تكوين RADIUS &؛ TACACS+ لواجهة المستخدم الرسومية (GUI) و AMP؛ مصادقة واجهة سطر الأوامر (CLI) على 9800 WLCs

المحتويات

المقدمة

يصف هذه الوثيقة كيفية أن يشكل مادة حفازة 9800 لـ RADIUS أو TACACS+ صحة هوية خارجية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- نموذج تكوين Catalyst Wireless 9800
- مفاهيم المصادقة والتفويض والمحاسبة (AAA) و RADIUS و+TACACS

المكونات المستخدمة

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

- C9800-CL الإصدار 17.9.2
- ISE 3.2.0

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

معلومات أساسية

عندما يحاول مستعمل أن ينفذ الـ CLI أو الـ gui من الـ WLC، هو حضضت أن يدخل username وكلمة. وبشكل افتراضي، تتم مقارنة بيانات الاعتماد هذه مع قاعدة البيانات المحلية للمستخدمين، الموجودة على الجهاز نفسه. بدلاً من ذلك، يمكن توجيه عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمقارنة بيانات اعتماد الإدخال مقابل خادم AAA بعيد: يمكن أن تتحدث عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مع الخادم باستخدام RADIUS أو TACACS+.

التكوين

في هذا المثال، تم تكوين نوعين من المستخدمين على خادم AAA (ISE)، على التوالي adminuser، وhelpdeskuser. هؤلاء المستخدمون جزء من admin-group المجموعات و helpdesk-group المجموعات على التوالي. من المتوقع منح المستخدم adminuser، وهو جزء من admin-group عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، حق الوصول الكامل إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). من ناحية أخرى، helpdeskuser، جزء من helpdesk-group الـ، يعني أن يتم منح امتيازات المراقبة إلى WLC. وبالتالي، الـ وصول إلى التكوين فقط.

تقوم هذه المقالة بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وما يعادل ISE لمصادقة RADIUS، ثم تقوم بتنفيذ الأمر نفسه الخاص بـ TACACS+.

قيود المستخدم للقراءة فقط

عند إستخدام TACACS+ أو RADIUS لمصادقة 9800 WebUI، تكون هذه القيود موجودة:

- يتواجد المستخدمون الذين لديهم مستوى الامتياز 0 ولكن ليس لديهم حق الوصول إلى واجهة المستخدم الرسومية
- يمكن للمستخدمين الذين لديهم امتيازات من 1 إلى 14 فقط عرض علامة التبويب شاشة" (وهذا يعادل مستوى الامتياز لمستخدم تتم مصادقته محليا للقراءة فقط)
- المستخدمون الذين لديهم مستوى الامتياز 15 لديهم حق الوصول الكامل
- الـ يتم دعم المستخدمين الذين لديهم مستوى الامتياز 15 ومجموعة الأوامر التي تتيح أوامر معينة فقط. الـ يزال

إمكان المستخدم تنفيذ تغييرات التكوين من خلال WebUI

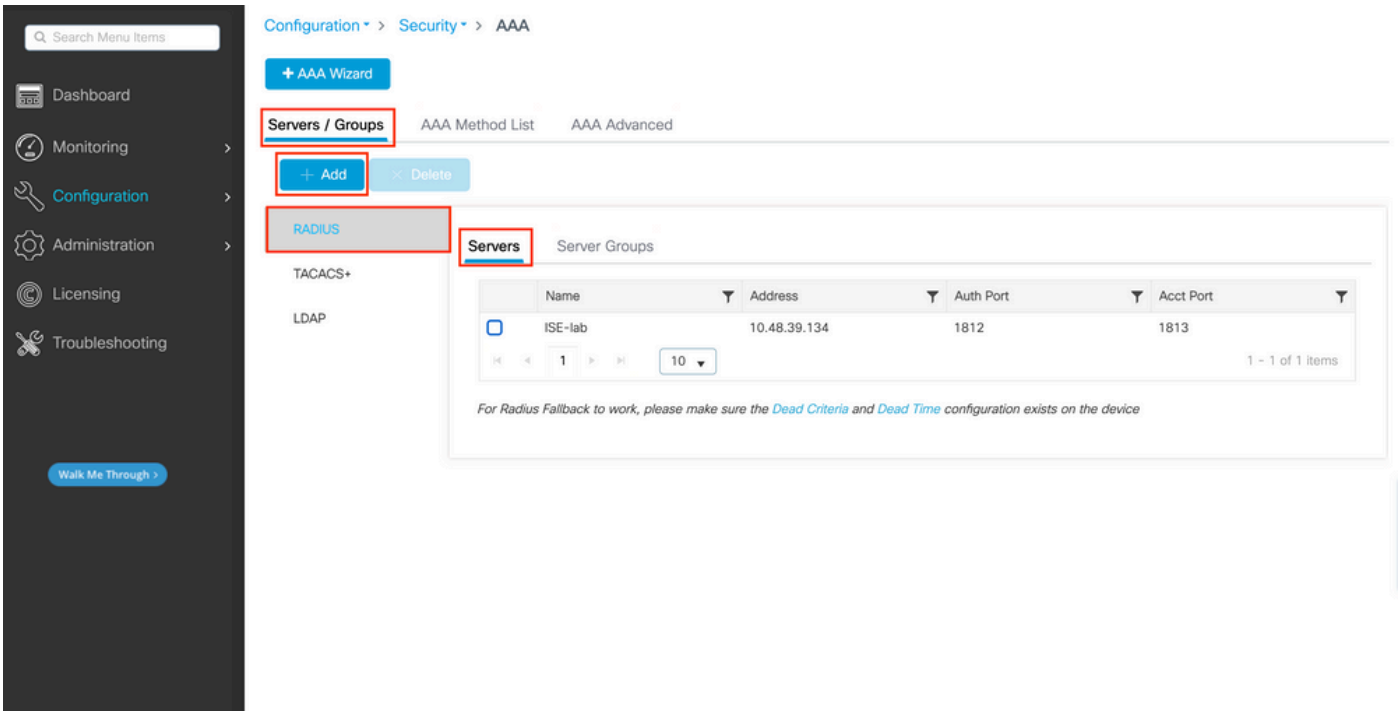
لا يمكن تغيير هذه الاعتبارات أو تعديلها.

تكوين مصادقة RADIUS ل WLC

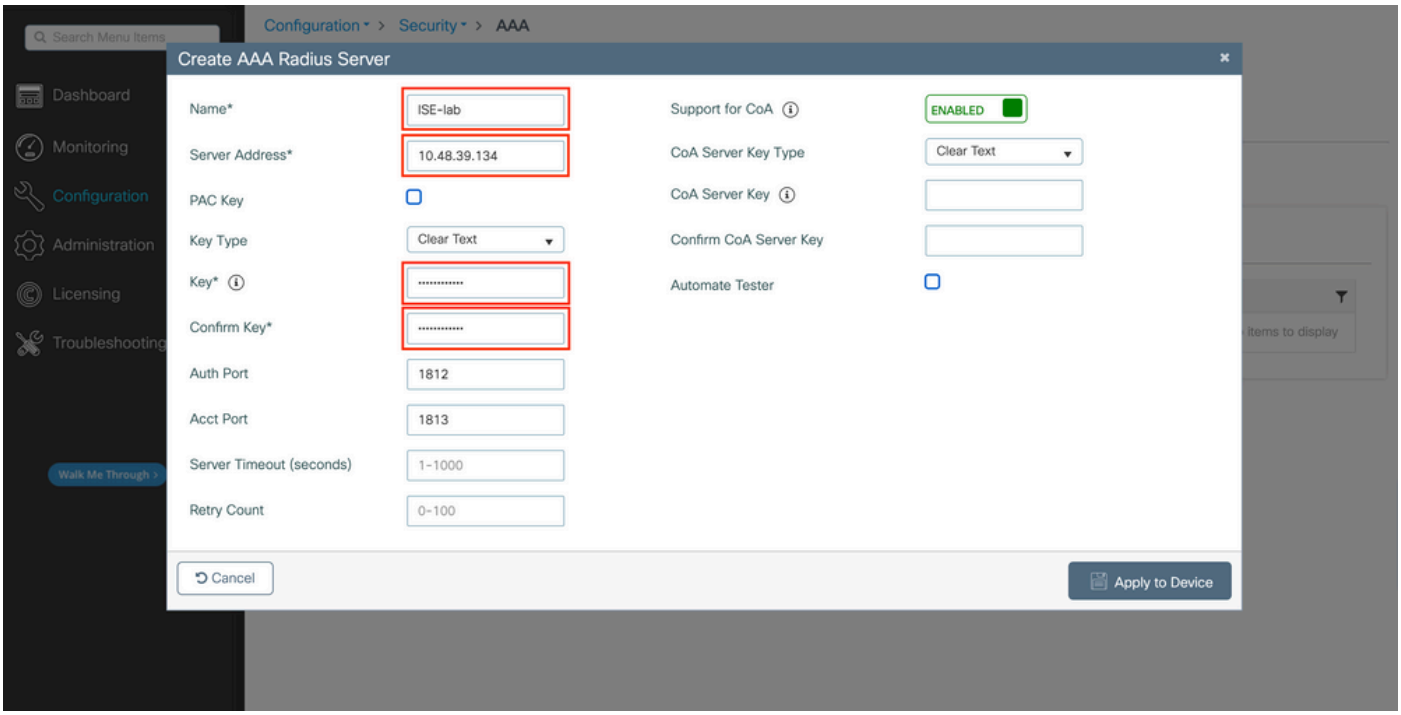
الخطوة 1. إعلان خادم RADIUS.

من واجهة المستخدم الرسومية:

أولا، قم بإنشاء خادم ISE RADIUS على WLC. يمكن القيام بذلك من علامة التبويب Servers/Groups > RADIUS > Servers من صفحة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لواجهة المستخدم الرسومية (GUI) التي يمكن الوصول إليها في https://<WLC-IP>/webui/#/aaa، وأ إذا قمت بالانتقال إلى Configuration > Security > AAA، كما هو موضح في هذه الصورة.



لإضافة خادم RADIUS على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر زر إضافة المؤطر باللأحمر في الصورة. يؤدي هذا إلى فتح النافذة المنبثقة المعروضة في لقطة الشاشة.



في هذه النافذة المنبثقة، يجب عليك توفير:

- اسم الخادم (لاحظ أنه لا يجب أن يطابق اسم نظام ISE)
- عنوان IP للخادم
- السر المشترك بين WLC وخادم RADIUS

يمكن تكوين معلمات أخرى، مثل المنافذ المستخدمة للمصادقة والمحاسبة، ولكن هذه ليست إلزامية وتترك كإعداد افتراضي لهذا المستند.

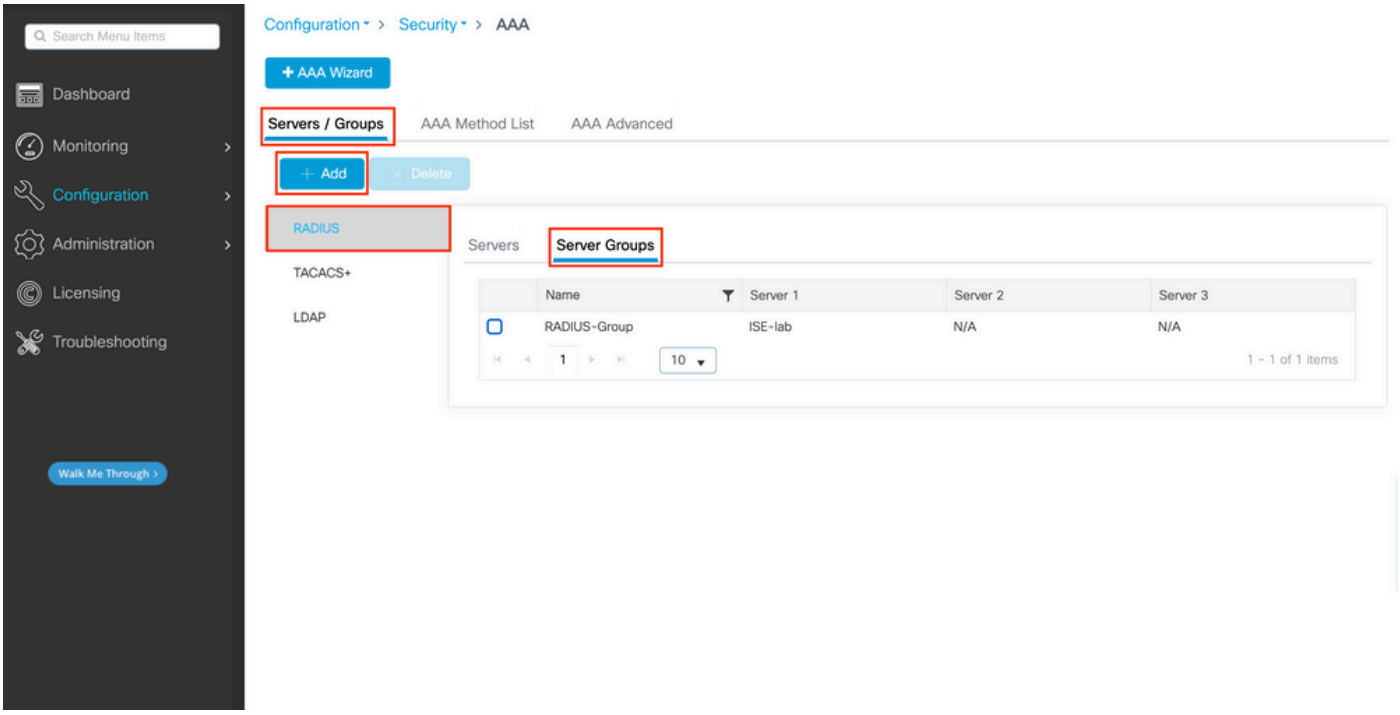
من واجهة سطر الأوامر:

```
<#root>

WLC-9800(config)#radius server

ISE-lab

 WLC-9800(config-radius-server)#address ipv4

10.48.39.134

auth-port 1812 acct-port 1813
WLC-9800(config-radius-server)#key

Cisco123
```

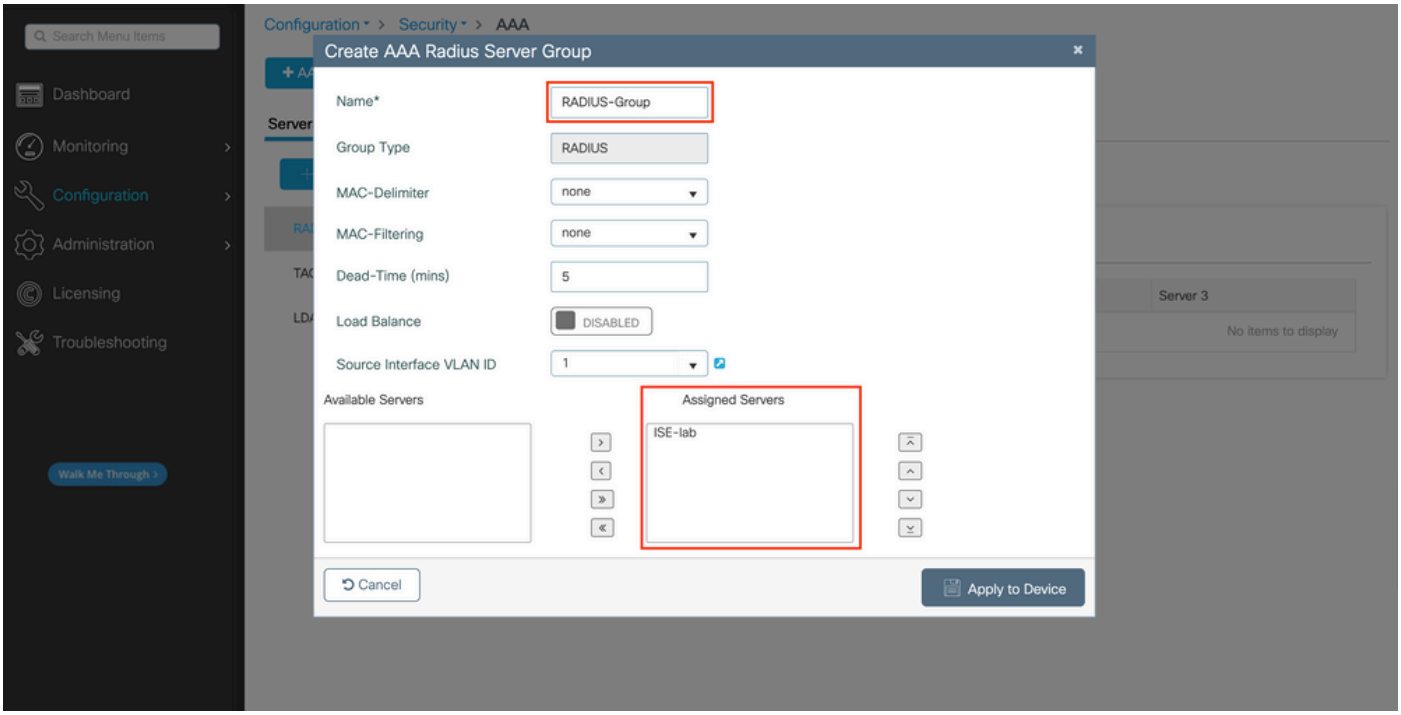
الخطوة 2. تخطيط خادم RADIUS إلى مجموعة خوادم.

