المصادقة المركزية للويب على مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية (WLC) للوصول المجمع والوصول الموحد

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين المصادقة المركزية للويب على وحدة التحكم في شبكة LAN اللاسلكية للوصول المجمع (WLC) وأيضا بين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) للوصول المجمع و WLC للوصول الموحد (5760 وأيضا بين 5760 و 5508).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية ب Cisco WLC 5508، 5760، 3850
- المعرفة الأساسية لمحرك خدمات الهوية (ISE)

- معرفة أساسية بقابلية التنقل اللاسلكي
- المعرفة الأساسية لإرساء الضيوف

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- WLC 5760 التي تعمل بنظام التشغيل Cisco IOS® XE، الإصدار 3.3.3
- WLC 5508 التي تعمل بنظام التشغيل Cisco Aironet OS، الإصدار 7.6
- المحول 3850 الذي يعمل بنظام التشغيل Cisco IOS XE، الإصدار 3.3.3
- Cisco ISE الذي يشغل الإصدار 1.2

التكوين

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

يتضمن التدفق الخطوات التالية:

يرتبط المستخدم بمعرف مجموعة خدمة مصادقة الويب (SSID)، والذي يكون في الواقع open+Macfiltering وبدون أمان من الطبقة 3.

2. يقوم المستخدم بفتح المستعرض.

3. يقوم WLC بإعادة التوجيه إلى بوابة الضيف.

4. يقوم المستخدم بالمصادقة على البوابة.

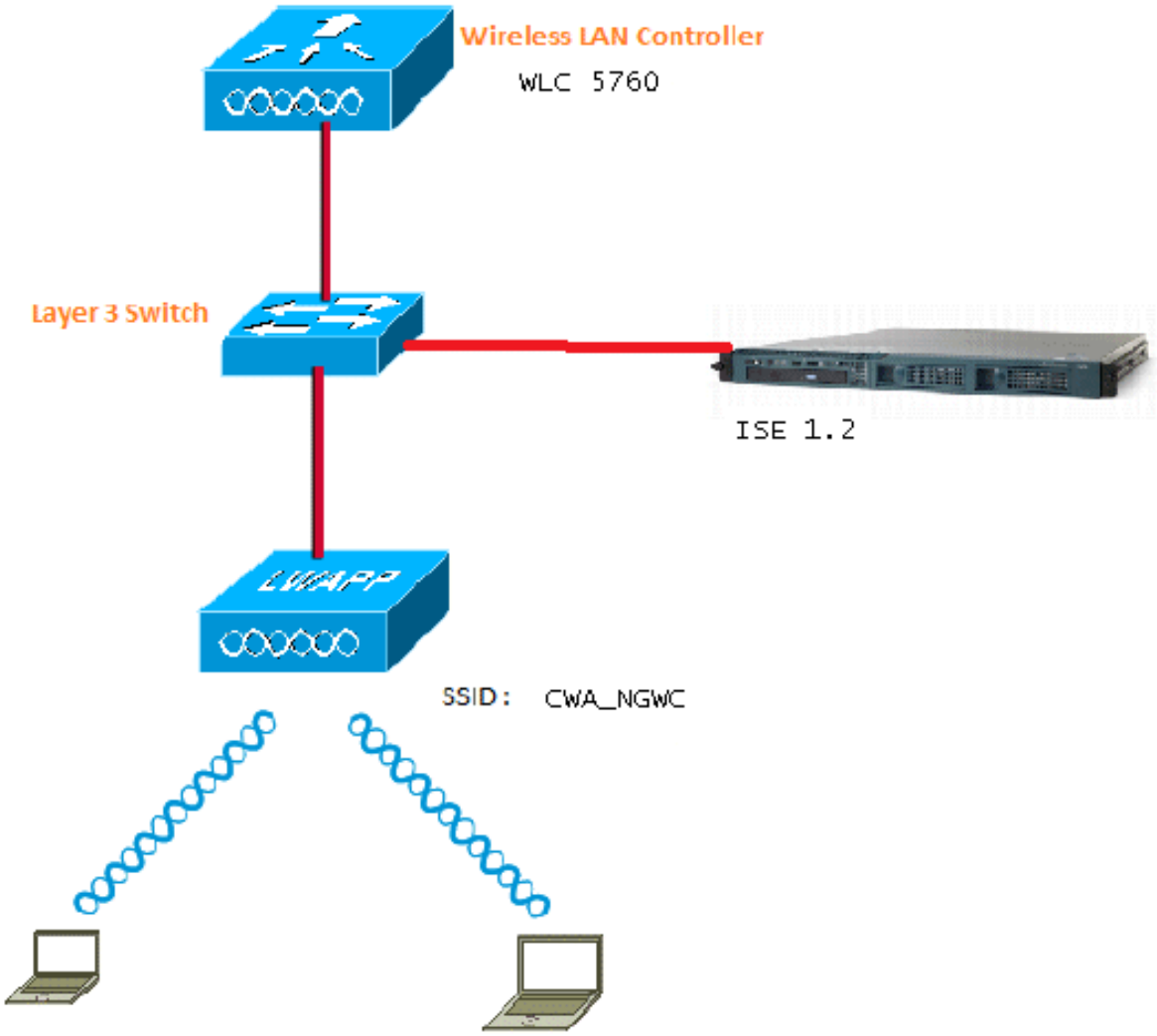
5. يرسل ISE تغيير RADIUS للتخويل (CoA - UDP ميناء 1700) in order to تشير إلى وحدة التحكم أن المستخدم صالح، ويدفع أخيرا سمات RADIUS مثل قائمة التحكم بالوصول (ACL).

6. تتم مطالبة المستخدم بإعادة محاولة عنوان URL الأصلي.

تستخدم Cisco ثلاث مجموعات نشر مختلفة تغطي جميع السيناريوهات المختلفة لإنجاز المصادقة المركزية للويب (CWA).

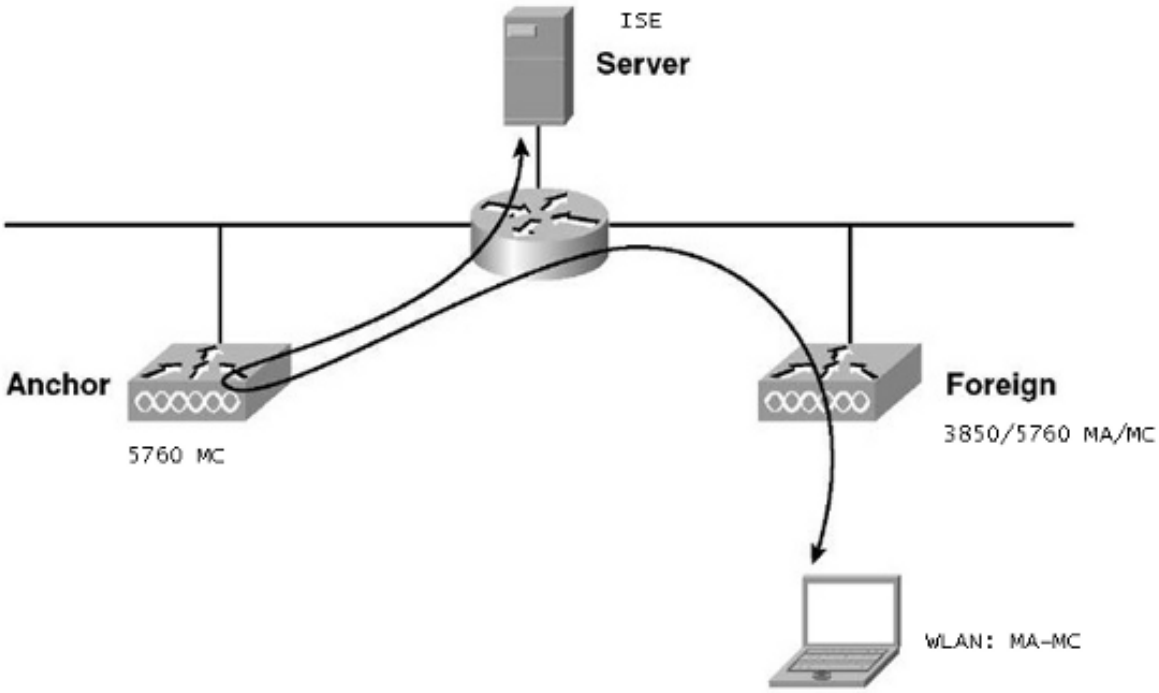
الطبولوجيا 1

تعمل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 5760 كعنصر تحكم في الشبكة المحلية اللاسلكية (WLC) مستقل وتنتهي نقاط الوصول في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) نفسه طراز 5760. يتم توصيل العملاء بشبكة LAN اللاسلكية (WLAN) ويتم مصادقتهم إلى ISE.



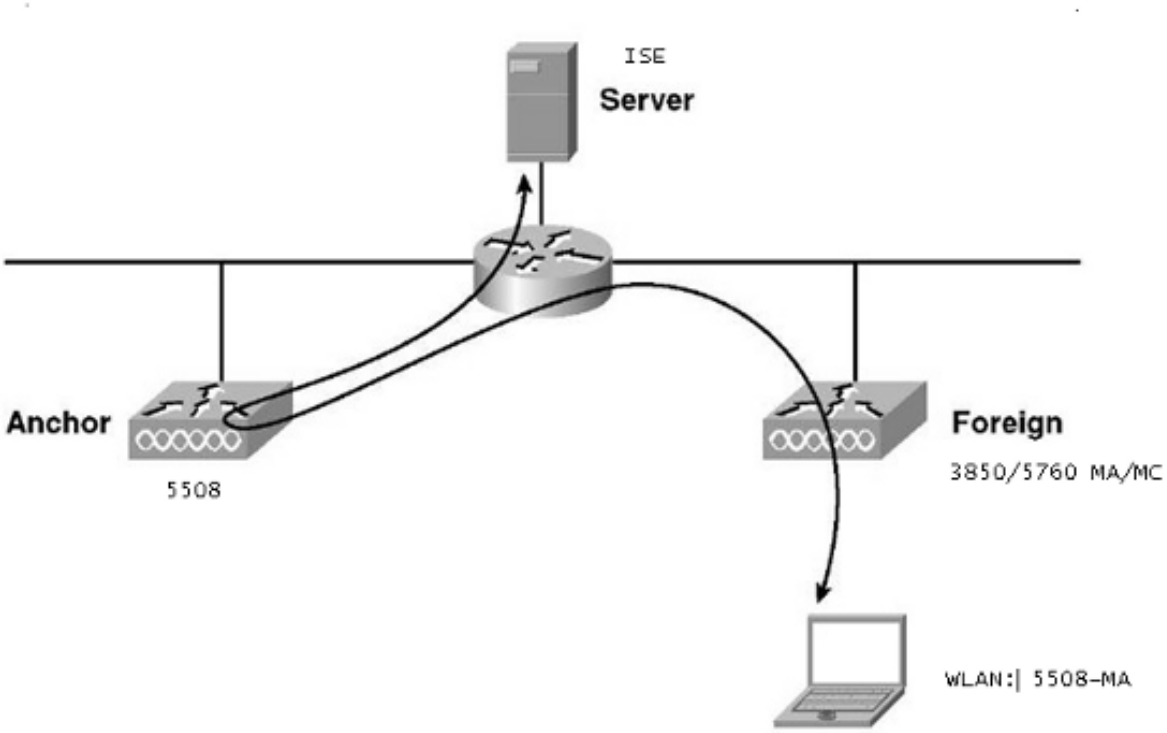
الطبولوجيا 2

تثبيت الضيف بين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للوصول المجمع باستخدام جهاز تحكم في التنقل وآخر يعمل كعميل قابلية التنقل. البرنامج العميل القابل للتنقل هو عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الخارجي ووحدة التحكم في قابلية التنقل هي المرسى.



الطوبولوجيا 3

ربط الضيف بين Cisco Unified WLC 5508 والوصول المجمع WLC 5760/3850 مع واحد يعمل كوحدة تحكم حركة والآخر أن يعمل كوكيل تنقل. البرنامج Mobility Agent/Mobility Controller هو عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الخارجي ووحدة التحكم في التنقل طراز 5508 هي المرسى.



ملاحظة: هناك الكثير من عمليات النشر التي يكون فيها المرسى هو وحدة التحكم في التنقل بينما يكون عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الخارجي هو "عميل التنقل" الذي يحصل على الترخيص من وحدة تحكم أخرى في التنقل. في هذه الحالة، ال WLC خارجي يتلقى فقط واحد ركيزة وأن ربط هو الذي يدفع السياسات. التثبيت المزدوج غير مدعوم ولا يعمل لأنه من غير المتوقع أن يعمل بهذه الطريقة.

مثال

يعمل عنصر التحكم في الشبكة المحلية اللاسلكية (5508 (WLC كمرسى، ويعمل عنصر التحكم في الشبكة المحلية اللاسلكية (5760 (WLC كوحدة تحكم في التنقل لمحول 3850 يعمل كعميل تنقل. بالنسبة للشبكة المحلية اللاسلكية (WLAN) الخارجية (Anchor Foreign WLC)، سيكون ال WLC 5508 هو المرسى للشبكة المحلية اللاسلكية (WLAN) الخارجية طراز 3850. لا حاجة إلى تكوين شبكة WLAN تلك على عنصر التحكم في الشبكة المحلية اللاسلكية (5760 (WLC على الإطلاق. إذا قمت بتوجيه المحول 3850 إلى نقطة الربط 5760، ثم من عنصر التحكم في الشبكة المحلية اللاسلكية (5760 (WLC هذا إلى عنصر التحكم في الشبكة المحلية اللاسلكية (5508 (WLC كرسى مزدوج، فلن يعمل نظرا لأن هذا يصبح إرساء مزدوج وأن السياسات موجودة على رابط 5508.

إن يتلقى أنت setup أن يتضمن WLC 5508 كارتساء، WLC 5760 كجهاز تحكم حركي، و 3850 مفتاح بما أن الحركة وكيل و WLC خارجي، بعد ذلك في أي وقت المرسى ل ال 3850 مفتاح إما ال WLC 5760 أو ال WLC 5508. لا يمكن أن يكون في نفس الوقت ولا يعمل المرسى المزدوج.

مخطط 1 تشكيل مثال

راجع المخطط 1 للحصول على الرسم التخطيطي للشبكة وشرحها.

التكوين هو عملية على خطوتين:

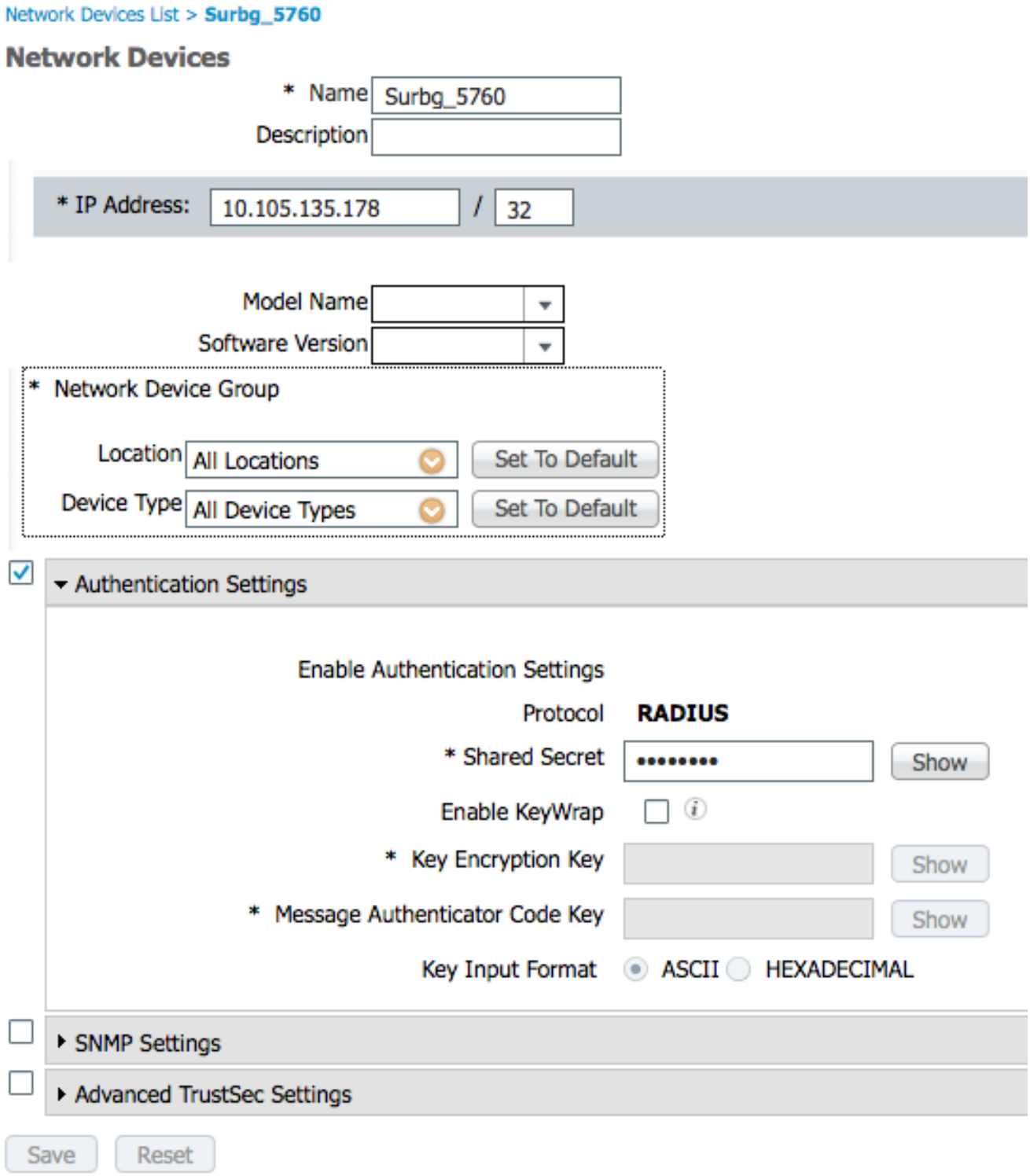
1. التكوين على ISE.

2. تشكيل على ال WLC.

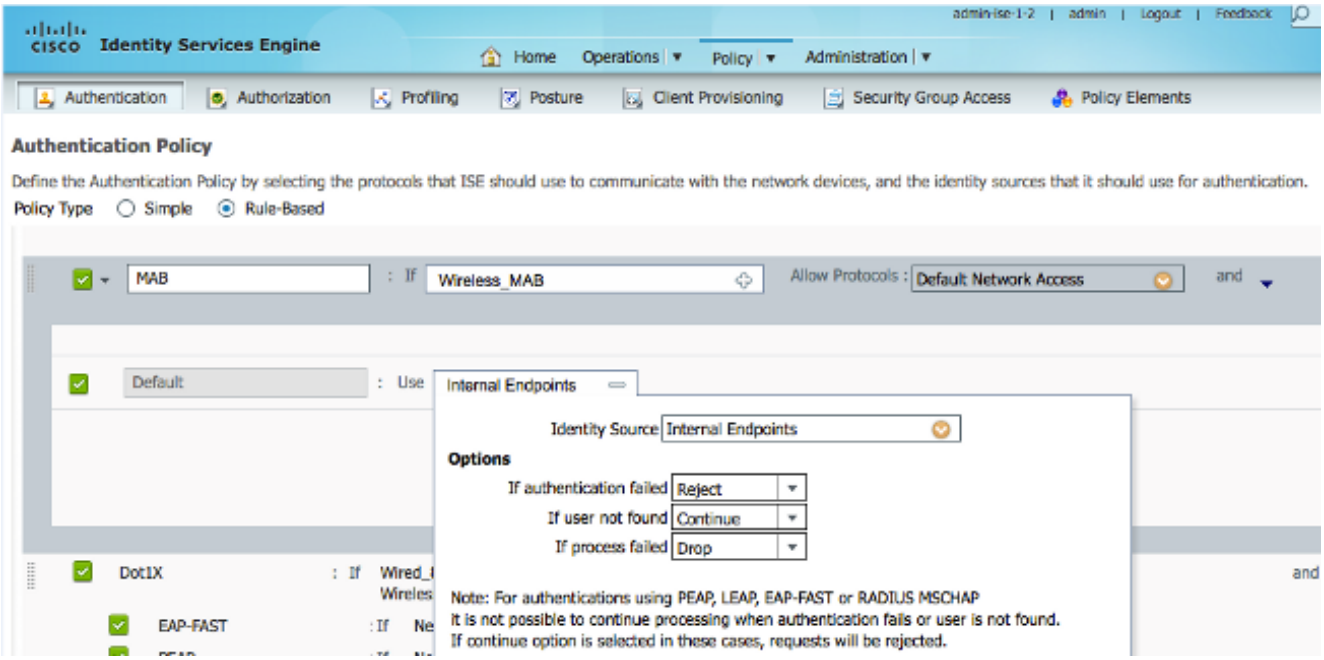
يعمل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 5760 كعنصر تحكم في الشبكة المحلية اللاسلكية (WLC) مستقل ويتم مصادقة المستخدمين على ISE.

