تكوين المصادقة المركزية للويب (CWA) على Catalyst 9800 WLC و ISE

المحتويات

[المقدمة](#)
[المتطلبات الأساسية](#)
  [المتطلبات](#)
  [المكونات المستخدمة](#)
[معلومات أساسية](#)
[التكوين](#)
  [الرسم التخطيطي للشبكة](#)
  [تكوين AAA على 9800 WLC](#)
  [تكوين شبكة WLAN](#)
  [تكوين ملف تعريف السياسة](#)
  [تكوين علامة السياسة](#)
  [تعيين علامة السياسة](#)
  [إعادة توجيه تكوين قائمة التحكم في الوصول (ACL)](#)
    [تمكين إعادة التوجيه ل HTTP أو HTTPS](#)
  [تكوين ISE](#)
    [إضافة 9800 WLC إلى محرك خدمات كشف الهوية (ISE)](#)
    [إنشاء مستخدم جديد على ISE](#)
    [إنشاء ملف تعريف التفويض](#)
    [تكوين قاعدة المصادقة](#)
    [تكوين قواعد المصادقة](#)
    [نقاط الوصول إلى المبدلات Flexconnect المحلية فقط](#)
    [الشهادات](#)
[التحقق من الصحة](#)
[استكشاف الأخطاء وإصلاحها](#)
  [قائمة التحقق](#)
  [دعم منفذ الخدمة ل RADIUS](#)
  [تجميع تصحيح الأخطاء](#)
  [الأمثلة](#)

المقدمة

يصف هذا وثيقة كيف أن يشكل CWA Wireless LAN على مادة حفازة 9800 WLC و ISE.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من 9800 السلكي lan جهاز تحكم (WLC) تشكيل.

المكونات المستخدمة

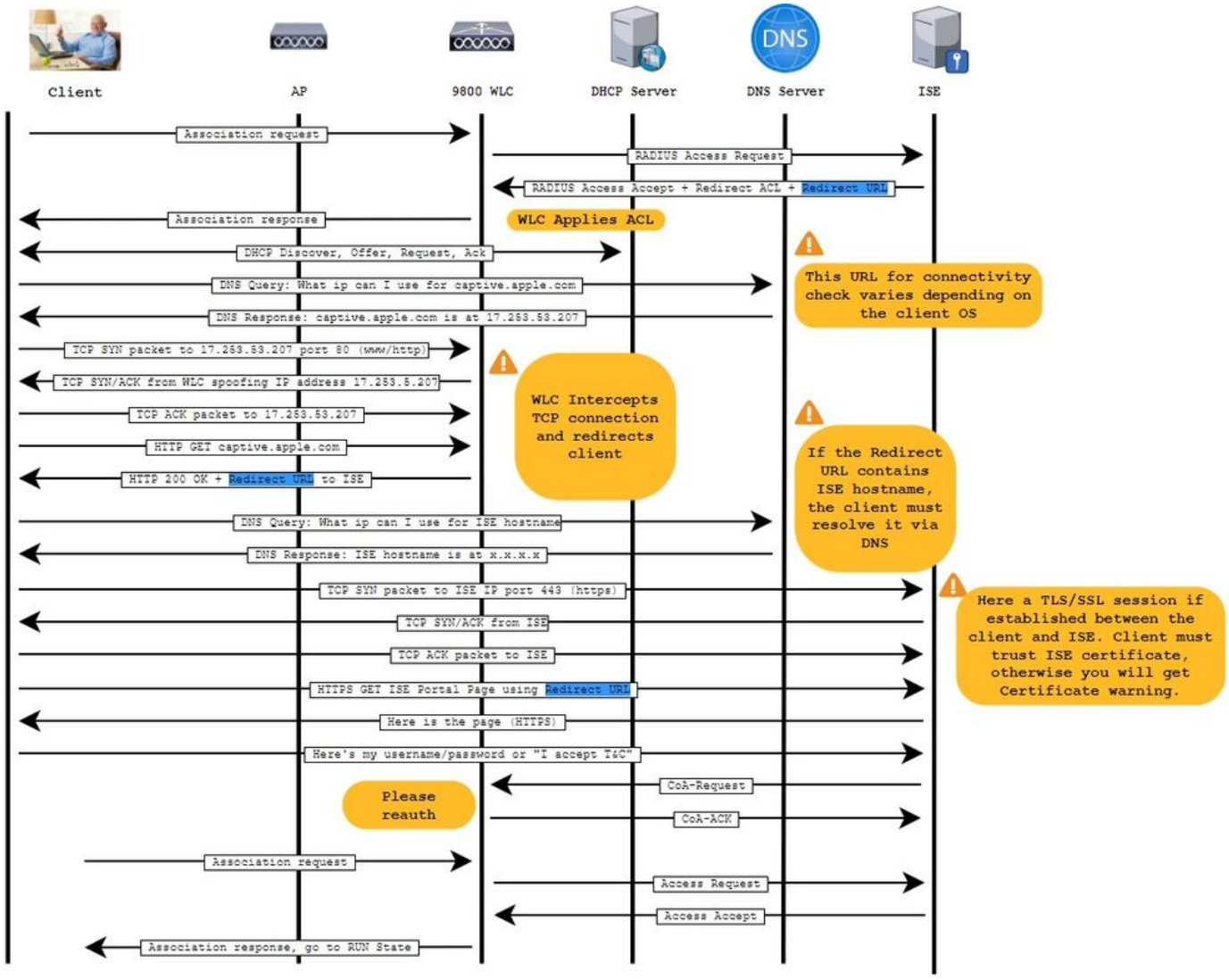
تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- 9800 WLC برنامج Cisco IOS® XE Gibraltar الإصدار 17.6.x
- Identity Service Engine (ISE) v3.0

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

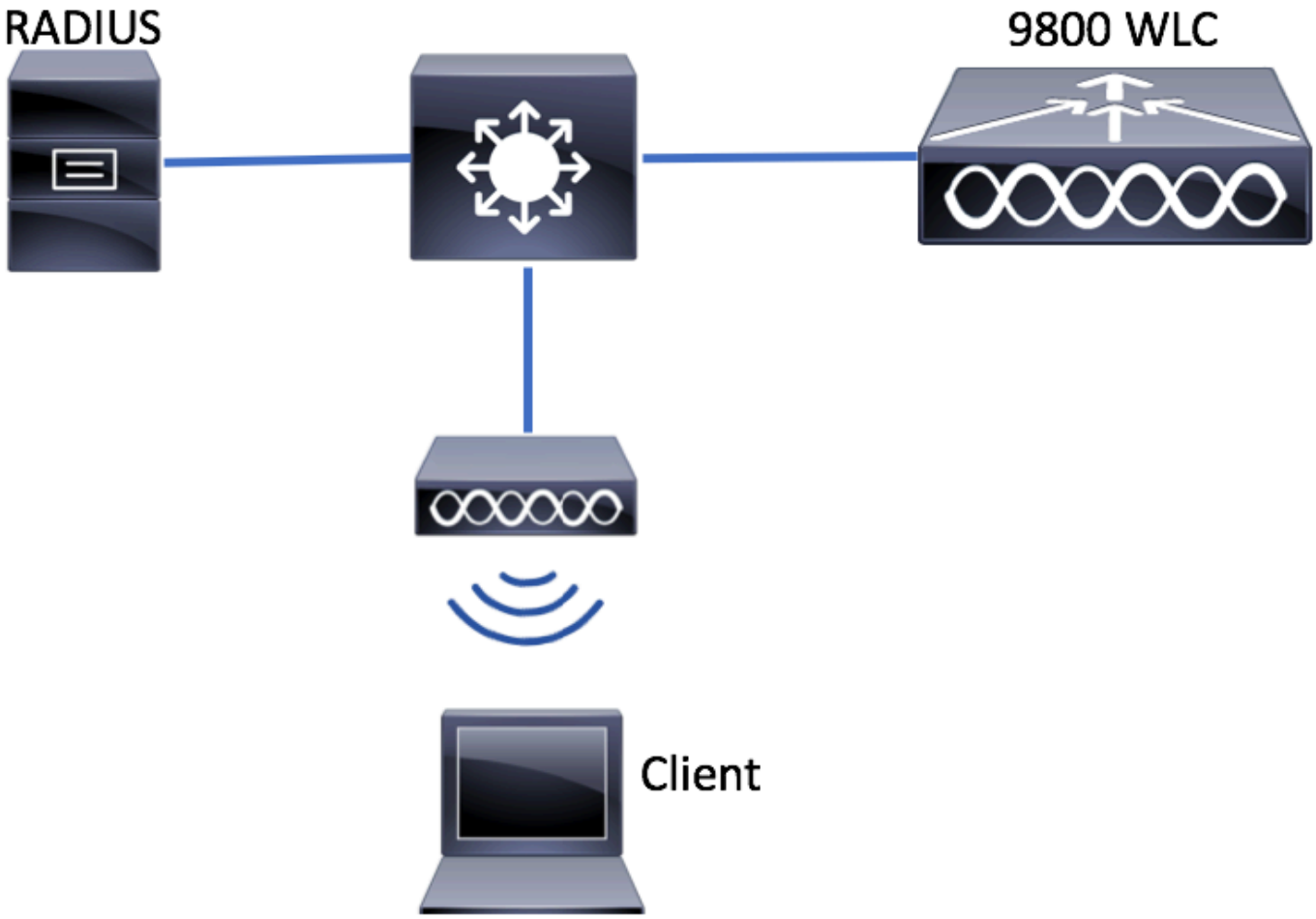
معلومات أساسية

يتم عرض عملية CWA هنا حيث يمكنك رؤية عملية CWA لجهاز Apple كمثال:



التكوين

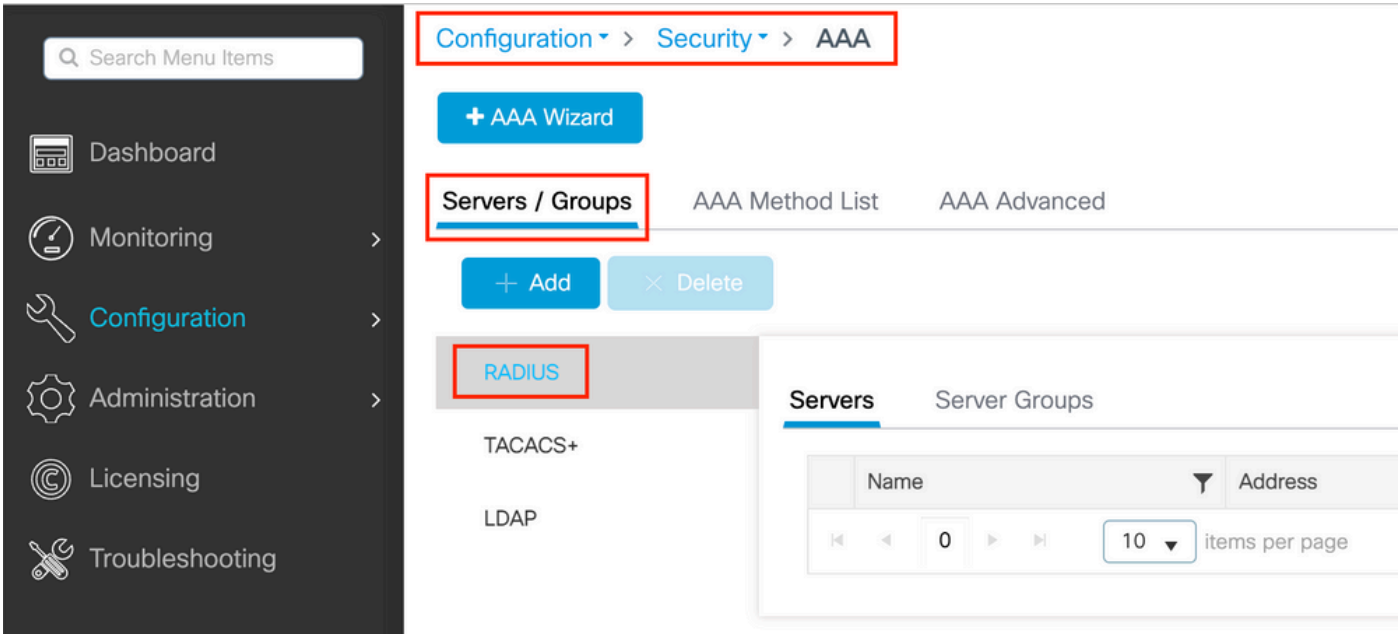
الرسم التخطيطي للشبكة



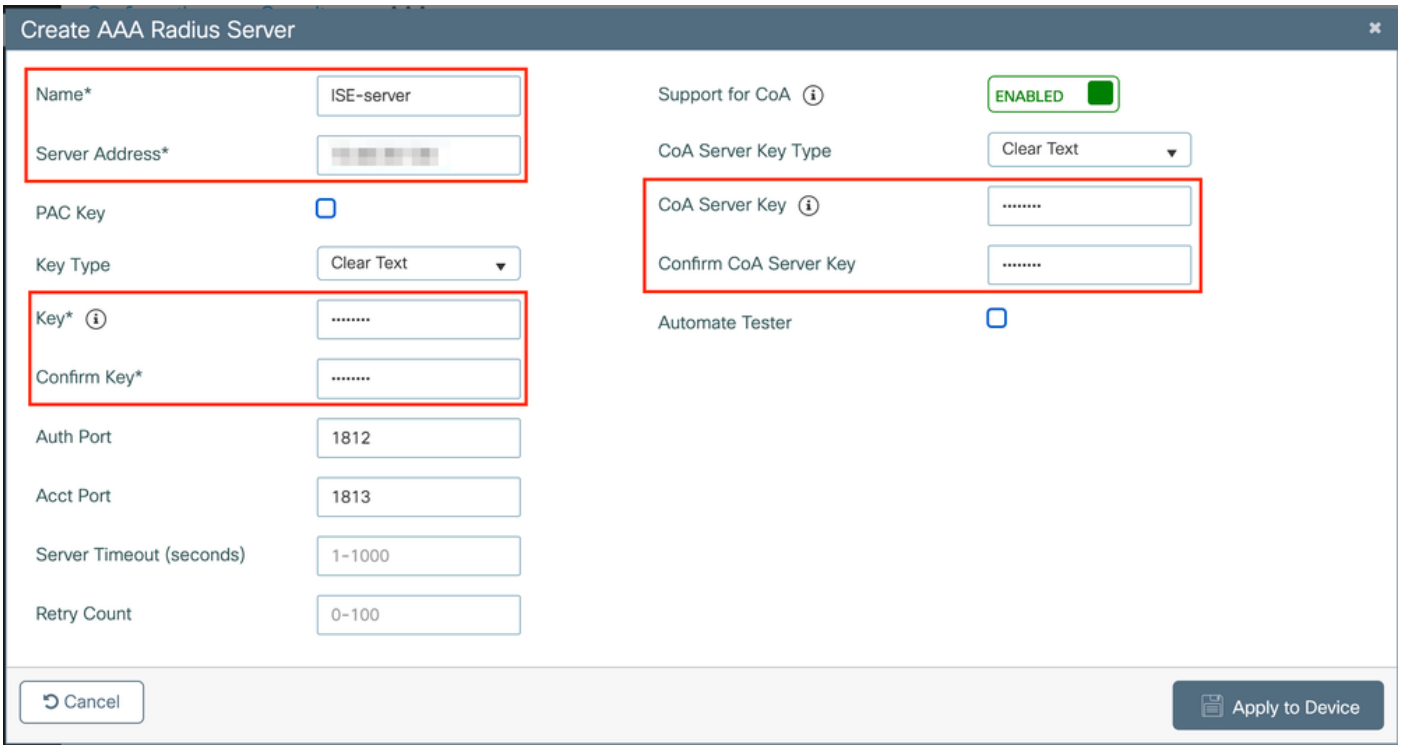
تكوين AAA على 9800 WLC

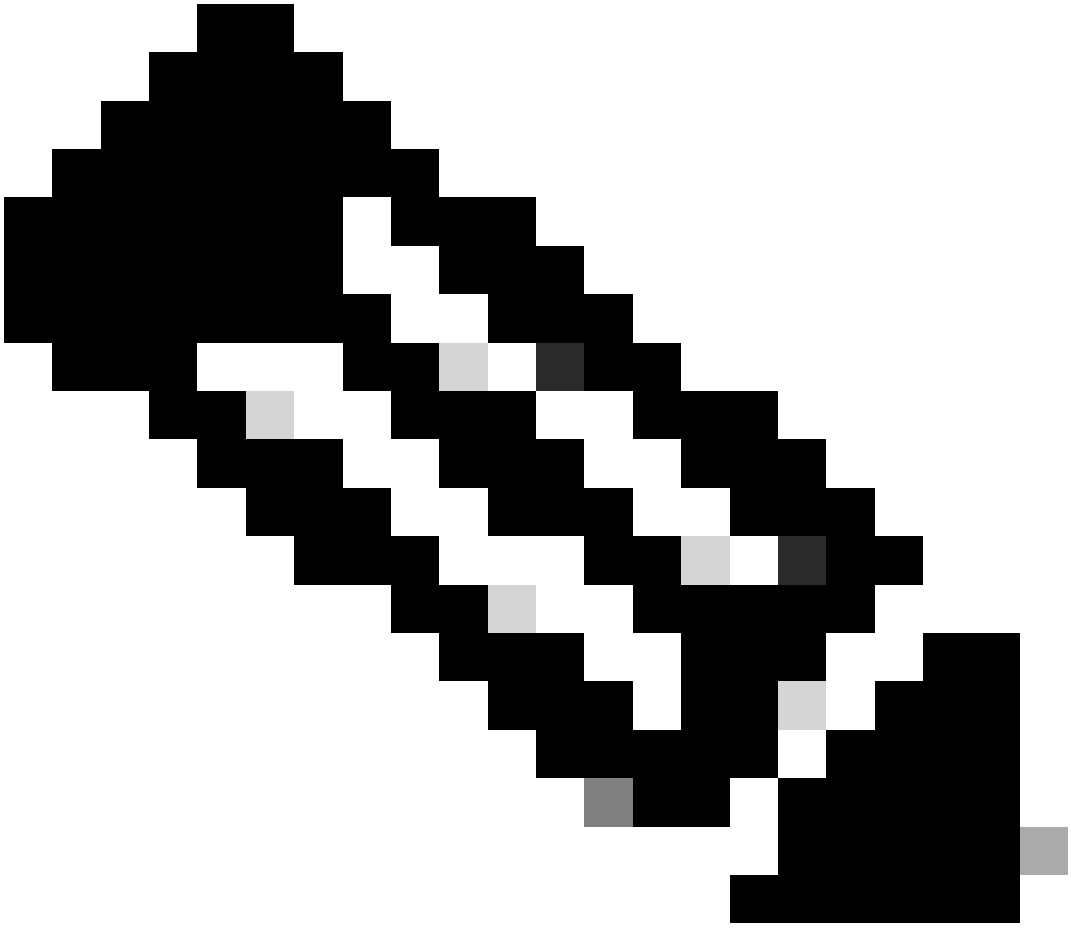
الخطوة 1. إضافة خادم ISE إلى تكوين 9800 WLC.

