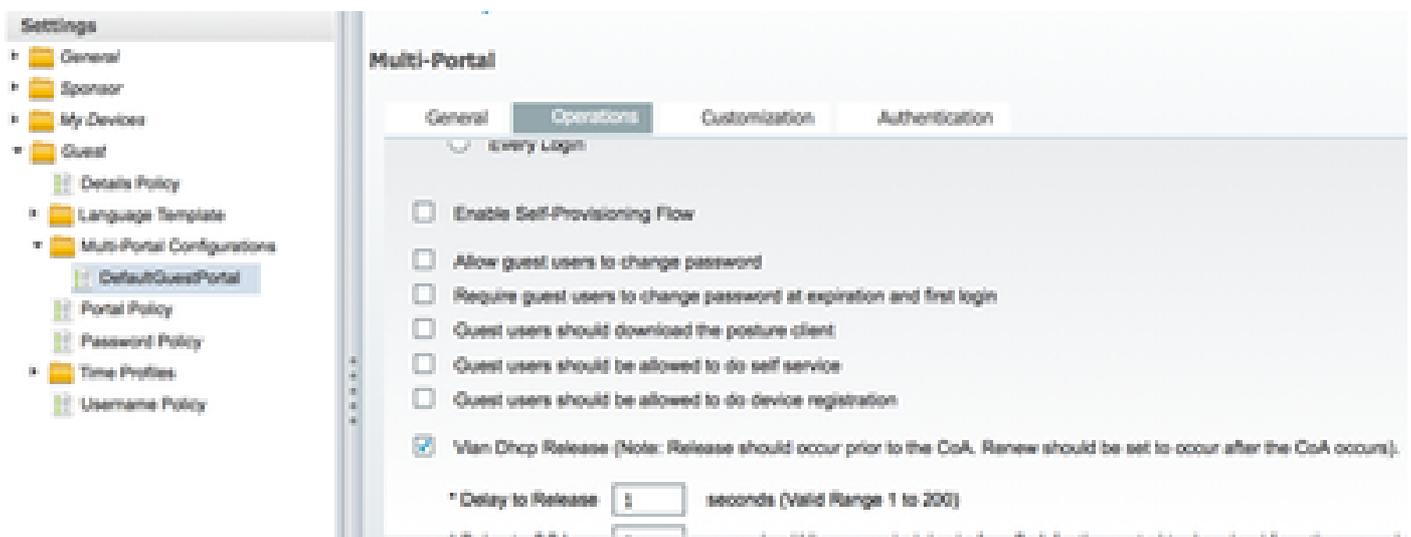
如果分配VLAN，最後一步是讓客戶端PC更新其IP地址。此步驟由Windows客戶端的訪客門戶實現。如果之前未為第2次身份驗證規則設定VLAN，則可以跳過此步驟。

請注意，在FlexConnect AP上，VLAN需要預先存在於AP上。因此，如果沒有，您可以在AP本身或不在要建立的新VLAN中應用任何ACL的Flex組上建立VLAN-ACL對映。實際上會建立一個VLAN (上面沒有ACL)。

如果分配了VLAN，請完成以下步驟以啟用IP續約：

1. 點選管理，然後點選訪客管理。
2. 按一下Settings。
3. 展開Guest，然後展開Multi-Portal Configuration。
4. 點選DefaultGuestPortal或您已建立的自定義門戶的名稱。
5. 按一下Vlan DHCP Release 覈取方塊。

注意：此選項僅適用於Windows客戶端。



Click Vlan DHCP Release 覈取方塊

流量傳輸

在這種情況下，要瞭解將哪些流量傳送到何處，似乎很困難。以下是快速評論：

- 使用者端會透過SSID空中傳送關聯要求。
- WLC使用ISE處理MAC過濾身份驗證（在其中接收重定向屬性）。
- 客戶端只在MAC過濾完成後收到關聯響應。
- 客戶端提交一個DHCP請求，該請求由存取點在本地進行LOCALLY交換，以獲取遠端站點的IP地址。
- 在Central_webauth狀態下，重新導向ACL（因此通常是HTTP）上標籤為拒絕的流量會進行中央交換。因此，進行重新導向的並非AP，而是WLC；例如，當使用者端要求任何網站時，AP會將此重新導向封裝在CAPWAP中的WLC，而WLC會偽裝該網站的IP位址並重新導向至ISE。
- 客戶端被重定向到ISE重定向URL。這會再次在本機進行交換（因為它會在Flex重新導向ACL上命中Permit）。
- 一旦處於RUN狀態，流量就進行本地交換。