التكوين على ISE

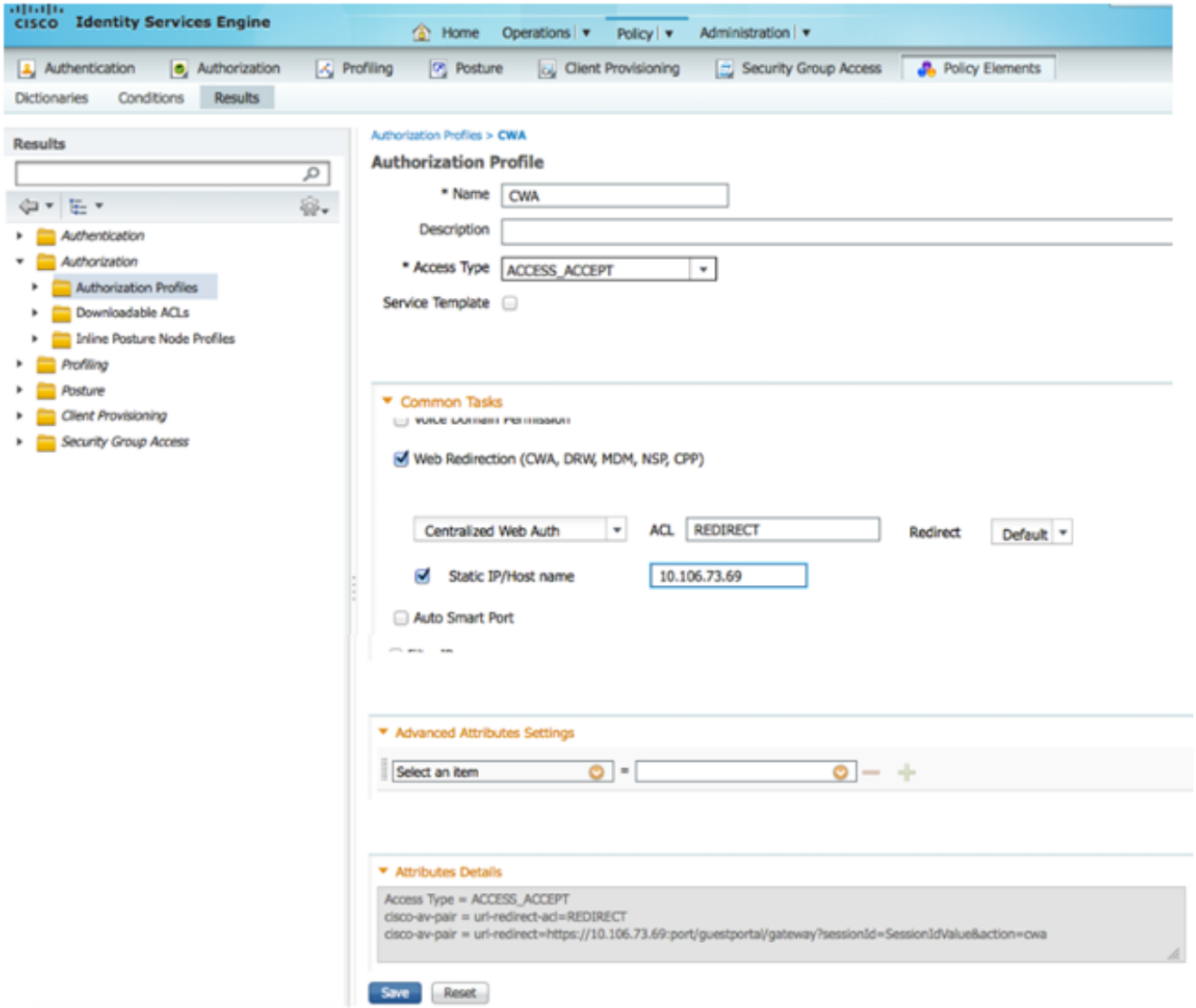
1. أخترت **ISE GUI>إدارة>شبكة مورد>شبكة قائمة أجهزة الشبكة>إضافة** in order to أضفت ال WLC على ال ISE كالمصادقة، التفويض، والمحاسبة (AAA) زبون. ضمنت أن يدخل أنت ال نفسه مشترك سر على ال WLC أن يكون أضفت على ال RADIUS نادل. **ملاحظة**: أثناء نشر Anchor-Foreign، تحتاج فقط إلى إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الخارجي. لا توجد حاجة لإضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الخاص بالارتباط على ISE كعميل AAA. يتم إستخدام تكوين ISE نفسه لجميع سيناريوهات النشر الأخرى في هذا
المستند.



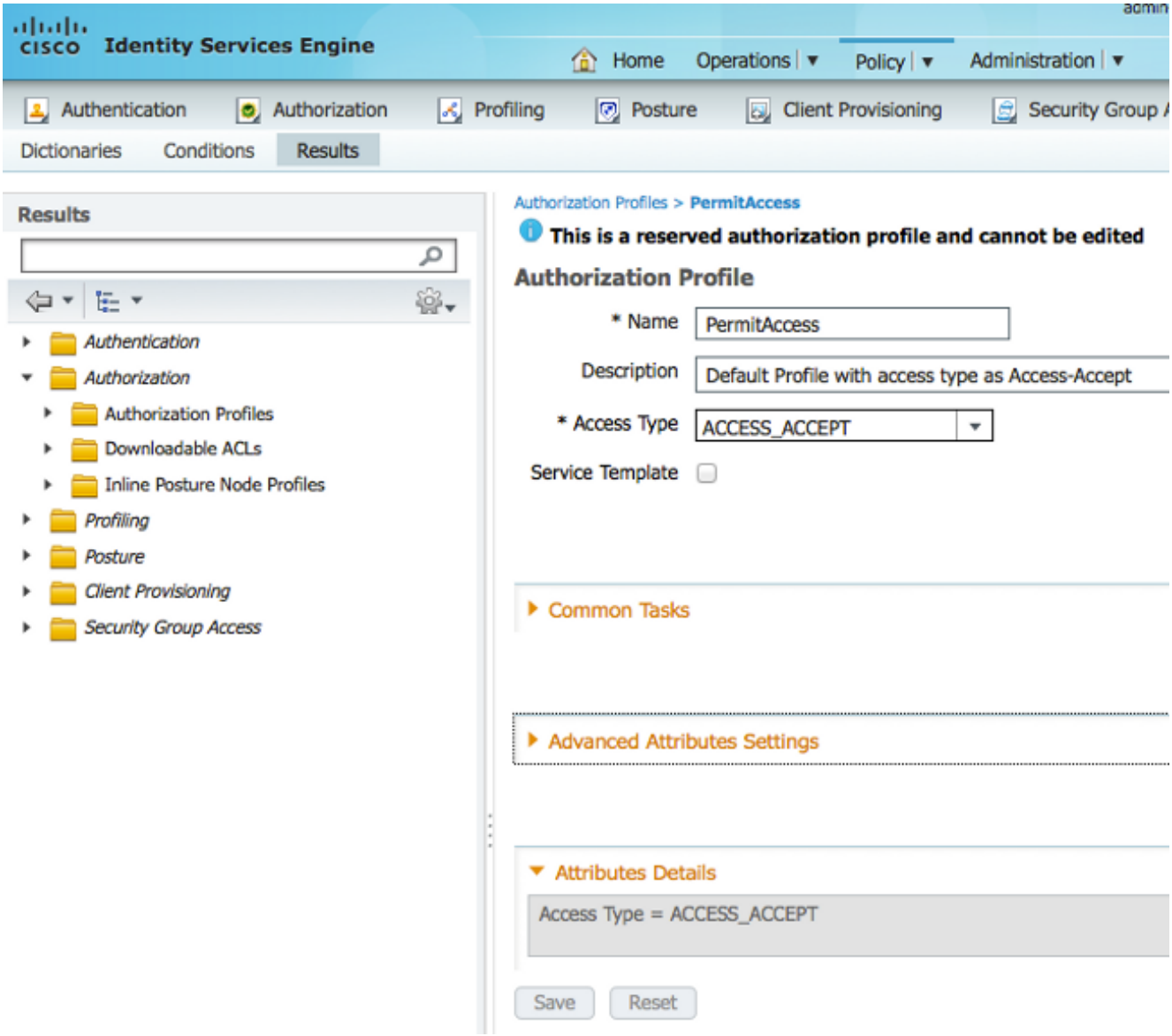
2. من واجهة المستخدم الرسومية ISE، أختر **سياسة > مصادقة > MAB > تحرير** in order to خلقت المصادقة سياسة. يقبل نهج المصادقة عنوان MAC الخاص بالعميل، والذي يشير إلى نقاط النهاية الداخلية. أختر تلك التحديدات في قائمة الخيارات:من القائمة المنسدلة إذا فشلت مصادقة If ، أختر **رفض**.من القائمة المنسدلة "إذا لم يعثر المستخدم على"، أختر **متابعة**.من القائمة المنسدلة إذا فشلت العملية، أختر **إسقاط**.عندما تقوم بالتكوين باستخدام هذه الخيارات، ينتقل العميل الذي يفشل في تفويض MAC مع مدخل الضيف.



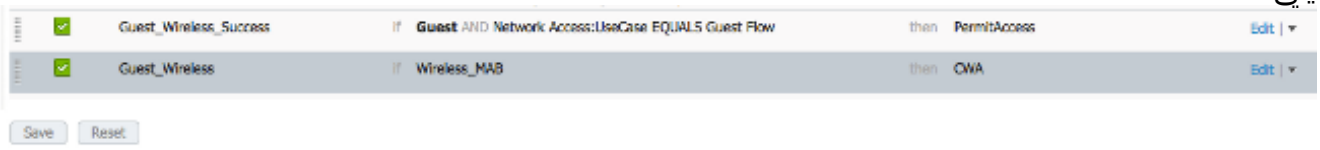
3. من واجهة المستخدم الرسومية ISE، أختر **سياسة > تخويل > نتائج > ملفات تخصيص تخويل > إضافة**. قم بتعبئة التفاصيل وانقر فوق **حفظ** لإنشاء ملف تعريف التفويض. يساعد هذا التوصيف العملاء على الحصول على إعادة التوجيه إلى URL لإعادة التوجيه بعد مصادقة MAC، حيث يدخل العملاء اسم مستخدم/كلمة مرور الضيف.



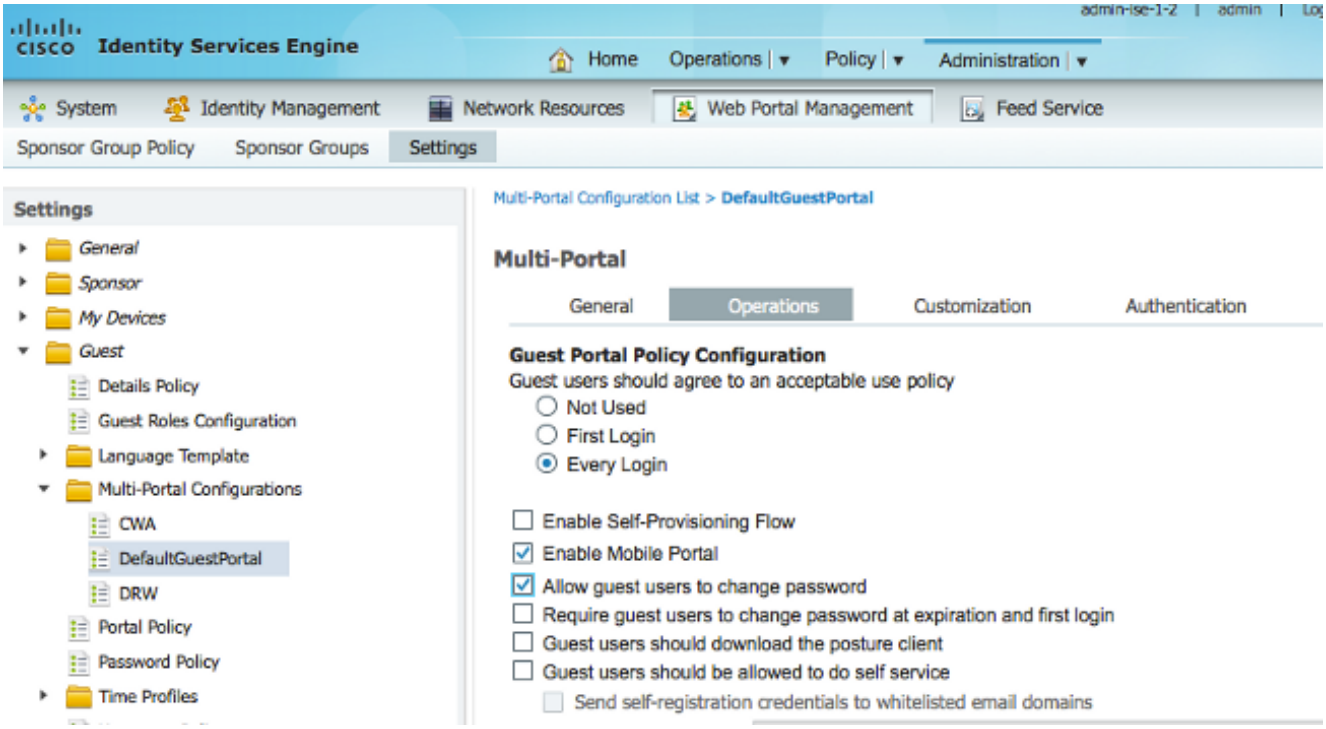
4. من واجهة المستخدم الرسومية ISE، أختر **سياسة > تفويض > نتائج > ملفات تعريف التفويض > إضافة** لإنشاء ملف تعريف تخويل آخر للسماح بالوصول إلى المستخدمين باستخدام بيانات الاعتماد الصحيحة.



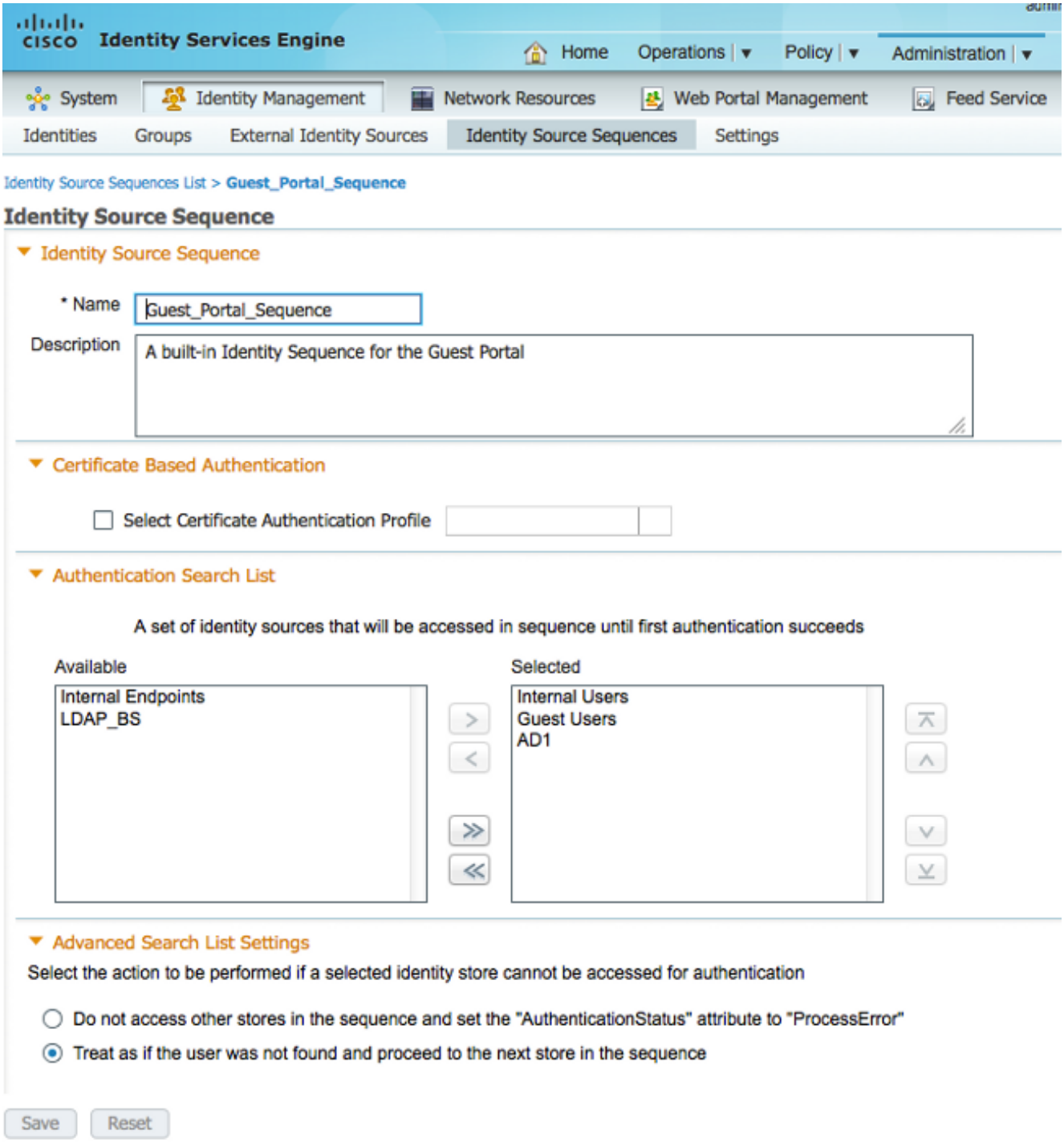
5. قم بإنشاء نهج التخويل. يقوم نهج التخويل "guest_wireless" بدفع عنوان URL لإعادة التوجيه وقائمة التحكم في الوصول (ACL) لإعادة التوجيه إلى جلسة عمل العميل. ملف التعريف الذي تم دفعه هنا هو CWA كما هو موضح مسبقا.تمنح سياسة التخويل "Guest_Wireless-Susc" وصولا كاملا إلى مستخدم ضيف تتم مصادقته بنجاح عبر بوابة Guest. بعد مصادقة المستخدم بنجاح على مدخل الضيف، يتم إرسال التخويل الديناميكي بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يؤدي هذا إلى إعادة مصادقة جلسة عمل العميل باستخدام السمة 'Network Access:UseAse يساوي 'Guest Flow.تبدو سياسات التفويض النهائية كما يلي:



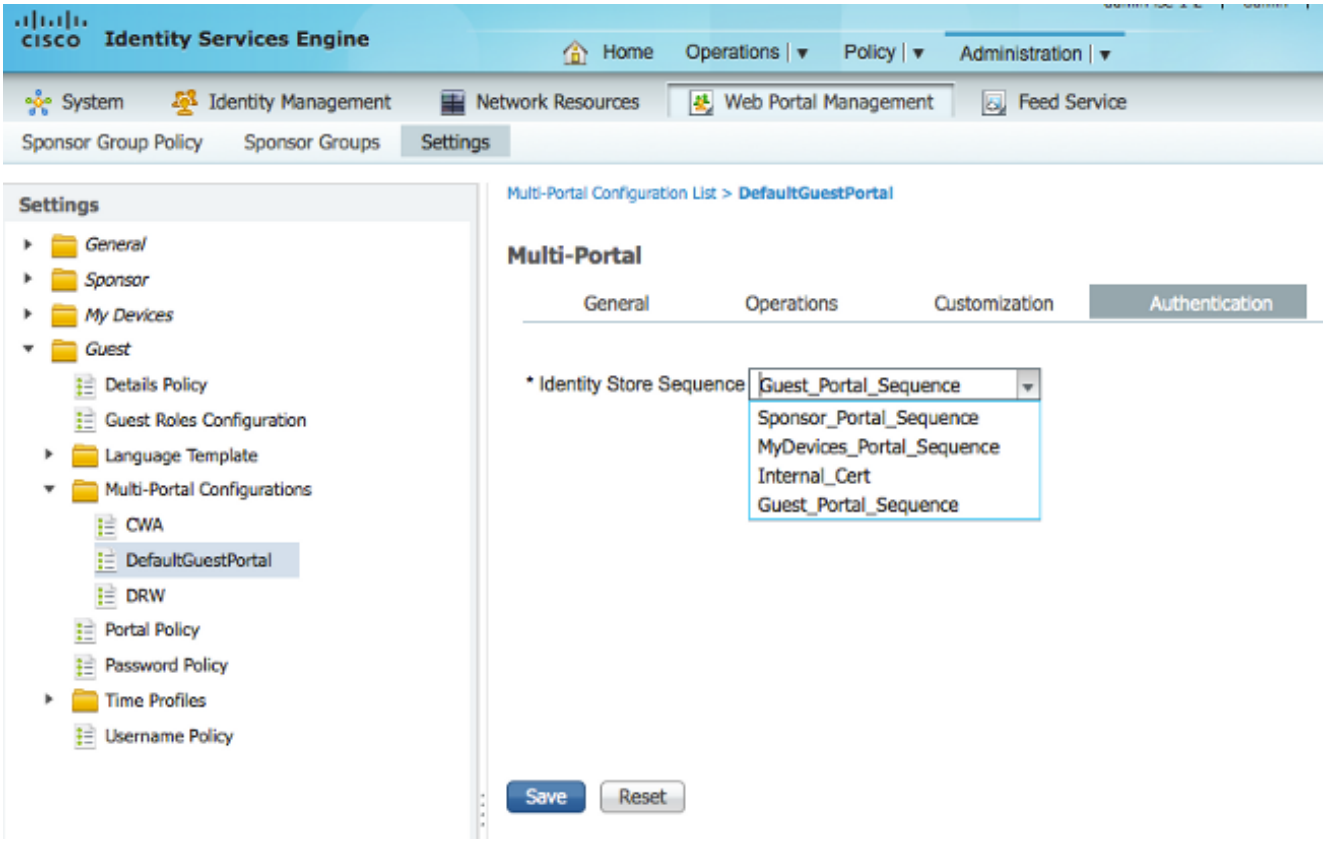
6. إختياري: في هذه الحالة يتم إستخدام التكوينات الافتراضية متعددة المنافذ. واستنادا إلى المتطلبات، يمكن تغيير الأمر نفسه في واجهة المستخدم الرسومية (GUI). من واجهة المستخدم الرسومية (GUI) ل ISE، أختر **إدارة > إدارة مدخل الويب > تكوينات متعددة المنافذ > DefaultGuestPortal**.