انتقل إلى Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add وأدخل معلومات خادم RADIUS كما هو موضح في الصور.



تأكد من تمكين دعم عملية تغيير التفويض(CoA) إذا كنت تخطط لاستخدام مصادقة الويب المركزية (أو أي نوع من أنواع الأمان يتطلب CoA) في المستقبل.

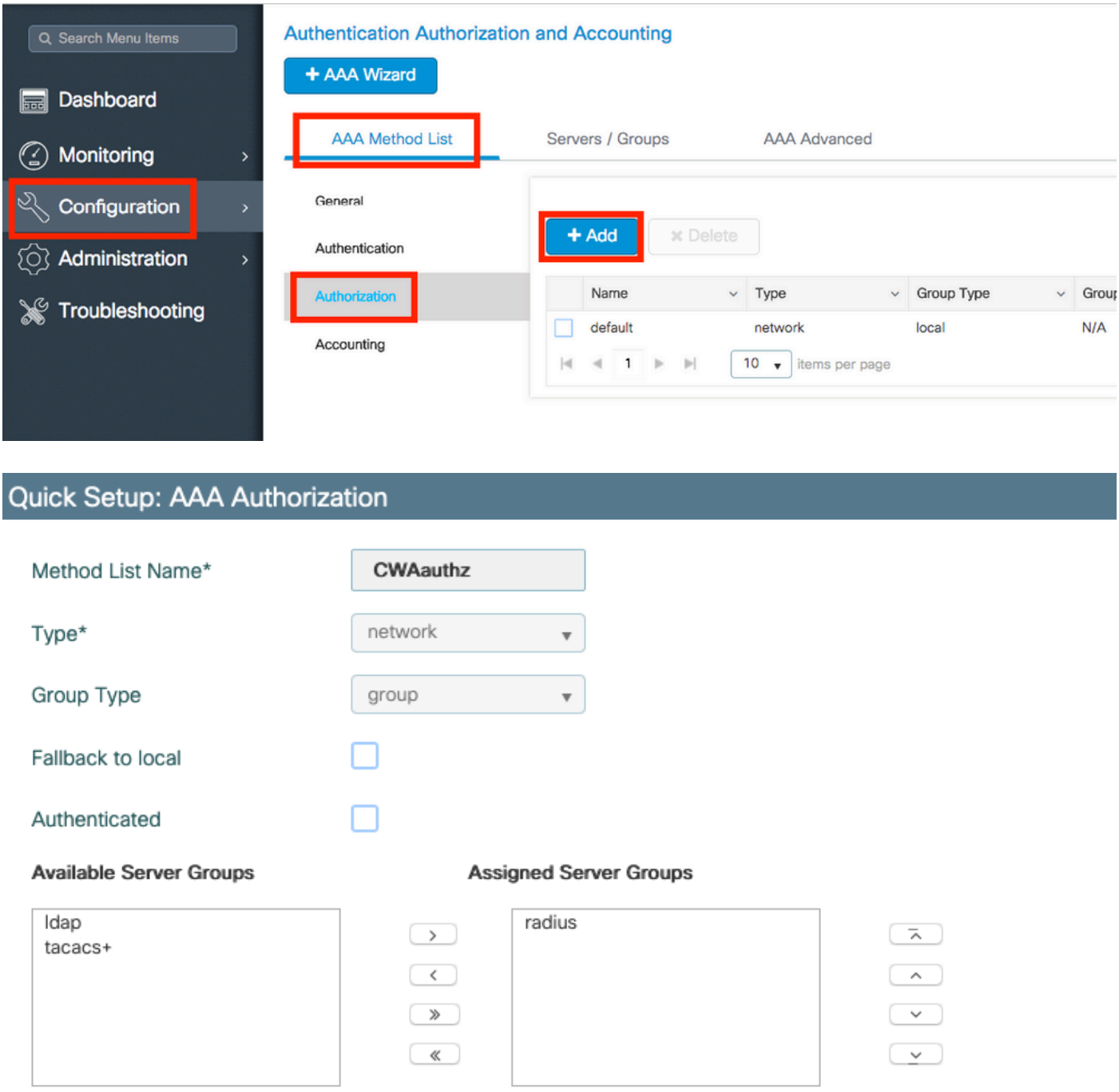




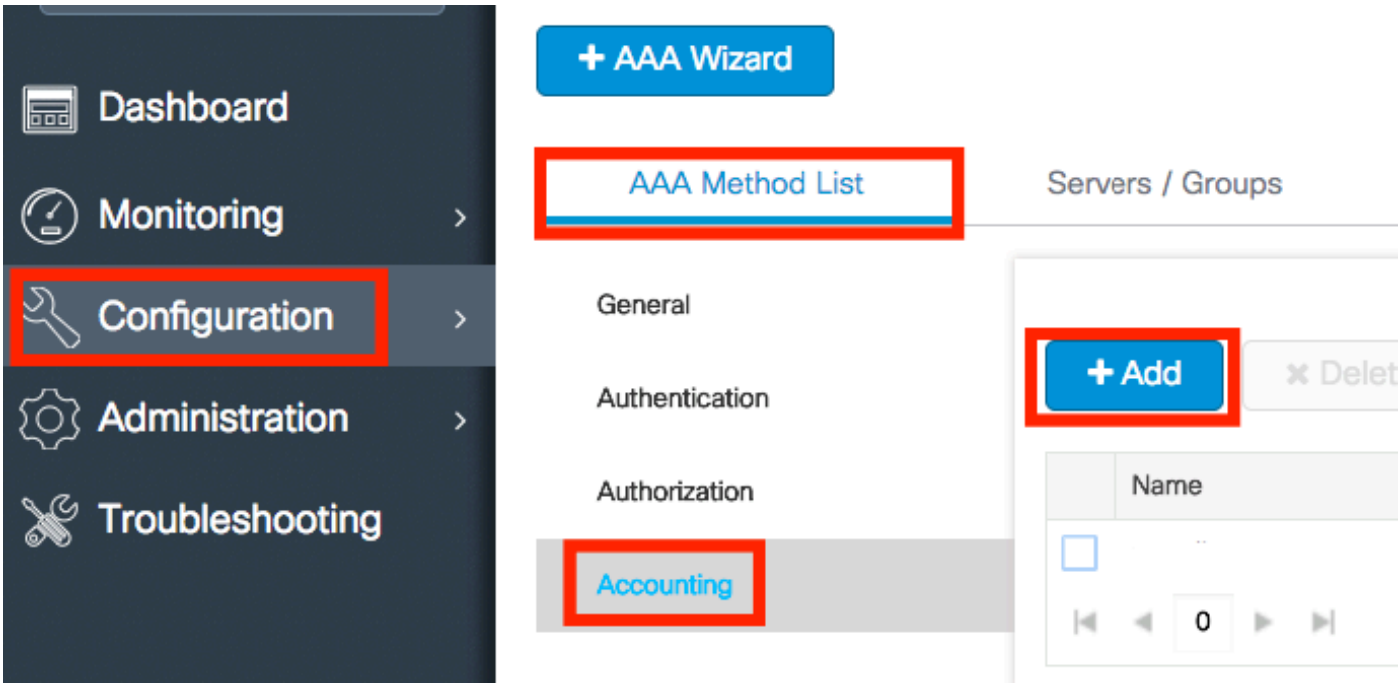
ةظحلام: في الإصدار 17.4.x والإصدارات الأحدث، تأكد أيضا من تكوين مفتاح خادم CoA عند تكوين خادم RADIUS. أستخدم المفتاح نفسه مثل السر المشترك (هو نفس التقصير على ISE). الغرض هو أن يشكل إختياري مفتاح مختلف ل CoA من المفتاح المشترك إن يكون هذا هو ما قام خادم RADIUS بتكوينه. في Cisco IOS XE 17.3، أستخدمت واجهة مستخدم الويب بسطاة نفس السر المشترك مثل مفتاح CoA.

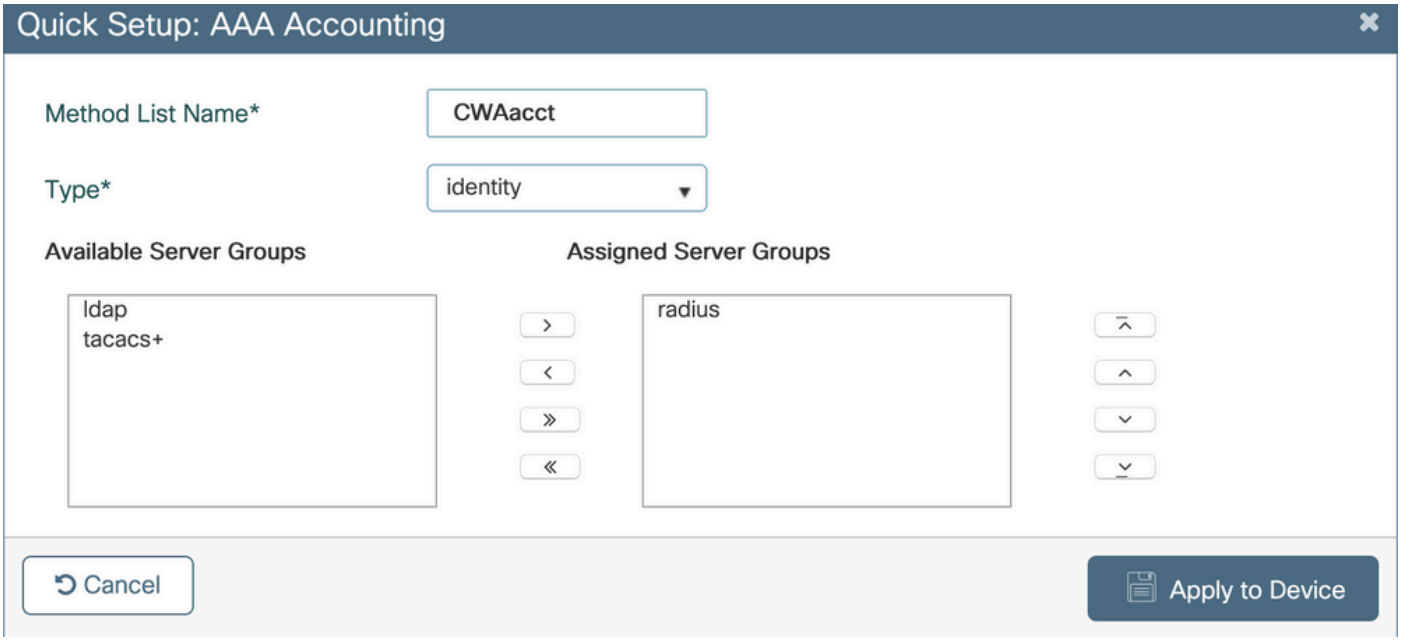
الخطوة 2. إنشاء قائمة أساليب التخويل.

انتقل إلى Configuration > Security > AAA > AAA Method List > Authorization > + Add كما هو موضح في الصورة.



الخطوة 3. (إختياري) قم بإنشاء قائمة أسلوب المحاسبة كما هو موضح في الصورة.

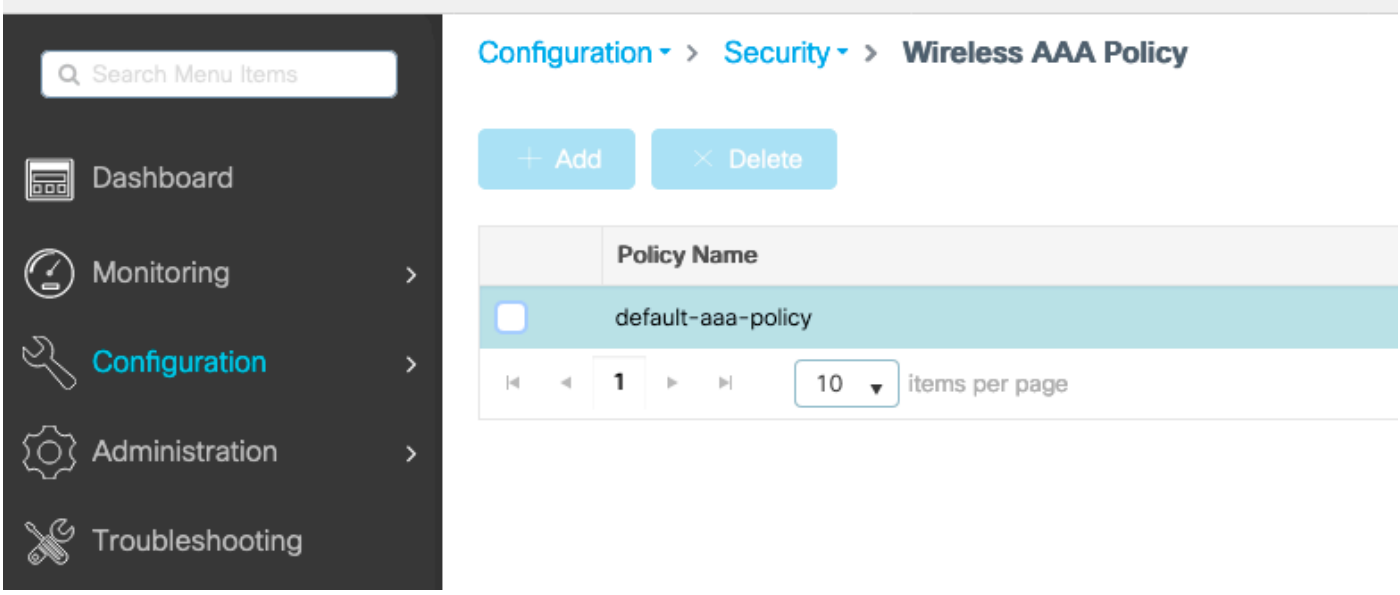




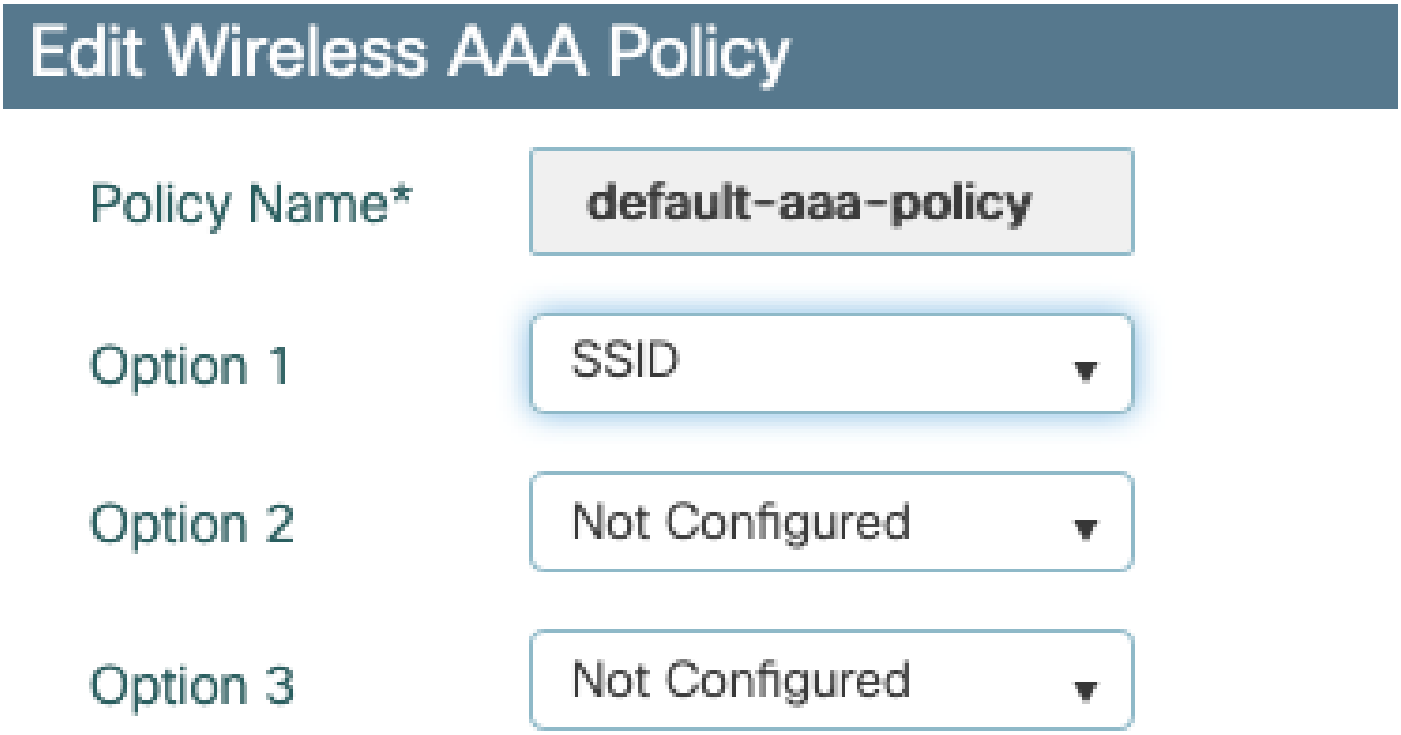
ملاحظة: إذا قررت أن تتوازن (من تكوين واجهة سطر الأوامر من Cisco IOS XE) خوادم RADIUS الخاصة بك بسبب معرفة تصحيح الأخطاء من Cisco CSCvh03827. مع ذلك، تأكد من أن موازن الحمل لديك يعمل على أساس كل عميل باستخدام سمة RADIUS لمعرفة المحطة الاستدعاء. الاعتماد على منفذ مصدر UDP ليس آلية مدعومة لموازنة طلبات RADIUS من 9800.

الخطوة 4. (إختياري) يمكنك تحديد سياسة AAA لإرسال اسم SSID كسمة Call-station-id، والتي يمكن أن تكون مفيدة إذا كنت تريد الاستفادة من هذا الشرط على ISE لاحقا في العملية.

انتقل إلى Configuration > Security > Wireless AAA Policy نهج AAA الافتراضي أو قم بإنشاء نهج جديد.