من واجهة المستخدم الرسومية:

في حالة وجود خوادم RADIUS متعددة يمكن استخدامها للمصادقة، يوصى بتعيين جميع هذه الخوادم إلى مجموعة الخوادم نفسها. تتم وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بتوزيع الأحمال بين عمليات المصادقة المختلفة بين الخوادم في مجموعة الخوادم. يتم تكوين مجموعات خوادم RADIUS من Servers/Groups > RADIUS > Server Groups علامة التبويب من نفس صفحة واجهة المستخدم الرسومية (GUI) المذكورة في الخطوة 1.، كما هو موضح في الصورة.



بالنسبة لإنشاء الخادم، تظهر نافذة منبثقة عند النقر فوق الزر إضافة (الإطار في الصورة السابقة)، والذي يتم تصفيفه هنا.



في القائمة المنبثقة، قم بتوفير اسم للمجموعة، ثم قم بنقل الخوادم المطلوبة إلى قائمة الخوادم المعينة.

من واجهة سطر الأوامر:

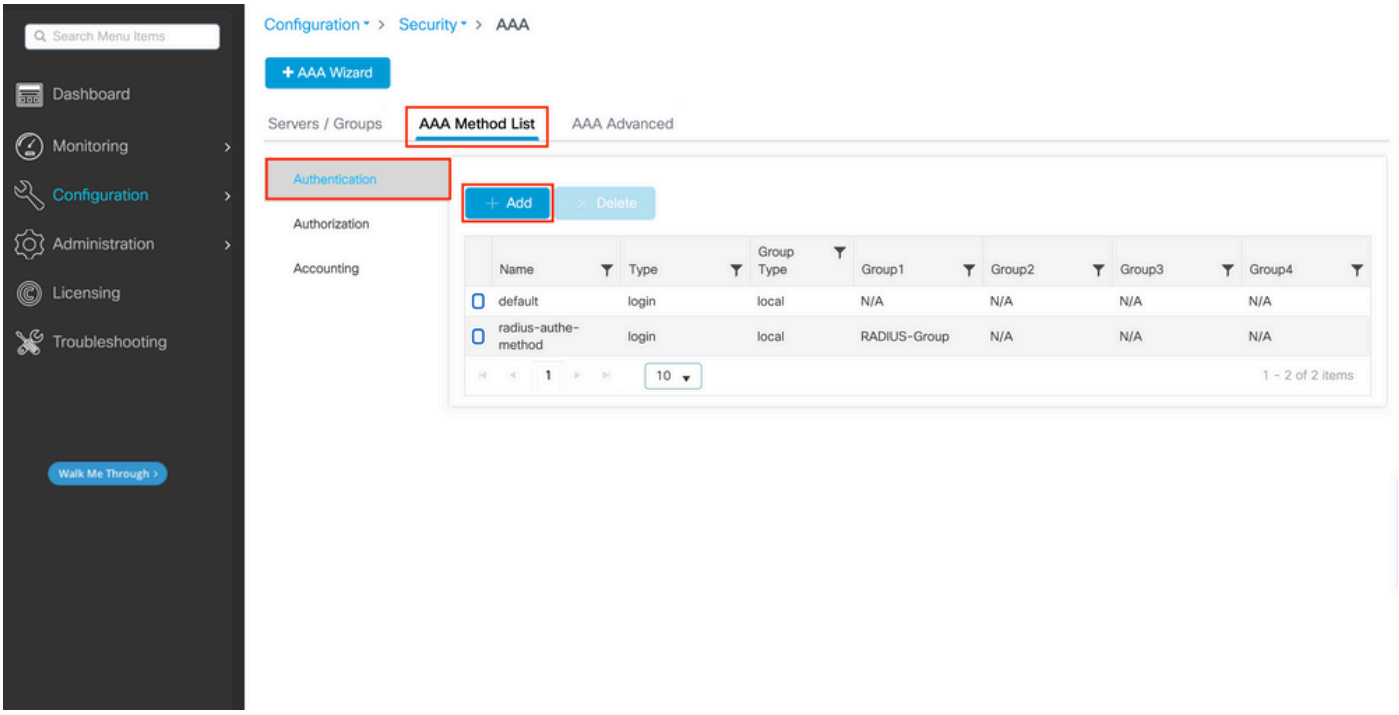
```
<#root>

WLC-9800(config)# aaa group server radius

RADIUS-Group

WLC-9800(config-sg-radius)# server name

ISE-lab
```

-

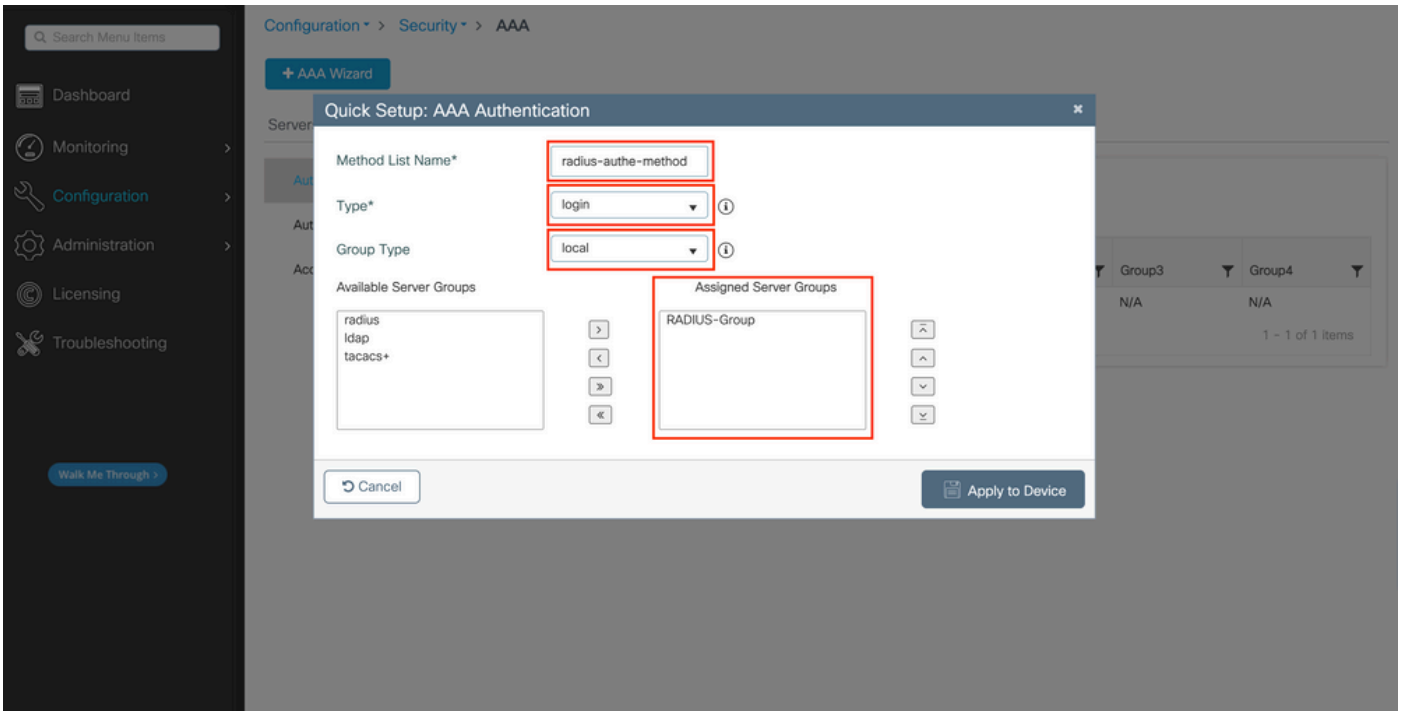
الخطوة 3. قم بإنشاء طريقة تسجيل دخول مصادقة AAA تشير إلى مجموعة خوادم RADIUS.

من واجهة المستخدم الرسومية:

بعد من صفحةhttps://<WLC-IP>/webui/#/aaa واجهة المستخدم الرسومية، انتقل إلى علامة التبويبAAA Method List > Authentication وأنشئ طريقة مصادقة كما هو موضح في هذه الصورة.



كما هو معتاد، عندما تستخدم زر إضافة لإنشاء طريقة مصادقة، تظهر نافذة منبثقة للتكوين، مماثلة للنافذة الموضحة في هذه الصورة.



في هذه النافذة المنبثقة، قم بتوفير اسم للأسلوب. أختر Type كسجل دخول، وقم بإضافة خادم المجموعة الذي تم إنشاؤه في الخطوة السابقة إلى Assigned Server Groups القائمة. فيما يتعلق بحقل نوع المجموعة، يمكن إجراء العديد من التكوينات.

- إذا أخترت "نوع المجموعة" محليا، يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) أولا مما إذا كانت بيانات اعتماد المستخدم موجودة محليا، ثم يعود مرة أخرى إلى مجموعة الخوادم.
-

إذا أخترت نوع المجموعة كمجموعة ولم تقم بالتحقق من الخيار رجوع إلى محلي، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يتحقق فقط من مسوغات المستخدم مقابل مجموعة الخوادم.

- إذا أخترت "نوع المجموعة" كمجموعة وفحصت الخيار "إحتياطي إلى محلي"، يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من بيانات اعتماد المستخدم مقابل مجموعة الخوادم ويستعلم عن قاعدة البيانات المحلية فقط إذا لم يستجب الخادم. إذا قام الخادم بإرسال رفض، ستتم مصادقة المستخدم، حتى وإن كان يمكن أن يكون موجودا على قاعدة البيانات المحلية.

من واجهة سطر الأوامر:

إذا كنت تريد التحقق من بيانات اعتماد المستخدم مع مجموعة خوادم فقط إذا لم يتم العثور عليها محليا أولا، أستخدم:

```
<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

 local group

RADIUS-Group
```

إذا كنت تريد التحقق من بيانات اعتماد المستخدم مع مجموعة خوادم فقط، أستخدم:

```
<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method
```

group

RADIUS-Group

إذا كنت تريد التحقق من بيانات اعتماد المستخدم مع مجموعة خوادم وإذا لم يستجب هذا الأخير مع الإدخال المحلي، فاستخدم:

<#root>

WLC-9800(config)#aaa authentication login

radius-authe-method

group

RADIUS-Group

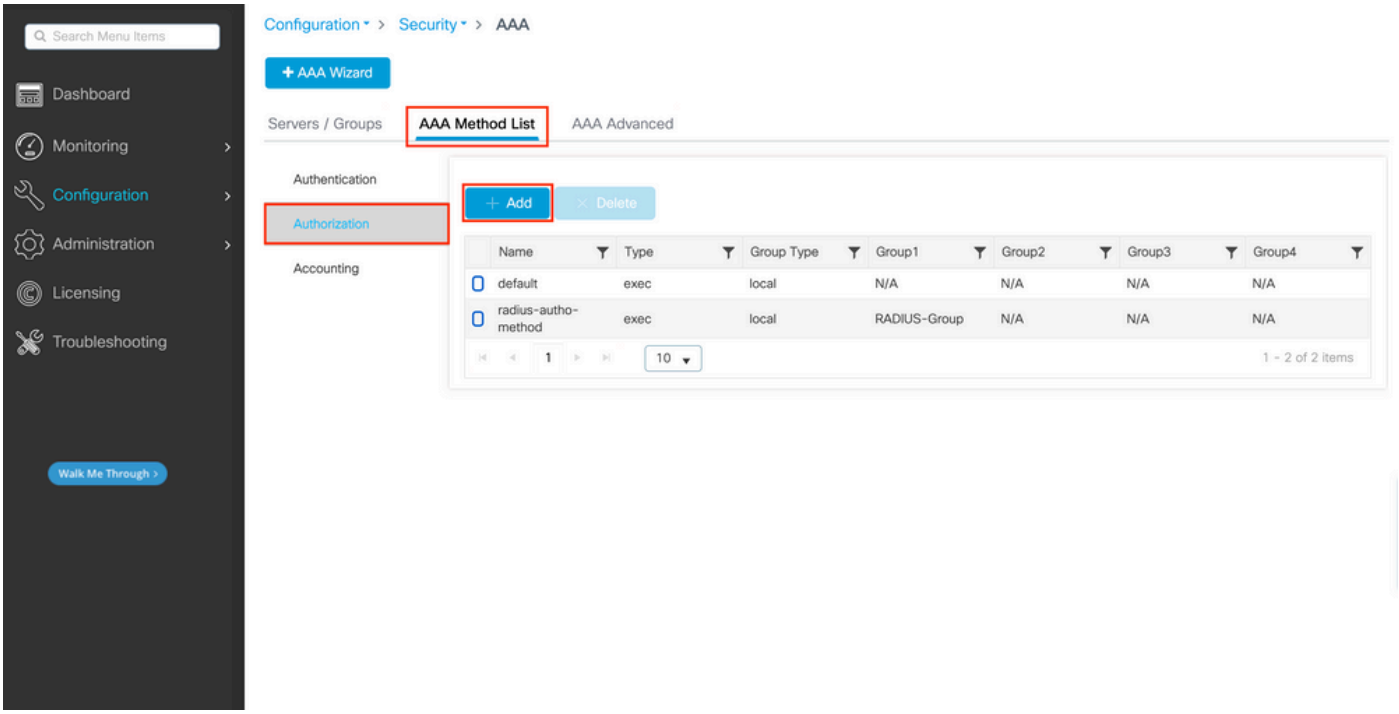
local

في هذا المثال، هناك بعض المستخدمين الذين تم إنشاؤهم محليا فقط، وبعض المستخدمين فقط على خادم ISE، وبالتالي، يستخدمون الخيار الأول.

الخطوة 4. قم بإنشاء طريقة EXEC لتفويض AAA تشير إلى مجموعة خوادم RADIUS.