يتم إنشاء GUEST_PORTAL_SEQUENCE الذي يسمح لمستخدمي الداخل والضيف والإعلان.



7. من واجهة المستخدم الرسومية ISE، أختر **Guest > تكوينات متعددة المنافذ > DefaultGuestPortal**. من القائمة المنسدلة تعريف تسلسل المتجر، أختر **Guest_Portal_Sequence**.



التكوين على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

1. قم بتعريف خادم ISE Radius على WLC 5760.
2. قم بتكوين خادم RADIUS ومجموعة الخوادم وقائمة الطرق باستخدام CLI (واجهة سطر الأوامر).

```
dot1x system-auth-control

radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
timeout 10
retransmit 3
key Cisco123


aaa group server radius ISE
server name ISE
deadtime 10

aaa authentication dot1x ISE group ISE
aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
client 10.106.73.69 server-key Cisco123
auth-type any
```

3. قم بتكوين شبكة WLAN باستخدام CLI.

```
wlan CWA_NGWC 10 CWA_NGWC
aaa-override
accounting-list ISE
client vlan VLAN0012
no exclusionlist
mac-filtering MACFILTER
nac
```

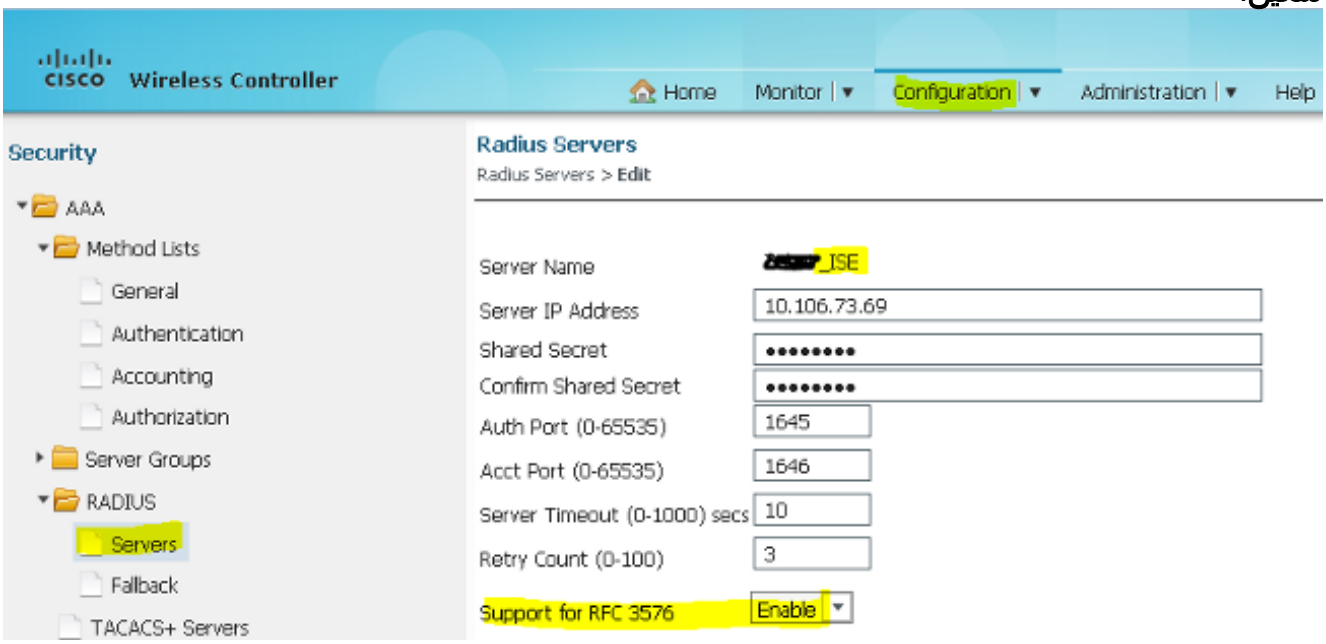
```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
session-timeout 1800
no shutdown
```

4. قم بتكوين قوائم التحكم في الوصول (ACL) المعاد توجيهها باستخدام واجهة سطر الأوامر. هذا هو قائمة التحكم في الوصول الخاصة ب URL-redirect التي يقوم ISE بإرجاعها كتجاوز AAA مع عنوان URL لإعادة توجيه مدخل الضيف. إنه قائمة تحكم في الوصول (ACL) مباشرة يتم إستخدامها حاليا على البنية الموحدة. هذه قائمة تحكم في الوصول (punt' (ACL' وهي نوع من قائمة تحكم في الوصول (ACL) عكسية التي كنت ستستخدمها عادة للبنية الموحدة. يجب حظر الوصول إلى DHCP وخادم DHCP و DNS وخادم DNS وخادم ISE. اسمح فقط ب 443، WWW، و 8443 حسب الحاجة. تستخدم بوابة ضيف ISE هذه المنفذ 8443 ولا تزال إعادة التوجيه تعمل مع قائمة التحكم في الوصول (ACL) الموضحة هنا. يتم تمكين ICMP هنا، ولكن استنادا إلى قواعد الأمان يمكنك إما الرفض أو السماح.