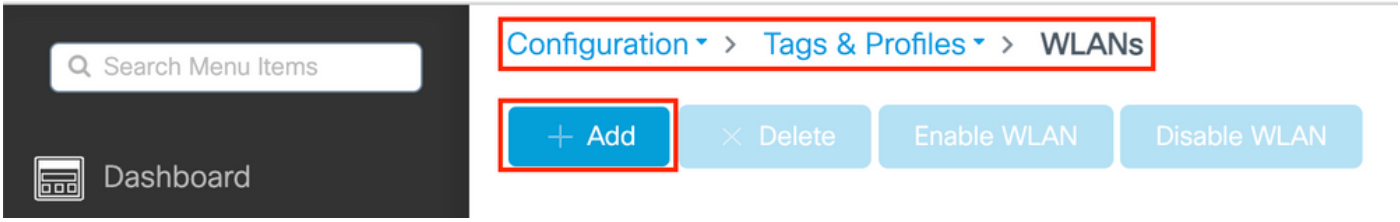
يمكنك الاختيار SSID كخيار 1. تذكر أنه حتى عندما تختار SSID فقط، فإن معرف المحطة المستدعى الى يزال إلحاق عنوان MAC لنقطة الوصول باسم SSID.



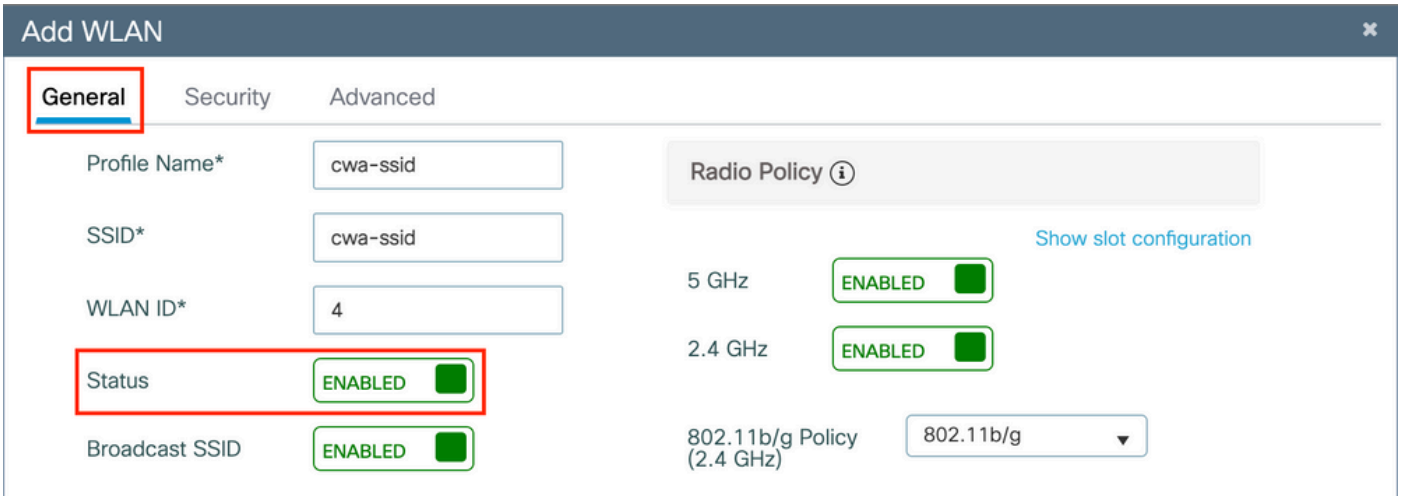
تكوين شبكة WLAN

الخطوة 1. قم بإنشاء شبكة WLAN.

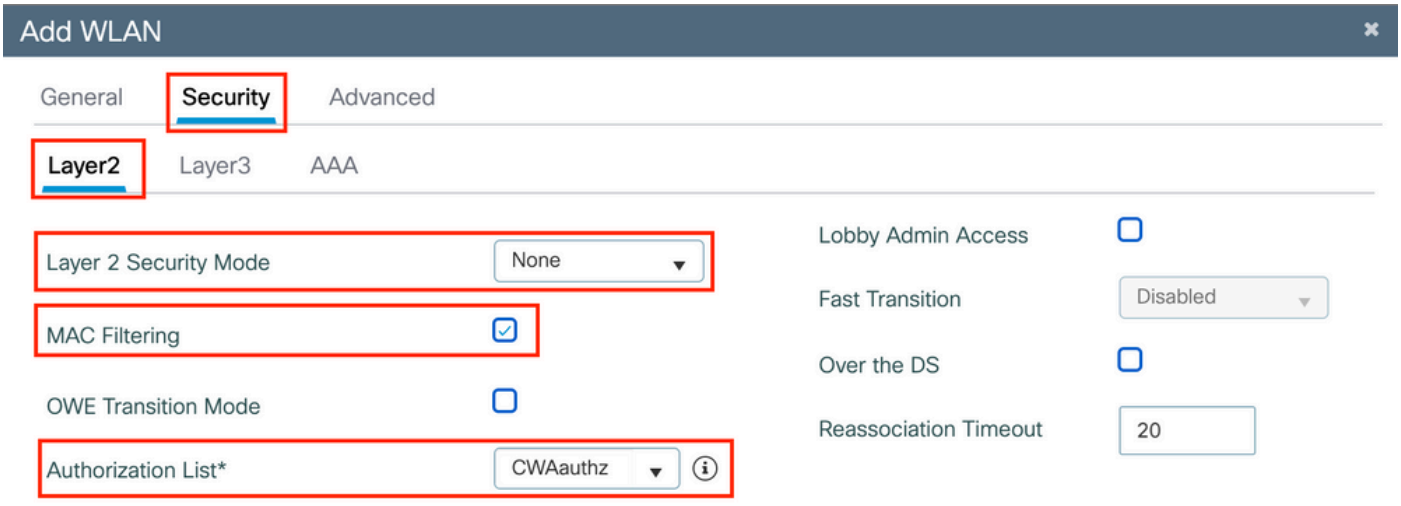
انتقل إلى الشبكة Configuration > Tags & Profiles > WLANs > + Add وتكوينها حسب الحاجة.



الخطوة 2. أدخل المعلومات العامة لشبكة WLAN.



الخطوة 3. انتقل إلى Security علامة التبويب واختر طريقة الأمان المطلوبة. في هذه الحالة، تكون هناك حاجة فقط إلى تصفية MAC' وقائمة تفويض AAA (التي قمت بإنشائها في الخطوة 2. في AAA Configuration القسم).



CLI:

```
#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive
```

(config-wlan)#no security wpa
(config-wlan)#no security wpa wpa2
(config-wlan)#no security wpa wpa2 ciphers aes
(config-wlan)#no security wpa akm dot1x
(config-wlan)#no shutdown

تكوين ملف تعريف السياسة

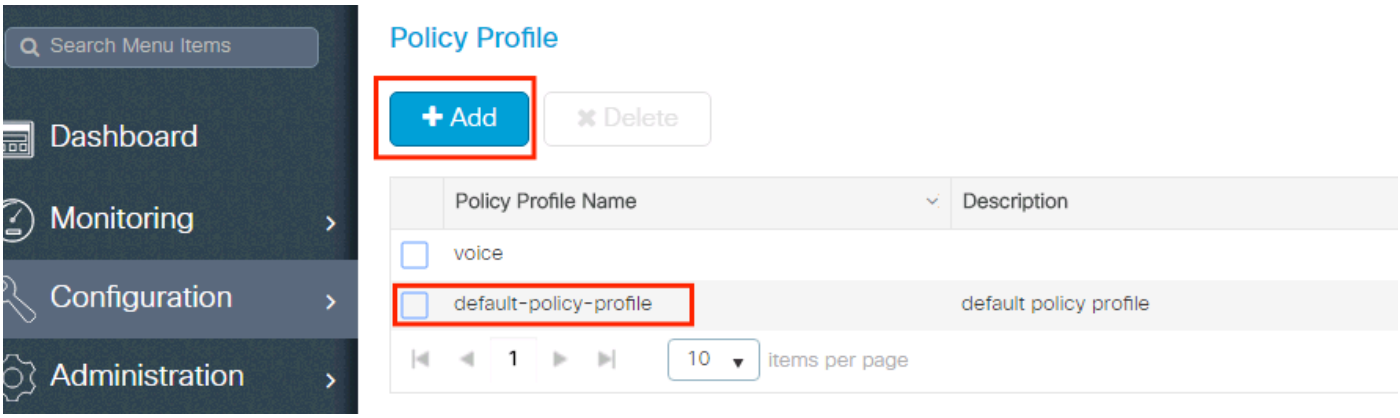
داخل ملف تعريف سياسة، يمكنك أن تقرر تخصيص العملاء الذين لديهم شبكة VLAN، من بين الإعدادات الأخرى (مثل قائمة التحكم في الوصول (ACLs)، جودة الخدمة (QoS)، Mobility Anchor، أجهزة التوقيت، وما إلى ذلك).

يمكنك إما استخدام ملف تعريف السياسة الافتراضي الخاص بك أو إنشاء ملف تعريف جديد.

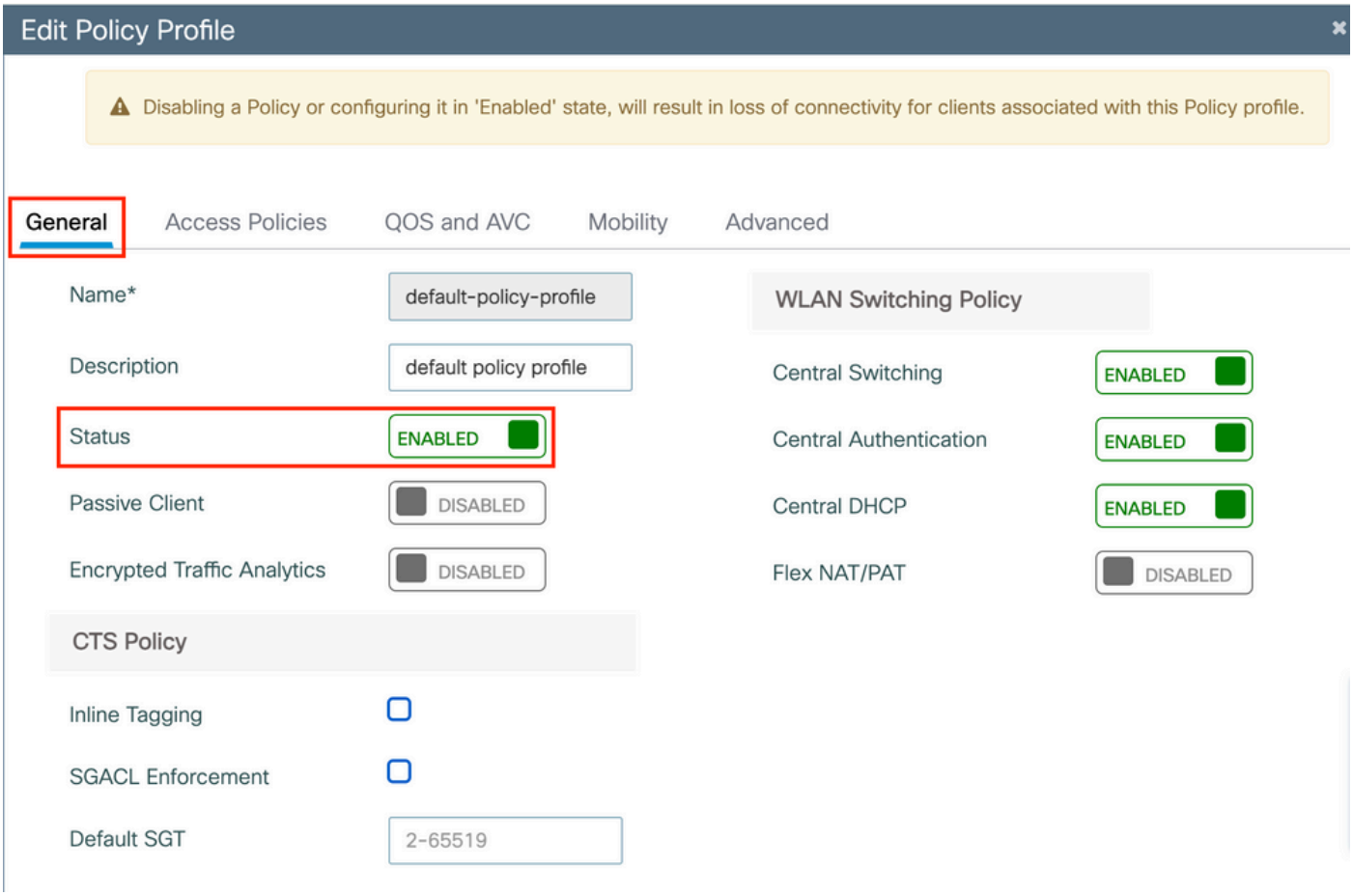
GUI:

الخطوة 1. إنشاء Policy Profile جديد.

انتقل إلى Configuration > Tags & Profiles > Policy وقم بتكوين أو default-policy-profile إنشاء واحد جديد.

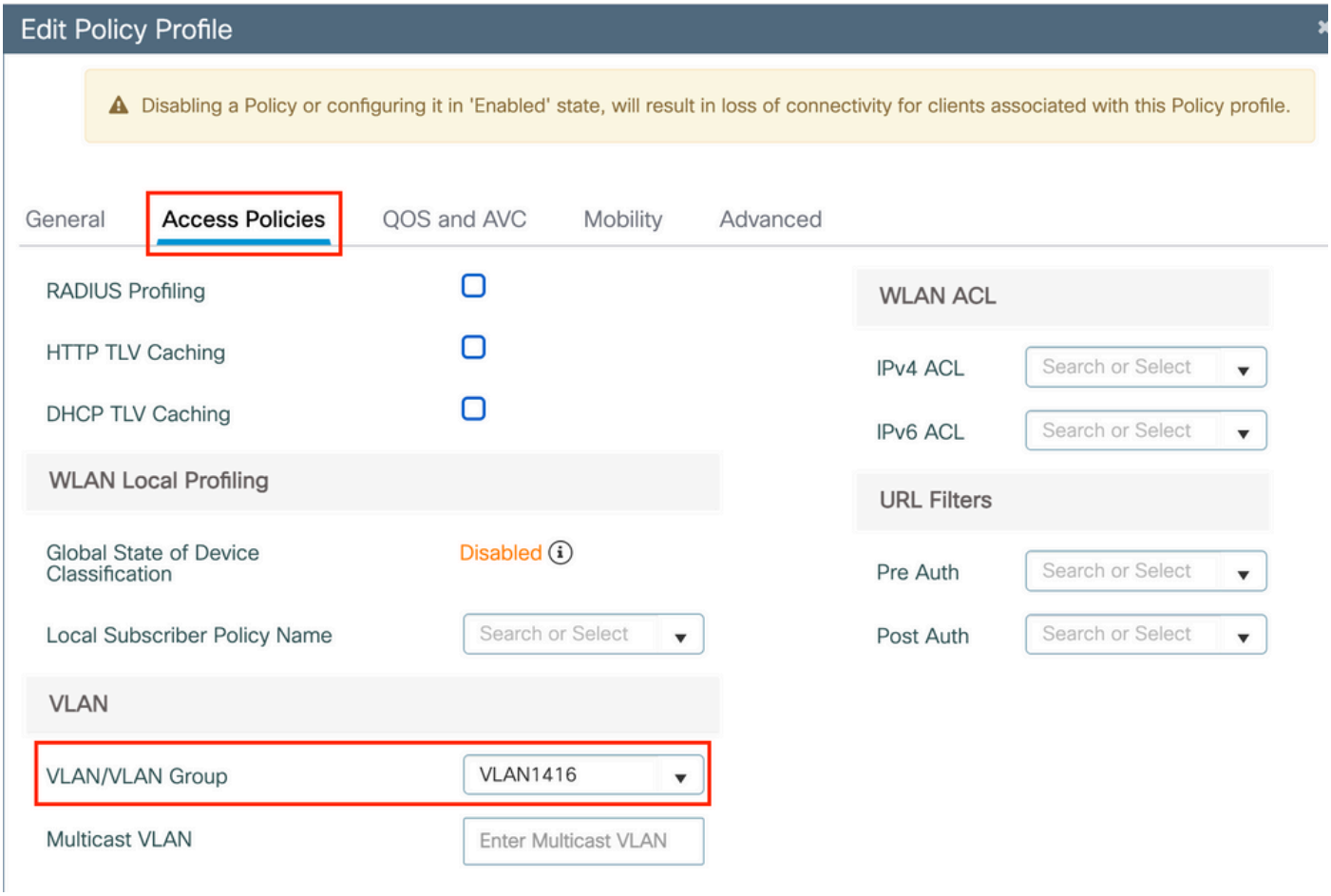


تأكد من تمكين ملف التعريف.

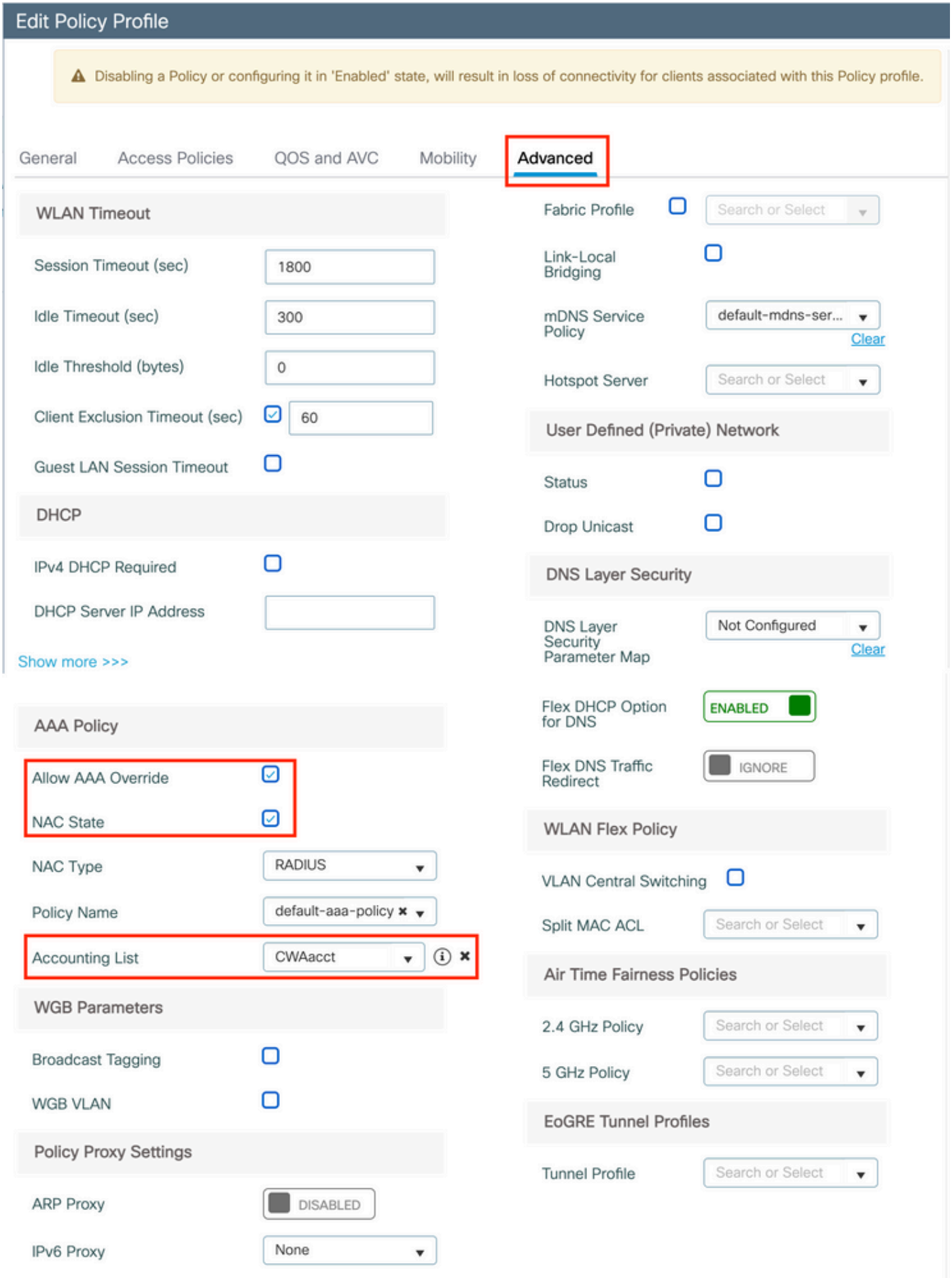


الخطوة 2. أختر ال VLAN.