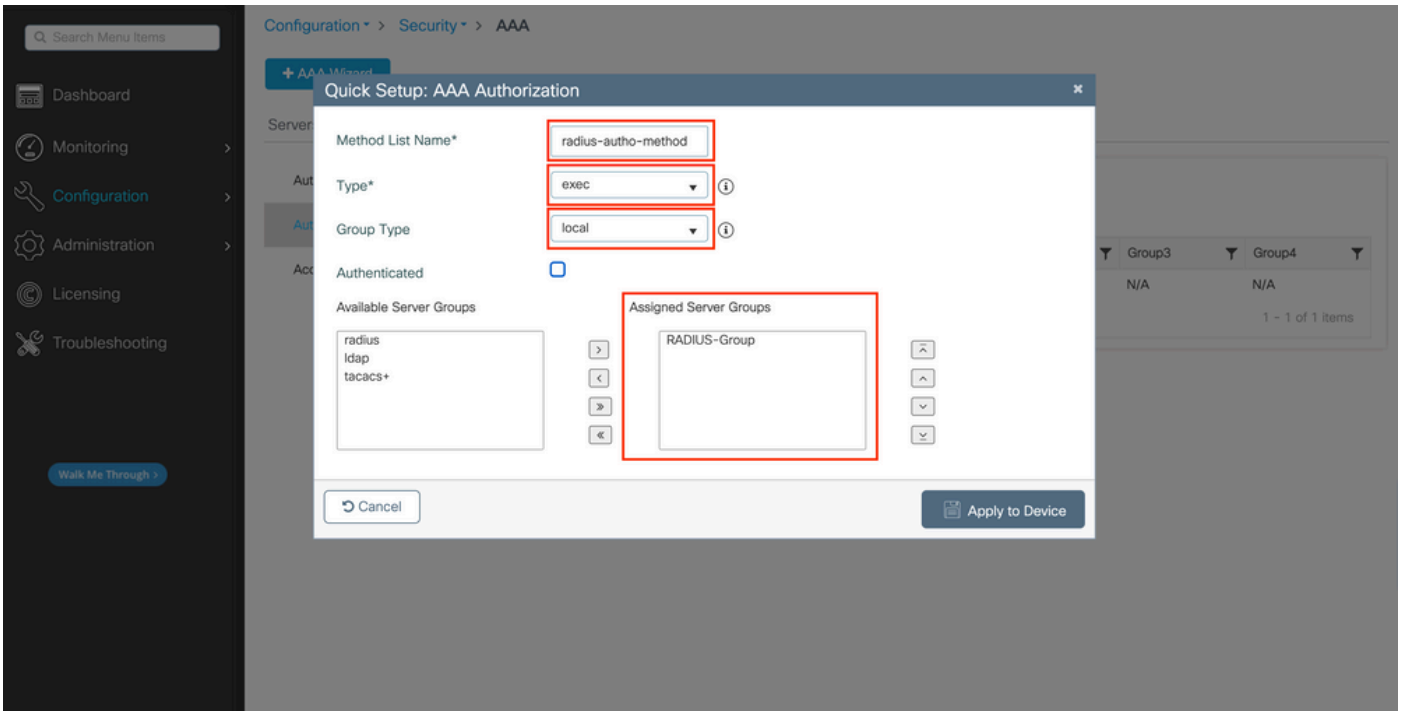
من واجهة المستخدم الرسومية:

يجب أيضا تخويل المستخدم حتى يتم منحه حق الوصول. بعد من GUI Page Configuration > Security > AAA، انتقل إلى AAA Method List > Authorization علامة التبويب، وقم بإنشاء طريقة اعتماد كما هو موضح في هذه الصورة.



إنشاء أسلوب التخويل

يظهر تكوين أسلوب تخويل مطابق مماثل للأسلوب الذي تم تصويره عند إضافة أسلوب جديد باستخدام الزر إضافة.



في هذا التكوين المطابق، قم بتوفير اسم طريقة التخويل، واختر النوع باسم exec، واستخدم نفس الترتيب لنوع المجموعة كالمستخدم طريقة المصادقة في الخطوة 3.

<u>من واجهة سطر الأوامر:</u>

أما بالنسبة لطريقة المصادقة، فيتم تعيين التخويل أولا للتحقق من المستخدمين مقابل الإدخالات المحلية، ثم مقابل الإدخالات في مجموعة خوادم.

WLC-9800(config)#aaa authorization exec

radius-autho-method

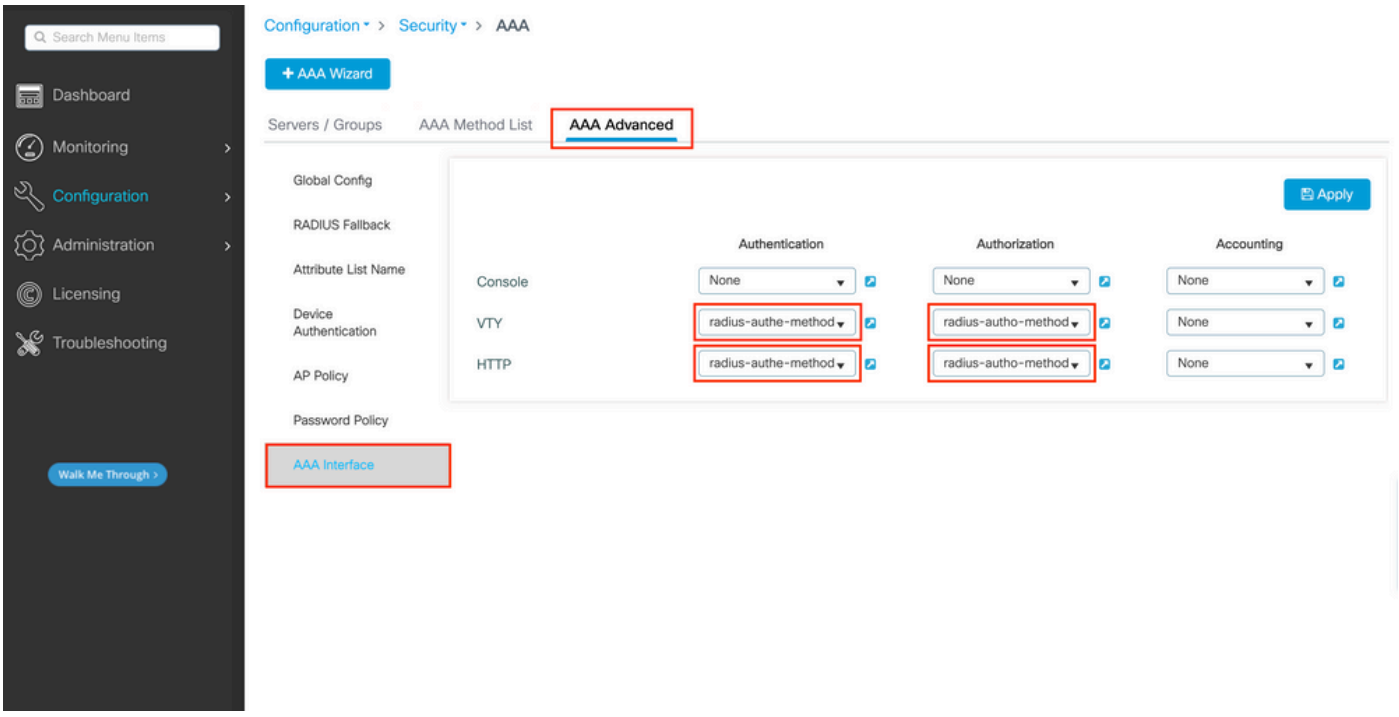
local group

RADIUS-Group

الخطوة 5. قم بتعيين الطرق إلى تكوينات HTTP وإلى خطوط vty المستخدمة لـ Telnet/SSH.

من واجهة المستخدم الرسومية:

يمكن استخدام طرق المصادقة والتفويض التي تم إنشاؤها لاتصال مستخدم HTTP و/أو Telnet/SSH، والتي يمكن تكوينها من صفحة GUI WLC التي يمكن الوصول إليها في AAA Advanced > AAA Interface علامة التبويب التي ال تزال من هذه الصورة: كما هو موضح في https://<WLC-IP>/webui/#/aaa،



CLI لمصادقة واجهة المستخدم الرسومية:

<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

radius-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

radius-autho-method

CLI لمصادقة Telnet/SSH:

<#root>

WLC-9800(config)#line vty 0 15 WLC-9800(config-line)#login authentication

radius-authe-method

WLC-9800(config-line)#authorization exec

radius-autho-method

لاحظ أنه عند إجراء التغييرات على تكوينات HTTP، فمن الأفضل إعادة تشغيل خدمات HTTP و HTTPS. يمكن تحقيق ذلك باستخدام الأوامر التالية:

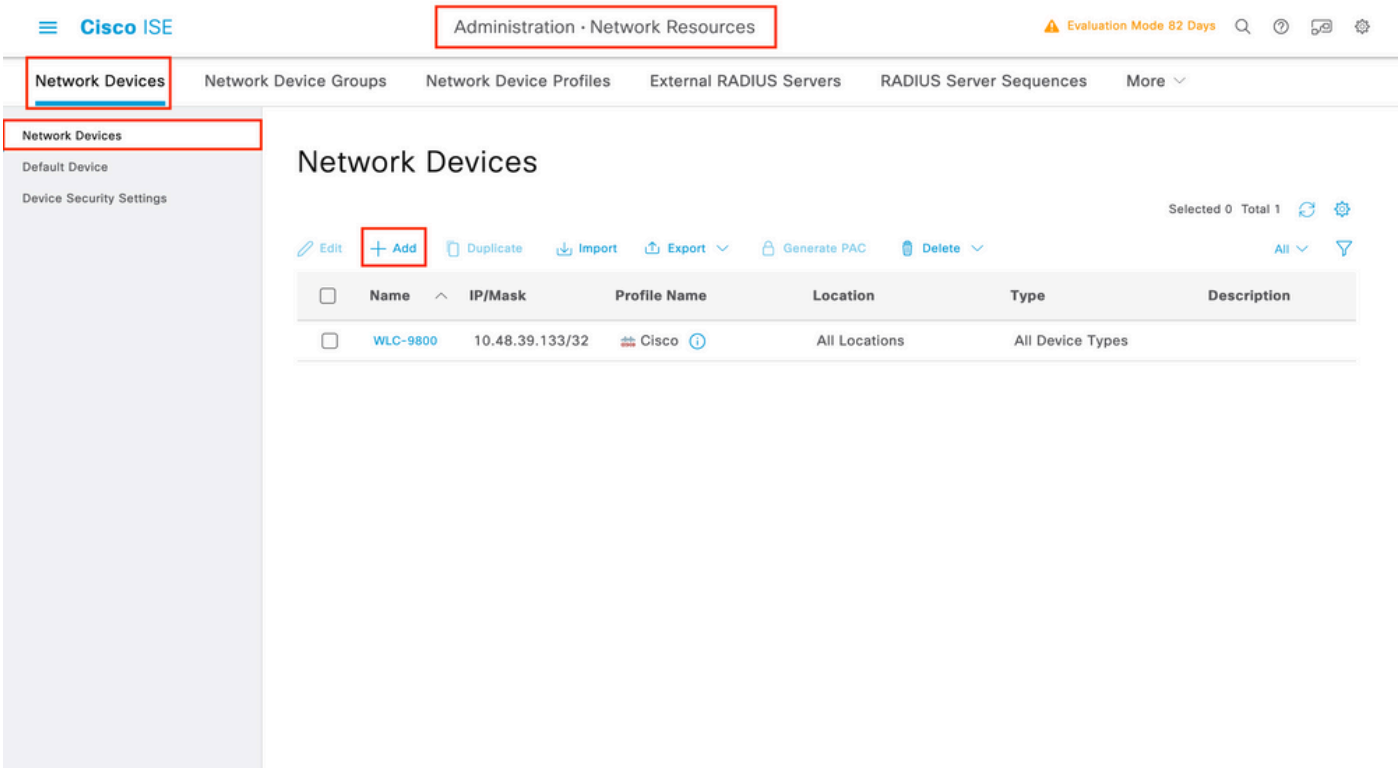
```
WLC-9800(config)#no ip http server WLC-9800(config)#no ip http secure-server WLC-9800(config)#ip http server WLC-9800(config)#ip http secure-serv
```

تكوين ISE ل RADIUS

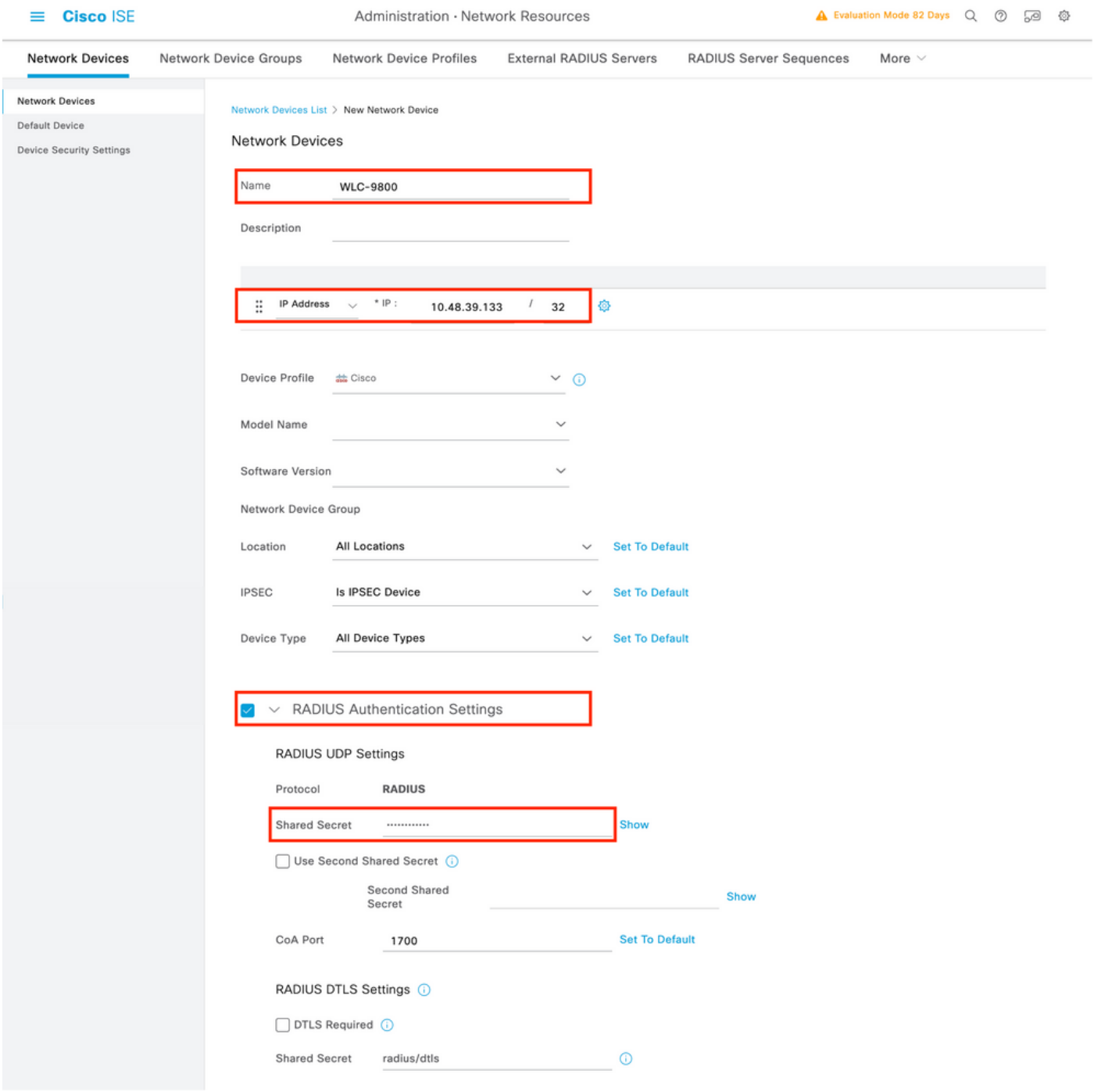
الخطوة 1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كجهاز شبكة ل RADIUS.

<u>من واجهة المستخدم الرسومية:</u>

لتوضيح استخدام عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في القسم السابق كجهاز شبكة ل RADIUS في ISE، انتقل إلى Administration > Network Ressources > Network Devices علامة التبويب أجهزة الشبكة وافتحها، كما هو موضح في الصورة التالية.



لإضافة جهاز شبكة، أستخدم الزر إضافة الذي يفتح نموذج تكوين جهاز الشبكة الجديد.