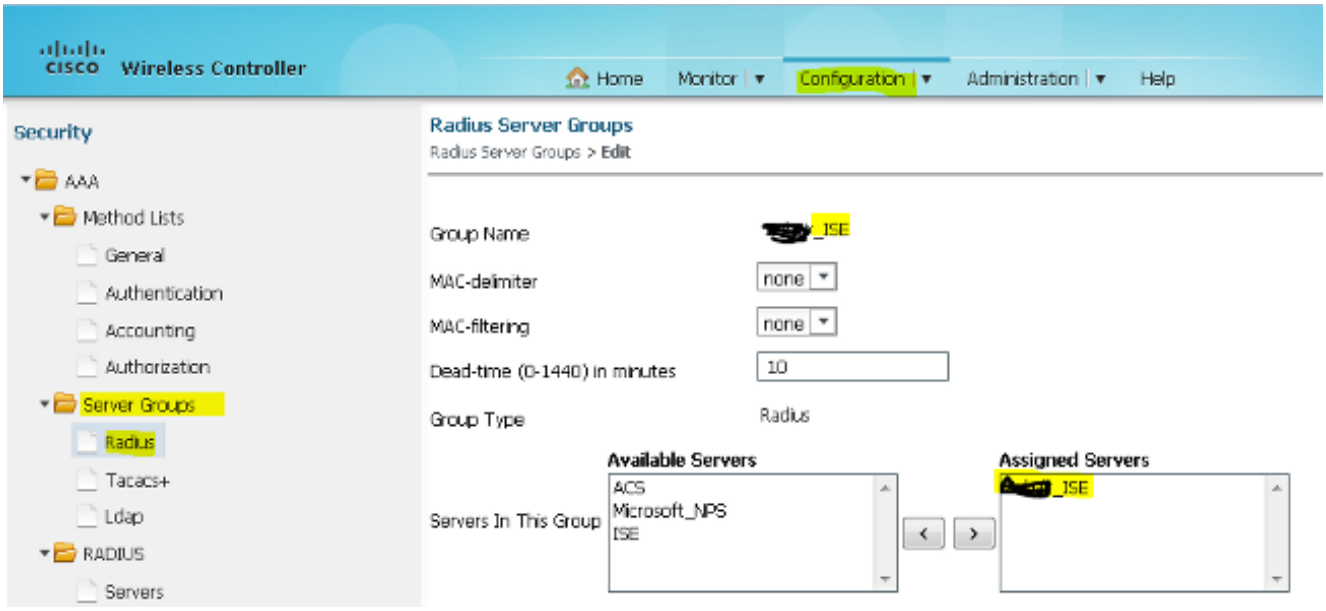
```
ip access-list extended REDIRECT
deny icmp any any
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

تحذير: عند تمكين HTTPS، قد يتسبب ذلك في بعض مشاكل وحدة المعالجة المركزية (CPU) الكبيرة بسبب قابلية التطوير. لا تقم بتمكين هذا الإجراء ما لم يوصى به من قبل فريق تصميم Cisco.

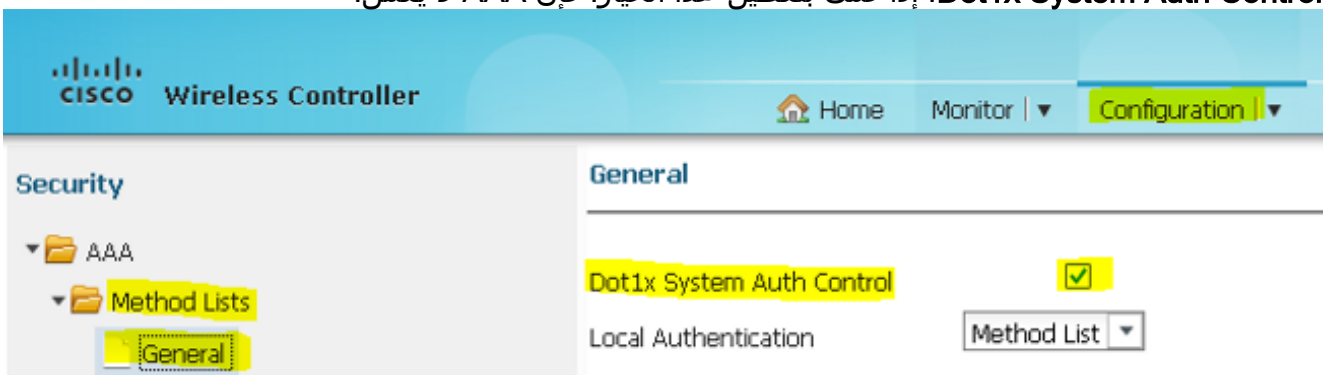
5. من واجهة المستخدم الرسومية (GUI) لوحدة التحكم اللاسلكية، أختر **AAA > RADIUS > الخوادم**. شكلت ال RADIUS نادل، نادل مجموعة، وأسلوب قائمة في ال gui. قم بتعبئة كافة المعلمات وتأكد من تطابق "السر المشترك" الذي تم تكوينه هنا مع ذلك الذي تم تكوينه على ISE لهذا الجهاز. من القائمة المنسدلة دعم RFC 3576، أختر **تمكين**.



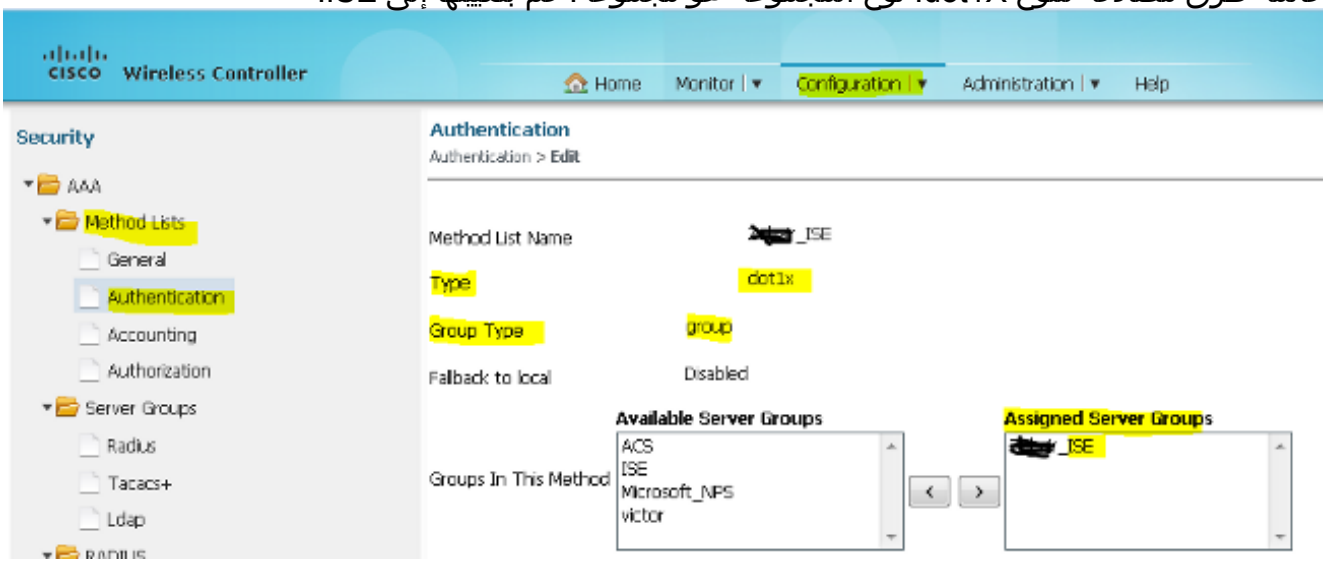
6. من واجهة المستخدم الرسومية (GUI) لوحدة التحكم اللاسلكية، أختر **AAA > مجموعات الخوادم > RADIUS**. إضافة خادم RADIUS الذي تم إنشاؤه مسبقا إلى مجموعات الخوادم.



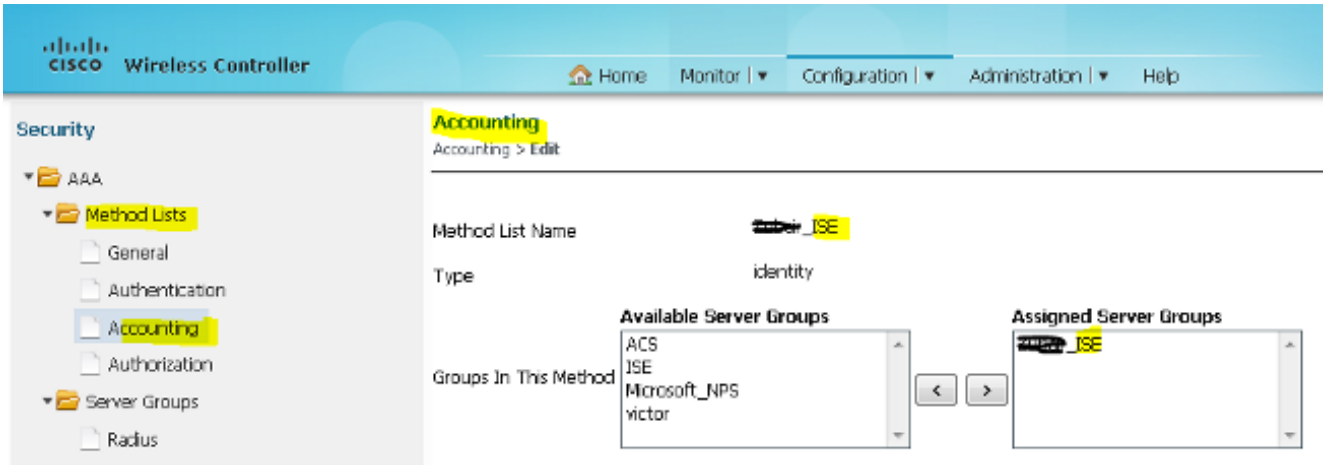
7. من واجهة المستخدم الرسومية لوحدة التحكم اللاسلكية، أختر **AAA > قوائم الطرق > عام**. حدد خانة الاختيار **Dot1x System Auth Control**. إذا قمت بتعطيل هذا الخيار، فإن AAA لا يعمل.



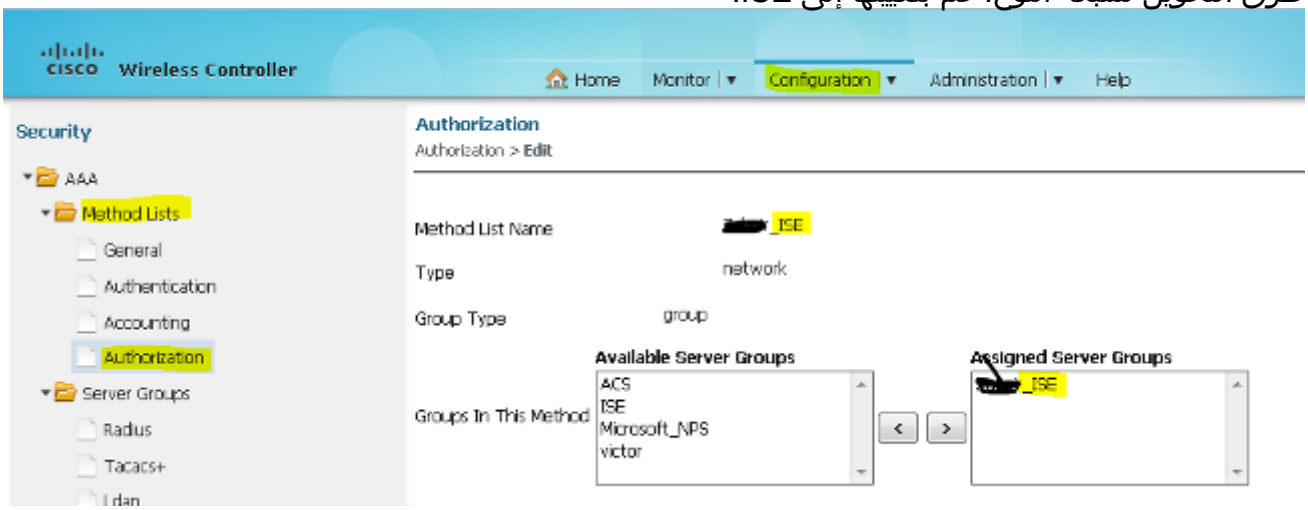
8. من واجهة المستخدم الرسومية لوحدة التحكم اللاسلكية، أختر **AAA > قوائم الطرق > المصادقة**. قم بإنشاء قائمة طرق مصادقة للنوع dot1X. نوع المجموعة هو مجموعة. قم بتعيينها إلى ISE.



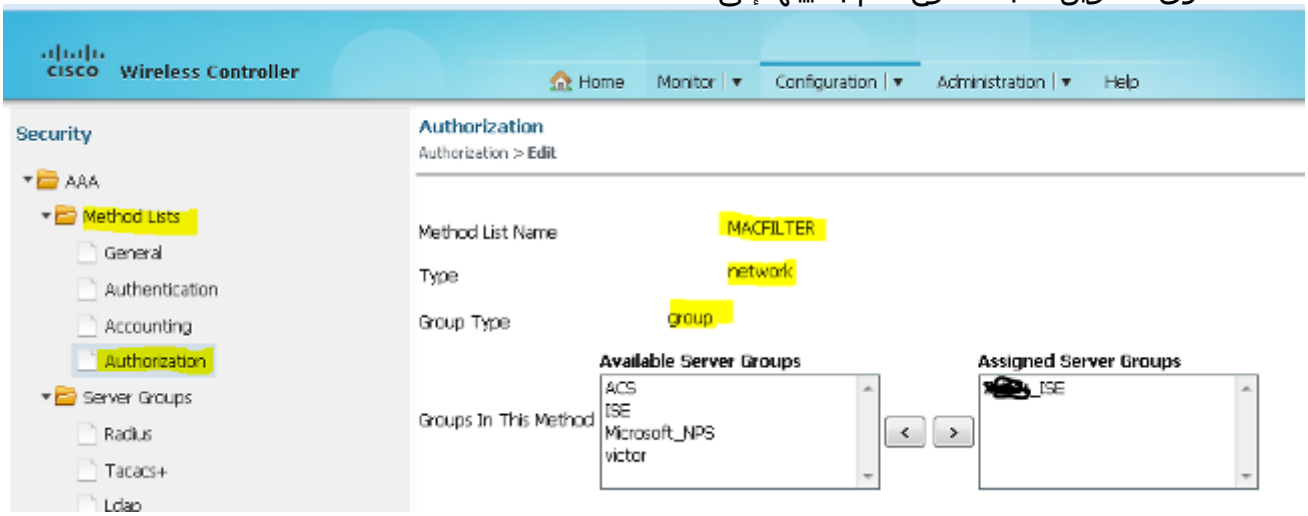
9. من واجهة المستخدم الرسومية لوحدة التحكم اللاسلكية، أختر **AAA > قوائم الطرق > المحاسبة**. إنشاء قائمة أسلوب محاسبة لهوية النوع. قم بتعيينها إلى ISE.



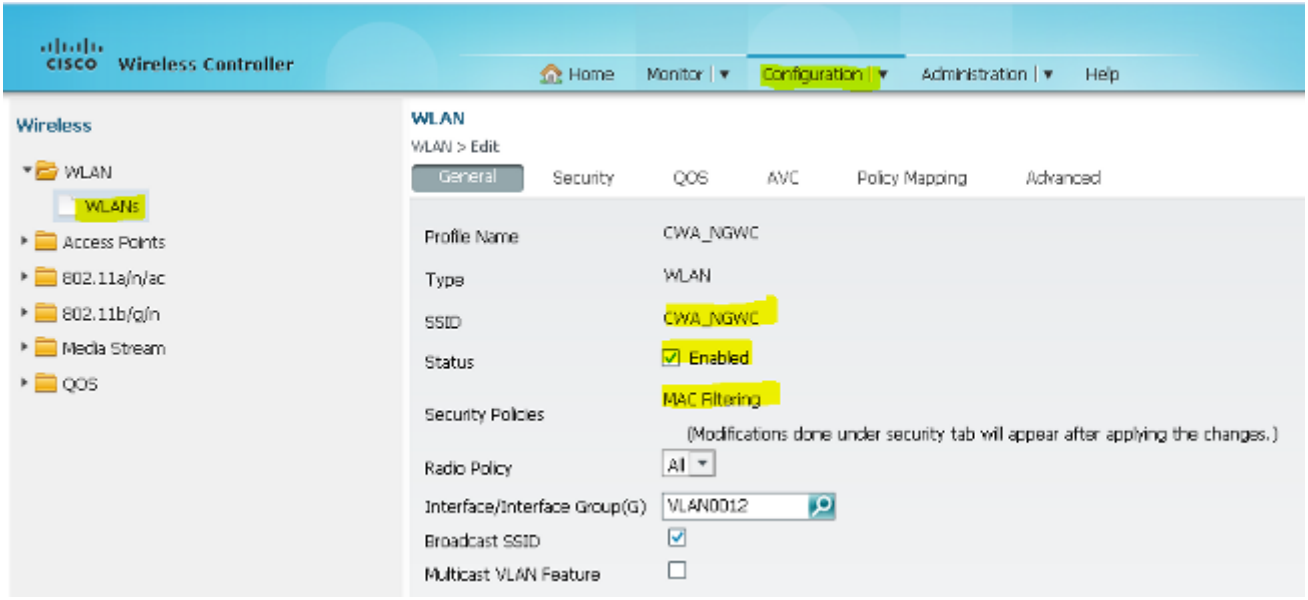
10. من واجهة المستخدم الرسومية لوحدة التحكم اللاسلكية، أختر **AAA > قوائم الطرق > التفويض**. إنشاء قائمة طرق التخويل لشبكة النوع. قم بتعيينها إلى ISE.



11. إختياري، نظرا لوجود ميزة التحكم في الوصول للوسائط (MAC) لدعم الأعطال كذلك. إنشاء MACfilter لقائمة طرق التخويل لشبكة النوع. قم بتعيينها إلى ISE.

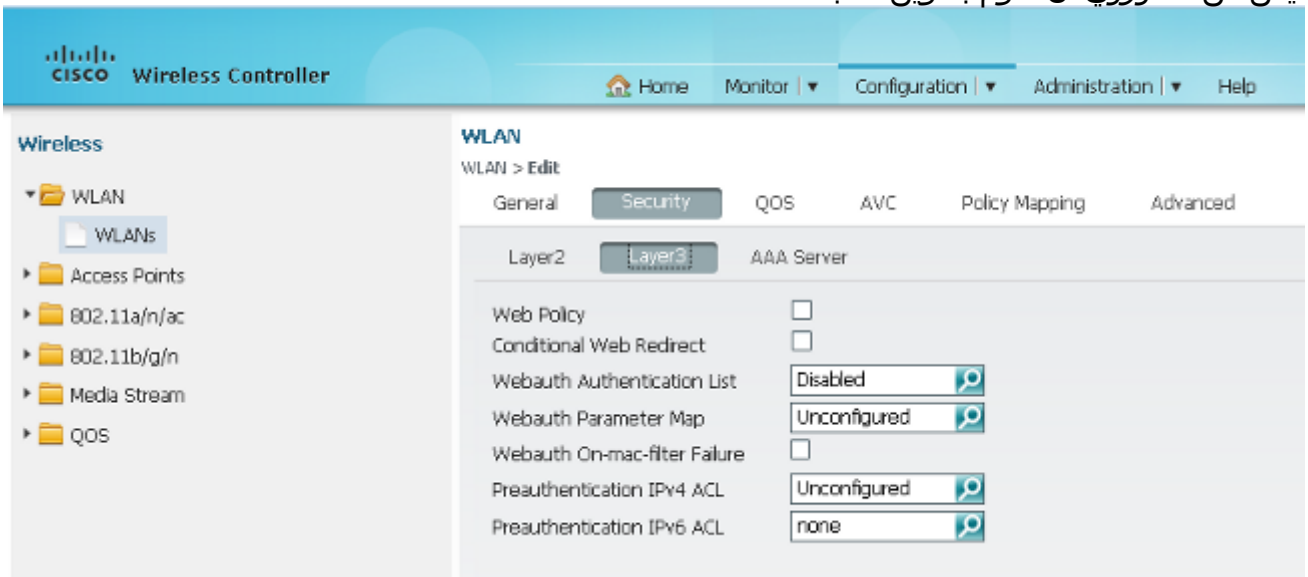


12. من واجهة المستخدم الرسومية (GUI) لوحدة التحكم اللاسلكية، أختر **WLAN > WLANs**. قم بإنشاء تكوين جديد باستخدام المعلمات الموضحة هنا.

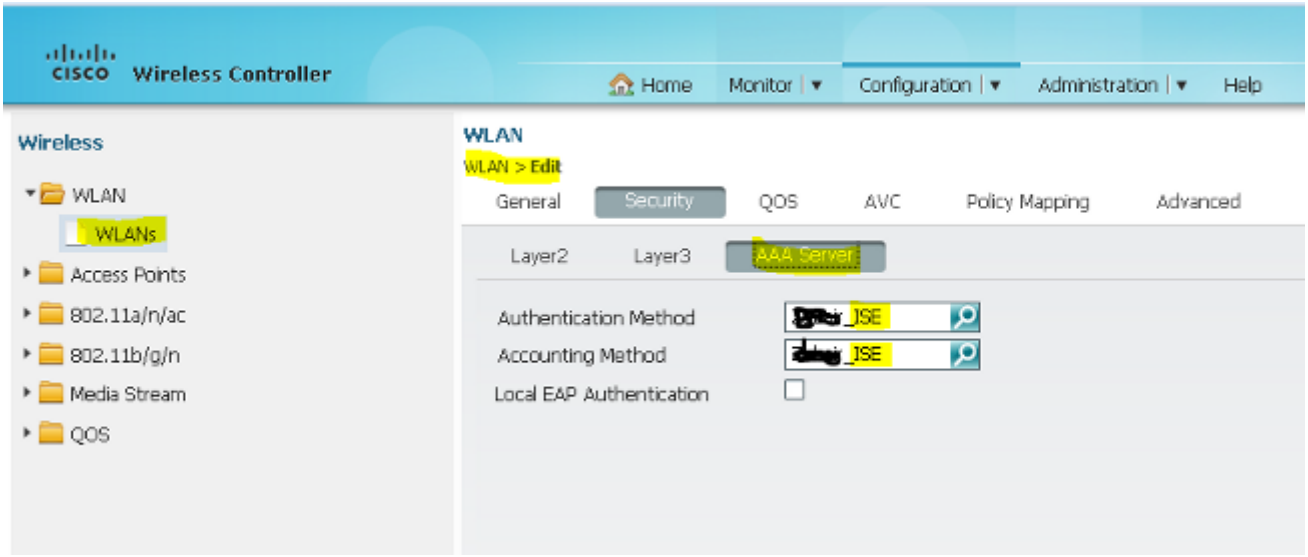


13. أختر **التأمين > الطبقة 2**. في حقل تصفية MAC، أدخل **MACfilter**.

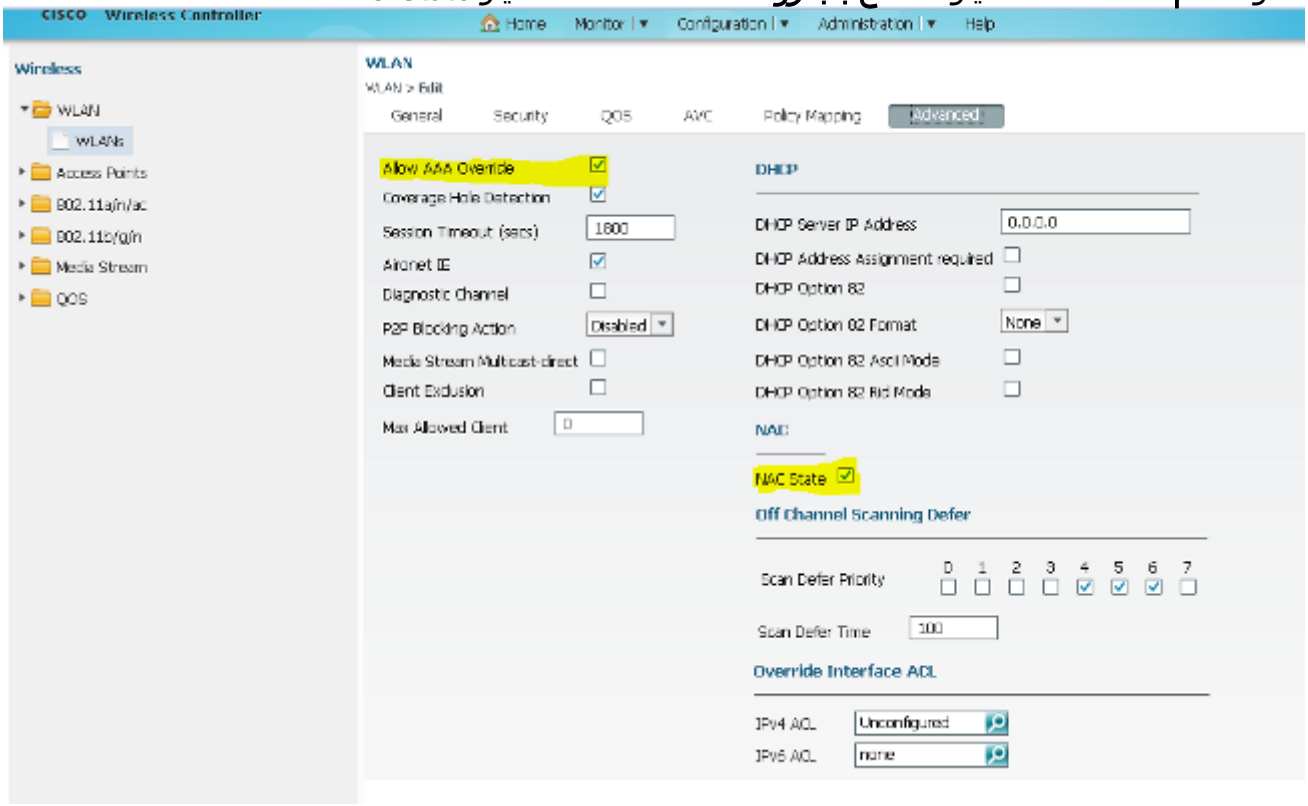
14. ليس من الضروري أن تقوم بتكوين الطبقة 3.



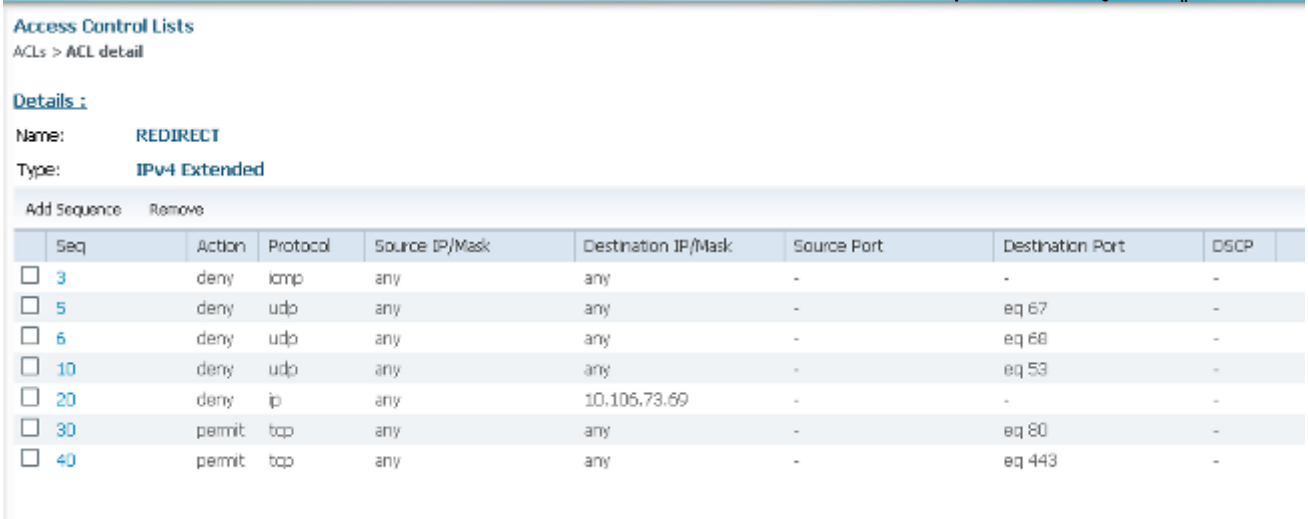
15. أختر **التأمين > خادم AAA**. من القائمة المنسدلة لأسلوب المصادقة، أختر **ISE**. من القائمة المنسدلة أسلوب المحاسبة، أختر **ISE**.



16. أختر **متقدم**. حدد خانة الاختيار **السماح بتجاوز AAA**. حدد خانة الاختيار **NAC State**.



17. قم بتكوين قوائم التحكم في الوصول (ACL) المعاد توجيهها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في واجهة المستخدم الرسومية (GUI).



Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
3	deny	icmp	any	any	-	-	-
5	deny	udp	any	any	-	eq 67	-
6	deny	udp	any	any	-	eq 68	-
10	deny	udp	any	any	-	eq 53	-
20	deny	ip	any	10.105.73.69	-	-	-
30	permit	tcp	any	any	-	eq 80	-
40	permit	tcp	any	any	-	eq 443	-

مخطط 2 تشكيل مثال

راجع المخطط 2 للحصول على الرسم التخطيطي للشبكة والشرح.

وهذا التكوين هو أيضا عملية على خطوتين.

التكوين على ISE

التكوين على ISE هو نفسه كما هو الحال بالنسبة لتكوين المخطط 1.

لا توجد حاجة لإضافة وحدة التحكم في الإرساء على ISE. أنت فقط تحتاج أن يضيف ال WLC خارجي على ال ISE، عينت ال RADIUS نادل على ال WLC خارجي، ورسم خريطة المعلومة سياسة تحت ال WLAN. على نقطة الربط تحتاج فقط أن يمكن ماك ييصفي.

في مثال التكوين هذا، هناك وحدتا WLC 5760s تعملان كمرسى خارجي. في حالة ما إذا كنت تريد إستخدام عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) 5760 كإرساء والمحول 3850 كعنصر إرساء خارجي، وهو وكيل التنقل، إلى وحدة تحكم أخرى في التنقل، فيكون التكوين نفسه صحيحا. ومع ذلك، لا توجد حاجة لتكوين شبكة WLAN على وحدة التحكم المتنقلة الثانية التي يحصل المحول 3850 عليها على التراخيص من. أنت فقط تحتاج أن يشير ال 3850 مفتاح إلى ال WLC 5760 أي يعمل كارتساء.

التكوين على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

1. على الخارجي، قم بتكوين خادم ISE باستخدام قائمة طرق AAA ل AAA وقم بتعيين WLAN إلى تفويض مرشح MAC. **ملاحظة**: تكوين قائمة التحكم في الوصول (ACL) المعاد توجيهها على كل من Anchor and Foreign وتصفية عناوين MAC أيضا.

```
dot1x system-auth-control

radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
timeout 10
retransmit 3
key Cisco123


aaa group server radius ISE
server name ISE
deadtime 10


aaa authentication dot1x ISE group ISE

aaa authorization network ISE group ISE

aaa authorization network MACFILTER group ISE
aaa accounting identity ISE start-stop group ISE
!

aaa server radius dynamic-author
client 10.106.73.69 server-key Cisco123
auth-type any

wlan MA-MC 11 MA-MC
aaa-override
accounting-list  ISE
client vlan VLAN0012
mac-filtering MACFILTER
```

```
mobility anchor 10.105.135.244
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE
session-timeout 1800
no shutdown
```

2. تكوين قوائم التحكم في الوصول لإعادة التوجيه باستخدام CLI. هذا هو قائمة التحكم في الوصول الخاصة ب URL-redirect التي يقوم ISE بإرجاعها كتجاوز AAA مع عنوان URL لإعادة توجيه مدخل الضيف. إنه قائمة تحكم في الوصول (ACL) مباشرة يتم إستخدامها حاليا على البنية الموحدة. هذه قائمة تحكم في الوصول (ACL) عكسية التي كنت ستستخدمها عادة للبنية الموحدة. يجب حظر الوصول إلى DHCP وخادم DHCP و DNS وخادم DNS وخادم ISE. اسمح فقط ب WWW، 443، و 8443 حسب الحاجة. تستخدم بوابة ضيف ISE هذه المنفذ 8443 ولا تزال إعادة التوجيه تعمل مع قائمة التحكم في الوصول (ACL) الموضحة هنا. يتم تمكين ICMP هنا، ولكن استنادا إلى قواعد الأمان يمكنك إما الرفض أو السماح.

```
ip access-list extended REDIRECT
deny icmp any any
deny udp any any eq bootps
deny udp any any eq bootpc
deny udp any any eq domain
deny ip any host 10.106.73.69
permit tcp any any eq www
permit tcp any any eq 443
```

تحذير: عند تمكين HTTPS، قد يتسبب ذلك في بعض مشاكل وحدة المعالجة المركزية (CPU) الكبيرة بسبب قابلية التطوير. لا تقم بتمكين هذا الإجراء ما لم يوصى به من قبل فريق تصميم Cisco.

3. قم بتكوين قابلية التنقل على المرسى.