انتقل إلى Access Policies علامة التبويب واختر اسم شبكة VLAN من القائمة المنسدلة أو اكتب معرف VLAN يدوي. ال تقم بتكوين قائمة التحكم في الوصول (ACL) في ملف تعريف السياسة.



الخطوة 3. قم بتكوين ملف تعريف السياسة لقبول تخطيات ISE (السماح بتجاوز AAA) وتغيير التفويض (CoA) (حالة NAC). يمكنك تحديد طريقة محاسبة بشكل اختياري أيضاً.


Edit Policy Profile
Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.
General
Access Policies
QOS and AVC
Mobility
Advanced
WLAN Timeout
Session Timeout (sec)
1800
Idle Timeout (sec)
300
Idle Threshold (bytes)
0
Client Exclusion Timeout (sec)
60
Guest LAN Session Timeout
DHCP
IPv4 DHCP Required
DHCP Server IP Address
Show more >>>
AAA Policy
Allow AAA Override
NAC State
NAC Type
RADIUS
Policy Name
default-aaa-policy
Accounting List
CWAacct
WGB Parameters
Broadcast Tagging
WGB VLAN
Policy Proxy Settings
ARP Proxy
DISABLED
IPv6 Proxy
None
Fabric Profile
Search or Select
Link-Local Bridging
mDNS Service Policy
default-mdns-ser...
Clear
Hotspot Server
Search or Select
User Defined (Private) Network
Status
Drop Unicast
DNS Layer Security
DNS Layer Security Parameter Map
Not Configured
Clear
Flex DHCP Option for DNS
ENABLED
Flex DNS Traffic Redirect
IGNORE
WLAN Flex Policy
VLAN Central Switching
Split MAC ACL
Search or Select
Air Time Fairness Policies
2.4 GHz Policy
Search or Select
5 GHz Policy
Search or Select
EoGRE Tunnel Profiles
Tunnel Profile
Search or Select

CLI:

config # wireless profile policy <policy-profile-name> # aaa-override
nac
vlan <vlan-id_or_vlan-name>
accounting-list <acct-list>
no shutdown

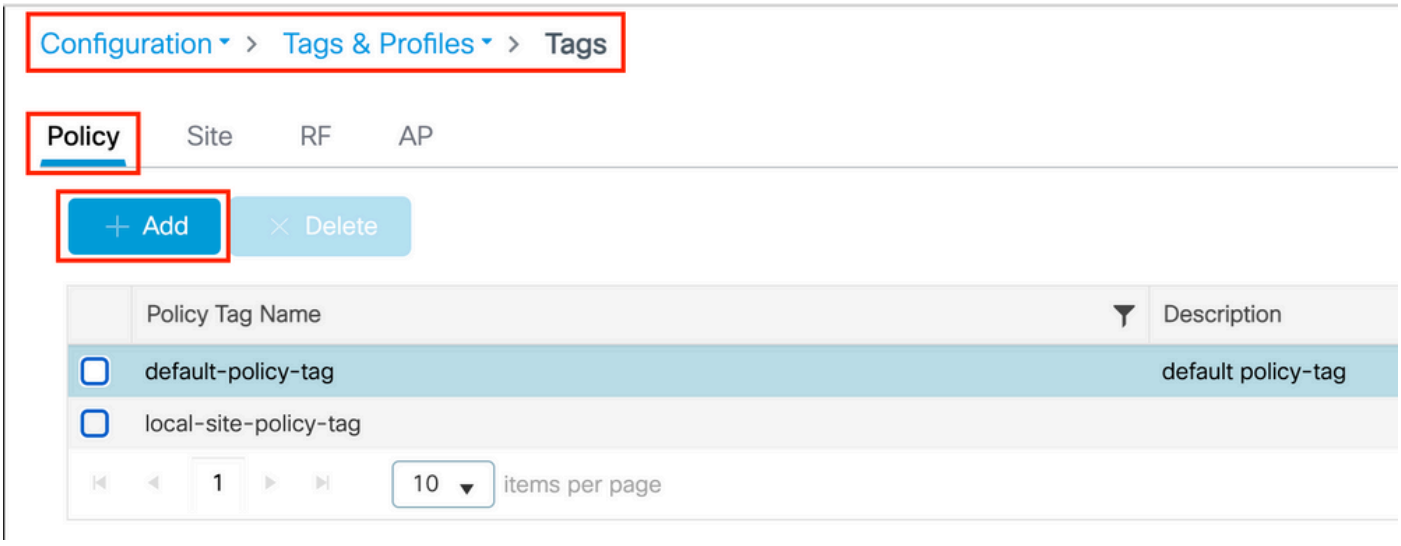
تكوين علامة السياسة

داخل علامة السياسة وه المكان الذي تقوم فيه برطب SSID بملف تعريف السياسة الخاص بك. يمكنك إما إنشاء علامة سياسة جديدة أو استخدام علامة السياسة الافتراضية.

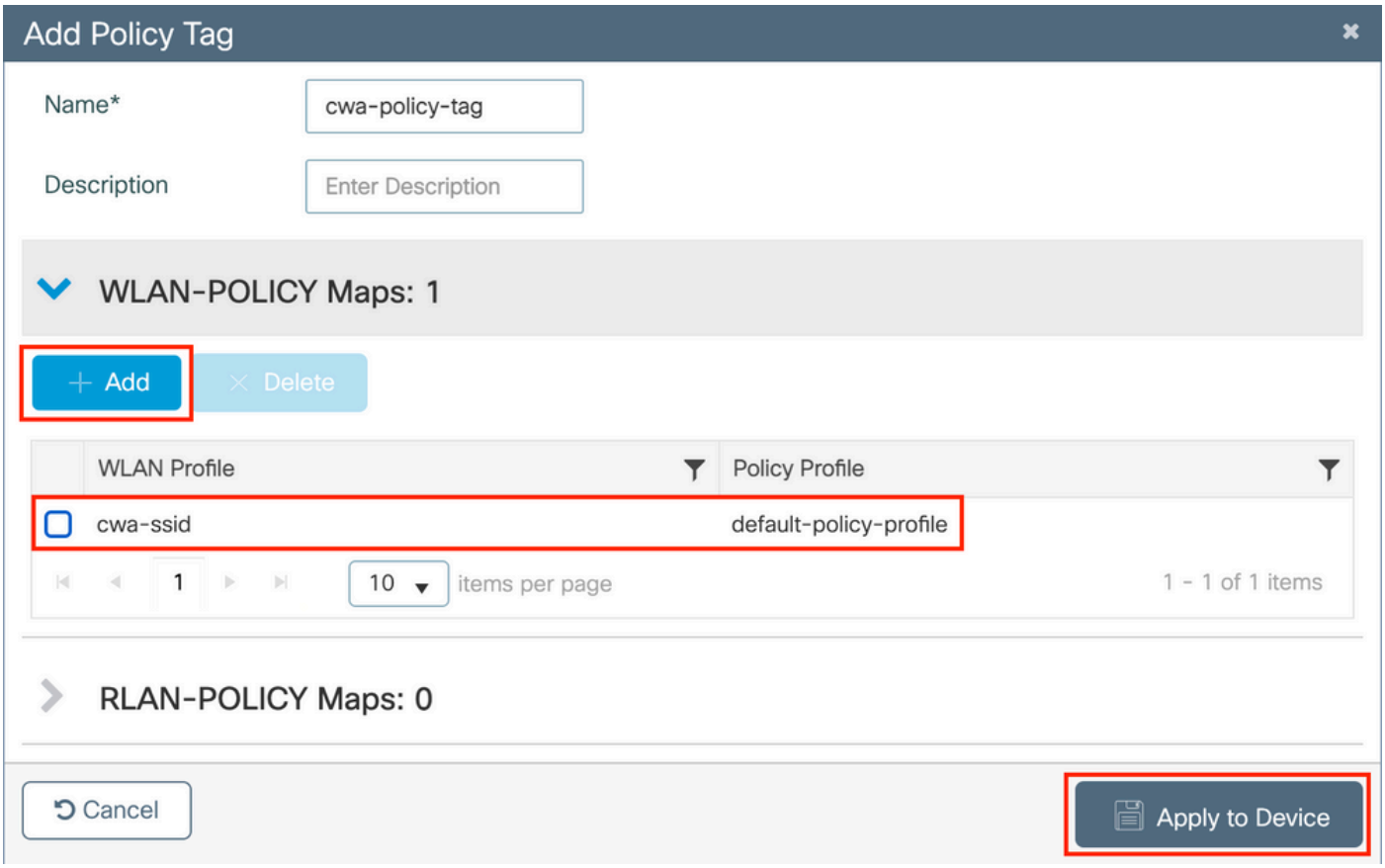
ملاحظة: تترجم علامة النهج الافتراضي تلقائيا أي SSID بمعرف WLAN بين 1 و 16 إلى ملف تعريف النهج الافتراضي. لا يمكن تعديله أو حذفه. إذا كانت لديك شبكة WLAN بالمعرف 17 أو إصدار أحدث، لا يمكن استخدام علامة النهج الافتراضي.

GUI:

انتقل إلى Configuration > Tags & Profiles > Tags > Policy أو اضغط على جديد إذا لزم الأمر كما هو موضح في الصورة.



قم برطب ملف تعريف WLAN بملف تعريف السياسة المطلوب.



CLI:

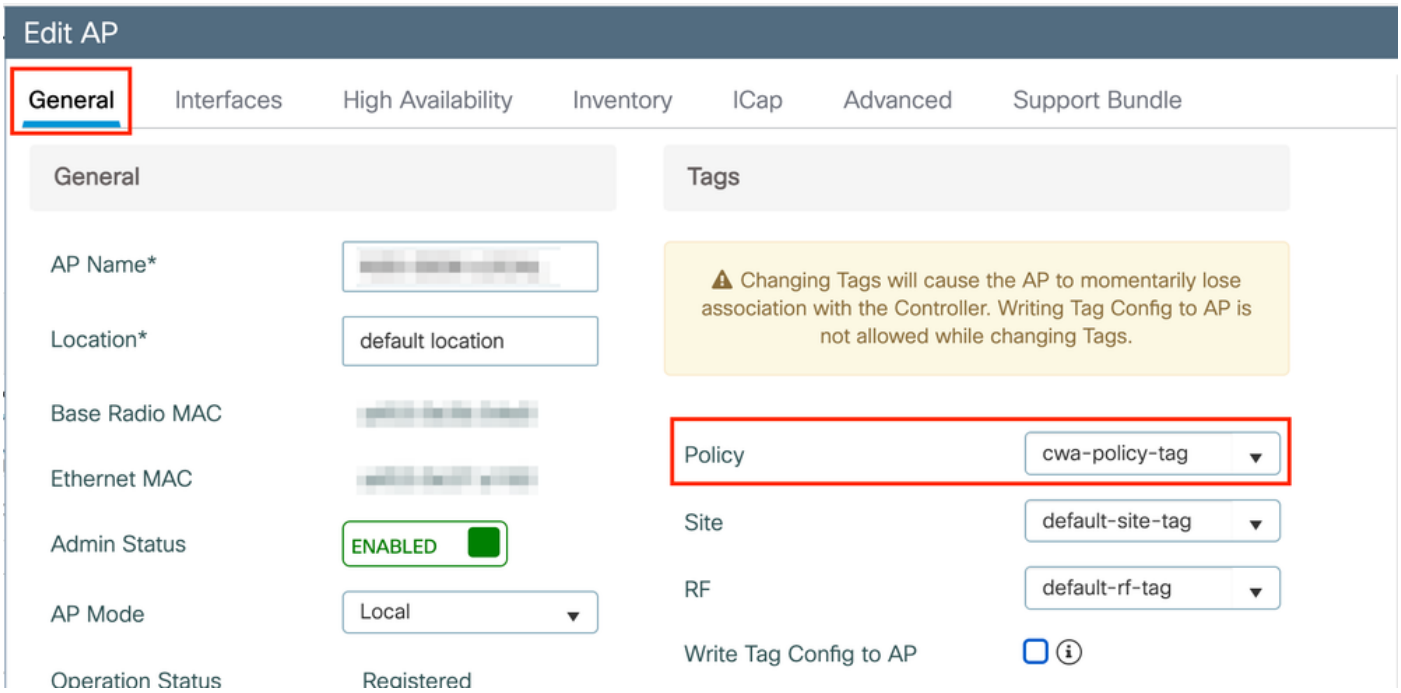
config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>

تعيين علامة السياسة

قم بتعيين علامة السياسة لنقاط الوصول المطلوبة.

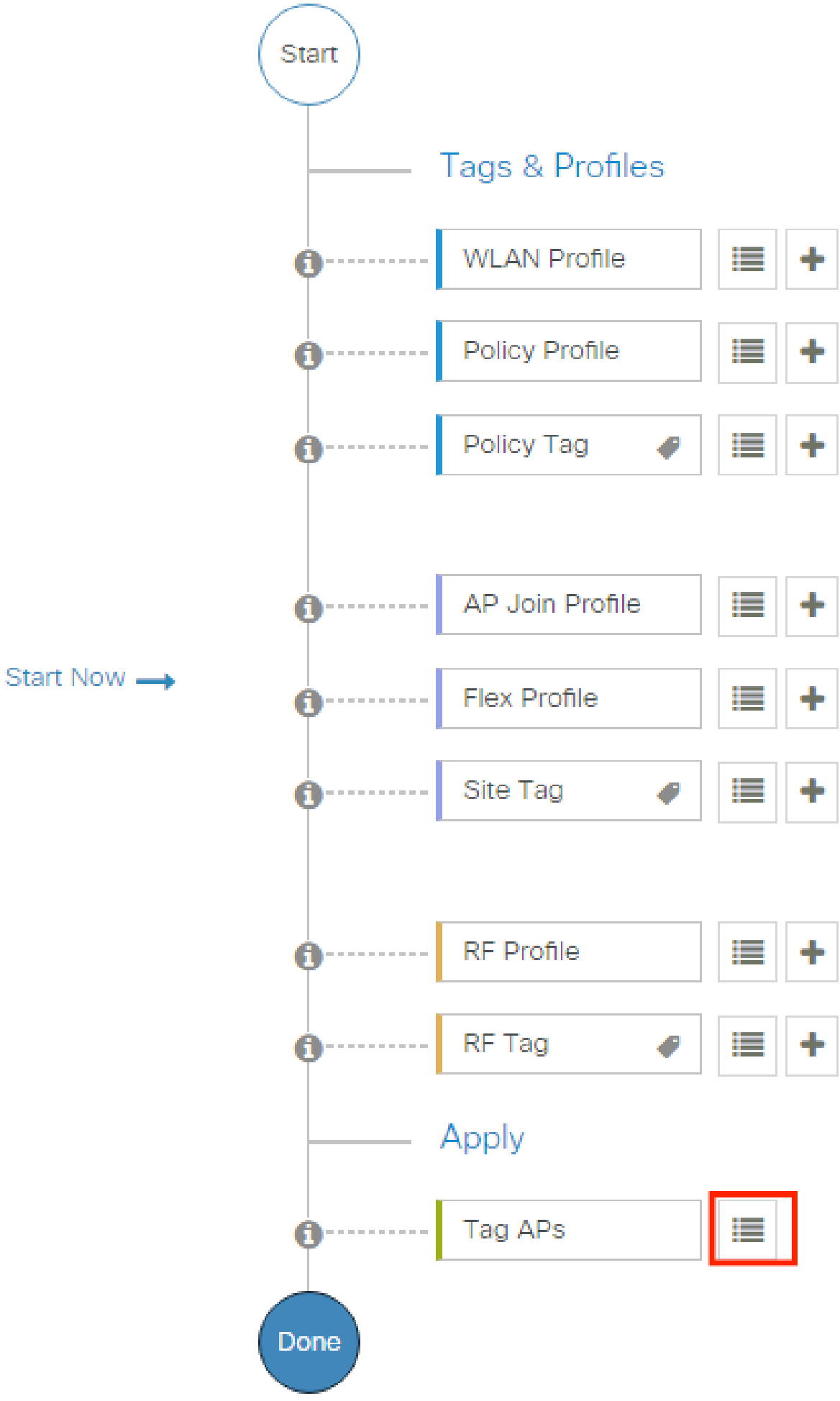
GUI:

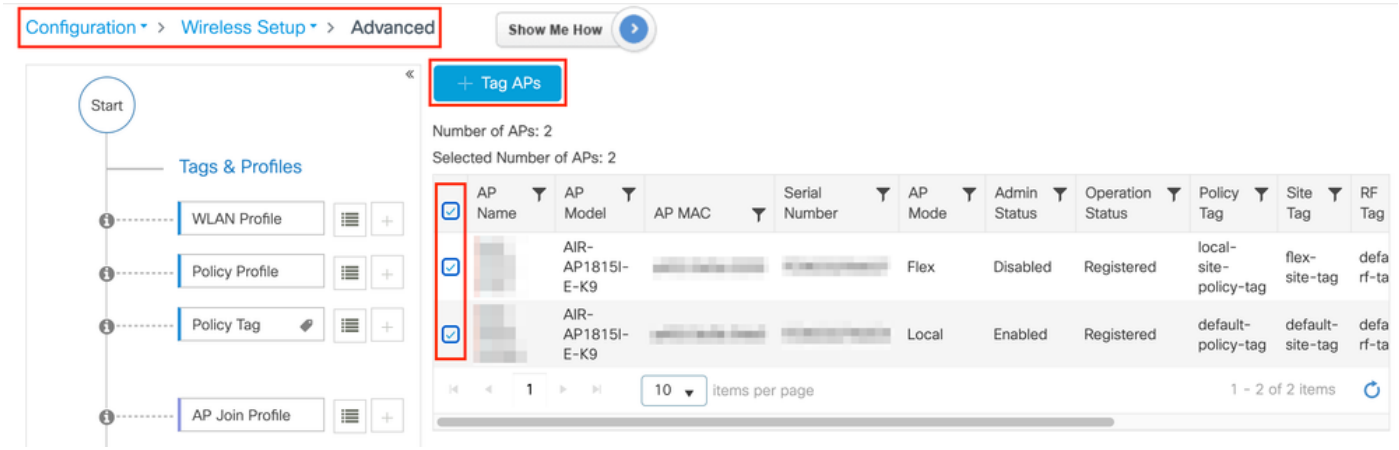
لتعيين العلامة إلى نقطة وصول واحدة، انتقل إلى Configuration > Wireless > Access Points > AP Name > General Tags، وقم بتعيين المهمة المطلوبة، ثم انقر Update & Apply to Device.