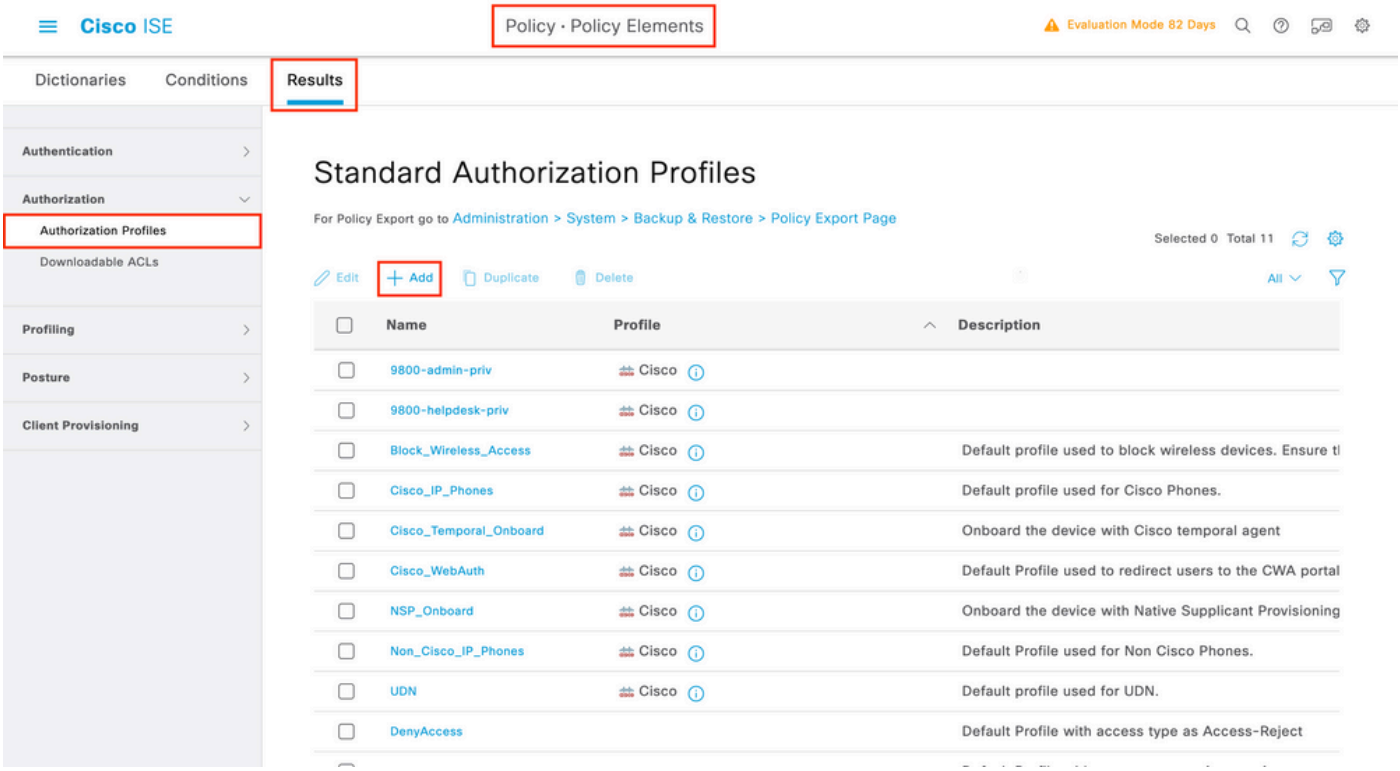


في الإطار الجديد، قم بتوفير اسم لجهاز الشبكة، وإضافة عنوان IP الخاص به. أخترت ال RADIUS مصادقة عملية إعداد وشكلت ال نفسه RADIUS مشترك سر بما أن الواحد يستعمل على ال WLC.

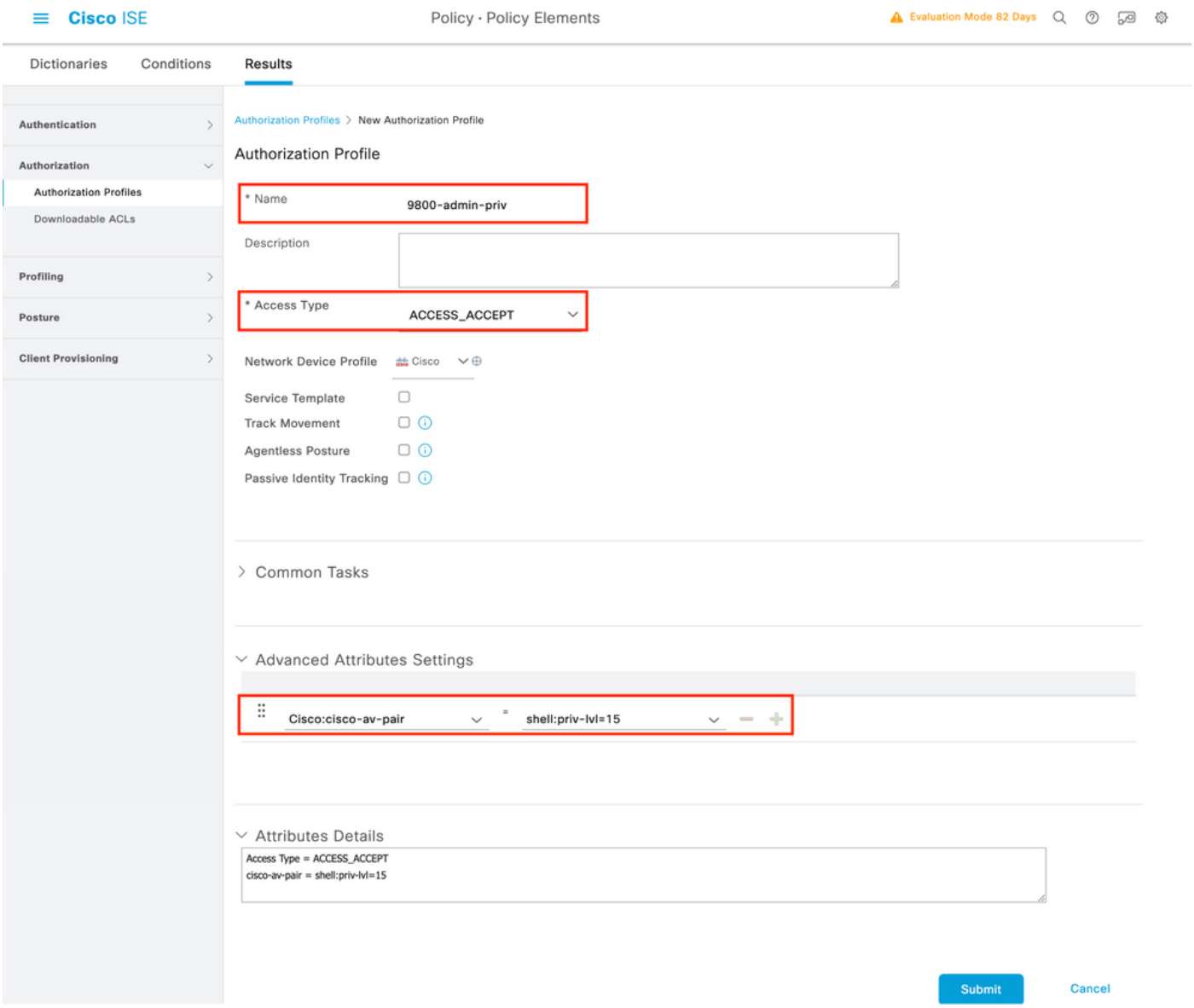
الخطوة 2. قم بإنشاء نتيجة تخويل، لإرجاع المتياز.

<u>من واجهة المستخدم الرسومية:</u>

للحصول على حقوق الوصول للمسؤول، يلزمadminuser أن يكون مستوى المتياز 15، والذي يسمح بالوصول إلى طبقة مطالبة exec. من ناحية أخرى، الhelpdeskuser يحتاج الأمر إلى وصول موجه أوامر EXEC إلى Shell وبالتالي يمكن تعيينه بمستوى امتياز أقل من 15. لتعيين مستوى المتياز المناسب للمستخدمين، يمكن إستخدام ملفات تعريف التخويل. يمكن تكوين هذه العناصر من ISE GUI Page Policy > Policy Elements > Results، أسفل علامة التبويب Authorization > Authorization Profiles الموضحة في الصورة التالية.



لتكوين ملف تعريف تخويل جديد، أستخدم الزر إضافة الذي يفتح نموذج تكوين ملف تعريف التخويل الجديد. يجب أن يبدو هذا النموذج على وجه الخصوص لتكوين ملف التعريف الذي يتم تعيينه adminuser.



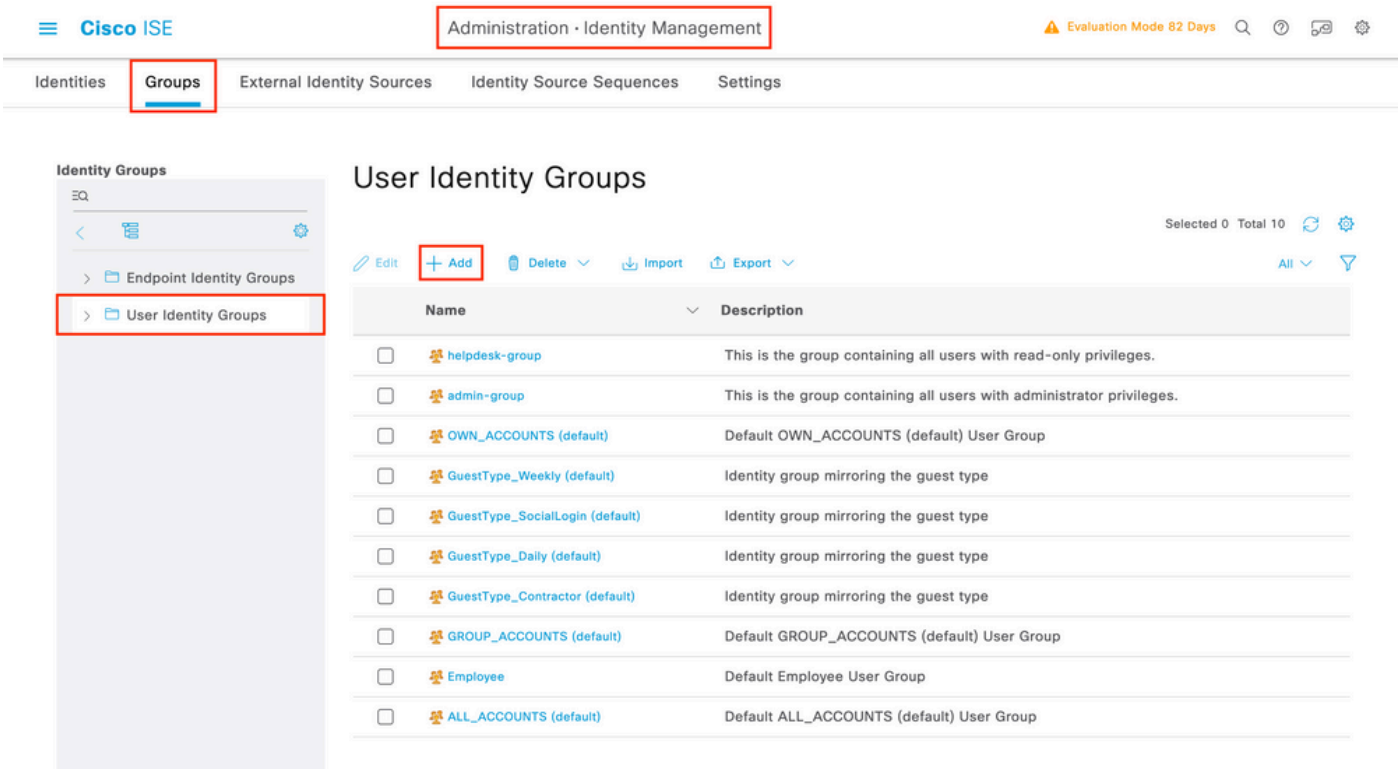
عرض التكوين مستوى امتياز منح 15 لأي مستخدم مرتبط به. وكما تم ذكره من قبل، هذا هو السلوك المتوقع adminuser من قبل والذي يتم إنشاؤه أثناء الخطوة التالية. ومع ذلك، helpdeskuser يجب أن يكون مستوى الامتيازات أقل، وبالتالي يجب إنشاء عنصر سياسة ثان.

عنصر السياسة Jhelpdeskuser ال ممائل إلى واحد خلق أعلاه فقط، مامدا أن السلسلة shell:priv-lvl=15 ينبغي غيرت إلى shell:priv-lvl=X، واستبدلت X مع الامتياز مستوى ب رغب. في هذا المثال، يتم إستخدام رقم 1.

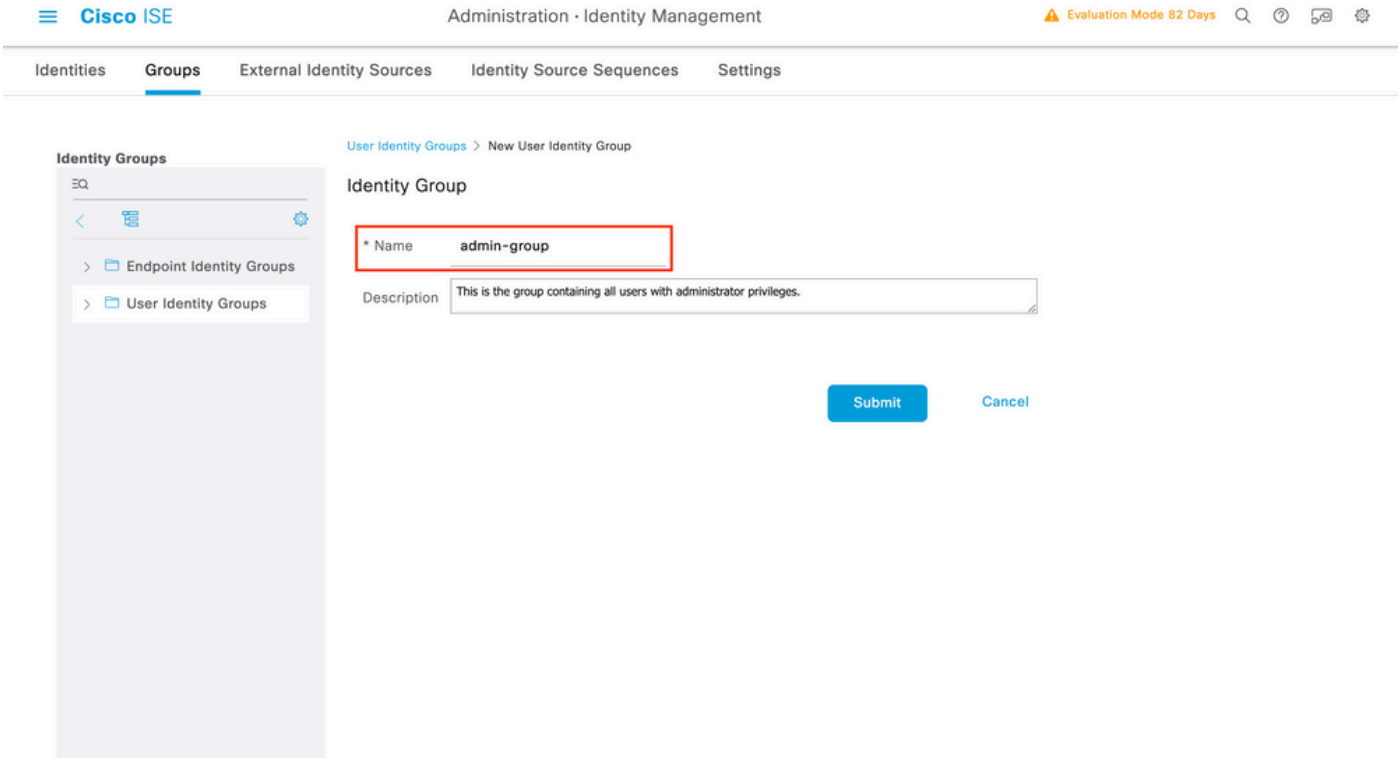
الخطوة 3. إنشاء مجموعات مستخدمين على ISE.

<u>من واجهة المستخدم الرسومية:</u>

يتم إنشاء مجموعات مستخدمي ISE من علامة التبويب مجموعات هوية المستخدم في Administration > Identity Management > Groups GUI Page الشاشة، والذي يظهر في التقاط الشاشة.



لإنشاء مستخدم جديد، أستخدم الزر إضافة الذي يفتح نموذج تكوين مجموعة هوية المستخدم الجديدة كما هو موضح.