```
wireless mobility group member ip 10.105.135.244 public-ip 10.105.135.244 group surbg
```

ملاحظة: إذا قمت بتكوين نفسه باستخدام المحول switch 3850 كمحول خارجي، فتأكد من تحديد مجموعة نظير المحول على وحدة التحكم في التنقل والعكس بالعكس على وحدة التحكم في التنقل. ثم قم بتكوين تكوينات CWA المذكورة أعلاه على المحول 3850.

4. التكوين على المرسى. على المرسى، لا توجد حاجة لتكوين أي تكوينات ISE. أنت فقط تحتاج إلى تكوين شبكة WLAN.

```
wlan MA-MC 6 MA-MC
aaa-override
client vlan VLAN0012
mac-filtering MACFILTER
mobility anchor
nac
nbsp;no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
session-timeout 1800
no shutdown
```

5. قم بتكوين قابلية التنقل على المرسى. قم بتعريف عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الآخر كعضو قابلية التنقل على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هذا.

```
wireless mobility group member ip 10.105.135.178 public-ip 10.105.135.178 group surbg
```

6. تكوين قوائم التحكم في الوصول لإعادة التوجيه باستخدام CLI. هذا هو قائمة التحكم في الوصول الخاصة ب URL-redirect التي يقوم ISE بإرجاعها كتجاوز AAA مع عنوان URL لإعادة توجيه مدخل الضيف. إنه قائمة تحكم في الوصول (ACL) مباشرة يتم إستخدامها حاليا على البنية الموحدة. هذه قائمة تحكم في الوصول (ACL) عكسية التي كنت ستستخدمها عادة للبنية الموحدة. يجب حظر الوصول إلى DHCP وخادم DHCP و DNS وخادم DNS وخادم ISE. اسمح فقط ب WWW، 443، و 8443 حسب الحاجة. تستخدم بوابة ضيف ISE هذه المنفذ 8443 ولا تزال إعادة التوجيه تعمل

مع قائمة التحكم في الوصول (ACL) الموضحة هنا. يتم تمكين ICMP هنا، ولكن استنادا إلى قواعد الأمان يمكنك إما الرفض أو السماح.

```
ip access-list extended REDIRECT
                deny icmp any any
            deny udp any any eq bootps
            deny udp any any eq bootpc
            deny udp any any eq domain
        deny ip any host 10.106.73.69
            permit tcp any any eq www
            permit tcp any any eq 443
```

تحذير: عند تمكين HTTPS، قد يتسبب ذلك في بعض مشاكل وحدة المعالجة المركزية (CPU) الكبيرة بسبب قابلية التطوير. لا تقم بتمكين هذا الإجراء ما لم يوصى به من قبل فريق تصميم Cisco.

مثال تكوين المخطط 3

راجع المخطط 3 لمخطط الشبكة وشرحها.

وهذه أيضا عملية ذات خطوتين.

التكوين على ISE

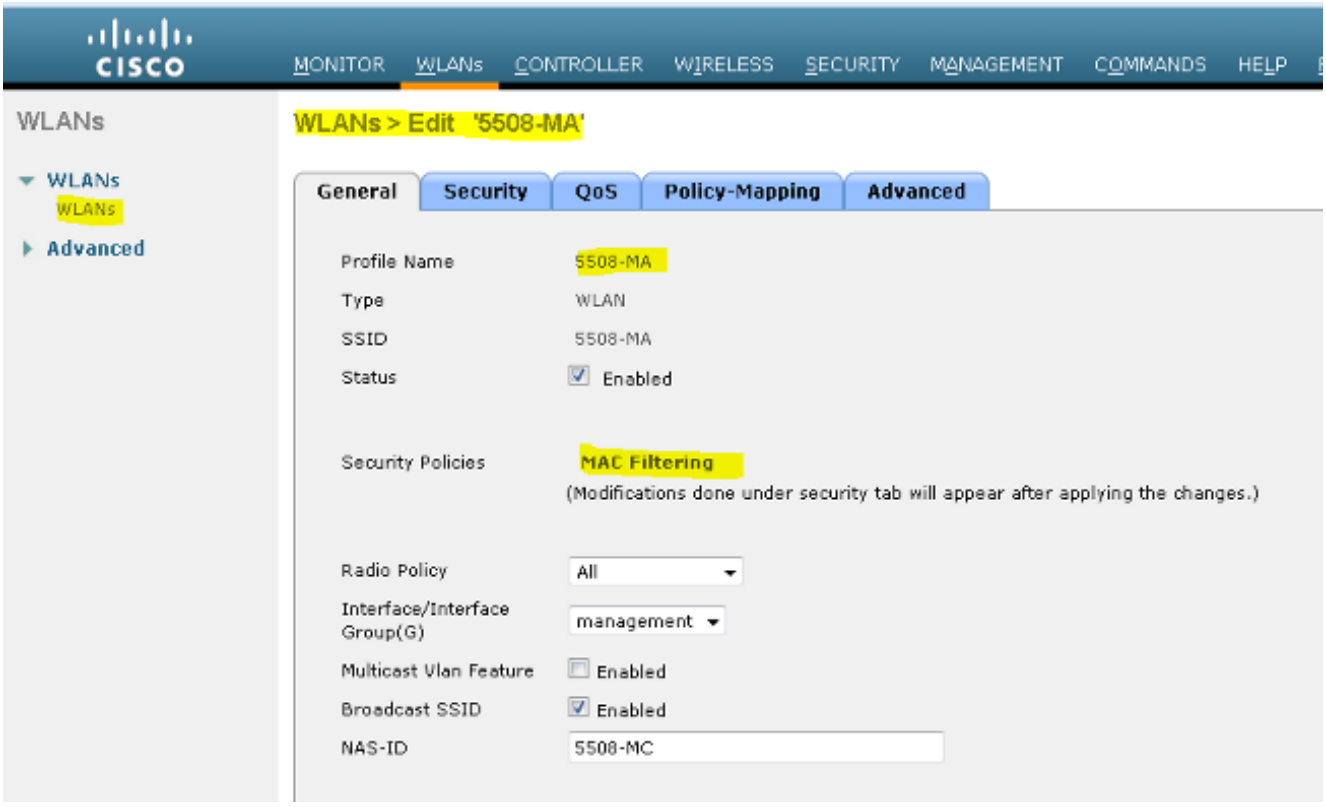
التكوين على ISE هو نفسه كما هو الحال بالنسبة لتكوين المخطط 1.

لا توجد حاجة لإضافة وحدة التحكم في الإرساء على ISE. أنت فقط تحتاج أن يضيف ال WLC خارجي على ال ISE، عينت ال RADIUS نادل على ال WLC خارجي، ورسم خريطة المعلومة سياسة تحت ال WLAN. على نقطة الربط تحتاج فقط أن يمكن ماك بيصفي.

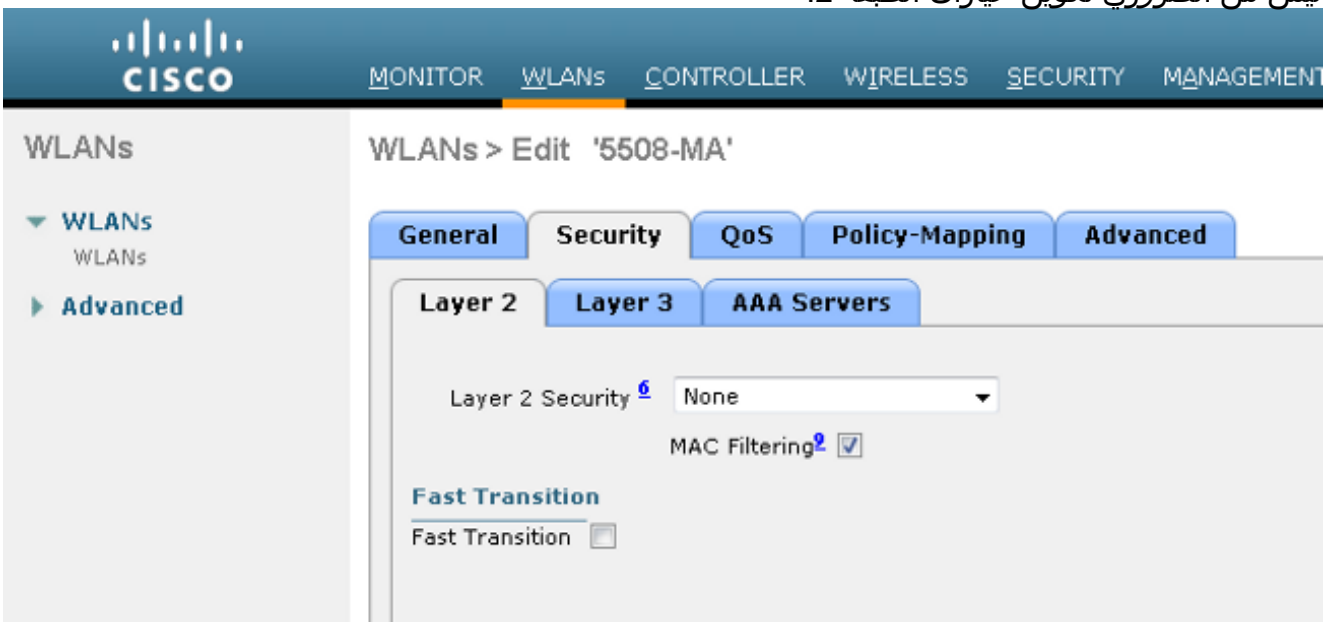
في هذا المثال، هناك عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) رقم 5508 الذي يعمل كمرسى وعنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 5760 الذي يعمل كعنصر تحكم في الشبكة المحلية اللاسلكية (WLC) خارجي. إن يريد أنت أن يستعمل 5508 WLC كربط و 3850 مفتاح و WLC خارجي، أي يكون حركي وكيل، إلى آخر حركية جهاز تحكم بعد ذلك ال نفسه تشكيل صحيح. ومع ذلك، لا توجد حاجة لتكوين شبكة WLAN على وحدة التحكم المتنقلة الثانية التي يحصل المحول 3850 عليها على التراخيص من. أنت فقط تحتاج أن يشير المفتاح 3850 إلى ال WLC 5508 الذي يعمل كمرسى.

التكوين على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

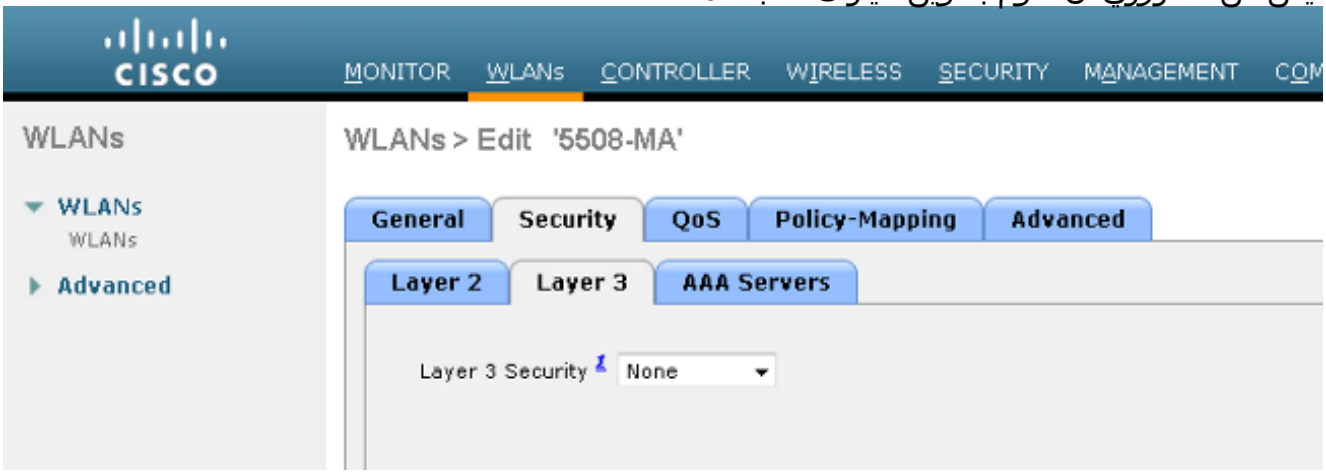
1. على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الأجنبية، قم بتكوين خادم ISE باستخدام قائمة أساليب AAA ل AAA وقم بتعيين شبكة WLAN إلى تفويض عامل تصفية MAC. هذا غير ضروري على المرسى. **ملاحظة**: تكوين قائمة التحكم في الوصول (ACL) لإعادة التوجيه على كل من Anchor and Foreign WLC وكذلك تصفية MAC.
2. من ال WLC 5508 GUI، أخترت **WLANs>جديد** in order to شكلت المادة إرساء 5508. املأ التفاصيل لتمكين تصفية MAC.



3. ليس من الضروري تكوين خيارات الطبقة 2.

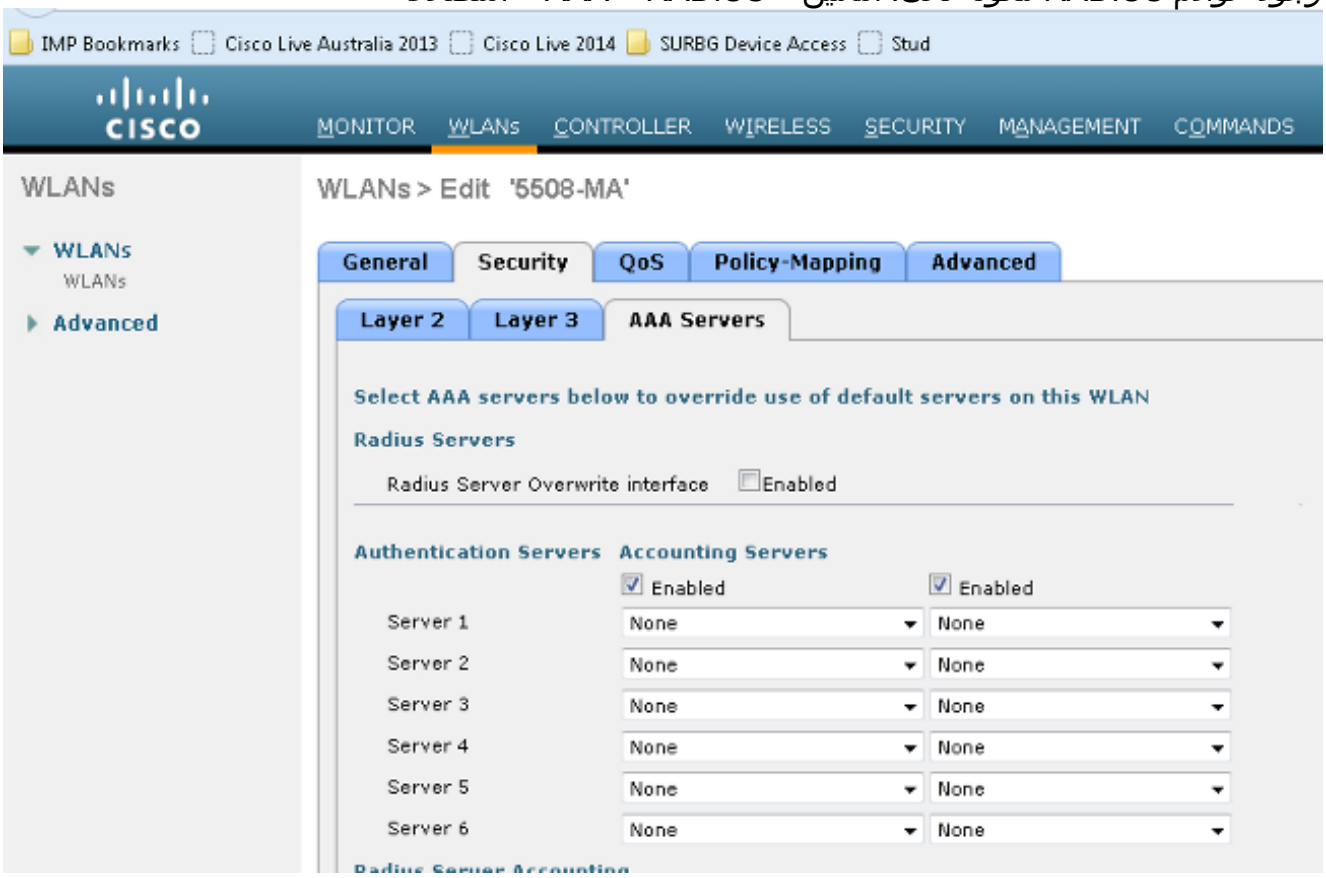


4. ليس من الضروري أن تقوم بتكوين خيارات الطبقة 3.

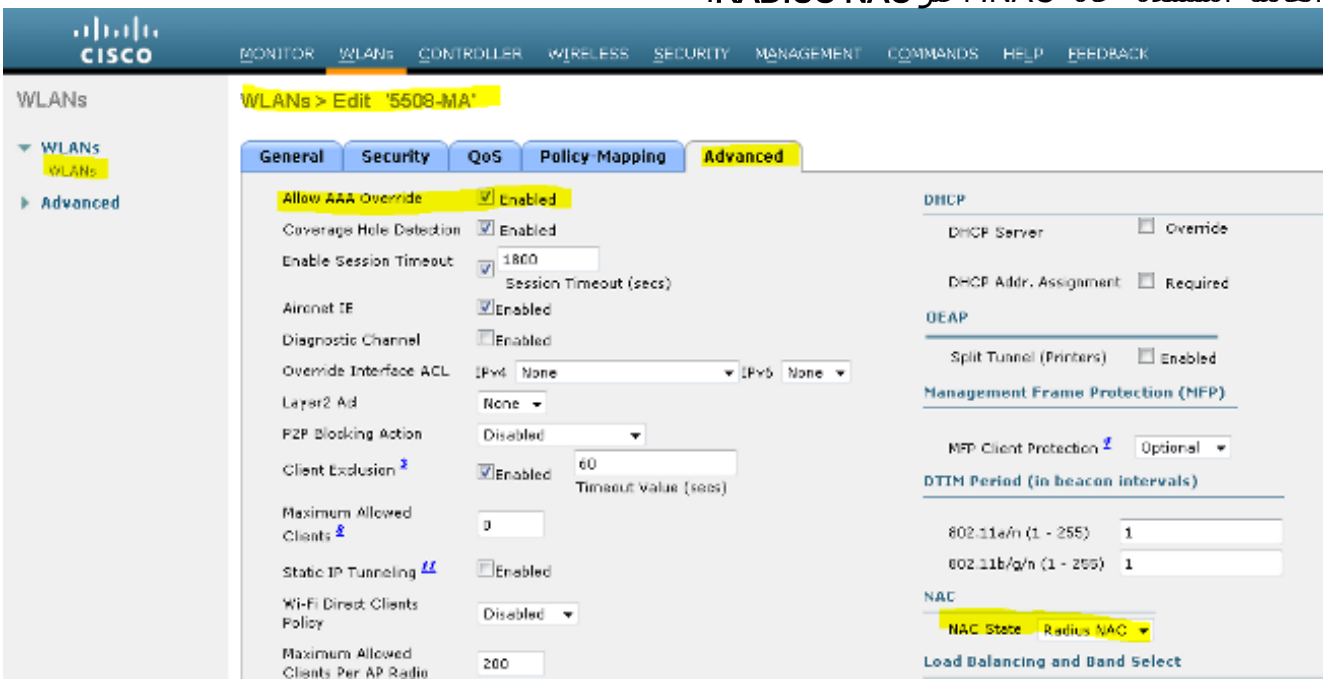


5. يجب تعطيل خوادم AAA في عنصر التحكم Anchor AireOS WLC حتى تتم معالجة CoA بواسطة NGWC

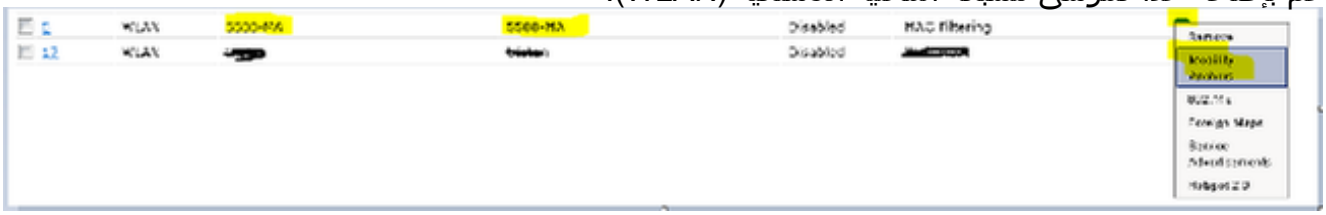
الخارجي. لا يمكن تمكين خوادم AAA في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في حالة عدم وجود خوادم RADIUS مكونة تحت: التأمين > RADIUS > AAA > المصادقة



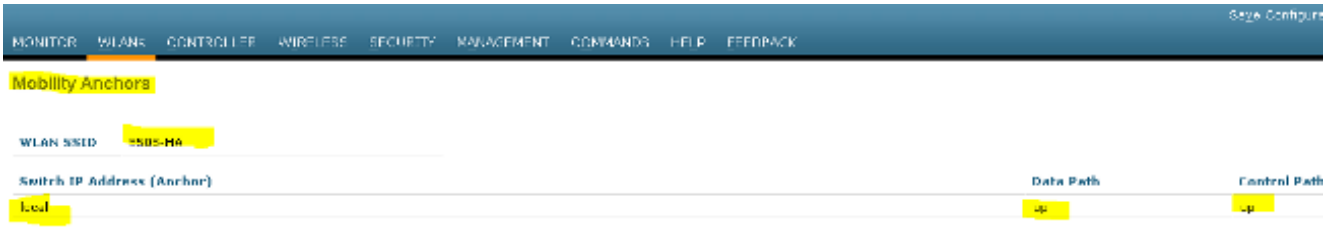
6. أختر **شبكات WLAN > شبكات WLAN > تحرير > خيارات متقدمة**. حدد خانة الاختيار **السماح بتجاوز AAA**. من القائمة المنسدلة حالة NAC، أختر **RADIUS NAC**.



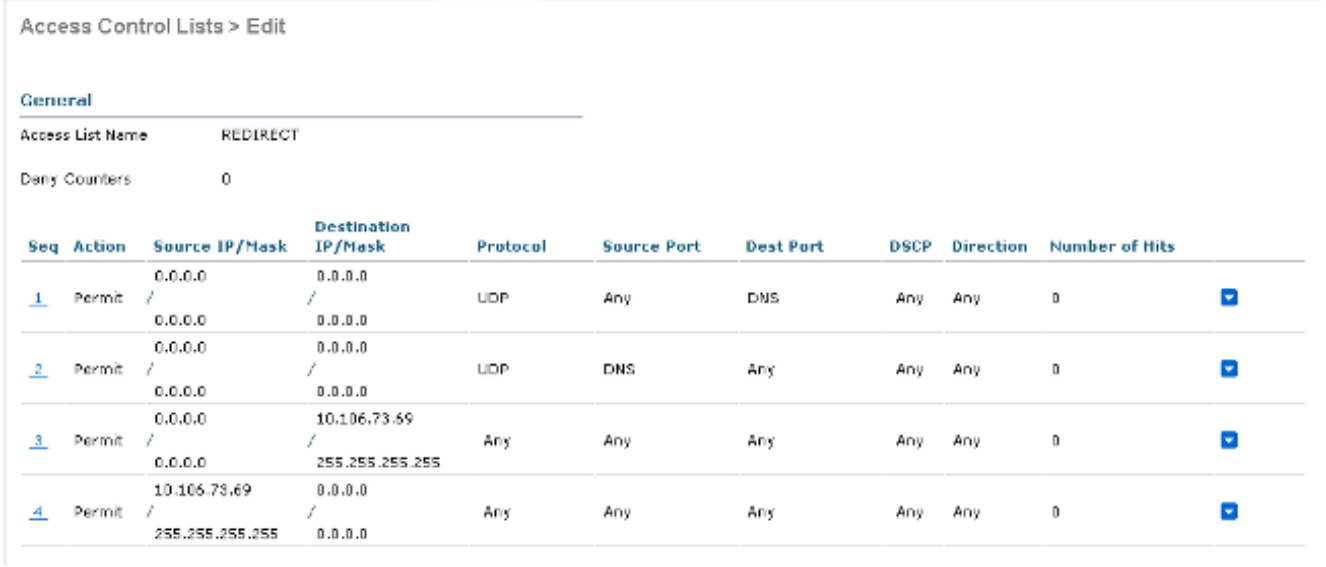
7. قم بإضافة هذا كمرسى للشبكة المحلية اللاسلكية (WLAN).



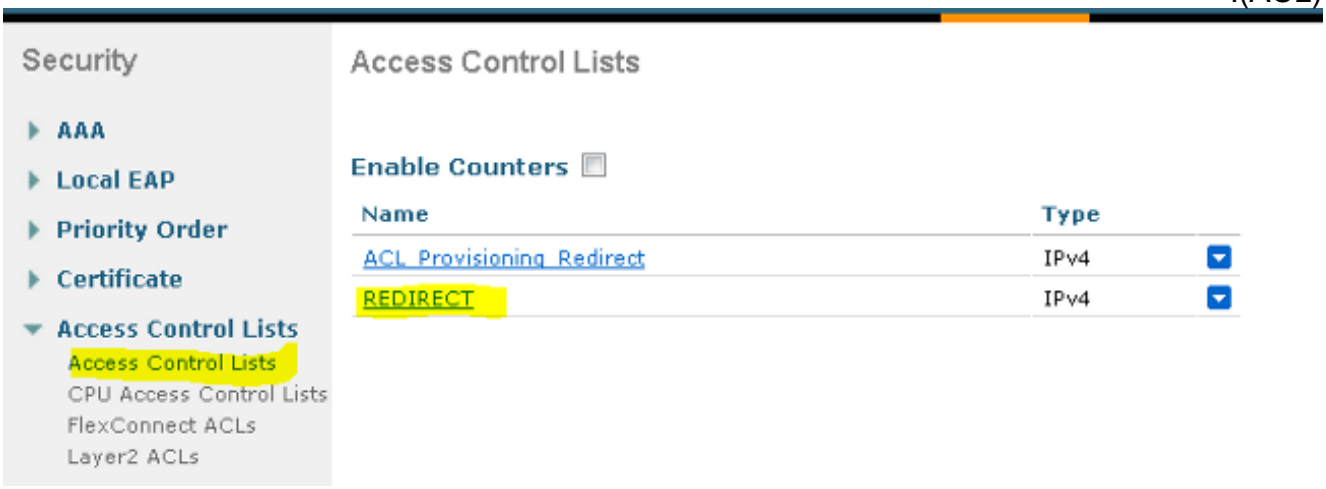
8. بعد الإشارة إلى المحلية، يجب أن تنظر إلى هذا باستخدام Control و Data Path Up/Up.



9. قم بإنشاء قائمة التحكم في الوصول (ACL) لإعادة التوجيه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). هذا ينكر DHCP و DNS. وهو يسمح ببروتوكول HTTP/HTTPs.



هكذا تبدو بعد إنشاء قائمة التحكم في الوصول (ACL).



10. قم بتعريف خادم ISE RADIUS على WLC 5760.
11. قم بتكوين خادم RADIUS ومجموعة الخوادم وقائمة الطرق باستخدام CLI (واجهة سطر الأوامر).