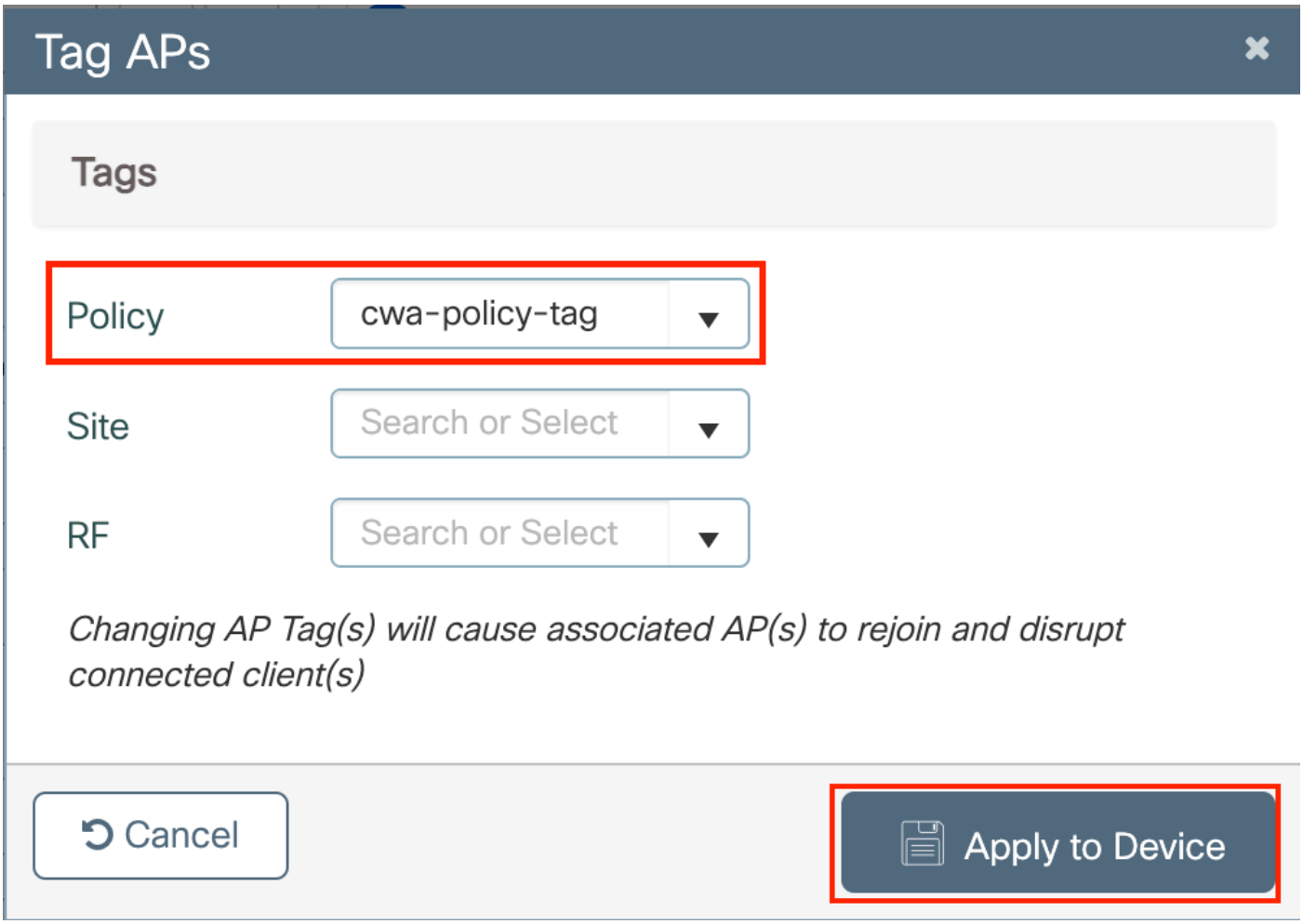
ملاحظة: اعلم أنه بعد تغيير علامة السياسة على نقطة وصول، فإنها تفقد ارتباطها مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800 وترجع للانضمام في غضون دقيقة واحدة تقريبا.

لتعيين نفس علامة النهج إلى نقاط وصول متعددة، انتقل إلى Configuration > Wireless > Wireless Setup > Advanced > Start Now.


Start
Tags & Profiles
WLAN Profile
Policy Profile
Policy Tag
AP Join Profile
Start Now
Flex Profile
Site Tag
RF Profile
RF Tag
Apply
Tag APs
Done



أختر علامة التمييز ذات اللون الأبيض وانقر Save & Apply to Device كما هو موضح في الصورة.



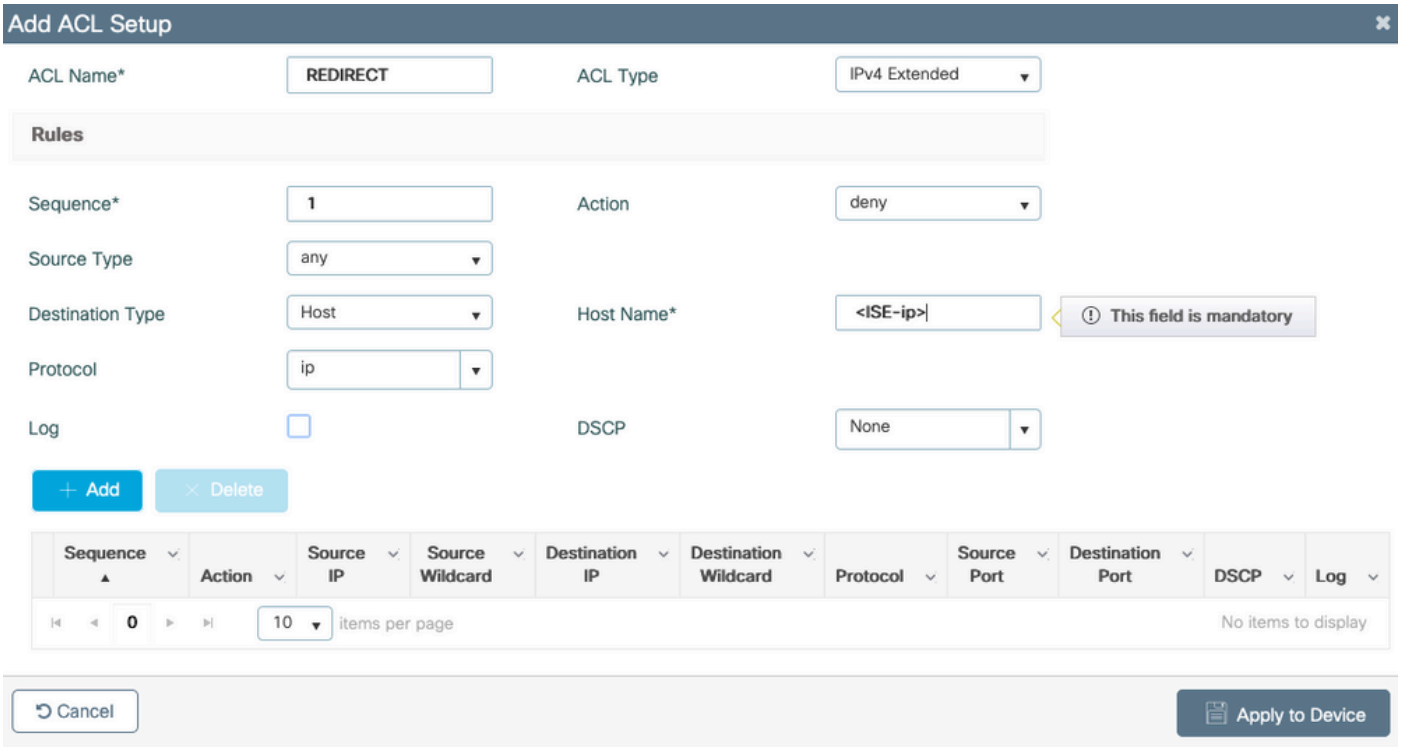
CLI:

config t # ap <ethernet-mac-addr> # policy-tag <policy-tag-name> # end

إعادة توجيه تكوين قائمة التحكم في الوصول (ACL)

الخطوة 1. انتقل إلى Configuration > Security > ACL > + Add لإنشاء قائمة تحكم في الوصول (ACL) جديدة.

أختر اسم لقائمة التحكم بالوصول (ACL)، وحدد IPv4 Extended وتكتب وتضيف كل قاعدة كتسلسل كما هو موضح في الصورة.



تحتاج إلى رفض حركة المرور إلى عُقد خدمة السياسة (PSN) لمحرك ISE وكذلك رفض DNS والسماح بالباقي. قائمة التحكم في الوصول (ACL) المعاد توجيهها هذه ليست قائمة تحكم في الوصول (ACL) أمنية ولكنها قائمة تحكم في الوصول إلى النقطة التي تحدد حركة المرور التي تنتقل إلى وحدة المعالجة المركزية (على الترانخيص) لمزيد من المعالجة (مثل إعادة التوجيه) وما هي حركة المرور التي تبقى على مستوى البيانات (عند الرفض) وتجنب إعادة التوجيه.

يجب أن تبدو قائمة التحكم في الوصول (ACL) كما يلي (استبدل 10.48.39.28 بعنوان IP الخاص بك في هذا المثال):

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
10	deny	any		10.48.39.28		ip			None	Disabled
20	deny	10.48.39.28		any		ip			None	Disabled
30	deny	any		any		udp		eq domain	None	Disabled
40	deny	any		any		udp	eq domain		None	Disabled
50	permit	any		any		tcp		eq www	None	Disabled

1 10 items per page 1 - 5 of 5 items

ملاحظة: بالنسبة لقائمة التحكم في الوصول (ACL) الخاصة بإعادة التوجيه، اعتبر deny الإجراء إعادة توجيه للرفض (عدم رفض حركة المرور) permitوالإجراء هو إعادة التوجيه المسموح بها. تنظر عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) فقط في حركة المرور التي يمكنها إعادة التوجيه (المنافذ 80 و 443 بشكل افتراضي).

CLI:

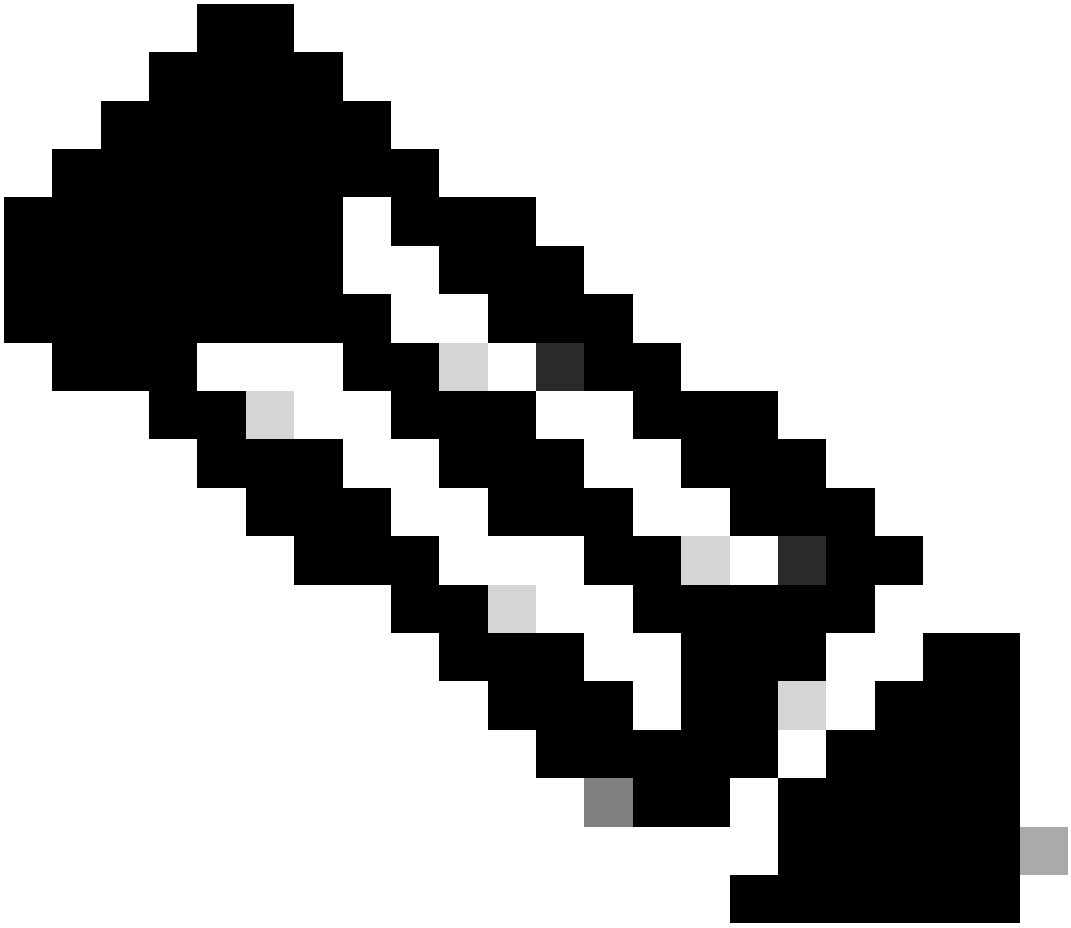
```
ip access-list extended REDIRECT
 deny ip any host <ISE-IP>
 deny ip host<ISE-IP> any
 deny udp any any eq domain
 deny udp any eq domain any
 permit tcp any any eq 80
```

ملاحظة: إذا قمت بإنهاء قائمة التحكم في الوصول permit ip any any باستخدام تصريح ركز على المنفذ 80، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يقوم بإعادة توجيه HTTPS، والذي غالبا ما يكون غير مرغوب فيه لأنه يجب أن يوفر شهادته الخاصة ويقوم بإنشاء انتهاك لشهادة. هذه إستثناء من الجملة السابقة التي تقول أنك لا تحتاج إلى شهادة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في حالة تمكين اعتراض HTTPS ولكنها تعتبر حالة على أية حال. تحتاج إلى شهادة إذا تم

يمكنك تحسين قائمة التحكم في الوصول (ACL) من خلال الإجراء لرفض منفذ الضيف 8443 قطع إلى خادم ISE.

تمكين إعادة التوجيه ل HTTP وأ HTTPS

يتم ربط تكوين مدخل مسؤول الويب بتكوين مدخل مصادقة الويب ويجب أن يستمع على المنفذ 80 لإعادة التوجيه. لذلك، يجب تمكين HTTP حتى تعمل إعادة التوجيه بشكل صحيح. يمكنك إما إختيار تمكينه بشكل عام (باستخدام الأمرip http server) أو تمكين HTTP للوحدة النمطية لمصادقة الويب فقط (باستخدام الأمر webauth-http-enable أسفل خريطة المعلمة).