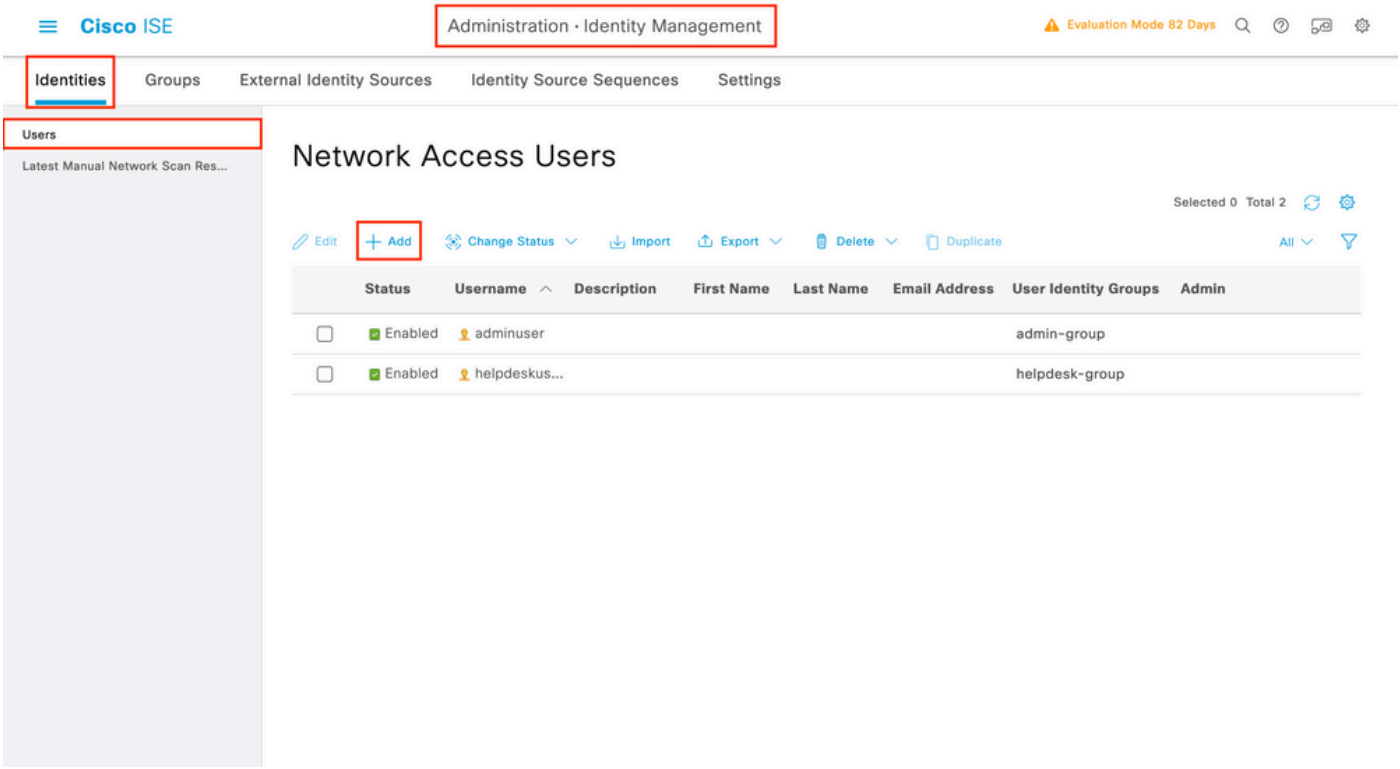


قم بتوفير اسم المجموعة التي تم إنشاؤها. قم بإنشاء مجموعتي المستخدمين اللتين تمت مناقشتهما أعلاه، وهما admin-group وhelpdesk-group.

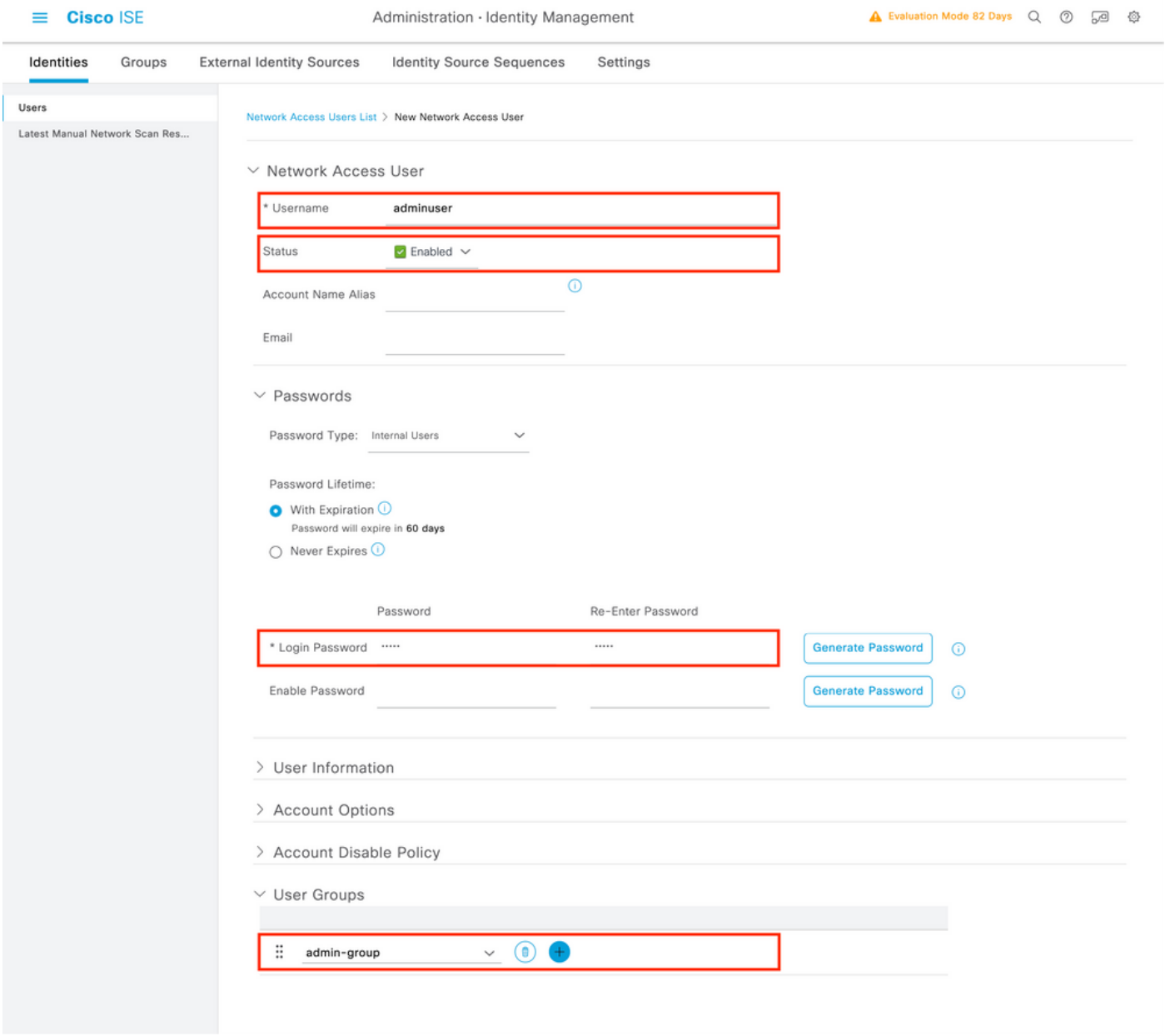
الخطوة 4. إنشاء مستخدمين على ISE.

من واجهة المستخدم الرسومية:

يتم إنشاء مستخدمي ISE من مستخدمي علامة التبويب لمستخدمي Administration > Identity Management > Identities GUI Page علامة التبويب، والتي تظهر في التقاط الشاشة.



لإنشاء مستخدم جديد، أستخدم الزر "إضافة" لفتح نموذج تكوين مستخدم الوصول إلى الشبكة الجديد كما هو موضح.



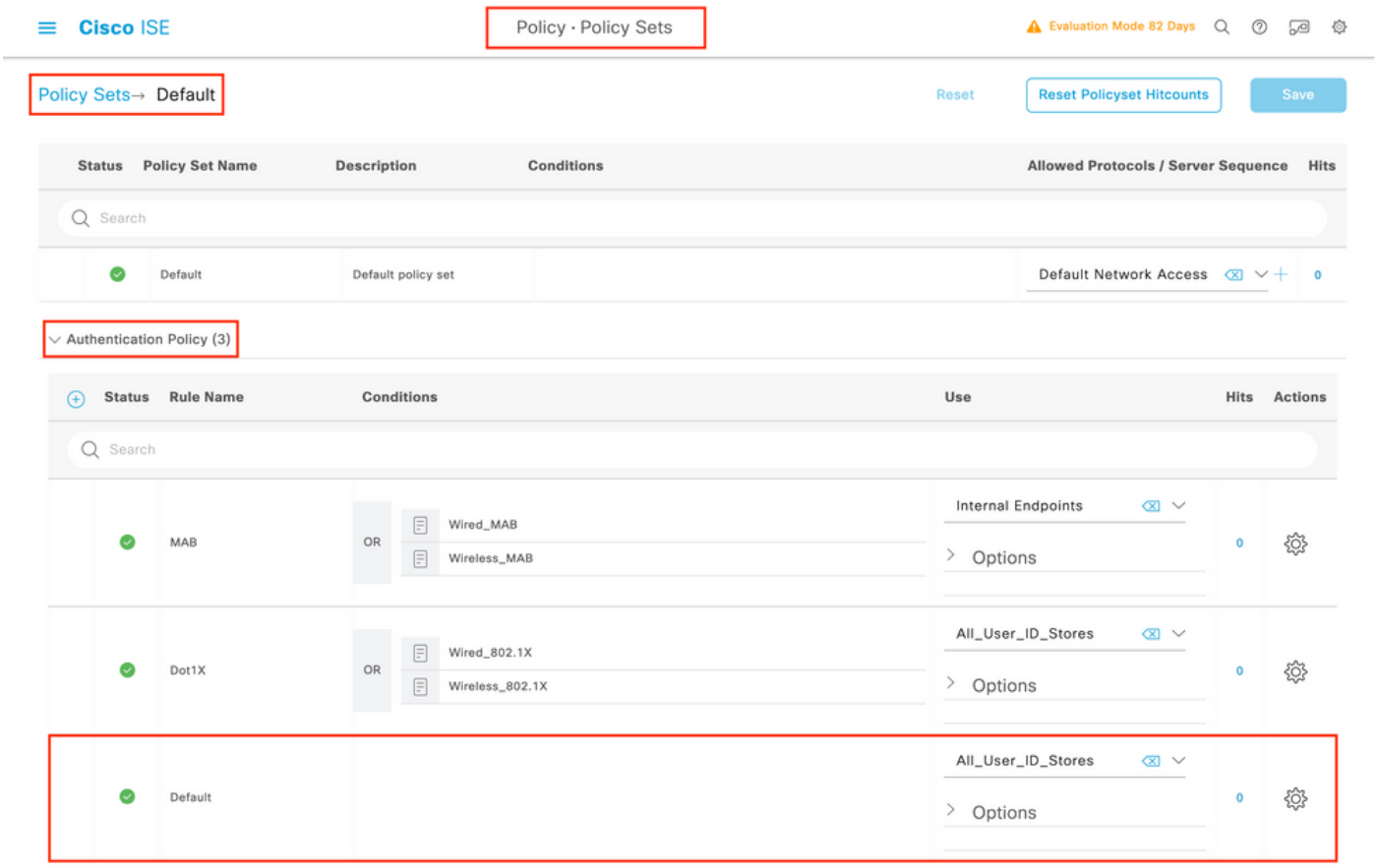
قم بتوفير بيانات الاعتماد للمستخدمين، أي اسم المستخدم وكلمة المرور الخاصين به/بها، وهما المستخدمين للمصادقة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تأكد أيضا من أن حالة المستخدم Enabled. أخيرا، أضف المستخدم إلى مجموعته ذات الصلة، والتي تم إنشاؤها في الخطوة 4.، مع القائمة المنسدلة مجموعات المستخدمين في نهاية النموذج.

قم بإنشاء المستخدمين الذين تمت مناقشتهما أعلاه، وهما adminuser وhelpdeskuser.

الخطوة 5. مصادقة المستخدمين.

من واجهة المستخدم الرسومية:

في هذا السيناريو، تسمح سياسة المصادقة الخاصة بمجموعات النهج الافتراضية ل ISE، والتي تم تكوينها مسبقا بالفعل، بالوصول الافتراضي إلى الشبكة. يمكن مالحظة مجموعة النهج هذه من Policy > Policy Sets صفحة واجهة المستخدم الرسومية (GUI) الخاصة ب ISE، كما هو موضح في هذه الصورة. لذلك ال حاجة إلى تغييره.

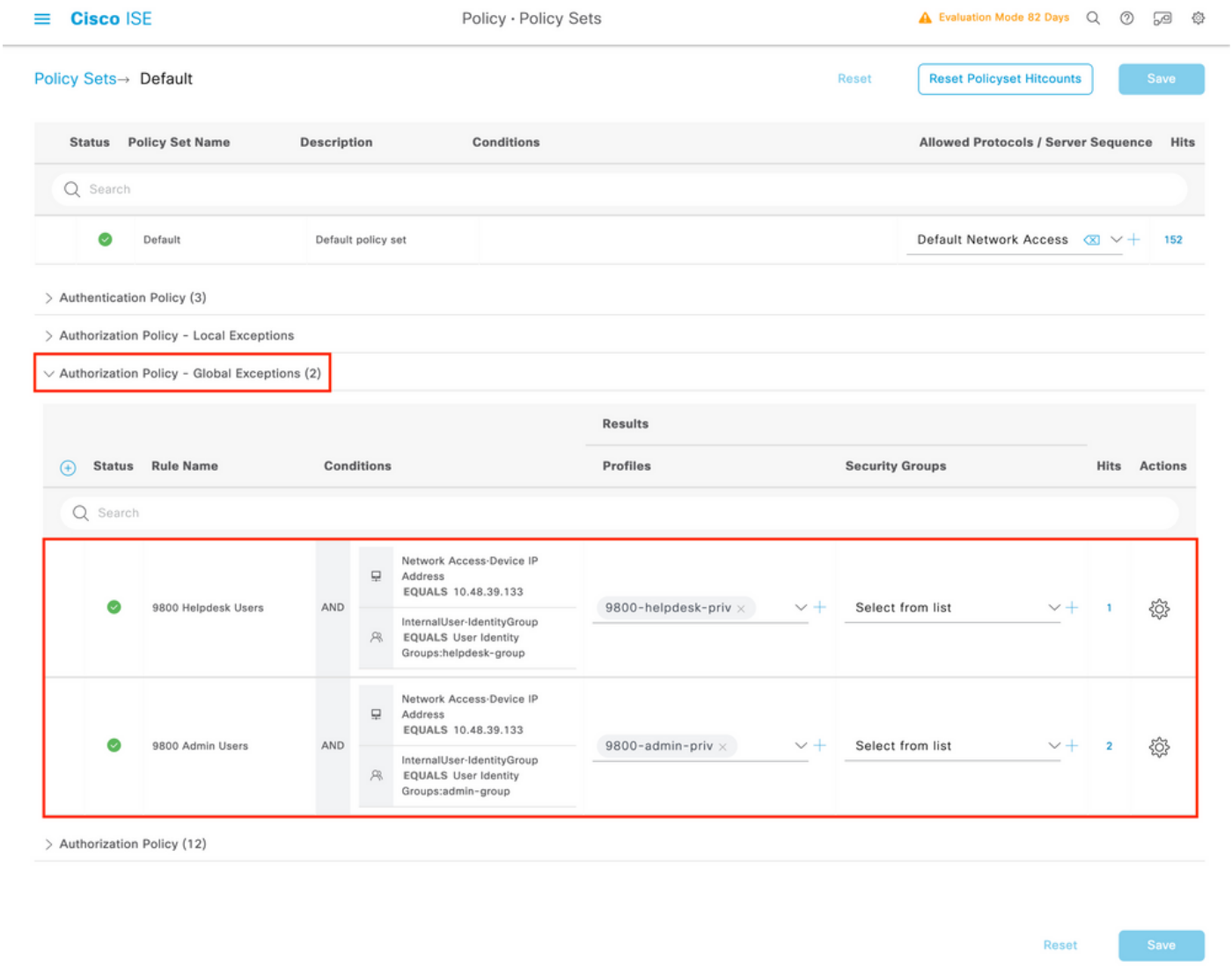


الخطوة 6. تخويل المستخدمين.