```
dot1x system-auth-control

radius server ISE
address ipv4 10.106.73.69 auth-port 1645 acct-port 1646
timeout 10
retransmit 3
key Cisco123


aaa group server radius ISE
server name ISE
deadtime 10

aaa authentication dot1x ISE group ISE

aaa authorization network ISE group ISE
```

```
aaa authorization network MACFILTER group ISE

aaa accounting identity ISE start-stop group ISE

!

aaa server radius dynamic-author
 client 10.106.73.69 server-key Cisco123
  auth-type any
```

12. قم بتكوين شبكة WLAN من واجهة سطر الأوامر.

```
wlan 5508-MA 15 5508-MA
 aaa-override
 accounting-list ISE
 client vlan VLAN0012
 mac-filtering MACFILTER
 mobility anchor 10.105.135.151
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE
 session-timeout 1800
 shutdown
```

13. قم بتعريف عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الآخر كعضو قابلية التنقل على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هذا.

```
wireless mobility group member ip 10.105.135.151public-ip 10.105.135.151 group Mobile-1
```

ملاحظة: إذا قمت بتكوين نفسه باستخدام عنصر التحكم في الشبكة المحلية اللاسلكية (3850 WLC) كعنصر تحكم خارجي، فتأكد من تحديد مجموعة نظير المحول على وحدة التحكم في التنقل والعكس بالعكس على وحدة التحكم في التنقل. ثم قم بتكوين تكوينات CWA السابقة على عنصر التحكم في الشبكة المحلية اللاسلكية (3850 WLC).

14. تكوين قوائم التحكم في الوصول لإعادة التوجيه باستخدام CLI. هذا هو قائمة التحكم في الوصول الخاصة ب URL-redirect التي يقوم ISE بإرجاعها كتجاوز AAA مع عنوان URL لإعادة توجيه مدخل الضيف. إنه قائمة تحكم في الوصول (ACL) مباشرة يتم إستخدامها حاليا على البنية الموحدة. هذه قائمة تحكم في الوصول (ACL) عكسية التي كنت ستستخدمها عادة للبنية الموحدة. يجب حظر الوصول إلى DHCP وخادم DHCP و DNS وخادم DNS وخادم ISE. اسمح فقط ب WWW، 443، و 8443 حسب الحاجة. تستخدم بوابة ضيف ISE هذه المنفذ 8443 ولا تزال إعادة التوجيه تعمل مع قائمة التحكم في الوصول (ACL) الموضحة هنا. يتم تمكين ICMP هنا، ولكن استنادا إلى قواعد الأمان يمكنك إما الرفض أو السماح.

```
ip access-list extended REDIRECT
 deny icmp any any
 deny udp any any eq bootps
 deny udp any any eq bootpc
 deny udp any any eq domain
 deny ip any host 10.106.73.69
 permit tcp any any eq www
 permit tcp any any eq 443
```

تحذير: عند تمكين HTTPS، قد يتسبب ذلك في بعض مشاكل وحدة المعالجة المركزية (CPU) الكبيرة بسبب قابلية التطوير. لا تقم بتمكين هذا الإجراء ما لم يوصى به من قبل فريق تصميم Cisco.

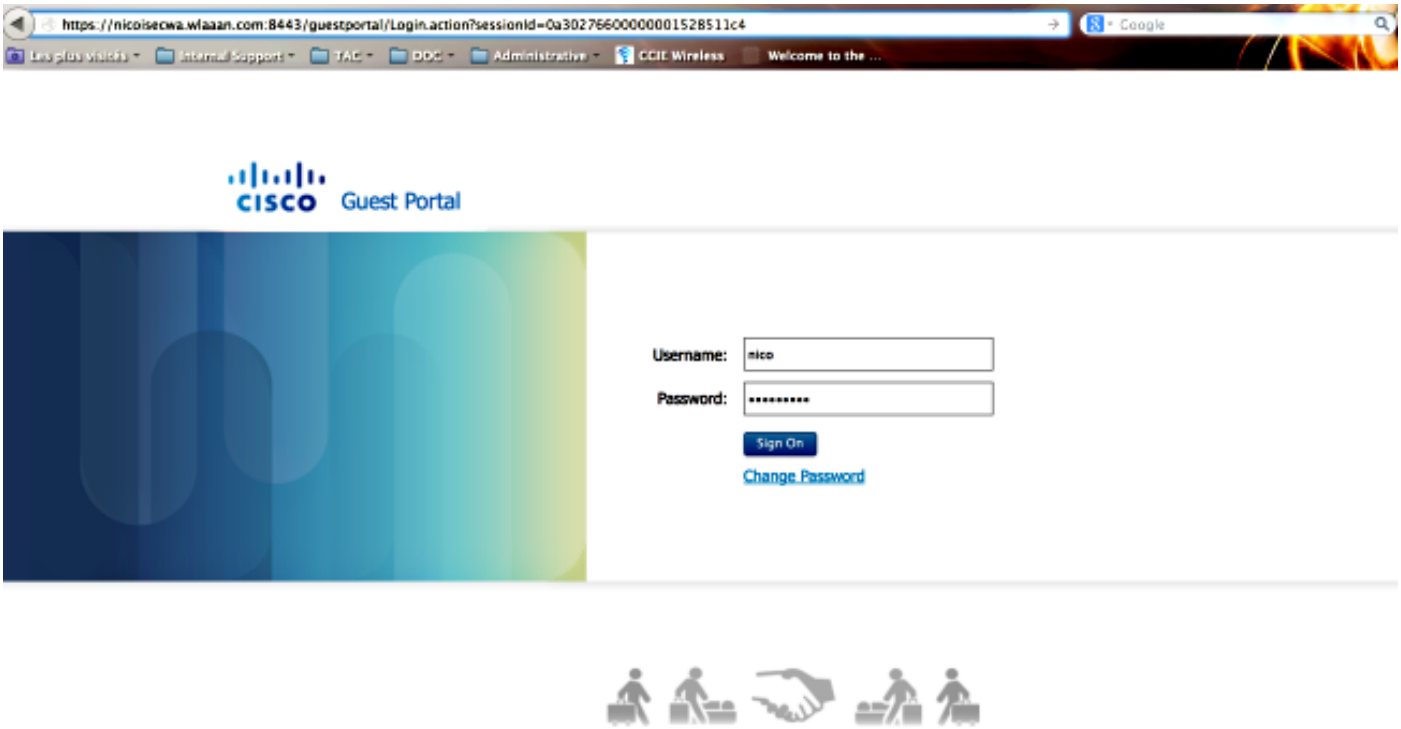
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

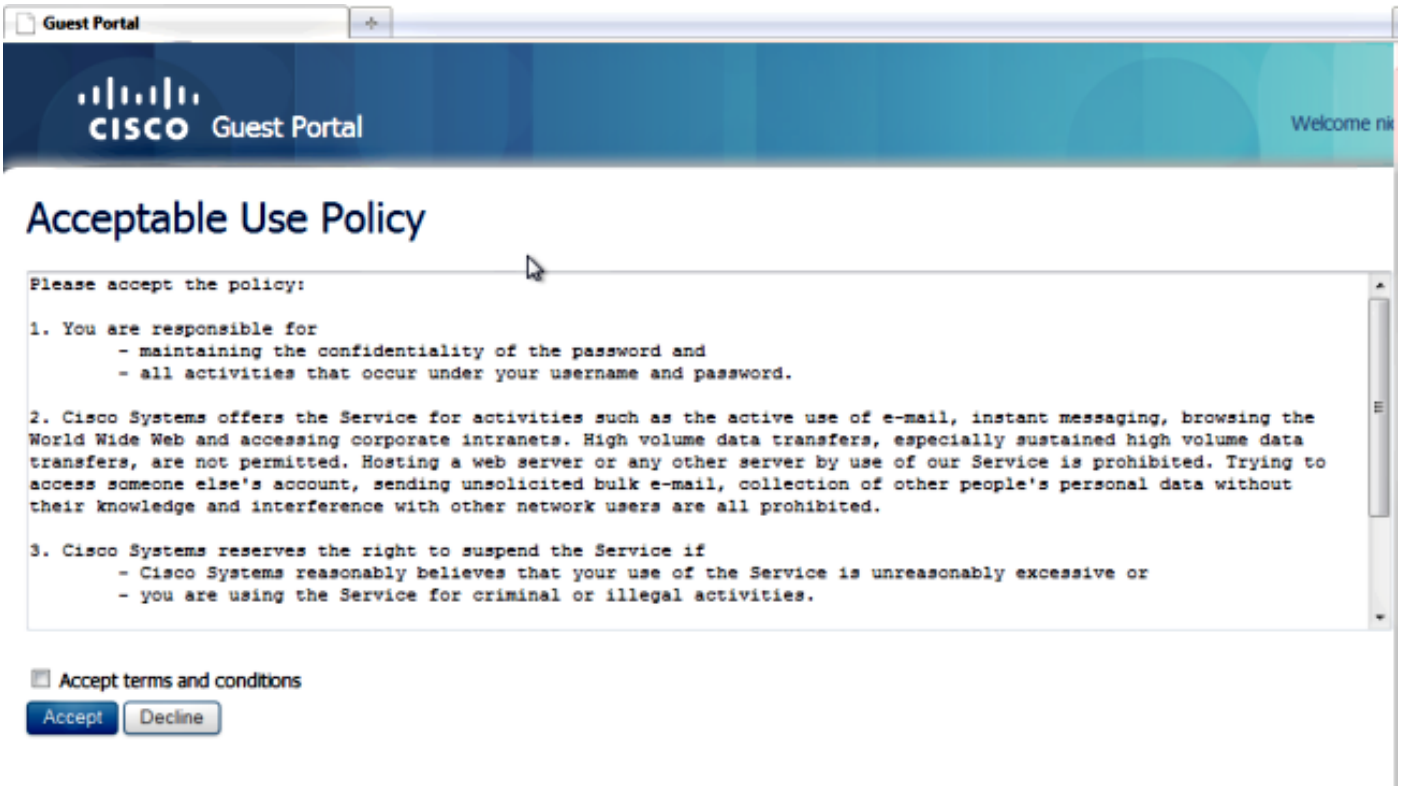
تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل

لمُخرَج الأمر **show**.

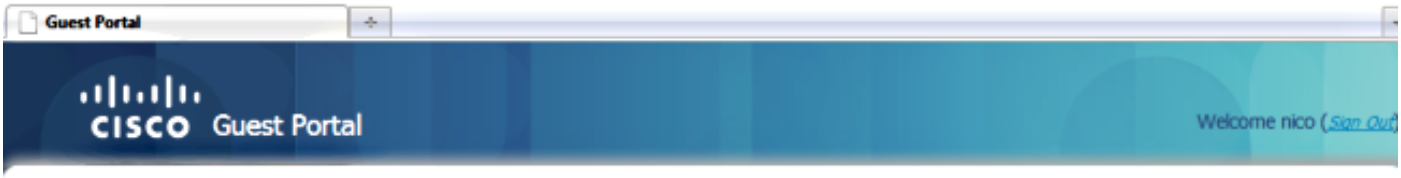
قم بتوصيل العميل ب SSID الذي تم تكوينه. بمجرد إستلام عنوان IP وعندما ينتقل العميل إلى حالة "طلب مصادقة الويب"، افتح المستعرض. أدخل بيانات اعتماد العميل الخاصة بك في البوابة.



بعد المصادقة الناجحة، حدد خانة الاختيار **قبول البنود والشروط**. انقر فوق **قبول**.

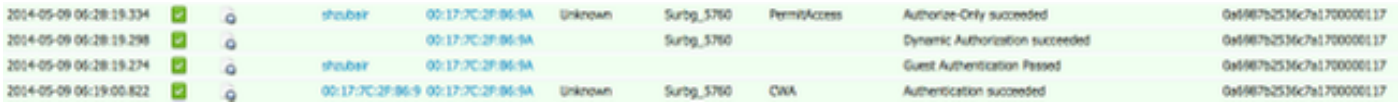


ستتلقى رسالة تأكيد وستتمكن الآن من الاستعراض إلى الإنترنت.



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

في ISE، يبدو تدفق العميل كما يلي:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للوصول المجمع، يوصى بتشغيل المسارات بدلا من تصحيح الأخطاء. على Aironet OS 5508 WLC أنت تحتاج فقط أن يدخل **debug زبون <client mac>** و**debug web-auth redirect enable mac <client mac>**.