ةظحالم: تحدث إعادة توجيه حركة مرور HTTP داخل CAPWAP، حتى في حالة التحويل المحلي ل FlexConnect. بما أنه لا يمكن لل WLC إعتراض، لا ap يرسل ال HTTP(s) ربط داخل ال capwap نفق ويستلم ال redirection من ال WLC في الخلف CAPWAP

إذا كنت ترغب في إعادة التوجيه عند محاولة الوصول إلى عنوان URL ل HTTPS، فقم بإضافة الأمرintercept-https-enable أسفل خريطة المعلمة ولكن الحظ أن هذا ليس التكوين الأمثل، وأنه يؤثر على وحدة المعالجة المركزية الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) ويولد أخطاء في الشهادة على أية حال:

<#root>

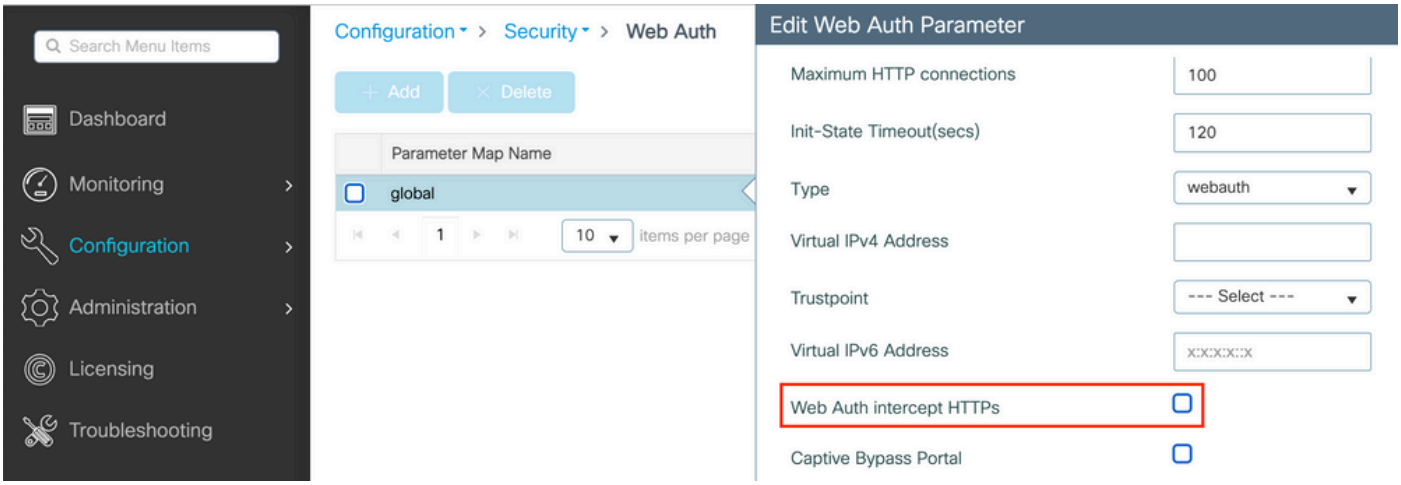
parameter-map type webauth global

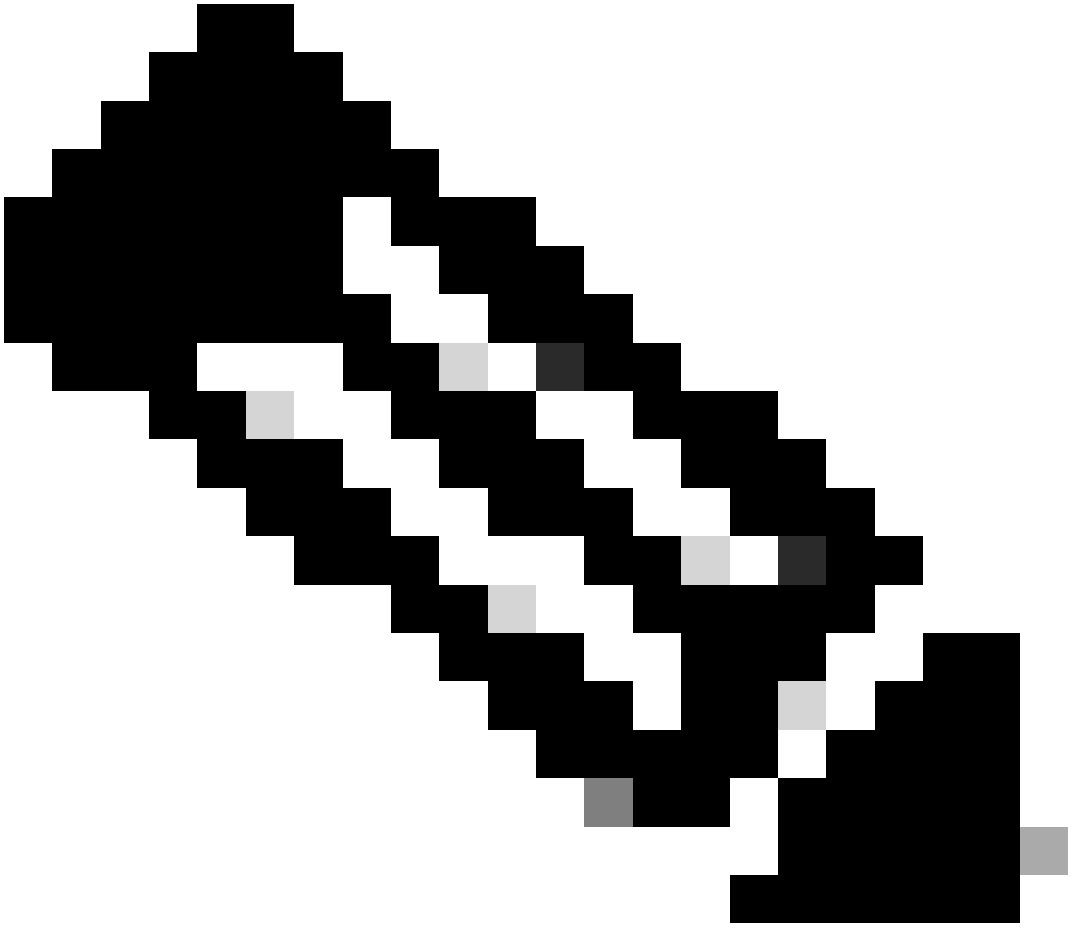
type webauth

intercept-https-enable

trustpoint xxxxx

أنت يستطيع أيضا فعلت ذلك عبر ال gui مع الخيار 'Web Auth يعترض HTTPS'تدقيق في المعلمة خريطة (Configuration > Security > Web Auth).



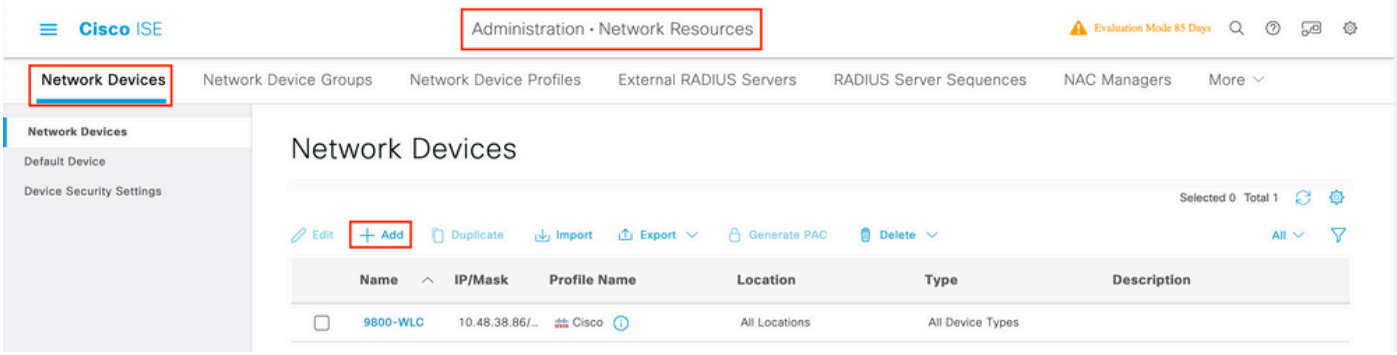


ملاحظة: بشكل افتراضي، تستخدم المستعرضات موقع ويب HTTP لبدء عملية إعادة التوجيه، إذا كانت هناك حاجة إلى إعادة توجيه HTTPS، فيجب التحقق من اعتراض مصادقة الويب HTTPS؛ ومع ذلك، يوصى بهذا التكوين لأنه يزيد من استخدام وحدة المعالجة المركزية.

تكوين ISE

إضافة 9800 WLC إلى محرك خدمات كشف الهوية (ISE)

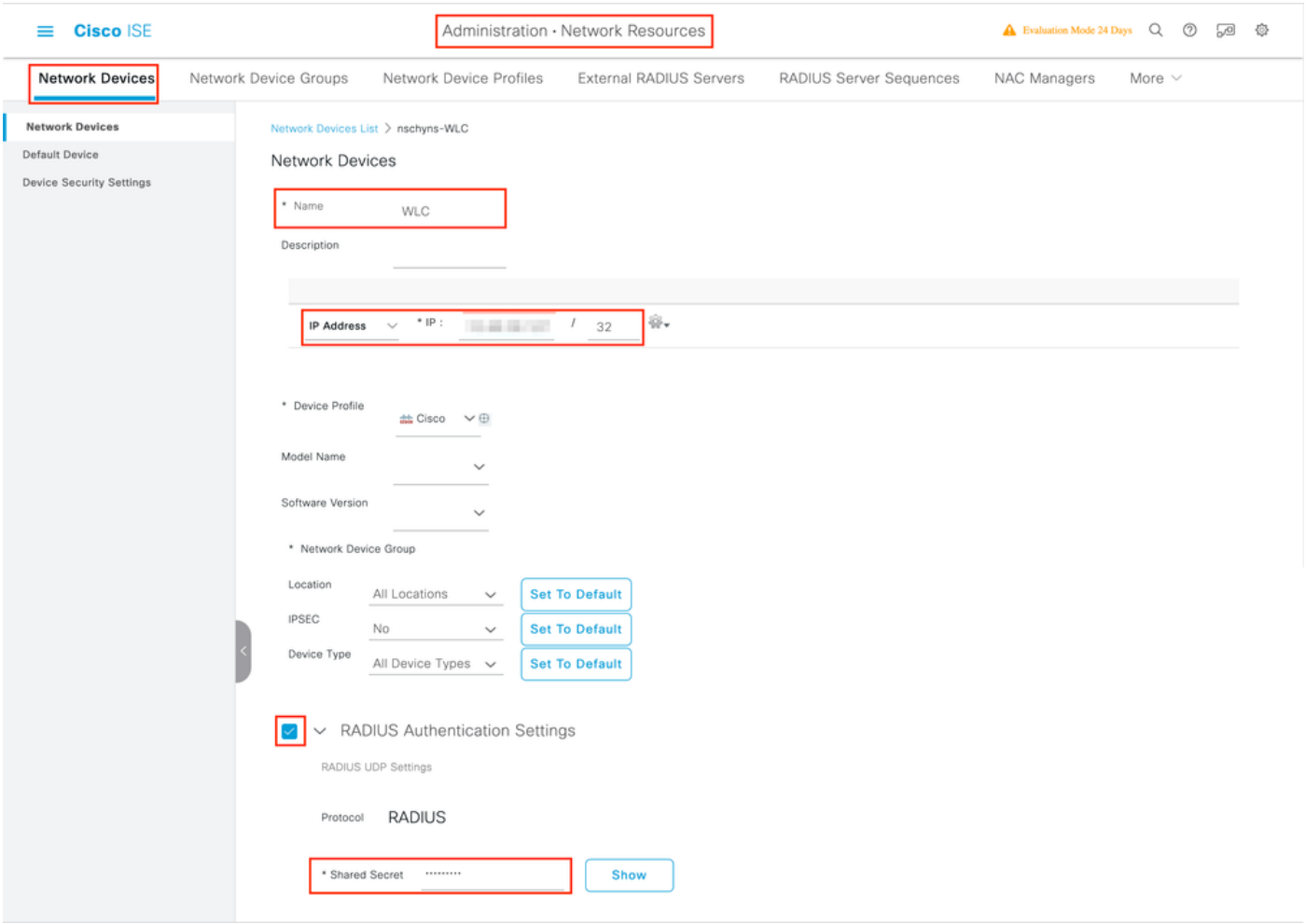
الخطوة 1. افتح وحدة تحكم ISE وانتقل إلىAdministration > Network Resources > Network Devices > Add كما هو موضح في الصورة.



الخطوة 2. قم بتكوين جهاز الشبكة.

وبشكل اختياري، يمكن أن يكون اسم طراز محدد أو إصدار برنامج أو وصف محدد، وتعيين مجموعات أجهزة الشبكة استنادا إلى أنواع الأجهزة أو الموقع أو أدوات التحكم في الشبكة المحلية اللاسلكية (WLC).

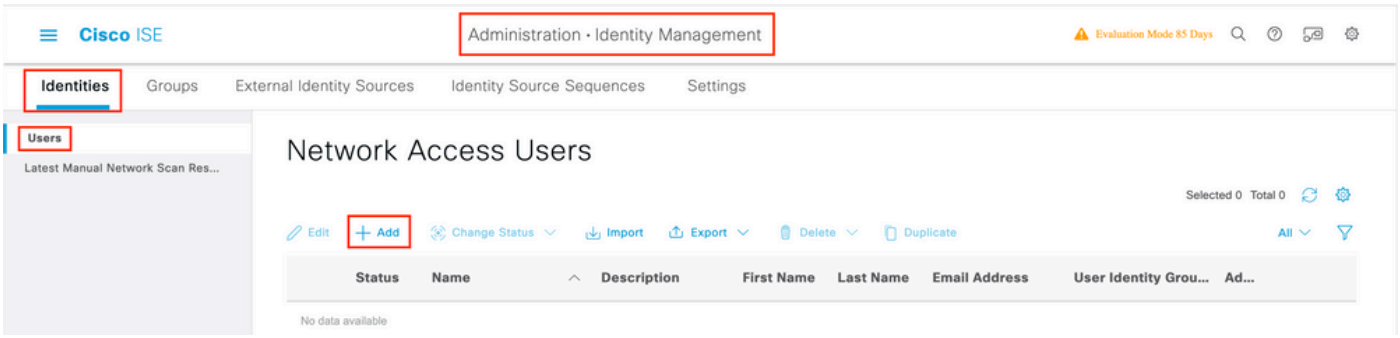
يماثل عنوان IP هنا واجهة WLC التي ترسل طلبات المصادقة. بشكل افتراضي، تكون هي واجهة الإدارة كما هو موضح في الصورة:



لمزيد من المعلومات حول مجموعات أجهزة الشبكة، راجع فصل دليل إدارة ISE: إدارة أجهزة الشبكة: ISE - مجموعات أجهزة الشبكة.

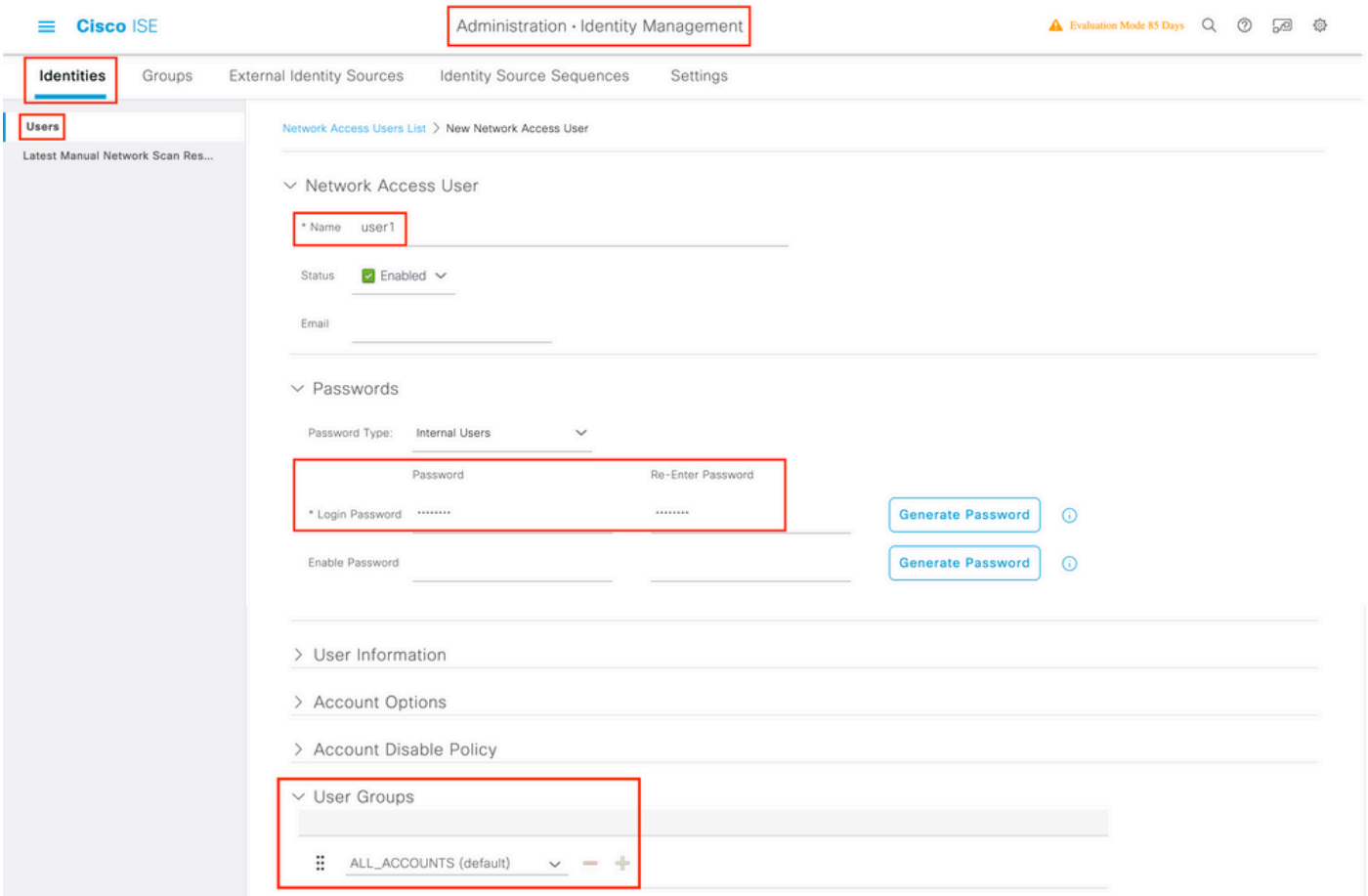
إنشاء مستخدم جديد على ISE

الخطوة 1. انتقل إلى Administration > Identity Management > Identities > Users > Add كما هو موضح في الصورة.



الخطوة 2. أدخل المعلومات.

في هذا المثال، ينتمي هذا المستخدم إلى مجموعة تسمى ALL_ACCOUNTS ولكن يمكن ضبطها حسب الحاجة، كما هو موضح في الصورة.