驗證

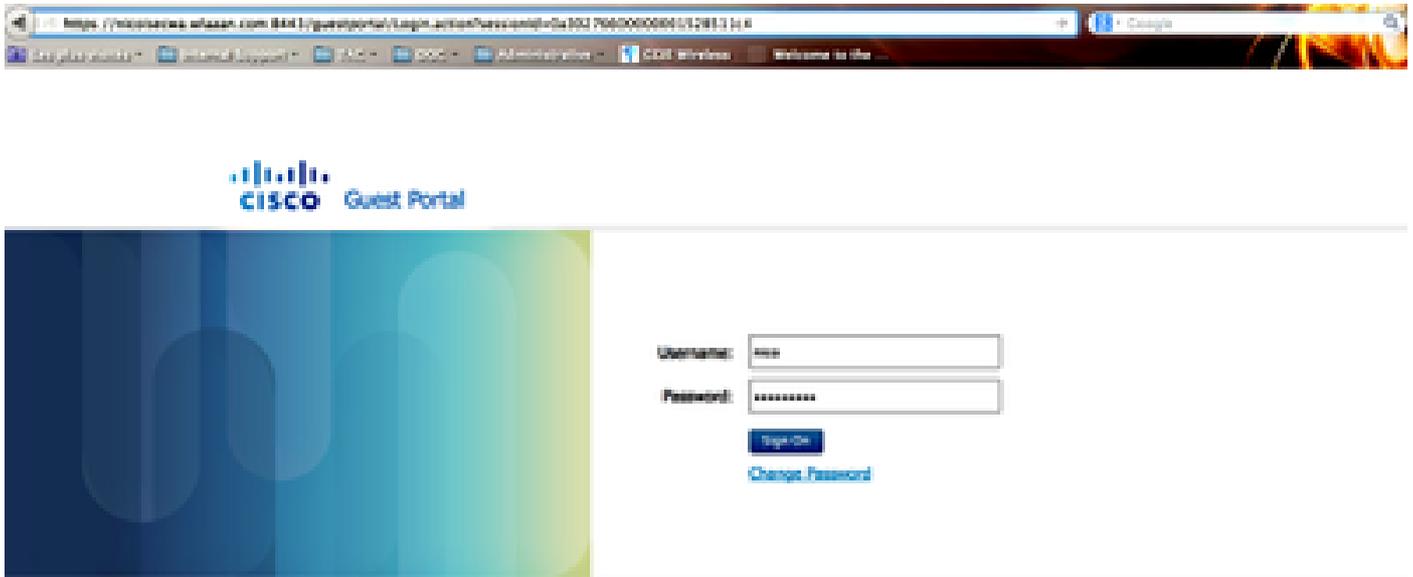
使用者與SSID關聯後，授權將顯示在ISE頁面中。

Apr 09, 2011 08:20:17 AM		Nico	08:23:30-21:70:13	nicowlc	Flex34	Guest	NotApplicable
Apr 09, 2011 08:20:17 AM				nicowlc			Dynamic Autho...
Apr 09, 2011 08:58:37 AM		Nico	08:23:30-21:70:13			Guest	Guest Authentic...
Apr 09, 2011 07:18:47 AM			08:23:30-21:70:13	08:23:30-21:70:13	nicowlc	CentralWebauth	Pending Authentication ...

顯示授權

從下到上，您可以看到返回CWA屬性的MAC地址過濾身份驗證。接下來是使用使用者名稱登入門戶。ISE然後向WLC傳送CoA，最後身份驗證是WLC端的第2層MAC過濾身份驗證，但ISE會記住客戶端和使用者名稱並應用我們在此示例中配置的必要VLAN。

當客戶端上打開任何地址時，瀏覽器會重定向到ISE。確定網域名稱系統(DNS)已正確設定。



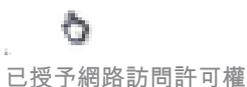
已重定向至ISE

使用者接受策略後，即會授予網路訪問許可權。



Signed on successfully
You can now type in the original URL in the browser's address bar.

You can now type in the original URL in the browser's address bar.



已授予網路訪問許可權

在控制器上，策略管理器狀態和RADIUS NAC狀態從POSTURE_REQD更改為RUN。

相關資訊

- [思科技術支援與下載](#)

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）。