```
set trace group-wireless-client level debug
set trace group-wireless-secure level debug

set trace group-wireless-client filter mac 0017.7c2f.b69a
set trace group-wireless-secure filter mac 0017.7c2f.b69a
```

يتم تضمين بعض العيوب المعروفة على Cisco IOS-XE و Aironet OS في معرف تصحيح الأخطاء من Cisco CSCun38344.

هذا هو ما يبدو عليه تدفق CWA الناجح على المسارات:

```
IST 63d7 8151] 0017.7c2f.b69a Association received from mobile 13:13:15.951 05/09/14]
                                                              on AP c8f9.f983.4260
  IST 63d8 8151] 0017.7c2f.b69a qos upstream policy is unknown 13:13:15.951 05/09/14]
                                                              and downstream policy is unknown

IST 63e0 8151] 0017.7c2f.b69a Applying site-specific IPv6 13:13:15.951 05/09/14]
override for station  0017.7c2f.b69a  - vapId 15, site 'default-group', interface
```

'VLAN0012'
IST 63e1 8151] 0017.7c2f.b69a Applying local bridging Interface 13:13:15.951 05/09/14]
'Policy for station 0017.7c2f.b69a - vlan 12, interface 'VLAN0012
IST 63e2 8151] 0017.7c2f.b69a 13:13:15.951 05/09/14]
**** Inside applyLocalProfilingPolicyAction ****

IST 63e3 8151] 0017.7c2f.b69a *** **Client State = START** 13:13:15.951 05/09/14]
instance = 1 instance Name POLICY_PROFILING_80211_ASSOC, OverrideEnable = 1
deviceTypeLen=0, deviceType=(null), userRoleLen=0, userRole=(null

IST 63eb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter 13:13:15.951 05/09/14]
request for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
IST 63ec 8151] 0017.7c2f.b69a AAAS: auth request sent 13:13:15.951 05/09/14]
IST 63ed 8151] 0017.7c2f.b69a apfProcessAssocReq 13:13:15.951 05/09/14
apf_80211.c:6149) Changing state for mobile 0017.7c2f.b69a on AP c8f9.f983.4260)
from Idle to AAA Pending

IST 63ee 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1 13:13:15.951 05/09/14]
IST 63ef 8151] 0017.7c2f.b69a Scheduling deletion of Mobile 13:13:15.951 05/09/14]
Station: (callerId: 20) in 10 seconds
IST 63f0 211] **Parsed CLID MAC Address = 0:23:124:47:182:154** 13:13:15.951 05/09/14]
IST 63f1 211] AAA SRV(00000118): process author req 13:13:15.951 05/09/14]
IST 63f2 211] **AAA SRV(00000118): Author method=SERVER_GROUP Zubair_ISE** 13:13:15.951 05/09/14]
IST 63f3 220] AAA SRV(00000118): protocol reply PASS for Authorization 13:13:16.015 05/09/14]
IST 63f4 220] AAA SRV(00000118): Return Authorization status=PASS 13:13:16.015 05/09/14]
IST 63f5 8151] 0017.7c2f.b69a AAAS: received response, cid=266 13:13:16.015 05/09/14]
IST 63f6 8151] 0017.7c2f.b69a AAAS: deleting context, cid=266 13:13:16.015 05/09/14]
IST 63f7 8151] 0017.7c2f.b69a Not comparing because the ACLs have 13:13:16.015 05/09/14]
.not been sent yet
,IST 63f8 8151] 0017.7c2f.b69a Final flag values are, epmSendAcl 1 13:13:16.015 05/09/14]
epmSendAclDone 0
IST 63f9 8151] 0017.7c2f.b69a 13:13:16.015 05/09/14]
client incoming attribute size are 193
IST 63fa 8151] 0017.7c2f.b69a AAAS: mac filter callback 13:13:16.015 05/09/14]
status=0 uniqueId=280
IST 63fb 8151] 0017.7c2f.b69a AAA Override Url-Redirect 13:13:16.015 05/09/14]
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'
set
IST 63fc 8151] **0017.7c2f.b69a Redirect URL received for** 13:13:16.015 05/09/14]
.client from RADIUS. for redirection
IST 63fd 8151] 0017.7c2f.b69a Setting AAA Override 13:13:16.015 05/09/14]
'Url-Redirect-Acl 'REDIRECT
IST 63fe 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 13:13:16.015 05/09/14]
'REDIRECT'
IST 63ff 8151] 0017.7c2f.b69a Local Policy: At the start of 13:13:16.015 05/09/14]
apfApplyOverride2. Client State START

IST 6400 8151] 0017.7c2f.b69a Applying new AAA override for 13:13:16.015 05/09/14]
station 0017.7c2f.b69a
IST 6401 8151] 0017.7c2f.b69a Local Policy: Applying new 13:13:16.015 05/09/14]
AAA override for station
,IST 6402 8151] 0017.7c2f.b69a Override Values: source: 2 13:13:16.015 05/09/14]
,valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff
sessionTimeout: -1
,IST 6403 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1 13:13:16.015 05/09/14]
:dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName
IST 6404 8151] 0017.7c2f.b69a Local Policy: Applying 13:13:16.015 05/09/14]
override policy
IST 6405 8151] 0017.7c2f.b69a Clearing Dhcp state for 13:13:16.015 05/09/14]
--- station
IST 6406 8151] 0017.7c2f.b69a Local Policy: Before 13:13:16.015 05/09/14]
Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and
apfMsTimeout is 1800

IST 6407 8151] 0017.7c2f.b69a Local Policy:Setting 13:13:16.015 05/09/14]
Interface name e VLAN0012

IST 6408 8151] 0017.7c2f.b69a Local Policy:Setting local 13:13:16.015 05/09/14]
bridging VLAN name VLAN0012 and VLAN ID 12

IST 6409 8151] 0017.7c2f.b69a Applying WLAN ACL 13:13:16.015 05/09/14]
policies to client
IST 640a 8151] 0017.7c2f.b69a No Interface ACL 13:13:16.015 05/09/14]
(used for Wireless client in WCM(NGWC
:IST 640b 8151] 0017.7c2f.b69a apfApplyWlanPolicy 13:13:16.015 05/09/14]
Retaining the ACL recieved in AAA attributes 255 on mobile
IST 640c 8151] 0017.7c2f.b69a Local Policy: After 13:13:16.015 05/09/14]
Applying WLAN policy AccessVLAN = 12 and SessionTimeout is 1800 and
apfMsTimeout is 1800

IST 641a 8151] 0017.7c2f.b69a WCDB_ADD: Platform 13:13:16.015 05/09/14]
ID allocated successfully ID:259
IST 641b 8151] 0017.7c2f.b69a WCDB_ADD: Adding 13:13:16.015 05/09/14]
opt82 len 0
IST 641c 8151] 0017.7c2f.b69a WCDB_ADD: ssid 13:13:16.015 05/09/14]
(5508-MA bssid c8f9.f983.4260 vlan 12 auth=ASSOCIATION(0
wlan(ap-group/global) 15/15 client 0 assoc 1 mob=Unassoc(0) radio 0
m_vlan 12 ip 0.0.0.0 src 0x506c800000000f dst 0x0 cid 0x47ad4000000145
glob rsc id 259dhcpsrv 0.0.0
IST 641d 8151] 0017.7c2f.b69a Change state to 13:13:16.015 05/09/14]
(AUTHCHECK (2) last state START (0

IST 641e 8151] 0017.7c2f.b69a Change state to 13:13:16.015 05/09/14]
(L2AUTHCOMPLETE (4) last state AUTHCHECK (2

IST 641f 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 13:13:16.015 05/09/14]
,IST 6420 8151] 0017.7c2f.b69a WCDB_LLM: NoRun Prev Mob 0 13:13:16.015 05/09/14]
Curr Mob 0 llmReq 1, return False
IST 6421 207] [WCDB] ==Add event: type Regular Wireless client 13:13:16.015 05/09/14]
(0017.7c2f.b69a) client id (0x47ad4000000145) client index (259) vlan (12)
(auth_state (ASSOCIATION) mob_state (INIT
(IST 6422 207] [WCDB] ===intf src/dst (0x506c800000000f)/(0x0 13:13:16.015 05/09/14]
(radio_id (0) p2p_state (P2P_BLOCKING_DISABLE) switch/asic (1/0
(IST 6423 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=L2_AUTH(1 13:13:16.015 05/09/14]
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=Unassoc(0) src_int
0x506c800000000f dst_int 0x0 ackflag 0 reassoc_client 0 llm_notif 0 ip 0.0.0.0
ip_learn_type 0
IST 6424 8151] 0017.7c2f.b69a WCDB_CHANGE: In L2 auth 13:13:16.015 05/09/14]
but l2ack waiting lfag not set,so set
IST 6425 8151] 0017.7c2f.b69a Not Using WMM Compliance code 13:13:16.015 05/09/14]
qosCap 00
(IST 6426 8151] 0017.7c2f.b69a **Change state to DHCP_REQD (7** 13:13:16.016 05/09/14]
(last state L2AUTHCOMPLETE (4

IST 6434 8151] 0017.7c2f.b69a Sending Assoc Response to 13:13:16.016 05/09/14]
station on BSSID c8f9.f983.4260 (status 0) ApVapId 15 Slot 0
IST 6435 8151] 0017.7c2f.b69a apfProcessRadiusAssocResp 13:13:16.016 05/09/14]
apf_80211.c:2316) Changing state for mobile 0017.7c2f.b69a on AP)
c8f9.f983.4260 from Associated to Associated

IST 6436 8151] 0017.7c2f.b69a 1XA: Session Push for 13:13:16.016 05/09/14]
Non-dot1x wireless client
IST 6437 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr 13:13:16.016 05/09/14]
to Push wireless session for client 47ad4000000145 uid 280
IST 6438 8151] 0017.7c2f.b69a Session Push for 13:13:16.016 05/09/14]
wireless client

```
           IST 6439 8151] 0017.7c2f.b69a Session Manager Call 13:13:16.016 05/09/14]
       Client 47ad4000000145, uid 280, capwap id 506c800000000f,Flag 1 Audit-Session
                                    (ID 0a6987b2536c871300000118 policy name (null

                :IST 643a 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF 13:13:16.016 05/09/14]
                     0017.7c2f.b69a, Ca2] Session start request from Client[1] for]
                      :0017.7c2f.b69a (method: No method, method list: none, aaa id
                                                0x00000118) - session-push,  policy
                :IST 643b 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF 13:13:16.016 05/09/14]
                :0017.7c2f.b69a, Ca2]  - client iif_id: 47AD4000000145, session ID]
                                       0a6987b2536c871300000118 for 0017.7c2f.b69a
                     :IST 643c 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.016 05/09/14]
                     0017.7c2f.b69a, Ca2] Delay add/update sync of auth-domain for]
                                                0017.7c2f.b69a / 0xFE000110
            :IST 643d 243] ACCESS-CORE-SM-CLIENT-DOT11-ERR 13:13:16.017 05/09/14]
       0017.7c2f.b69a, Ca2] Invalid client authorization notification: NO method]
                     :IST 643e 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.017 05/09/14]
              0017.7c2f.b69a, Ca2] Delay add/update sync of dc-profile-name for]
                                                0017.7c2f.b69a / 0xFE000110
                     :IST 643f 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.017 05/09/14]
               0017.7c2f.b69a, Ca2] Delay add/update sync of dc-device-name for]
                                                0017.7c2f.b69a / 0xFE000110
                     :IST 6440 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.017 05/09/14]
                                    0017.7c2f.b69a, Ca2] Delay add/update sync of]
                                 dc-device-class-tag for 0017.7c2f.b69a / 0xFE000110
                     :IST 6441 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.017 05/09/14]
          0017.7c2f.b69a, Ca2] Delay add/update sync of dc-certainty-metric for]
                                                0017.7c2f.b69a / 0xFE000110
                     :IST 6442 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.017 05/09/14]
                       0017.7c2f.b69a, Ca2] Delay add/update sync of dc-opaque for]
                                                0017.7c2f.b69a / 0xFE000110
                     :IST 6443 243] ACCESS-CORE-SM-SYNC-NOTF 13:13:16.017 05/09/14]
                0017.7c2f.b69a, Ca2] Delay add/update sync of dc-protocol-map for]
                                                0017.7c2f.b69a / 0xFE000110
(IST 6444 22] [WCDB] wcdb_ffcp_add_cb: client (0017.7c2f.b69a 13:13:16.017 05/09/14]
                   (client (0x47ad4000000145): FFCP operation (CREATE) return code (0
     :IST 6445 22] [WCDB] wcdb_send_add_notify_callback_event 13:13:16.017 05/09/14]
                                          Notifying other features about client add
           :IST 6446 22] [WCDB] wcdb_sisf_client_add_notify 13:13:16.017 05/09/14]
                Notifying SISF of DEASSOC to DOWN any old entry for 0017.7c2f.b69a
           :IST 6447 22] [WCDB] wcdb_sisf_client_add_notify 13:13:16.017 05/09/14]
                                  Notifying SISF of new Association for 0017.7c2f.b69a
  IST 6448 8151] 0017.7c2f.b69a WCDB SPI response msg handler 13:13:16.017 05/09/14]
                                                   client code 0 mob state 0
  IST 6449 8151] 0017.7c2f.b69a WcdbClientUpdate: L2 Auth ACK 13:13:16.017 05/09/14]
                                                                  from WCDB
   IST 644a 8151] 0017.7c2f.b69a WCDB_L2ACK: wcdbAckRecvdFlag 13:13:16.017 05/09/14]
                                                                    updated
  IST 644b 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 13:13:16.017 05/09/14]
   IST 644c 8151] 0017.7c2f.b69a WCDB_CHANGE: Suppressing SPI 13:13:16.017 05/09/14]
          Mobility state not known) pemstate 7 state LEARN_IP(2) vlan 12 client_id)
                                  0x47ad4000000145 mob=Unassoc(0) ackflag 2 dropd 1
                :IST 644d 8151] 0017.7c2f.b69a Local Policy 13:13:18.796 05/09/14]
 apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from apfMsSumOverride
   IST 644e 8151] 0017.7c2f.b69a Applying post-handoff policy 13:13:18.802 05/09/14]
                                    for station  0017.7c2f.b69a  - valid mask 0x0

    ,IST 644f 8151] 0017.7c2f.b69a     QOS Level: -1, DSCP: -1 13:13:18.802 05/09/14]
         dot1p: -1, Data Avg: -1, realtime Avg: -1, Data Burst -1, Realtime Burst -1
                                                                    --More--

               ,IST 6450 8151] 0017.7c2f.b69a     Session: -1 13:13:18.802 05/09/14]
                                                   User session: -1, User elapsed -1
                                 Interface: N/A ACL: N/A Qos Pol Down   Qos Pol Up
```

```
IST 6451 8151] 0017.7c2f.b69a Local Policy: At the start of 13:13:18.802 05/09/14]
                                        apfApplyOverride2. Client State DHCP_REQD

IST 6452 8151] 0017.7c2f.b69a Applying new AAA override for 13:13:18.802 05/09/14]
                                                    station  0017.7c2f.b69a
IST 6453 8151] 0017.7c2f.b69a Local Policy: Applying new AAA 13:13:18.802 05/09/14]
                                                      override for station
 ,IST 6454 8151] 0017.7c2f.b69a Override Values: source: 16 13:13:18.802 05/09/14]
         ,valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff
                                                      sessionTimeout: -1
    ,IST 6455 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1 13:13:18.802 05/09/14]
                            :dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName
       IST 6456 8151] 0017.7c2f.b69a Local Policy: Applying 13:13:18.802 05/09/14]
                                                        override policy
      IST 6457 8151] 0017.7c2f.b69a Clearing Dhcp state for 13:13:18.802 05/09/14]
                                                             ---  station
IST 6458 8151] 0017.7c2f.b69a Local Policy: Before Applying 13:13:18.802 05/09/14]
  WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and apfMsTimeout is 1800

IST 6459 8151] 0017.7c2f.b69a Local Policy:Setting Interface 13:13:18.802 05/09/14]
                                                        name e VLAN0012

   IST 645a 8151] 0017.7c2f.b69a Local Policy:Setting local 13:13:18.802 05/09/14]
                                     bridging VLAN  name VLAN0012 and VLAN ID  12

   IST 645b 8151] 0017.7c2f.b69a Applying WLAN ACL policies 13:13:18.802 05/09/14]
                                                          to client
    IST 645c 8151] 0017.7c2f.b69a No Interface ACL used for 13:13:18.802 05/09/14]
                                              (Wireless client in WCM(NGWC
         :IST 645d 8151] 0017.7c2f.b69a apfApplyWlanPolicy 13:13:18.802 05/09/14]
                        Retaining the ACL recieved in AAA attributes 255 on mobile
         IST 645e 8151] 0017.7c2f.b69a Local Policy: After 13:13:18.802 05/09/14]
             Applying WLAN policy AccessVLAN = 12 and SessionTimeout  is 1800 and
                                                        apfMsTimeout is 1800

 IST 645f 8151] 0017.7c2f.b69a Local Policy: After Applying 13:13:18.802 05/09/14]
            Site Override  policy AccessVLAN = 12 and SessionTimeout  is 1800 and
                                                        apfMsTimeout is 1800

IST 6460 8151] 0017.7c2f.b69a Inserting AAA Override struct 13:13:18.802 05/09/14]
                                     for mobile MAC:  0017.7c2f.b69a , source 16

IST 6461 8151] 0017.7c2f.b69a Inserting new RADIUS override 13:13:18.802 05/09/14]
                                          into chain for station  0017.7c2f.b69a
 ,IST 6462 8151] 0017.7c2f.b69a Override Values: source: 16 13:13:18.802 05/09/14]
         ,valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff
                                                      sessionTimeout: -1
    ,IST 6463 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1 13:13:18.802 05/09/14]
                            :dataBurstC: -1 rTimeBurstC: -1, vlanIfName: , aclName
      IST 6464 8151] 0017.7c2f.b69a Local Policy: After ovr 13:13:18.802 05/09/14]
                                                      check continuation
              :IST 6465 8151] 0017.7c2f.b69a Local Policy 13:13:18.802 05/09/14]
              apf_ms_radius_override.c apfMsSumOverride 447  Returning fail from
                                                        apfMsSumOverride
        IST 6466 8151] 0017.7c2f.b69a Local Policy: Calling 13:13:18.802 05/09/14]
                                    applyLocalProfilingPolicyAction from Override2

                              IST 6467 8151] 0017.7c2f.b69a 13:13:18.802 05/09/14]
                                 **** Inside applyLocalProfilingPolicyAction ****