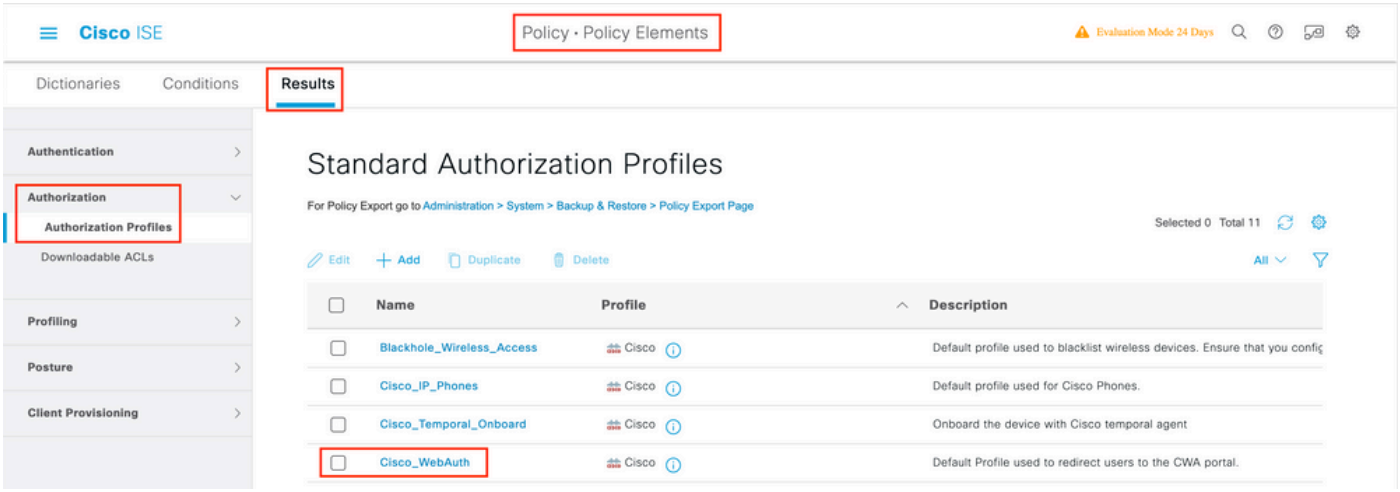


إنشاء ملف تعريف التفويض

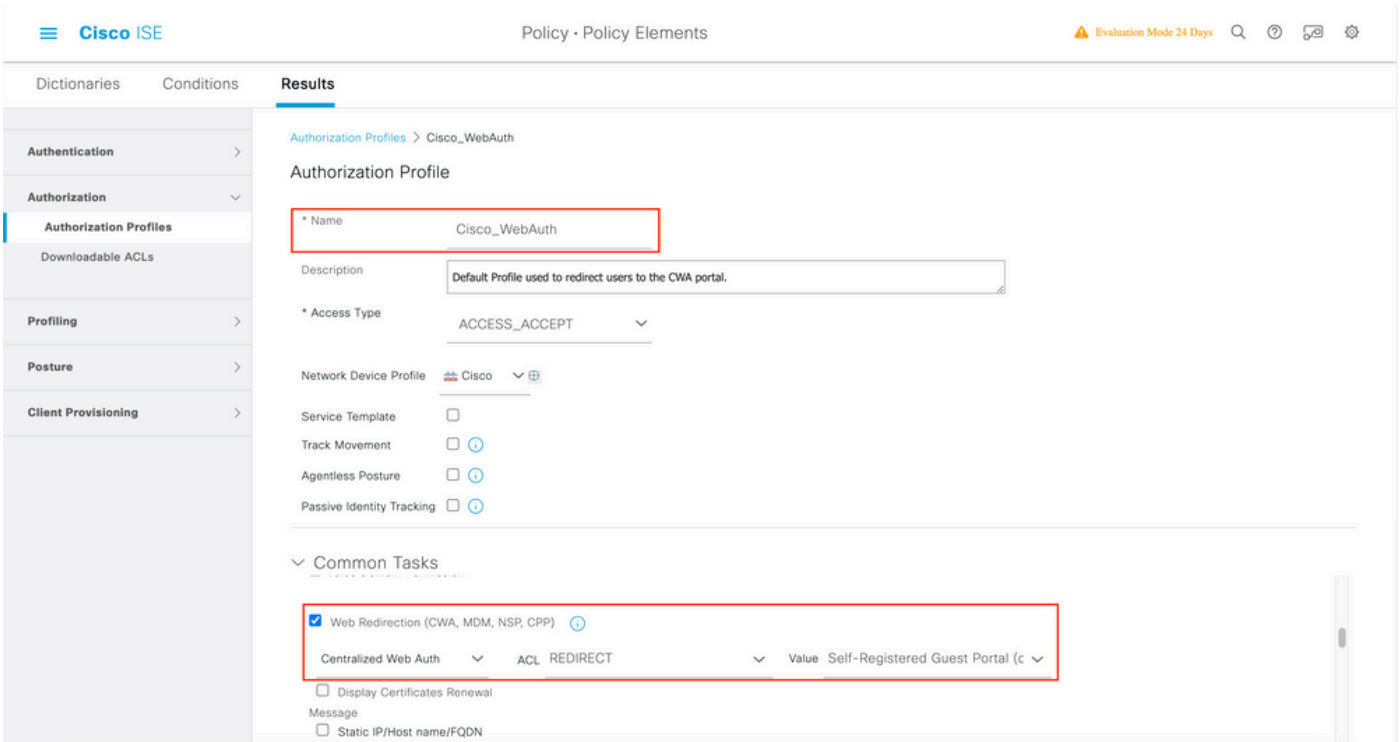
ملف تعريف النهج هو النتيجة المعينة لعميل استنادا إلى المعلمات الخاصة به (مثل عنوان MAC وبيانات الاعتماد وشبكة WLAN المستخدمة وما إلى ذلك). يمكنه تعيين إعدادات معينة مثل شبكة المنطقة المحلية الظاهرية (VLAN) وقوائم التحكم في الوصول (ACL) وإعادة توجيه محدد موقع الموارد الموحد (URL) وما إلى ذلك.

لاحظ أنه في الإصدارات الحديثة من ISE، توجد نتيجة تفويض Cisco_Webauth بالفعل. الآن يمكنك تحرير لتعديل اسم قائمة التحكم في الوصول (ACL) لإعادة التوجيه لمطابقة ما قمت بتكوينه على WLC.

الخطوة 1. انتقل إلى Policy > Policy Elements > Results > Authorization > Authorization Profiles. انقر add لإنشاء النتيجة الافتراضية الخاصة بك وأكCisco_Webauth تحريرها.

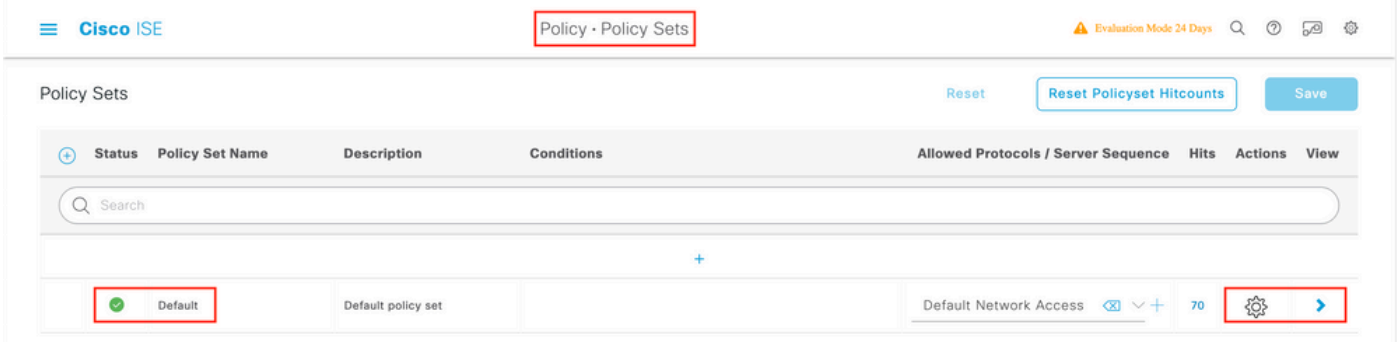


الخطوة 2. أدخل معلومات إعادة التوجيه. تأكد من أن اسم قائمة التحكم في الوصول (ACL) هو نفسه الذي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) طراز 9800.

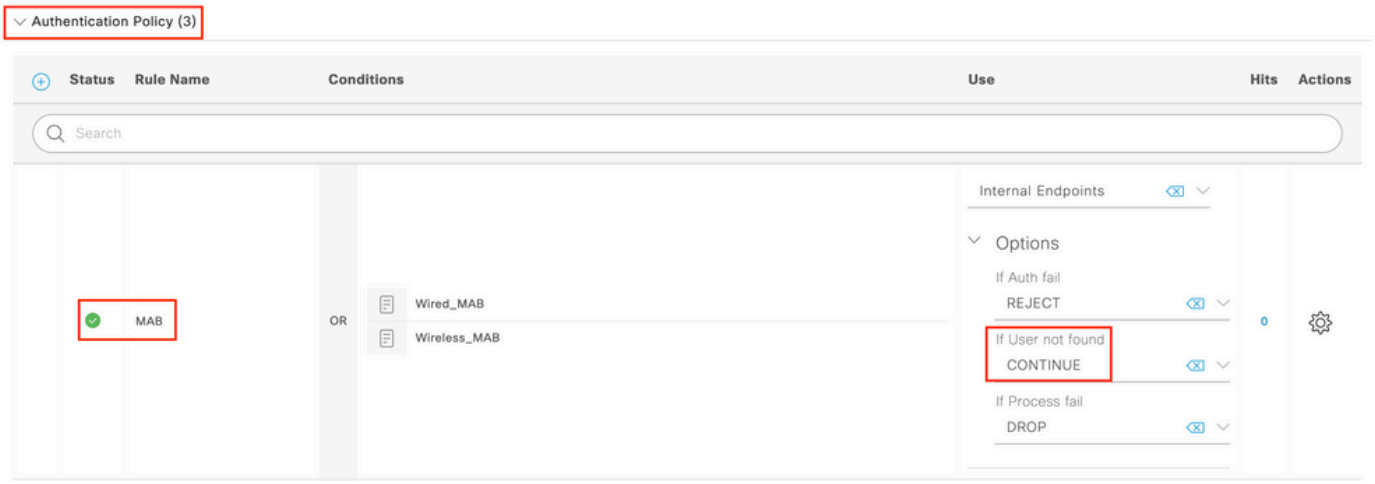


تكوين قاعدة المصادقة

الخطوة 1. تحدد مجموعة النهج مجموعة من قواعد المصادقة والتفويض. لإنشاء واحدة، انتقل إلىPolicy > Policy Sets، انقر فوق علامة تعيين أول مجموعة نهج في القائمة Insert new row ثم أختر السهم الأزرق الموجود على اليمين لاختيار مجموعة النهج الافتراضية.



الخطوة 2. توسيع النهجAuthentication. للقاعدة MAB (مطابقة على MAB سلكي أو السلكي)، مددت Options، واخترت الخيارCONTINUE في حالة كنت ترى 'إذا لم يوجد المستخدم'.



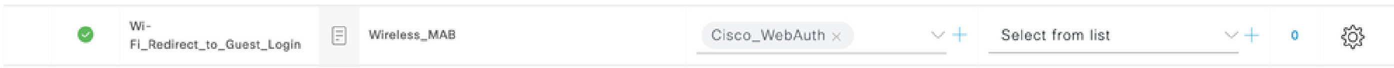
الخطوة 3. انقر فوق Save لحفظ التغييرات.

تكوين قواعد المصادقة

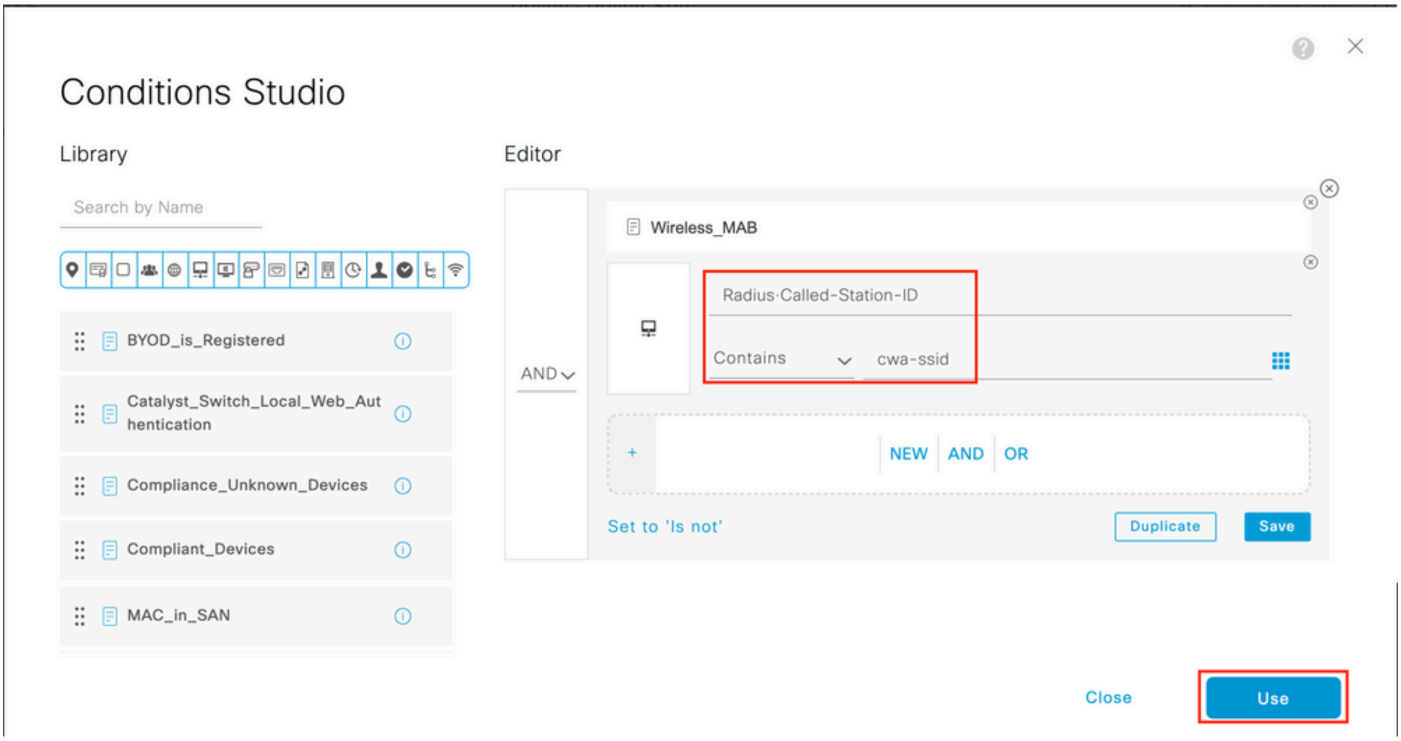
قاعدة التفويض هي القاعدة المسؤولة لتحديد أي نتيجة الأذونات (أي ملف تعريف تفويض) التي يتم تطبيقها على العميل.

الخطوة 1. في نفس صفحة مجموعة النهج، قم بإغلاق Authentication Policy والتوسع Authorziation Policy كما هو موضح في الصورة.

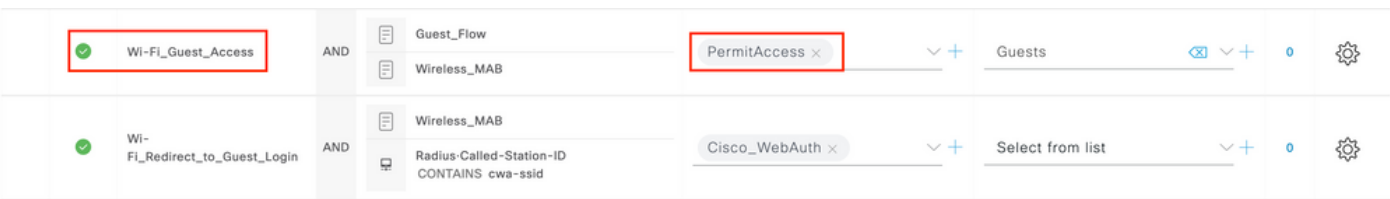
الخطوة 2. تبدأ إصدارات ISE الأخيرة بقاعدة تم إنشاؤها مسبقا تسمىWifi_Redirect_to_Guest_Login والتي تتطابق غالبا مع إحتياجاتنا. قم بتشغيل علامة الرمادي الموجودة على اليسار إلى enable.



الخطوة 3. تتطابق هذه القاعدة مع Wireless_MAB فقط وترجع سمات إعادة توجيه CWA. الآن، يمكنك إختياريا إضافة التفاف صغير وجعله يطابق SSID المحدد فقط. أختر الشرط (Wireless_MAB اعتبارا من الآن) لإظهار الشرط Studio. قم بإضافة شرط إلى اليمين واختر Radius القاموس باستخدام السمةCalled-Station-ID. اجعله يتطابق مع اسم SSID الخاص بك. قم بالتدقيق باستخدام Use الموجود بأسفل الشاشة كما هو موضح في الصورة.



الخطوة 4. تحتاج الآن إلى قاعدة ثانية، يتم تعريفها بأولوية أعلى، تطابق Guest Flow الشرط لإرجاع تفاصيل الوصول إلى الشبكة بمجرد مصادقة المستخدم على المدخل. يمكنك إستخدام القاعدة التيWifi Guest Access يتم إنشاؤها مسبقا أيضا بشكل افتراضي على إصدارات ISE الأخيرة. سيكون عليك حينئذٍ فقط تمكين القاعدة بوضع علامة خضراء على اليسار. يمكنك إرجاع PermitAccess الافتراضي أو تكوين قيود قائمة الوصول الأكثر دقة.



الخطوة 5. قم بحفظ القواعد.

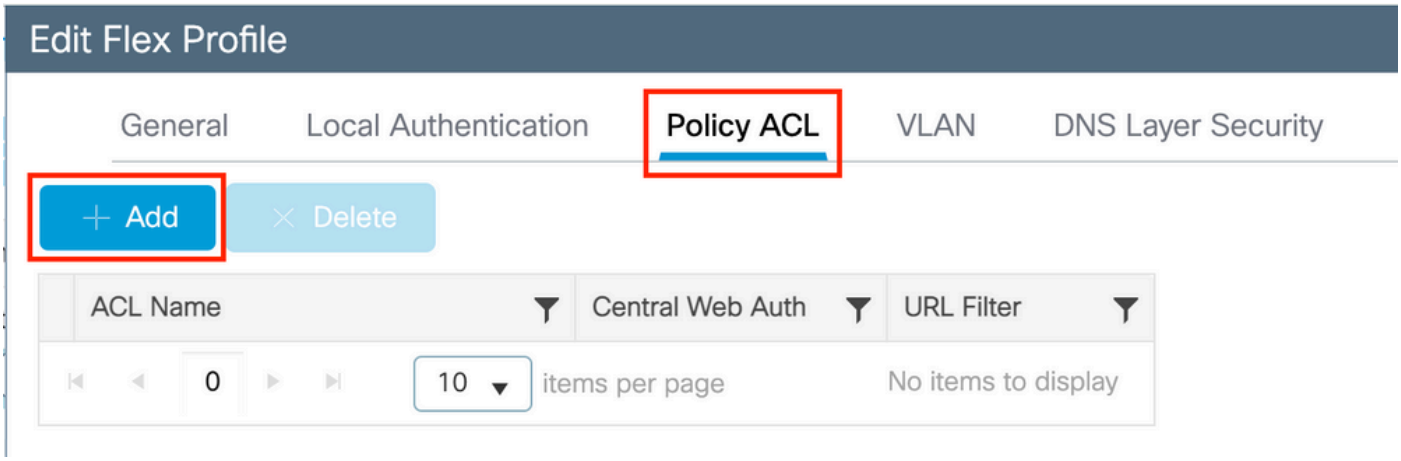
انقر Save أسفل القواعد.

نقاط الوصول إلى مجالات Flexconnect المحلية فقط

ماذا لو كانت لديك شبكات WLAN ونقاط الوصول إلى مجالات Flexconnect المحلية؟ الأقسام السابقة لا تزال صالحة. ومع ذلك، فأنت بحاجة إلى خطوة إضافية من أجل دفع قائمة التحكم في الوصول (ACL) إلاعادة التوجيه إلى نقاط الوصول (AP) مسبقا.