من واجهة المستخدم الرسومية:

بعد أن تقوم محاولة تسجيل الدخول بتمرير سياسة المصادقة، يجب تخويلها ويجب على ISE إرجاع ملف تعريف التخويل الذي تم إنشاؤه مسبقا (السماح بقبول، بالإضافة إلى مستوى الامتيازات).

في هذا المثال، تتم تصفية محاولات تسجيل الدخول استنادا إلى عنوان IP للجهاز (وهو عنوان IP الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)) وتمييز مستوى الامتياز الذي سيتم منحه استنادا إلى المجموعة التي ينتمي إليها المستخدم. هناك نهج آخر صالح لتصفية المستخدمين استنادا إلى أسماء المستخدمين الخاصة بهم حيث تحتوي كل مجموعة على مستخدم واحد فقط في هذا المثال.



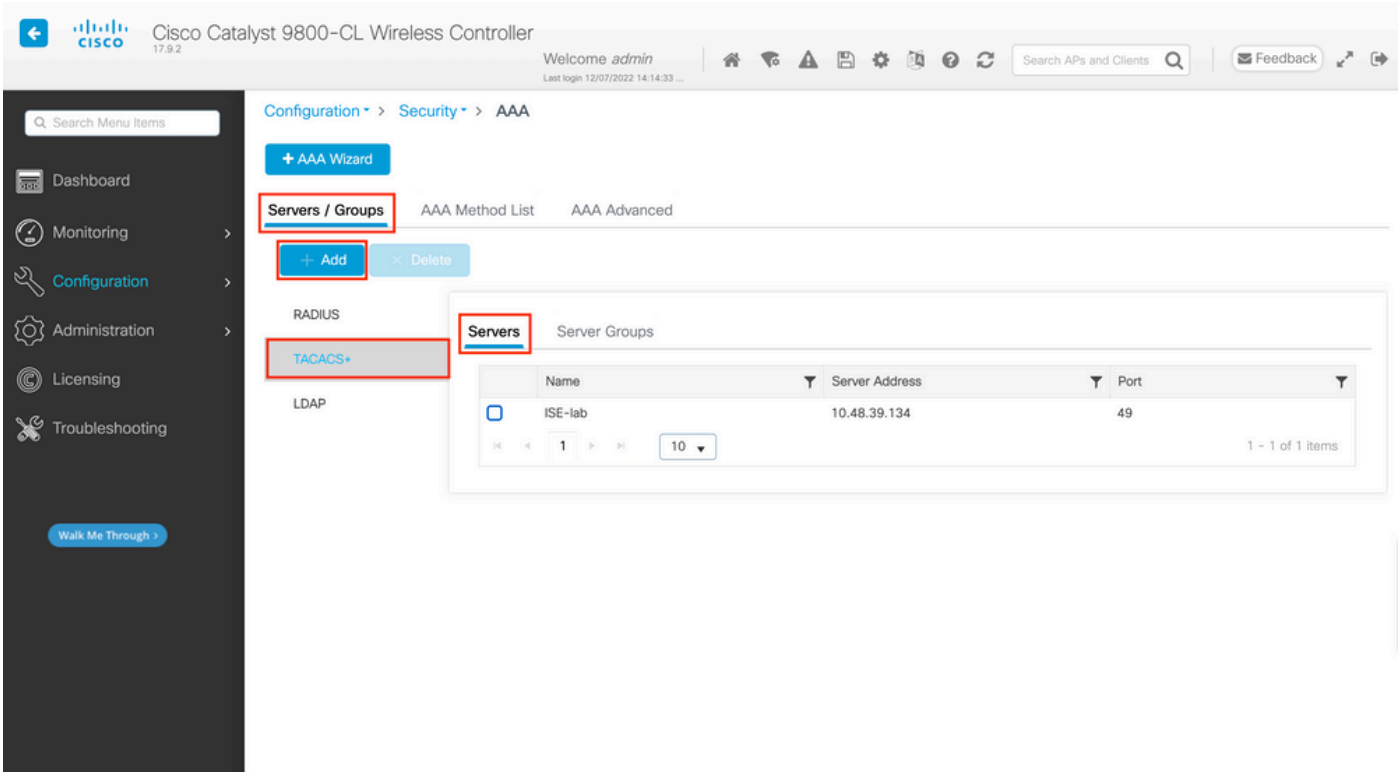
بعد اكتمال هذه الخطوة، يمكن إستخدام بيانات الاعتماد التي تم تكوينها ل adminuser المستخدمhelpdesk للمصادقة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عبر واجهة المستخدم الرسومية (GUI) أو من خلال برنامج Telnet/SSH.

تكوين TACACS+ WLC

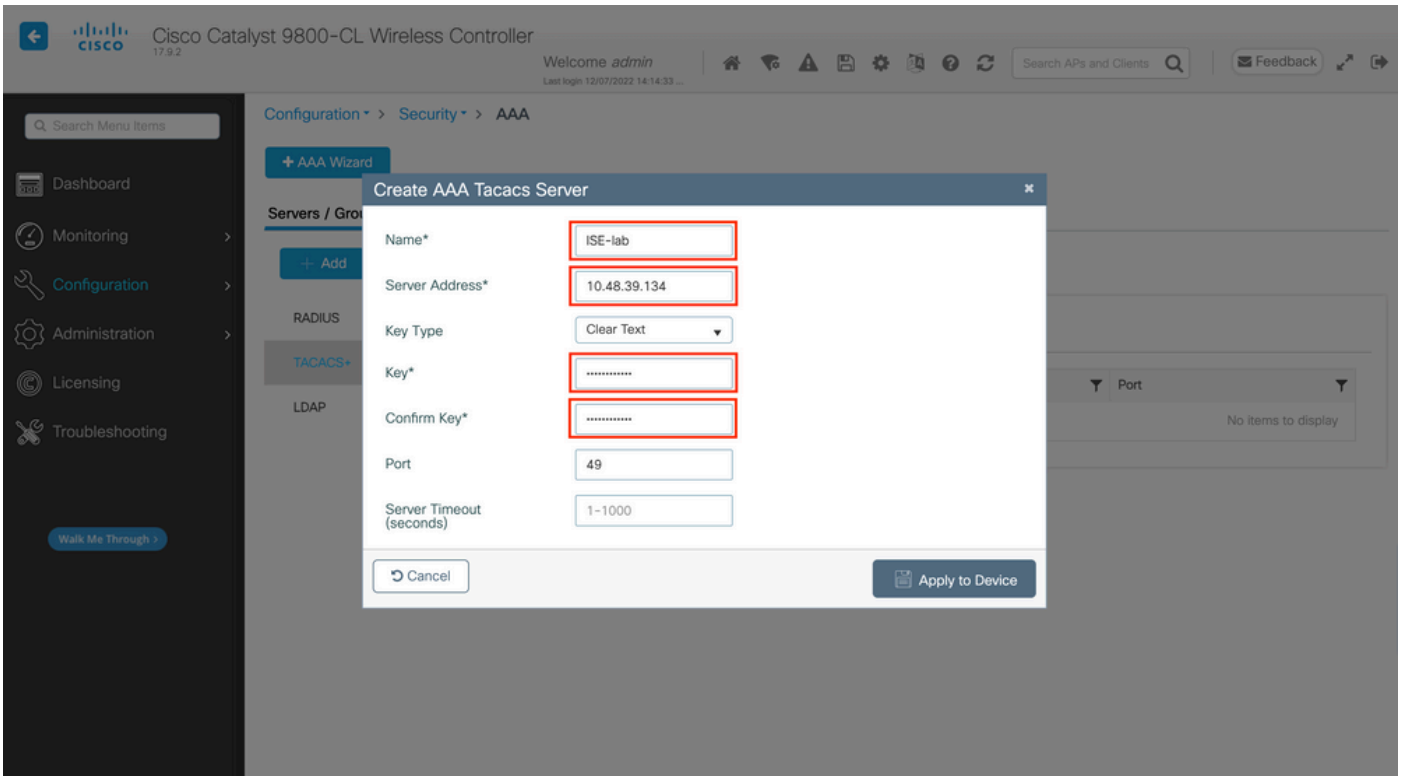
الخطوة 1. إعلان خادم TACACS+.

منواجهة المستخدم الرسومية:

أولا، قم بإنشاء ISE لخادم TACACS+ على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يمكن القيام بذلك من علامة التبويب Servers/Groups > TACACS+ > Servers من صفحة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) الخاصة بواجهة المستخدم الرسومية (GUI) التي يمكن الوصول إليها في https://<WLC-IP>/webui/#/aaa، أو إذا قمت بالانتقال إلى Configuration > Security > AAA، كما هو موضح في هذه الصورة.



لإضافة خادم TACACS على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق الزر إضافة المؤطر باللأحمر في الصورة أعلاه. يؤدي هذا إلى فتح النافذة المنبثقة المرسومة.



عندما تفتح النافذة المنبثقة، قم بتوفير اسم الخادم (لا يجب أن يطابق اسم نظام ISE)، عنوان IP الخاص به، المفتاح المشترك، المنفذ المستخدم، والمهلة.

في هذه النافذة المنبثقة، يجب عليك توفير:

-

اسم الخادم (لاحظ أنه ال يجب أن يطابق اسم نظام ISE)

- عنوان IP للخادم
- السر المشترك بين عنصر التحكم في الشبكة المحلية اللاسلكية وخادم TACACS+

يمكن تكوين معلمات أخرى، مثل المنافذ المستخدمة للمصادقة والمحاسبة، ولكن هذه ليست إلزامية وتترك كإعداد افتراضي لهذا المستند.

من واجهة سطر الأوامر:

<#root>

WLC-9800(config)#tacacs server

ISE-lab

WLC-9800(config-server-tacacs)#address ipv4

10.48.39.134

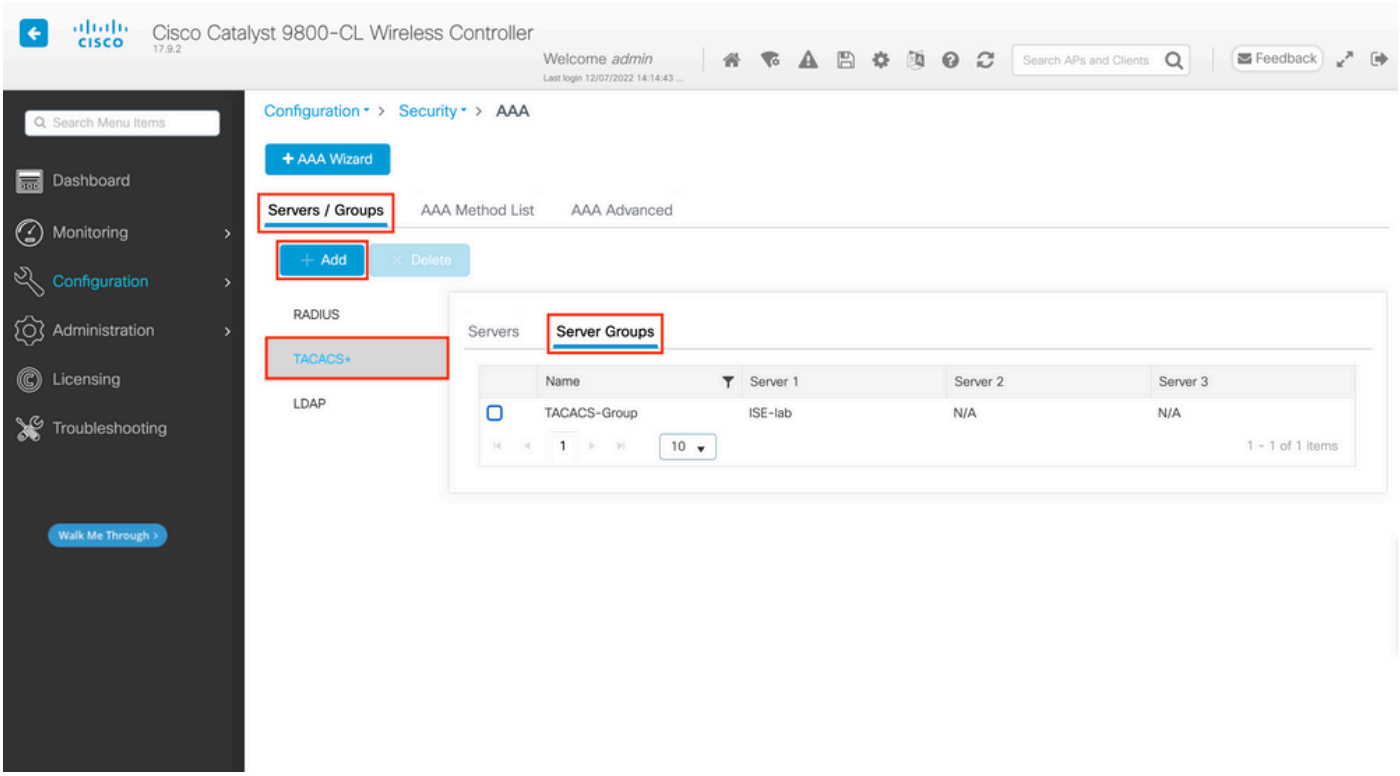
WLC-9800(config-server-tacacs)#key

Cisco123

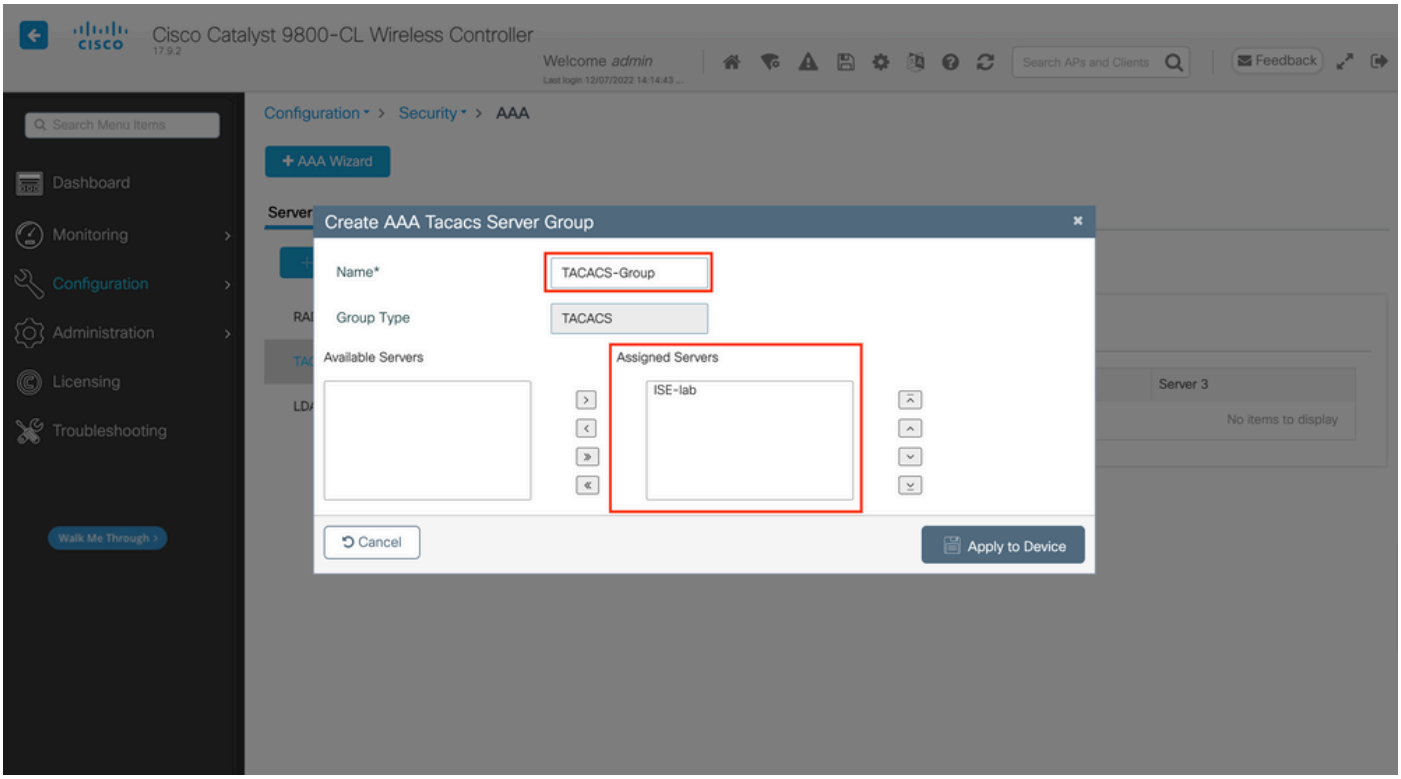
الخطوة 2. قم بتعيين خادم TACACS+ إلى مجموعة خوادم.