           = IST 6468 8151] 0017.7c2f.b69a *** Client State 13:13:18.802 05/09/14]
                     ,DHCP_REQD instance = 2 instance Name POLICY_PROFILING_L2_AUTH
             ,OverrideEnable = 1 deviceTypeLen=0, deviceType=(null), userRoleLen=0
```

(userRole=(null

: IST 6469 8151] 0017.7c2f.b69a Local Profiling Values 13:13:18.802 05/09/14]
,isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0
sessionTimeout=0, isSessionTORecdInDelete = 0 ProtocolMap = 0 ,applyPolicyAtRun= 0
,[] = IST 646a 8151] 0017.7c2f.b69a ipv4ACL 13:13:18.802 05/09/14]
[ipv6ACL = [], inQoS = [unknown], outQoS = [unknown
IST 646b 8151] 0017.7c2f.b69a Local Policy: At the End 13:13:18.802 05/09/14]
AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

IST 646c 8151] 0017.7c2f.b69a apfMsRunStateInc 13:13:18.802 05/09/14]
IST 646d 8151] 0017.7c2f.b69a Session Update for Non-dot1x client 13:13:18.802 05/09/14]

IST 646e 8151] 0017.7c2f.b69a 1XA: Session Push for Non-dot1x 13:13:18.802 05/09/14]
wireless client
IST 646f 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr to Push 13:13:18.802 05/09/14]
wireless session for client 47ad4000000145 uid 280
--More--
IST 6470 8151] 0017.7c2f.b69a Session Update for Pushed Sessions 13:13:18.802 05/09/14]

IST 6471 8151] 0017.7c2f.b69a Session Manager Call Client 13:13:18.802 05/09/14]
47ad4000000145, uid 280, capwap id 506c800000000f,Flag 0 Audit-Session ID
(0a6987b2536c871300000118 policy name (null

IST 6472 8151] 0017.7c2f.b69a Change state to RUN (20) last 13:13:18.802 05/09/14]
(state DHCP_REQD (7

IST 6473 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 13:13:18.802 05/09/14]
IST 6474 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 curr 13:13:18.802 05/09/14]
Mob State 3 llReq flag 1
IST 6475 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 0 13:13:18.802 05/09/14]
currMob State 3 afd action 1
IST 6476 8151] 0017.7c2f.b69a WCDB_LLM: pl handle 259 vlan_id 13:13:18.802 05/09/14]
auth RUN(4) mobility 3 client_id 0x47ad4000000145 src_interface 0x506c800000000f 12
dst_interface 0x75e18000000143 client_type 0 p2p_type 1 bssid c8f9.f983.4260 radio_id
wgbid 0000.0000.0000 0
IST 6477 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 13:13:18.802 05/09/14]
radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f 12
dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 1 ip 0.0.0.0
ip_learn_type 0
:IST 6478 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF 13:13:18.802 05/09/14]
,0017.7c2f.b69a, Ca2] Session update from Client[1] for 0017.7c2f.b69a]
ID list 0x00000000, policy
IST 6479 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 13:13:18.802 05/09/14]
IST 647a 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 13:13:18.802 05/09/14]
curr Mob State 3 llReq flag 0
(IST 647b 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4 13:13:18.802 05/09/14]
vlan 12 radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int
0x506c800000000f dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0
ip 0.0.0.0 ip_learn_type 0
IST 647c 8151] 0017.7c2f.b69a AAAS: creating accounting start 13:13:18.802 05/09/14]
record using method list Zubair_ISE, passthroughMode 1
IST 647d 8151] 0017.7c2f.b69a AAAS: initialised accounting 13:13:18.802 05/09/14]
start request, uid=280 passthrough=1
IST 647e 8151] 0017.7c2f.b69a AAAS: accounting request sent 13:13:18.802 05/09/14]
(IST 647f 207] [WCDB] ==Update event: client (0017.7c2f.b69a 13:13:18.803 05/09/14]
client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state
<L2_AUTH_DONE->RUN) mob_st<truncated)
IST 6480 207] [WCDB] ===intf src/dst 13:13:18.803 05/09/14]
(0x506c800000000f->0x506c800000000f)/(0x0->0x75e18000000143)
radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (true) addr v4/v6
<truncated>)
IST 6481 207] [WCDB] Foreign client add. Final llm 13:13:18.803 05/09/14]
notified = false

:IST 6482 207] [WCDB] wcdb_client_mcast_update_notify 13:13:18.803 05/09/14]
No mcast action reqd
IST 6483 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify 13:13:18.803 05/09/14]
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
:IST 6484 207] [WCDB] wcdb_client_state_change_notify 13:13:18.803 05/09/14]
update flags = 0x3
IST 6485 8151] 0017.7c2f.b69a aaa attribute list length is 79 13:13:18.803 05/09/14]
[IST 6486 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF: [0017.7c2f.b69a 13:13:18.803 05/09/14]
WCDB RUN notification for 0017.7c2f.b69a
IST 6487 8151] 0017.7c2f.b69a Sending SPI 13:13:18.803 05/09/14]
spi_epm_epm_session_create successfull
IST 6488 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 13:13:18.803 05/09/14]
!!! mmRole ExpForeign
IST 6489 8151] 0017.7c2f.b69a 0.0.0.0, auth_state 20 mmRole 13:13:18.803 05/09/14]
ExpForeign, updating wcdb not needed
IST 648a 8151] 0017.7c2f.b69a Tclas Plumb needed: 0 13:13:18.803 05/09/14]
:IST 648b 207] [WCDB] wcdb_sisf_client_update_notify 13:13:18.803 05/09/14]
Notifying SISF to remove assoc in Foreign
(IST 648c 207] [WCDB] ==Update event: client (0017.7c2f.b69a 13:13:18.803 05/09/14]
(client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN
<mob_st<truncated
IST 648d 207] [WCDB] ===intf src/dst 13:13:18.803 05/09/14]
(0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143)
(radio/bssid (0->0)/(c8f9.f983.4260->c8f9.f983.4260) llm_notify (false
<addr v4/v6 (<truncated
:IST 648e 207] [WCDB] wcdb_client_mcast_update_notify 13:13:18.803 05/09/14]
No mcast action reqd
IST 648f 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify 13:13:18.803 05/09/14]
client (0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0
:IST 6490 207] [WCDB] wcdb_client_state_change_notify 13:13:18.803 05/09/14]
update flags = 0x2
:IST 6491 207] ACCESS-CORE-SM-CLIENT-DOT11-NOTF 13:13:18.803 05/09/14]
0017.7c2f.b69a] WCDB RUN notification for 0017.7c2f.b69a]
:IST 6492 207] [WCDB] wcdb_sisf_client_update_notify 13:13:18.803 05/09/14]
Notifying SISF to remove assoc in Foreign
(IST 6493 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a 13:13:18.803 05/09/14]
(client (0x47ad4000000145): FFCP operation (UPDATE) return code (0
(IST 6494 386] [WCDB] wcdb_ffcp_cb: client (0017.7c2f.b69a 13:13:18.803 05/09/14]
(client (0x47ad4000000145): FFCP operation (UPDATE) return code (0
[IST 6495 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2 13:13:18.803 05/09/14]
Delay add/update sync of iif-id for 0017.7c2f.b69a / 0xFE000110
[IST 6496 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2 13:13:18.803 05/09/14]
Delay add/update sync of audit-session-id for 0017.7c2f.b69a / 0xFE000110
IST 6497 8151] 0017.7c2f.b69a Received session_create_response 13:13:18.803 05/09/14]
for client handle 20175213735969093
IST 6498 8151] 0017.7c2f.b69a Received session_create_response 13:13:18.803 05/09/14]
with EPM session handle 4261413136
IST 6499 8151] 0017.7c2f.b69a Splash Page redirect client 13:13:18.803 05/09/14]
or posture client
--More--
IST 649a 8151] 0017.7c2f.b69a REDIRECT ACL present in the 13:13:18.803 05/09/14]
attribute list
IST 649b 8151] 0017.7c2f.b69a Setting AAA Override 13:13:18.803 05/09/14]
'Url-Redirect-Acl 'REDIRECT
IST 649c 8151] 0017.7c2f.b69a AAA Override Url-Redirect-Acl 13:13:18.803 05/09/14]
'REDIRECT'
IST 649d 8151] 0017.7c2f.b69a AAA Override Url-Redirect 13:13:18.803 05/09/14]
'https://10.106.73.69:8443/guestportal/gateway?sessionId=0a6987b2536c871300000118&action=cwa'
set
IST 649e 8151] 0017.7c2f.b69a Wireless Client mobility role 13:13:18.803 05/09/14]
is not ExportAnchor/Local. Hence we are not sending request to EPM
IST 649f 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 0.0.0.0 13:13:20.445 05/09/14]
ip_learn_type 0 deleted ipv4 0.0.0.0
:IST 64a0 207] [WCDB] wcdb_foreign_client_ip_addr_update 13:13:20.446 05/09/14]

.Foreign client (0017.7c2f.b69a) ip addr update received
: [IST 64a1 207] [WCDB] SISF Update: IPV6 Addr[0 13:13:20.446 05/09/14]
fe80::6c1a:b253:d711:c7f
IST 64a2 207] [WCDB] SISF Update : Binding delete status 13:13:20.446 05/09/14]
for V6: = 0
:IST 64a3 207] [WCDB] wcdb_sisf_client_update_notify 13:13:20.446 05/09/14]
Notifying SISF to remove assoc in Foreign
,IST 64a4 8151] 0017.7c2f.b69a MS got the IP 13:13:20.448 05/09/14]
resetting the Reassociation Count 0 for client
IST 64a5 8151] 0017.7c2f.b69a AAAS: creating accounting interim 13:13:20.448 05/09/14]
record using method list Zubair_ISE, passthroughMode 1
IST 64a6 8151] 0017.7c2f.b69a AAAS: initialised accounting 13:13:20.449 05/09/14]
interim request, uid=280 passthrough=1
IST 64a7 8151] 0017.7c2f.b69a AAAS: accounting request sent 13:13:20.449 05/09/14]
IST 64a8 8151] 0017.7c2f.b69a Guest User() assigned IP Address 13:13:20.449 05/09/14]
(10.105.135.190)
IST 64a9 8151] 0017.7c2f.b69a Assigning Address 10.105.135.190 13:13:20.449 05/09/14]
to mobile
IST 64aa 8151] 0017.7c2f.b69a WCDB_IP_UPDATE: new ipv4 13:13:20.449 05/09/14]
ip_learn_type DHCP deleted ipv4 0.0.0.0 10.105.135.190
IST 64ab 8151] 0017.7c2f.b69a AAAS: creating accounting 13:13:20.449 05/09/14]
interim record using method list Zubair_ISE, passthroughMode 1
IST 64ac 8151] 0017.7c2f.b69a AAAS: initialised accounting 13:13:20.449 05/09/14]
interim request, uid=280 **passthrough=1**
IST 64ad 8151] 0017.7c2f.b69a AAAS: accounting request sent 13:13:20.449 05/09/14]
IST 64ae 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20 13:13:20.449 05/09/14]
!!! mmRole ExpForeign
IST 64af 207] [WCDB] wcdb_foreign_client_ip_addr_update: Foreign 13:13:20.449 05/09/14]
.client (0017.7c2f.b69a) ip addr update received
IST 64b0 8151] 0017.7c2f.b69a 10.105.135.190, auth_state 20 13:13:20.449 05/09/14]
mmRole ExpForeign, updating wcdb not needed
IST 64b1 8151] 0017.7c2f.b69a Tclas Plumb needed: 0 13:13:20.449 05/09/14]
: [IST 64b2 207] [WCDB] SISF Update: IPV6 Addr[0 13:13:20.449 05/09/14]
fe80::6c1a:b253:d711:c7f
IST 64b3 207] [WCDB] SISF Update : Binding delete status for V6: = 0 13:13:20.449 05/09/14]
IST 64b4 207] [WCDB] wcdb_sisf_client_update_notify: Notifying SISF 13:13:20.449 05/09/14]
to remove assoc in Foreign
IST 64b5 243] ACCESS-CORE-SM-SYNC-NOTF: [0017.7c2f.b69a, Ca2] Delay 13:13:20.449 05/09/14]
add/update sync of addr for 0017.7c2f.b69a / 0xFE000110
[IST 64b6 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2 13:13:49.429 05/09/14]
[Session authz update requested cmd 5, mac 0017.7c2f.b69a, attr-list 0x0 for Client[1
[IST 64b7 253] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2 13:13:49.430 05/09/14]
[Session authz update request sent to Client[1
IST 64b8 8151] 0017.7c2f.b69a 1XA: Processing update request from 13:13:49.430 05/09/14]
dot1x. COA type 5
,IST 64b9 8151] 0017.7c2f.b69a AAAS: authorization init, uid=280 13:13:49.430 05/09/14]
context=268
,IST 64ba 8151] 0017.7c2f.b69a AAAS: initialised auth request 13:13:49.430 05/09/14]
uinque id=280, context id = 268, context reqHandle 0xfefc172c
IST 64bb 8151] 0017.7c2f.b69a AAAS: Submitting mac filter request 13:13:49.430 05/09/14]
for user 00177c2fb69a, uniqueId=280 mlist=MACFILTER
IST 64bc 8151] 0017.7c2f.b69a AAAS: auth request sent 13:13:49.430 05/09/14]
IST 64bd 8151] 0017.7c2f.b69a processing COA type 5 13:13:49.430 05/09/14]
was successful
IST 64be 8151] 0017.7c2f.b69a processing COA type 5 13:13:49.430 05/09/14]
was successful
[IST 64bf 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca2 13:13:49.430 05/09/14]
[Session authz update response received for Client[1
IST 64c0 211] Parsed CLID MAC Address = 0:23:124:47:182:154 13:13:49.430 05/09/14]
IST 64c1 211] AAA SRV(00000118): process author req 13:13:49.430 05/09/14]
IST 64c2 211] AAA SRV(00000118): **Author method=SERVER_GROUP** 13:13:49.430 05/09/14]
Zubair_ISE
IST 64c3 211] Parsed CLID MAC Address = 0:23:124:47:182:154 13:13:49.430 05/09/14]
IST 64c4 211] AAA SRV(00000000): process response req 13:13:49.430 05/09/14]

IST 64c5 220] **AAA SRV(00000118): protocol reply PASS for** 13:13:49.469 05/09/14]
Authorization
IST 64c6 220] **AAA SRV(00000118): Return Authorization status=PASS** 13:13:49.469 05/09/14]
IST 64c7 8151] 0017.7c2f.b69a AAAS: received response, cid=268 13:13:49.469 05/09/14]
IST 64c8 8151] 0017.7c2f.b69a AAAS: deleting context, cid=268 13:13:49.469 05/09/14]
IST 64c9 8151] 0017.7c2f.b69a Not comparing because the ACLs 13:13:49.469 05/09/14]
.have not been sent yet
,IST 64ca 8151] 0017.7c2f.b69a Final flag values are 13:13:49.469 05/09/14]
epmSendAcl 1, epmSendAclDone 0
IST 64cb 8151] 0017.7c2f.b69a 13:13:49.469 05/09/14]
client incoming attribute size are 77
--More--
IST 64cc 8151] 0017.7c2f.b69a AAAS: mac filter callback status=0 13:13:49.469 05/09/14]
uniqueId=280
IST 64cd 8151] 0017.7c2f.b69a Local Policy: At the start of 13:13:49.469 05/09/14]
apfApplyOverride2. Client State RUN

IST 64ce 8151] 0017.7c2f.b69a Applying new AAA override for 13:13:49.469 05/09/14]
station 0017.7c2f.b69a
IST 64cf 8151] 0017.7c2f.b69a Local Policy: Applying new AAA 13:13:49.469 05/09/14]
override for station
,IST 64d0 8151] 0017.7c2f.b69a Override Values: source: 2 13:13:49.469 05/09/14]
valid_bits: 0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
:IST 64d1 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC 13:13:49.469 05/09/14]
:rTimeBurstC: -1, vlanIfName: , aclName -1
IST 64d2 8151] 0017.7c2f.b69a Local Policy: Applying override policy 13:13:49.469 05/09/14]
--- IST 64d3 8151] 0017.7c2f.b69a Clearing Dhcp state for station 13:13:49.469 05/09/14]
IST 64d4 8151] 0017.7c2f.b69a Local Policy: Before Applying WLAN 13:13:49.469 05/09/14]
policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

IST 64d5 8151] 0017.7c2f.b69a Local Policy:Setting Interface name 13:13:49.469 05/09/14]
e VLAN0012

IST 64d6 8151] 0017.7c2f.b69a Local Policy:Setting local bridging 13:13:49.469 05/09/14]
VLAN name VLAN0012 and VLAN ID 12

IST 64d7 8151] 0017.7c2f.b69a Applying WLAN ACL policies to client 13:13:49.469 05/09/14]
IST 64d8 8151] 0017.7c2f.b69a No Interface ACL used for Wireless 13:13:49.469 05/09/14]
(client in WCM(NGWC
IST 64d9 8151] 0017.7c2f.b69a apfApplyWlanPolicy: Retaining the 13:13:49.469 05/09/14]
ACL recieved in AAA attributes 255 on mobile
IST 64da 8151] 0017.7c2f.b69a Local Policy: After Applying WLAN 13:13:49.469 05/09/14]
policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

IST 64db 8151] 0017.7c2f.b69a Local Policy: After Applying Site 13:13:49.469 05/09/14]
Override policy AccessVLAN = 12 and SessionTimeout is 1800 and apfMsTimeout is 1800

IST 64dc 8151] 0017.7c2f.b69a Inserting AAA Override struct for mobile 13:13:49.469 05/09/14]
MAC: 0017.7c2f.b69a , source 2

IST 64dd 8151] 0017.7c2f.b69a Inserting new RADIUS override into 13:13:49.469 05/09/14]
chain for station 0017.7c2f.b69a
:IST 64de 8151] 0017.7c2f.b69a Override Values: source: 2, valid_bits 13:13:49.469 05/09/14]
0x0000, qosLevel: -1 dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
:IST 64df 8151] 0017.7c2f.b69a dataAvgC: -1, rTAvgC: -1, dataBurstC 13:13:49.469 05/09/14]
:rTimeBurstC: -1, vlanIfName: , aclName -1
IST 64e0 8151] 0017.7c2f.b69a Local Policy: After ovr check 13:13:49.469 05/09/14]
continuation
IST 64e1 8151] 0017.7c2f.b69a Local Policy: apf_ms_radius_override.c 13:13:49.469 05/09/14]
apfMsSumOverride 447 Returning fail from apfMsSumOverride
IST 64e2 8151] 0017.7c2f.b69a Local Policy: Calling 13:13:49.469 05/09/14]
applyLocalProfilingPolicyAction from Override2

IST 64e3 8151] 0017.7c2f.b69a 13:13:49.469 05/09/14]

```
                                                **** Inside applyLocalProfilingPolicyAction ****

    IST 64e4 8151] 0017.7c2f.b69a *** Client State = RUN instance = 2 13:13:49.469 05/09/14]
                 ,instance Name POLICY_PROFILING_L2_AUTH, OverrideEnable = 1 deviceTypeLen=0
                                          (deviceType=(null), userRoleLen=0, userRole=(null

           : IST 64e5 8151] 0017.7c2f.b69a     Local Profiling Values 13:13:49.469 05/09/14]
                ,isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0
        sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,applyPolicyAtRun= 0
                 ,[] = IST 64e6 8151] 0017.7c2f.b69a          ipv4ACL 13:13:49.469 05/09/14]
                                       [ipv6ACL = [], inQoS = [unknown], outQoS = [unknown
    IST 64e7 8151] 0017.7c2f.b69a Local Policy: At the End AccessVLAN 13:13:49.469 05/09/14]
                                  and SessionTimeout  is 1800 and apfMsTimeout is 1800 12 =

      IST 64e8 8151] 0017.7c2f.b69a In >= L2AUTH_COMPLETE for station 13:13:49.469 05/09/14]
                                                                                  0017.7c2f.b69a
      IST 64e9 8151] 0017.7c2f.b69a AAAS: creating accounting interim 13:13:49.469 05/09/14]
                                       record using method list Zubair_ISE, passthroughMode 1
   IST 64ea 8151] 0017.7c2f.b69a AAAS: initialised accounting interim 13:13:49.469 05/09/14]
                                                          request, uid=280 passthrough=1
         IST 64eb 8151] 0017.7c2f.b69a AAAS: accounting request sent 13:13:49.469 05/09/14]
IST 64ec 8151] 0017.7c2f.b69a Not Using WMM Compliance code qosCap 00 13:13:49.469 05/09/14]
     IST 64ed 8151] 0017.7c2f.b69a In SPI call for >= L2AUTH_COMPLETE 13:13:49.469 05/09/14]
                                                        for station  0017.7c2f.b69a
         IST 64ee 8151] 0017.7c2f.b69a WCDB_AUTH: Adding opt82 len 0 13:13:49.469 05/09/14]
    IST 64ef 8151] 0017.7c2f.b69a WCDB_LLM: prev Mob state 3 curr Mob 13:13:49.469 05/09/14]
                                                                  State 3 llReq flag 0
      IST 64f0 8151] 0017.7c2f.b69a WCDB_CHANGE: auth=RUN(4) vlan 12 13:13:49.469 05/09/14]
         radio 0 client_id 0x47ad4000000145 mobility=ExpForeign(3) src_int 0x506c800000000f
         dst_int 0x75e18000000143 ackflag 2 reassoc_client 0 llm_notif 0 ip  10.105.135.190
                                                                    ip_learn_type DHCP
                                                                          --More--
                      IST 64f1 8151] 0017.7c2f.b69a apfMsAssoStateInc 13:13:49.469 05/09/14]
      (IST 64f2 8151] 0017.7c2f.b69a apfPemAddUser2 (apf_policy.c:197 13:13:49.469 05/09/14]
       Changing state for mobile  0017.7c2f.b69a  on AP  c8f9.f983.4260  from AAA Pending to
                                                                          Associated

    IST 64f3 8151] 0017.7c2f.b69a Reason code 0, Preset 4, AAA cause 1 13:13:49.469 05/09/14]
 :IST 64f4 8151] 0017.7c2f.b69a Scheduling deletion of Mobile Station 13:13:49.469 05/09/14]
                                                        callerId: 49) in 1800 seconds)
                    ,IST 64f5 8151] 0017.7c2f.b69a Ms Timeout = 1800 13:13:49.469 05/09/14]
                                                                  Session Timeout = 1800

        (IST 64f6 207] [WCDB] ==Update event: client (0017.7c2f.b69a 13:13:49.469 05/09/14]
       (client id:(0x47ad4000000145) vlan (12->12) global_wlan (15->15) auth_state (RUN->RUN
                                                                    <mob_st<truncated
                               IST 64f7 207] [WCDB] ===intf src/dst 13:13:49.469 05/09/14]
       0x506c800000000f->0x506c800000000f)/(0x75e18000000143->0x75e18000000143) radio/bssid)
          <c8f9.f983.4260->c8f9.f983.4260) llm_notify (false) addr v4/v6 (<truncated)/(0<0-)
       IST 64f8 207] [WCDB] wcdb_client_mcast_update_notify: No mcast 13:13:49.469 05/09/14]
                                                                    action reqd
      IST 64f9 207] [WCDB] wcdb_ffcp_wcdb_client_update_notify client 13:13:49.469 05/09/14]
                             0017.7c2f.b69a) id 0x47ad4000000145 ffcp update with flags=0x0)
          IST 650a 8151] 0017.7c2f.b69a Acct-interim update sent for 13:15:47.411 05/09/14]
                                                                  station 0017.7c2f.b69a
                                       IST 650b 8151] 0017.7c2f.b69a 13:16:38.431 05/09/14]
       Client stats update: Time now in sec 1399621598, Last Acct Msg Sent at 1399621547 sec
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).