انتقل إلى Configuration > Tags & Profiles > Flex واختر ملف تعريف Flex. بعد ذلك، انتقل إلى Policy ACL علامة التبويب.

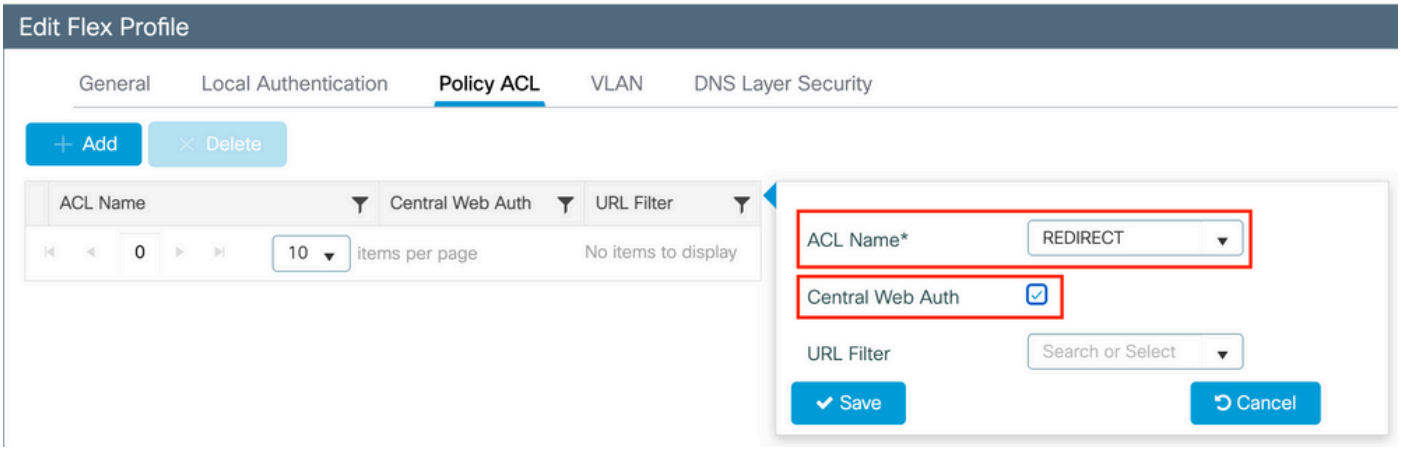
انقر Add كما هو موضح في الصورة.



أختر اسم قائمة التحكم في الوصول (ACL) المعاد توجيهه وقم بتمكين المصادقة المركزية للويب. يعكس خانة الاختيار هذه قائمة التحكم في الوصول (ACL) تلقائيا على نقطة الوصول نفسها (وذلك لأن عبارة 'deny' تعني 'ال تقم بإعادة التوجيه إلى هذا IP' على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في Cisco IOS XE. غير أن بيان "الرفض" يعني العكس على الأسوشيتد برس. لذا، فإن خانة الاختيار هذه تقوم تلقائيا بتبديل جميع التصاريح ورفضها عندما تقوم بالدفع إلى نقطة الوصول. يمكنك التحقق من ذلك باستخدام واجهة سطر أوامر show ip access list (CLI) لنقطة الوصول (AP).

ملاحظة: في سيناريو التحويل المحلي ل FlexConnect، يجب أن تشير قائمة التحكم في الوصول (ACL) بشكل خاص إلى عبارات الإرجاع (وهو أمر غير مطلوب بالضرورة في الوضع المحلي)، لذا تأكد من أن جميع قواعد قائمة التحكم في الوصول (ACL) لديك تغطي الكل من طرق حركة المرور (إلى واجهة سطر الأوامر (ISE) ومنه على سبيل المثال).

انس أن تضرب Save ثم Update and apply to the device.



الشهادات

لجعل العميل يثق بشهادة مصادقة الويب، ال يلزم تثبيت أي شهادة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) حيث إن الشهادة الوحيدة المقدمة هي شهادة ISE (التي يجب أن تكون موثوق بها من قبل العميل).

التحقق من الصحة

يمكنك استخدام هذه الأوامر للتحقق من التكوين الحالي.

<#root>

show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
show ap tag summary
show ap name <AP-name> tag detail
show wlan { summary | id | nme | all }
show wireless tag policy detailed <policy-tag-name>
show wireless profile policy detailed <policy-profile-name>

هنا الجزء ذو الصلة من تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الذي يماثل هذا المثال:

<#root>

aaa new-model !
aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE
 mac-filtering CWAauthz
 no security ft adaptive
 no security wpa
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no security wpa akm dot1x
 no shutdown
ip http server (or "webauth-http-enable" under the parameter map)
ip http secure-server

استكشاف الأخطاء وإصلاحها

قائمة التحقق

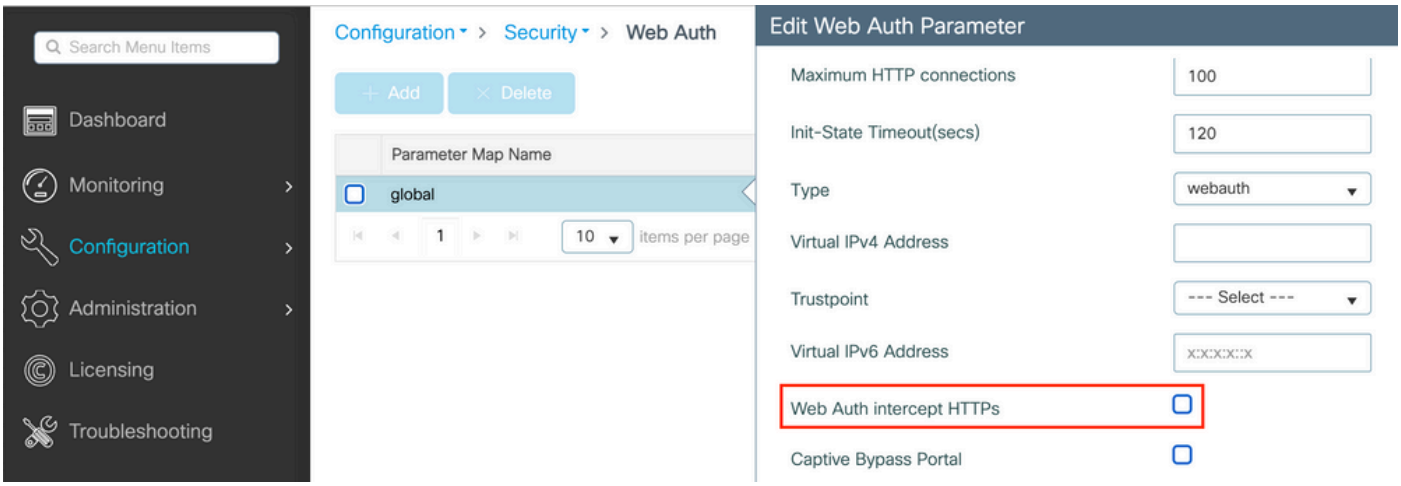
- تأكد من اتصال العميل وعنوان IP صالح وحصوله عليه.
- إذا لم تكن عملية إعادة التوجيه تلقائية، فافتح المستعرض وحاول استخدام عنوان IP عشوائي. على سبيل المثال، 10.0.0.1. إذا عملت إعادة التوجيه، فمن المحتمل أن تكون لديك مشكلة في حل DNS. تحقق من توفر خادم DNS صالح لديك عبر DHCP وهو قدرته على حل أسماء المضيف.
- تأكد من أن لديك الأمر ip http server الذي تم تكوينه لإعادة التوجيه على HTTP للعمل. يتم ربط تكوين خدم مسؤول الويب بتكوين خدم لمصادقة الويب ويجب إدراجه على المنفذ 80 لإعادة التوجيه. يمكنك إما اختيار تمكينه بشكل عام (باستخدام الأمرip http server) أو يمكنك تمكين HTTP للوحدة النمطية لمصادقة الويب فقط (باستخدام الأمر webauth-http-enable أسفل خريطة المعلمة).
- إذا لم تتم إعادة توجيهك عند محاولة الوصول إلى عنوان URL ل HTTPS وهو مطلوب، فتحقق بعد ذلك من أن لديك الأمر intercept-https-enable أسفل خريطة المعلمات:

```
<#root>
parameter-map type webauth global
 type webauth

intercept-https-enable

 trustpoint xxxxx
```

أنت يستطيع أيضا فحصت عن طريق ال gui أن أنت تتلقى الخيار Web Auth يعترض HTTPS' فحصت في المعلمة خريطة:



دعم منفذ الخدمة ل RADIUS

تحتوي وحدة التحكم اللاسلكية Cisco Catalyst 9800 Series على منفذ خدمة يشار إليه باسم GigabitEthernet 0المنفذ. اعتبارا من الإصدار 17.6.1، يتم دعم RADIUS (الذي يتضمن CoA) من خلال هذا المنفذ.

إذا كنت ترغب في إستخدام منفذ الخدمة ل RADIUS، فأنت بحاجة إلى هذا التكوين:

<#root>

aaa server radius dynamic-author
client 10.48.39.28

```
vrf Mgmt-intf
 server-key cisco123

interface GigabitEthernet0


vrf forwarding Mgmt-intf


 ip address x.x.x.x x.x.x.x

!if using aaa group server:
aaa group server radius group-name
 server name nicoISE

 ip vrf forwarding Mgmt-intf


 ip radius source-interface GigabitEthernet0
```

تجميع تصحيح الأخطاء

يوفر WLC 9800 إمكانات التتبع الدائمة. وهذا يضمن تسجيل جميع الأخطاء المتعلقة باتصال العميل والتحذيرات ورسائل

مستوى الإشعار بشكل مستمر، كما يمكنك عرض السجلات الخاصة بحادثة أو حالة فشل بعد حدوثها.

ملاحظة: يمكنك الرجوع بضع ساعات إلى عدة أيام في السجلات ولكنها تعتمد على حجم السجلات التي تم إنشاؤها.

عرض المسارات التي تم تجميعها بواسطة 9800 WLC بشكل افتراضي، يمكنك الاتصال عبر SSH/Telnet بـ 9800 WLC وإجراء هذه الخطوات (تأكد من تسجيل الجلسة إلى ملف نصي).

الخطوة 1. فحص الـ WLC حالي وقت ذلك أنت يستطيع تتبعت السجل في الوقت back to عندما الإصدار حدث.

```
<#root>

# show clock
```

الخطوة 2. قم بتجميع syslog من المخزن المؤقت لـ WLC أو syslog الخارجي كما هو محدد بواسطة تكوين النظام. يوفر ذلك طريقة عرض سريعة لسلامة النظام والأخطاء إن وجدت.

```
<#root>

# show logging
```

الخطوة 3. تحقق إذا تم تمكين أي شروط تصحيح أخطاء.

```
<#root>

# show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d
```

ملاحظة: إذا رأيت أي شرط مدرج في القائمة، فهذا يعني أن التتبع يتم تسجيله إلى مستوى تصحيح الأخطاء لجميع العمليات التي تواجه الشروط الممكنة (عنوان IP أو عنوان MAC). هذا يزيد من حجم السجلات. لذلك، يوصى بمسح جميع الشروط عند الانتهاء من تصحيح الأخطاء بشكل فعال.

الخطوة 4. باستثناء أي شرط تم إدراجه في الخطوة 3.، قم بتجميع آثار مستوى الإشعار تحت الاختبار لم يتم إدراج عنوان MAC تحت افتراض أن عنوان MAC المحدد هو عنوان MAC الموجود.

```
<#root>
```

show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>

يمكنك إما عرض المحتوى على الجلسة أو يمكنك نسخ الملف إلى خادم TFTP خارجي.

<#root>

more bootflash:always-on-<FILENAME.txt>
or
copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>

التصحيح الشرطي والتتبع النشط اللاسلكي

إذا لم تمنحك المسارات الدائمة معلومات كافية لتحديد مشغل المشكلة قيد التحقيق، يمكنك تمكين تصحيح الأخطاء مع طوابع التاريخ والوقت تتبع Radio Active (RA)، الذي يوفر تتبع مستوى تصحيح الأخطاء لجميع العمليات التي تتفاعل مع الشرط المحدد (عنوان MAC للعميل في هذه الحالة). لتمكين تصحيح الأخطاء المشروط، استمر في هذه الخطوات.

الخطوة 5. تأكد من عدم تمكين شروط تصحيح الأخطاء.

<#root>

clear platform condition all

الخطوة 6. قم بتمكين شرط تصحيح الأخطاء لعنوان MAC للعميل اللاسلكي الذي تريد مراقبته.

أدبت هذه الأوامر بمراقبة عنوان mac المتوفر لمدة 30 دقيقة (1800 ثانية). يمكنك زيادة الوقت اختياريًا حتى 2085978494 ثانية.

<#root>

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}

ملاحظة: من أجل مراقبة أكثر من عميل واحد في كل مرة، قم بتشغيل الأمر debug wireless mac<aaaa.bbbb.cccc> لكل عنوان

MAC.

ملاحظة: ال ترى إخراج نشاط العميل على جلسة العمل الطرفية، حيث يتم تخزين كل شيء مؤقتا داخليا لعرضه لاحقا.

الخطوة 7'. قم بإعادة إنتاج المشكلة أو السلوك الذي تريد مراقبته.

الخطوة 8. قم بإيقاف تصحيح الأخطاء إذا تم نسخ المشكلة قبل انتهاء وقت المراقبة الافتراضي أو المكون.

<#root>

no debug wireless mac <aaaa.bbbb.cccc>

ما إن انقضى وقت المدرب أو ال debug لاسلكي يكون، ال 9800 WLC دلي مبرد محلي مع الإسم:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

الخطوة 9. تجميع ملف نشاط عنوان MAC. يمكنك إما نسخ ra trace .logالمخرجات إلى خادم خارجي أو عرضها مباشرة على الشاشة.

التحقق من اسم ملف تتبع مسار RA.

<#root>

dir bootflash: | inc ra_trace

نسخ الملف إلى خادم خارجي:

<#root>

copy bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d/ra-FILENAME.txt

عرض المحتوى:

<#root>

more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

الخطوة 10. إذا كان السبب الجذري الا يزال غير واضح، فقم بجمع السجلات الداخلية التي تعد طريقة عرض توضيحية أكبر للسجلات على مستوى تصحيح الأخطاء. الا تحتاج إلى تصحيح أخطاء العميل مرة أخرى حيث إننا نلقي نظرة أكثر تفصيلا على سجلات تصحيح الأخطاء التي تم تجميعها بالفعل وتخزينها داخليا.

<#root>

show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt

ملاحظة: ينتج هذا الأمر آثارا لجميع مستويات السجل لجميع العمليات وهو كبير الحجم إلى حد ما. أشرك cisco TAC للمساعدة في التحليل خلال هذه المسارات.

يمكنك إما نسخ ra-internal-FILENAME.txtالمخرجات إلى خادم خارجي أو عرضها مباشرة على الشاشة.

نسخ الملف إلى خادم خارجي:

<#root>

copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt

عرض المحتوى:

<#root>

more bootflash:ra-internal-<FILENAME>.txt

الخطوة 11. قم بإزالة شروط تصحيح الأخطاء.

<#root>

clear platform condition all

ملاحظة: تأكد من إزالة شروط تصحيح الأخطاء دائما بعد جلسة أستكشاف الأخطاء وإصلاحها.

الأمثلة

إذا لم تكن نتيجة المصادقة كما تتوقع، فمن المهم الانتقال إلى صفحة ISEOperations > Live logs والحصول على تفاصيل نتيجة المصادقة.

تعرض عليك مع سبب الفشل (إذا كان هناك فشل) وجميع سمات Radius التي تلقاها ISE.

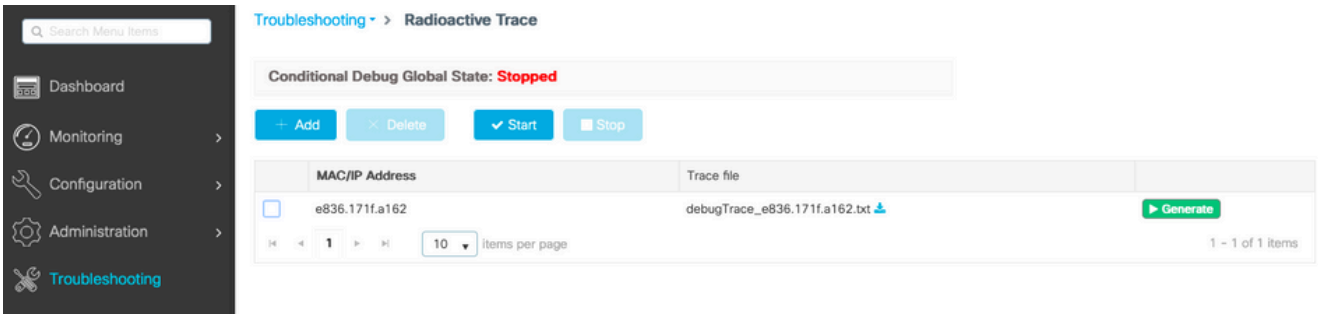
في المثال التالي، رفض محرك خدمات كشف الهوية (ISE) المصادقة لأنه لا توجد قاعدة تفويض مطابقة. وذلك لأنك ترى سمة معرف المحطة المستدعى مرسلة كاسم SSID ملحق بعنوان AP MAC، بينما يكون التخويل مطابقا تماما لاسم SSID. يتم إصلاحها مع تغيير هذه القاعدة إلى "يحتوي" بدلا من "يساوي".

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule-results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

15048 Queried PIP - Radius.NAS-Port-Type
15048 Queried PIP - Network Access.UserName
15048 Queried PIP - IdentityGroup.Name (2 times)
15048 Queried PIP - EndPoints.LogicalProfile
15048 Queried PIP - Radius.Called-Station-ID
15048 Queried PIP - Network Access.AuthenticationStatus
15016 Selected Authorization Profile - DenyAccess
15039 Rejected per authorization profile
11003 Returned RADIUS Access-Reject

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicoise26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifier	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-iif-id=3003124185, vlan-id=1468, cisco-wlan-ssid=cwa-ssid,



في هذه الحالة، تكمن المشكلة في حقيقة أنك قمت بعمل خطأ إملائي عندما قمت بإنشاء اسم قائمة التحكم في الوصول ووه ال يطابق اسم قائمة التحكم في الوصول الذي تم إرجاعه من قبل ISE أو أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يشتكي من عدم وجود قائمة التحكم في الوصول (ACL) كتلك التي طلبها ISE:

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

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).