من واجهة المستخدم الرسومية:

في حالة وجود خوادم TACACS+ متعددة يمكن إستخدامها للمصادقة، يوصى بتعيين جميع هذه الخوادم إلى مجموعة الخوادم نفسها. وعندئذ تهتم وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بتوزيع الأحمال لمصادقات مختلفة بين الخوادم في مجموعة الخوادم. يتم تكوين مجموعات خوادم TACACS+ منServers/Groups > TACACS > Server Groups علامة التبويب من نفس صفحة واجهة المستخدم الرسومية (GUI) المذكورة في الخطوة 1.، والموضحة في الصورة.



باللنسبة لإنشاء الخادم، تظهر نافذة منبثقة عند النقر فوق الزر إضافة في إطار الصورة السابقة، والموضح في الصورة.



في القائمة المنبثقة، قم بتسمية المجموعة وانقل الخوادم المطلوبة إلى قائمة الخوادم المعينة.

من واجهة سطر الأوامر:

<#root>

WLC-9800(config)#aaa group server tacacs+

TACACS-Group

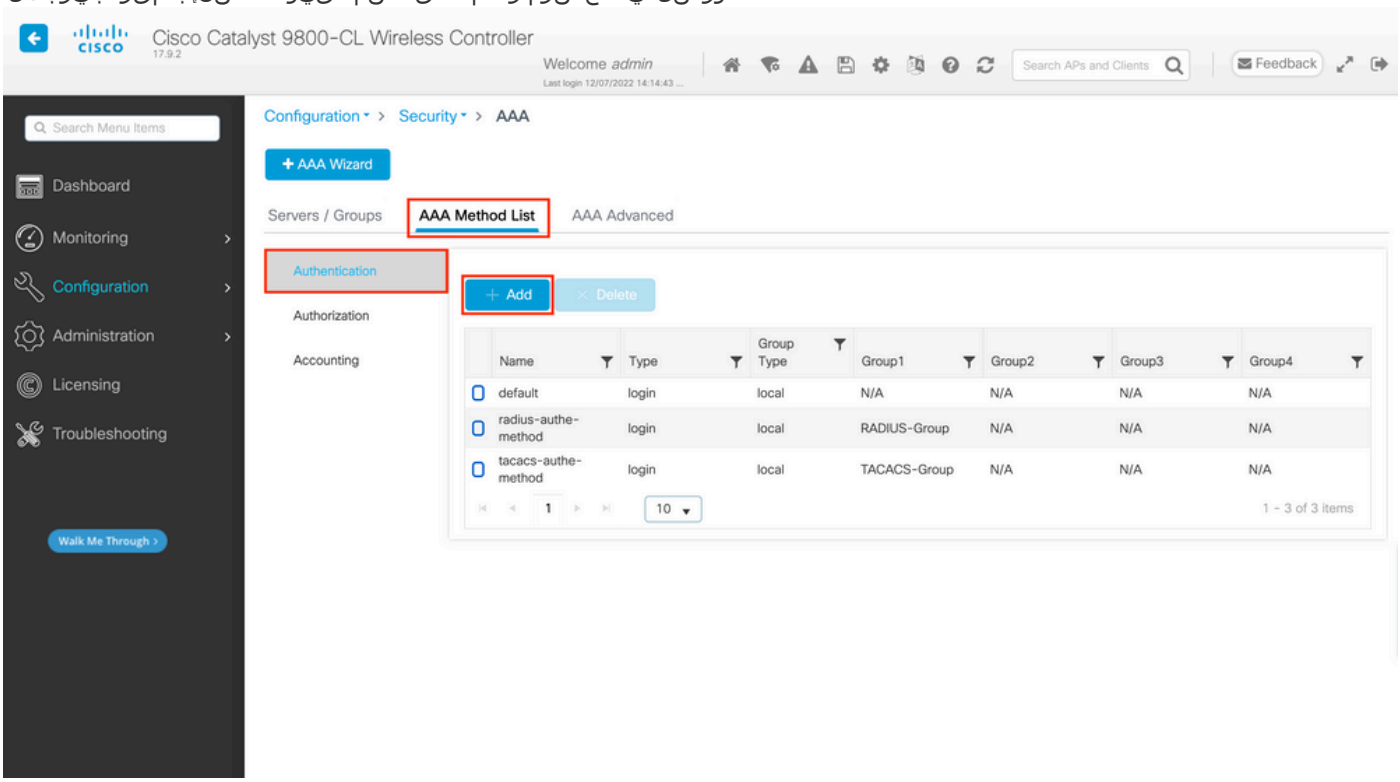
```
WLC-9800(config-sg-tacacs+)#server name
```

ISE-lab

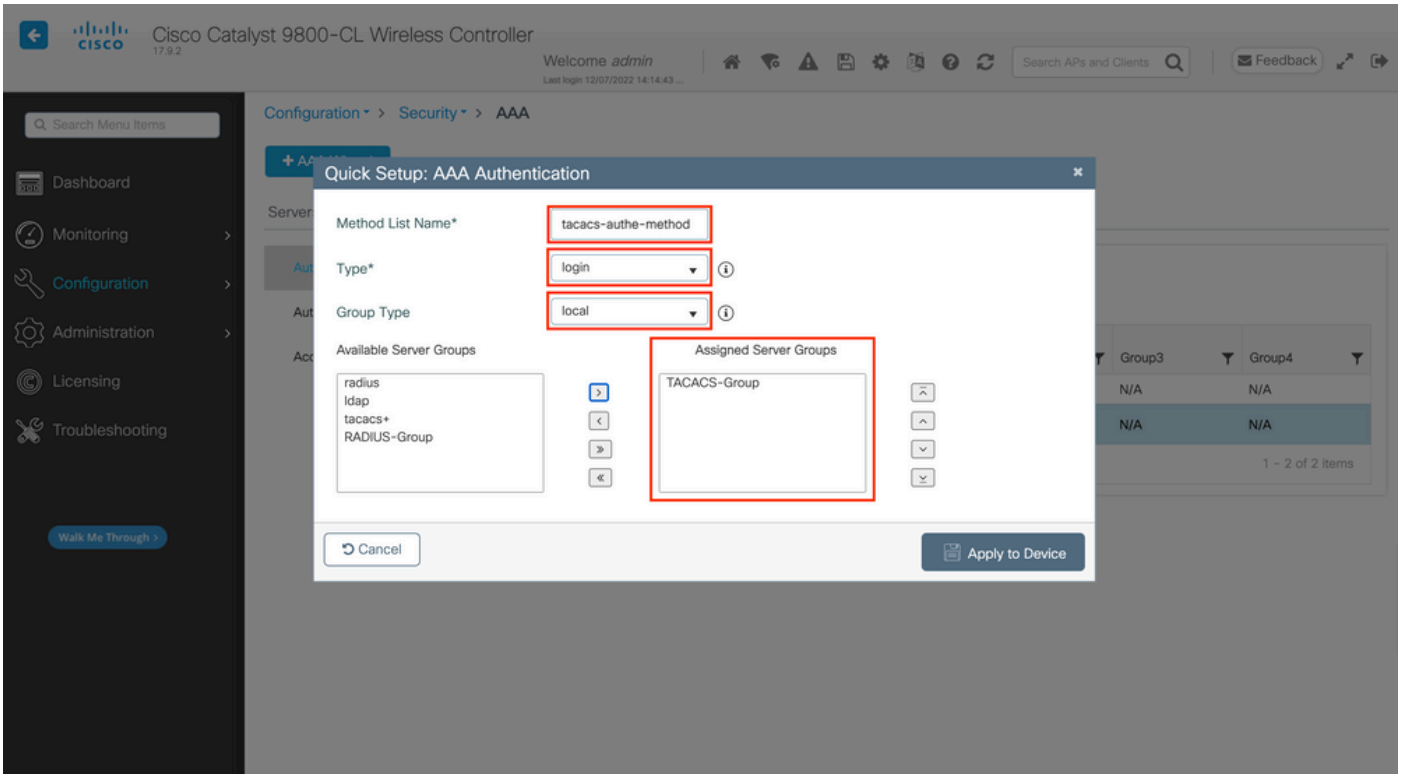
الخطوة 3. قم بإنشاء طريقة تسجيل دخول مصادقة AAA تشير إلى مجموعة خوادم TACACS+.

من واجهة المستخدم الرسومية:

بعد من صفحةhttps://<WLC-IP>/webui/#/aaa واجهة المستخدم الرسومية، انتقل إلى AAA Method List > Authentication علامة التبويب، وقم بإنشاء طريقة مصادقة كما هو موضح في الصورة.



كما هو معتاد، عندما تستخدم زر إضافة لإنشاء طريقة مصادقة، تظهر نافذة منبثقة للتكوين، مماثلة للنافذة الموضحة في هذه الصورة.



في هذا الإطار المنبثق، قم بتوفير اسم للأسلوب، واختر الكتابة باسمlogin، وقم بإضافة خادم المجموعة الذي تم إنشاؤه في الخطوة السابقة إلى قائمة مجموعات الخوادم المعينة. فيما يتعلق بحقل نوع المجموعة، يمكن إجراء العديد من التكوينات.

- إذا أخترت "نوع المجموعة" محليا، يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) أولا مما إذا كانت بيانات اعتماد المستخدم موجودة محليا، ثم يعود مرة أخرى إلى مجموعة الخوادم.

- إذا أخترت نوع المجموعة كمجموعة ولم تقم بالتحقق من الخيار رجوع إلى محلي، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يتحقق فقط من مسوغات المستخدم مقابل مجموعة الخوادم.

- إذا أخترت "نوع المجموعة" كمجموعة وفحصت الخيار "إحتياطي إلى محلي"، يتحقق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من بيانات اعتماد المستخدم مقابل مجموعة الخوادم ويستعلم عن قاعدة البيانات المحلية فقط إذا لم يستجب الخادم. إذا قام الخادم بإرسال رفض، ستتم مصادقة المستخدم، حتى وإن كان يمكن أن يكون موجودا على قاعدة البيانات المحلية.

من واجهة سطر الأوامر:

إذا كنت تريد التحقق من بيانات اعتماد المستخدم مع مجموعة خوادم فقط إذا لم يتم العثور عليها محليا أولا، أستخدم:

```
<#root>

WLC-9800(config)#aaa authentication login
```

tacacs-authe-method

local group

TACACS-Group

إذا كنت تريد التحقق من بيانات اعتماد المستخدم مع مجموعة خوادم فقط، أستخدم:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

group

TACACS-Group

إذا كنت تريد التحقق من بيانات اعتماد المستخدم مع مجموعة خوادم وإذا كان هذا الأخير لا يستجيب مع إدخال محلي، فاستخدم:

<#root>

WLC-9800(config)#aaa authentication login

tacacs-authe-method

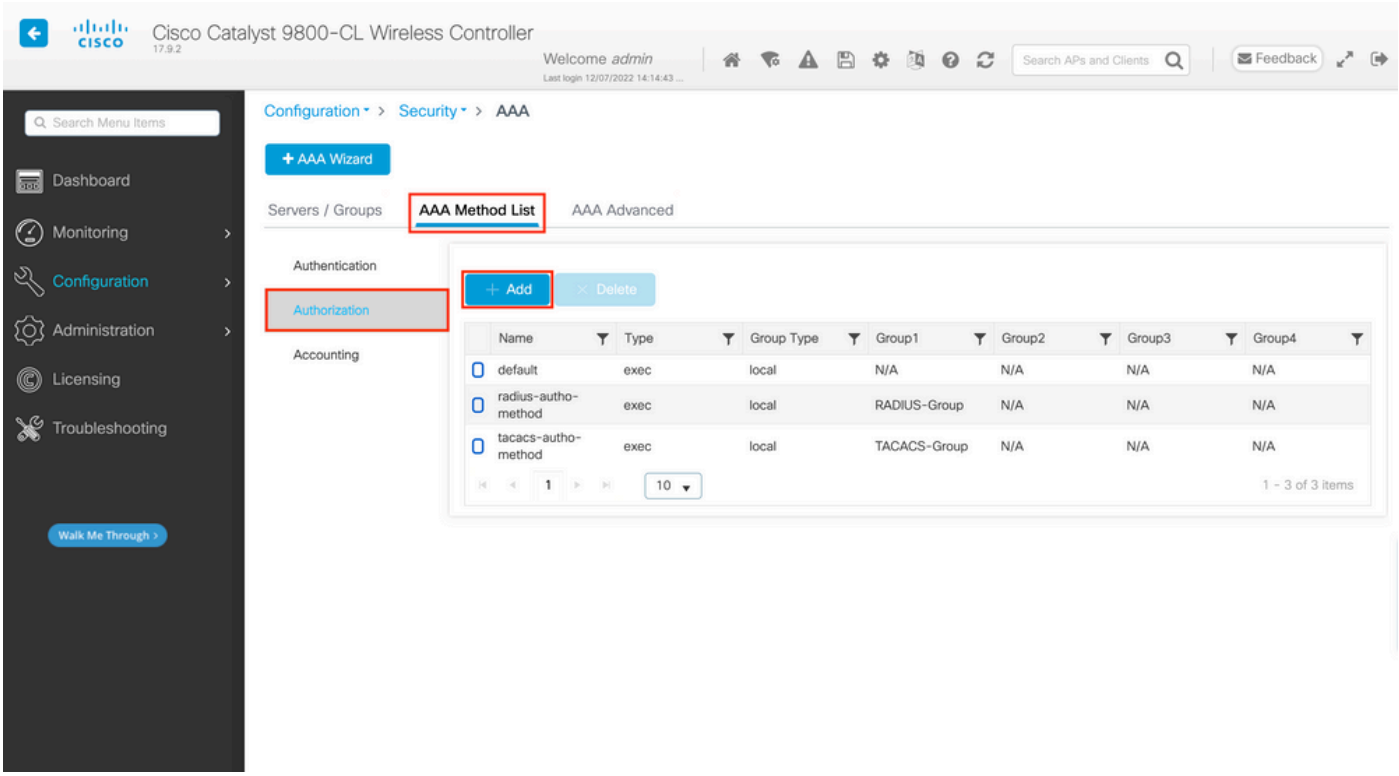
group

TACACS-Group

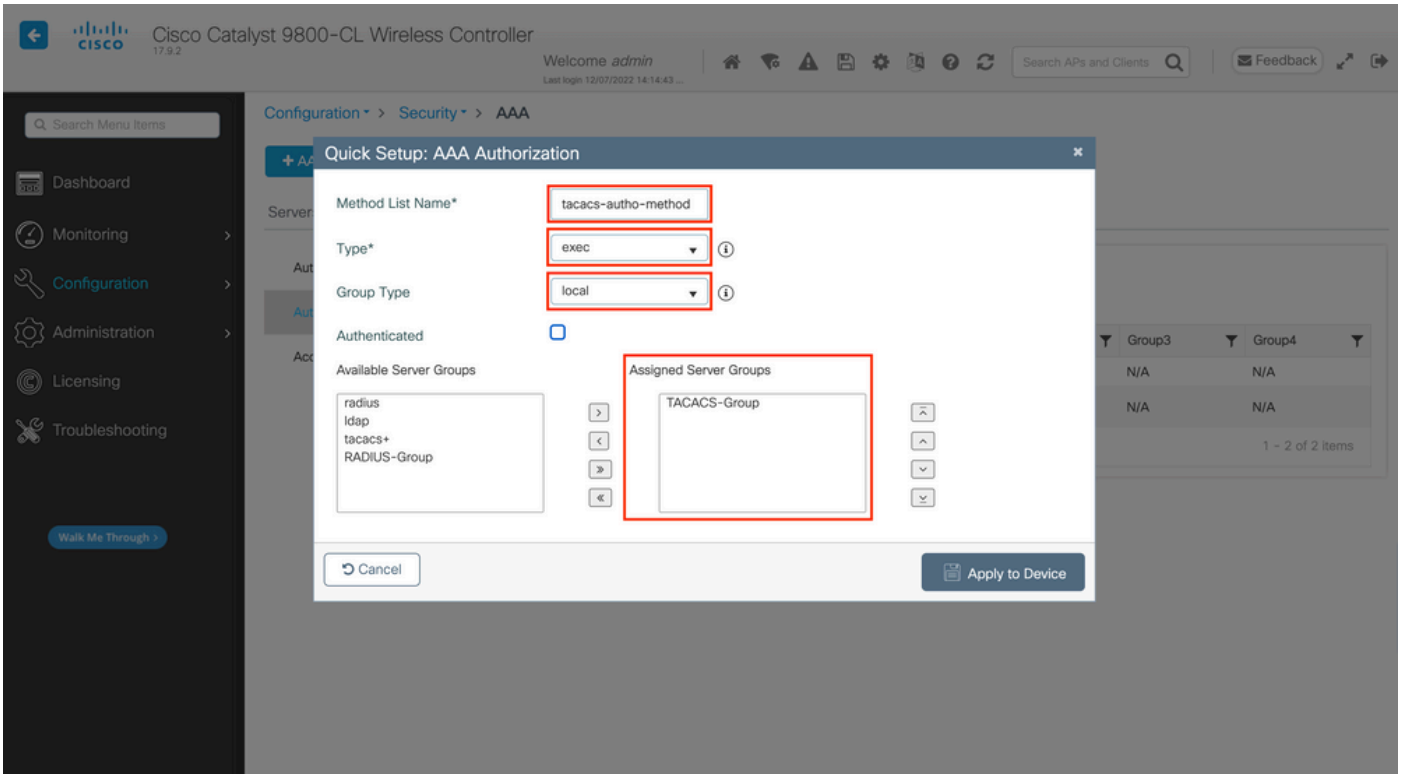
local

في هذا المثال، هناك بعض المستخدمين الذين تم إنشاؤها محليا فقط، وبعض المستخدمين فقط على خادم ISE، وبالتالي إستخدام الخيار الأول.

الخطوة 4. قم بإنشاء أسلوب AAA للتخويل الذي يشير إلى مجموعة خوادم TACACS+.
من واجهة المستخدم الرسومية:
كما يجب تخويل المستخدم حتى يتم منحه حق الوصول. بعد من صفحة واجهة المستخدم الرسومية، Configuration > Security > AAA، انتقل إلى علامةAAA Method List > Authorization التبويب، وقم بإنشاء طريقة اعتماد كما هو موضح في الصورة.



يظهر تكوين أسلوب تخويل منبثق مماثل للأسلوب الذي تم تصويره عند إضافة أسلوب جديد باستخدام الزر إضافة.



في هذا التكوين المنبثق، قم بتوفير اسم لطريقة التخويل، واختر النوع باسم exec، واستخدم نفس الترتيب لنوع المجموعة كالمستخدم لطريقة المصادقة في الخطوة السابقة.

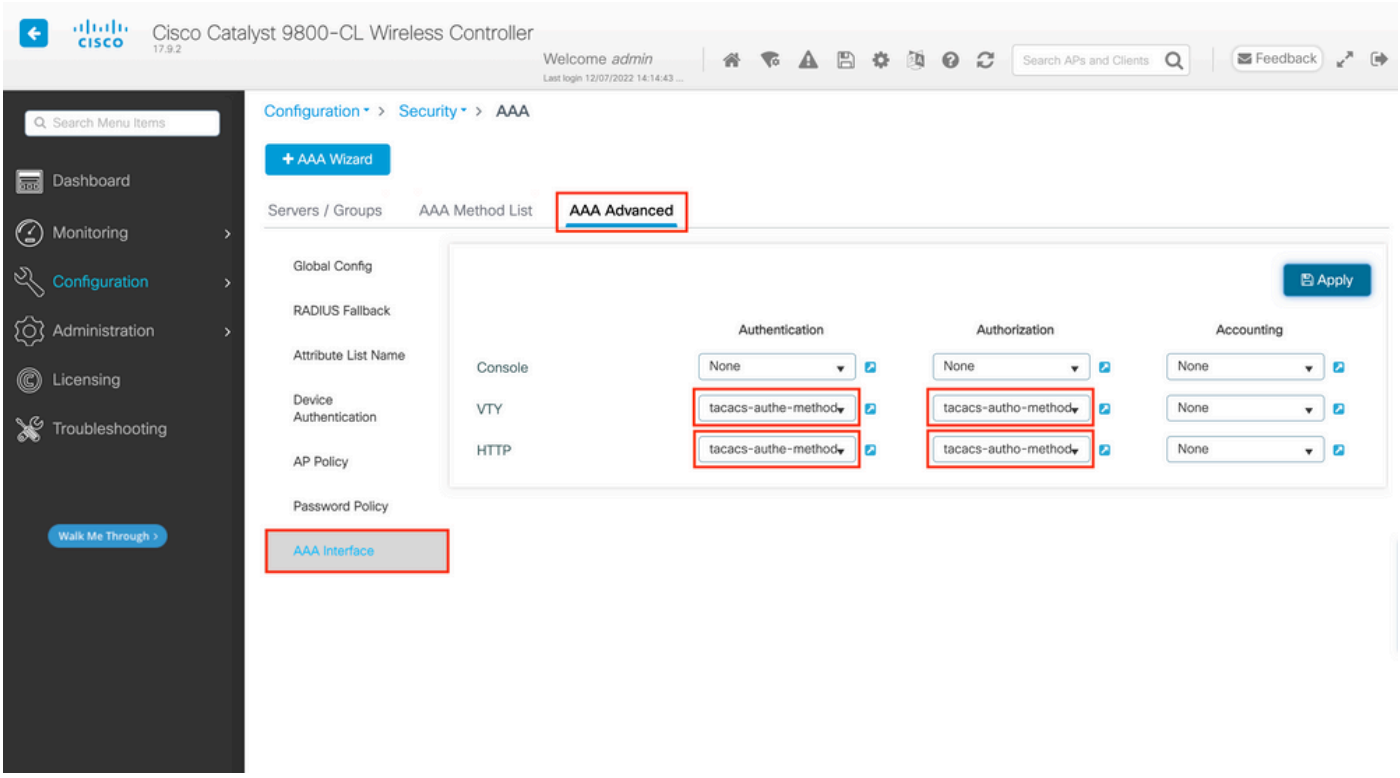
من واجهة سطر الأوامر:

```
<#root>

WLC-9800(config)#aaa authorization exec

tacacs-autho-method

 local group

TACACS-Group
```

الخطوة 5. قم بتعيين الطرق إلى تكوينات HTTP وإلى خطوط vty المستخدمة لـ Telnet/SSH.

من واجهة المستخدم الرسومية:

يمكن إستخدام طرق المصادقة والتفويض التي تم إنشاؤها لاتصال مستخدم HTTP و/أو Telnet/SSH، والتي يمكن تكوينها من AAA Advanced > AAA Interface علامة التبويب التي لا تزال من صفحة GUI WLC التي يمكن الوصول إليها في https://<WLC-IP>/webui/#/aaa، كما هو موضح في الصورة.



من واجهة سطر الأوامر:

بالنسبة لمصادقة واجهة المستخدم الرسومية (GUI):

```
<#root>

WLC-9800(config)#ip http authentication aaa login-authentication

tacacs-authe-method

WLC-9800(config)#ip http authentication aaa exec-authorization

tacacs-autho-method
```

لمصادقة Telnet/SSH:

```
<#root>

WLC-9800(config)#line vty 0 15
WLC-9800(config-line)#login authentication

tacacs-authe-method

WLC-9800(config-line)#authorization exec

tacacs-autho-method
```

لاحظ أنه عند إجراء التغييرات على تكوينات HTTP، فمن الأفضل إعادة تشغيل خدمات HTTP و HTTPS. يمكن تحقيق ذلك باستخدام هذه الأوامر.

```
WLC-9800(config)#no ip http server
WLC-9800(config)#no ip http secure-server
WLC-9800(config)#ip http server
WLC-9800(config)#ip http secure-server
```

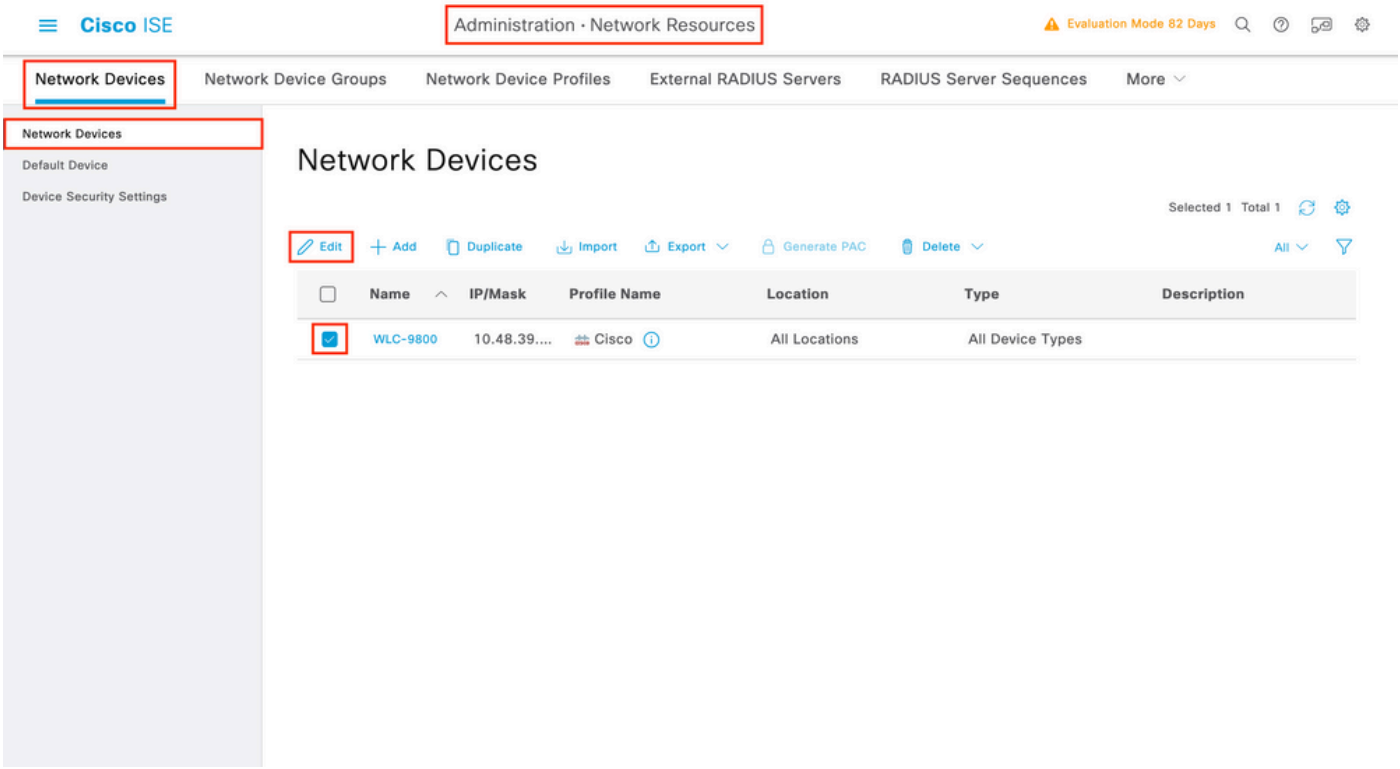
تكوين TACACS+ ISE

الخطوة 1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كجهاز شبكة لـ TACACS+.

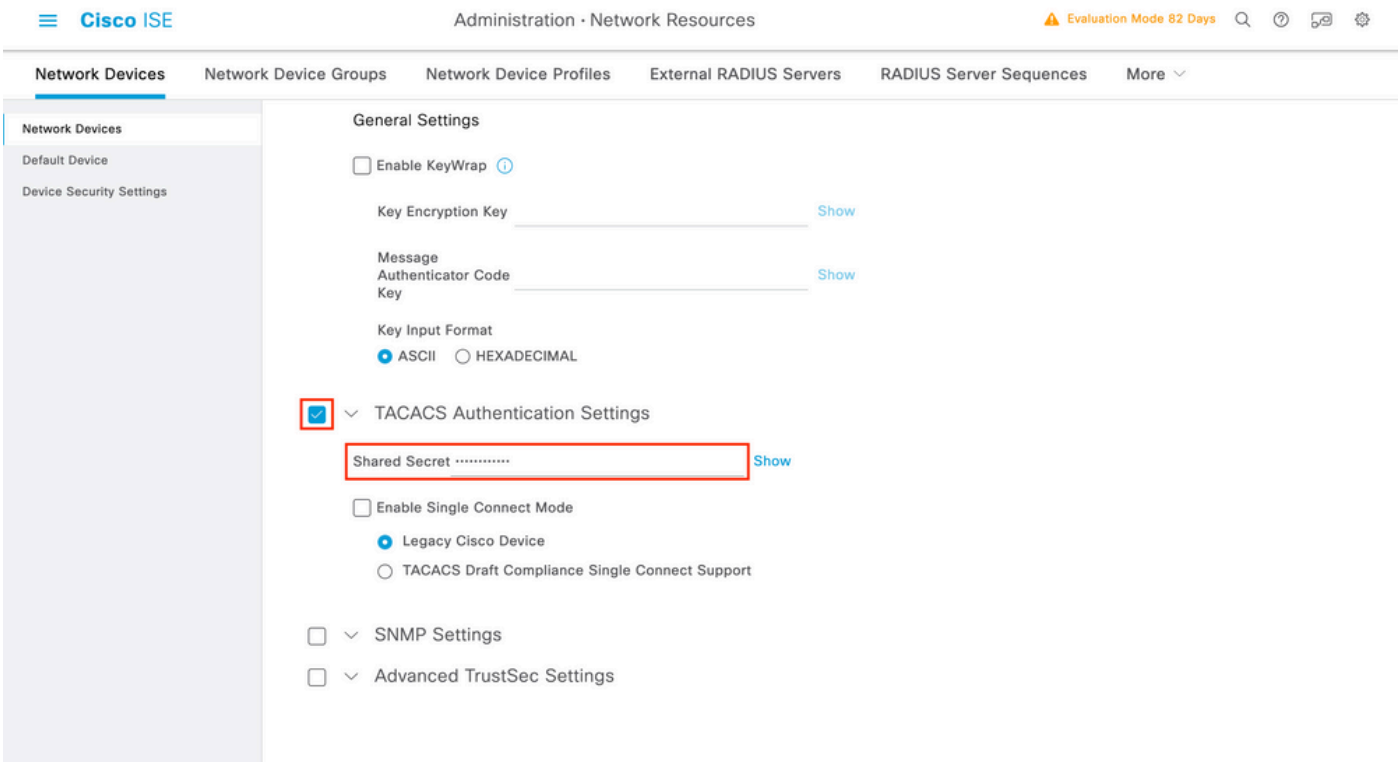
من واجهة المستخدم الرسومية:

لتوضيح استخدام عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في القسم السابق كجهاز شبكة لـ RADIUS

في ISE، انتقل إلى Administration > Network Resources > Network Devices علامة التبويب أجهزة الشبكة وافتحها، كما هو موضح في هذه الصورة.

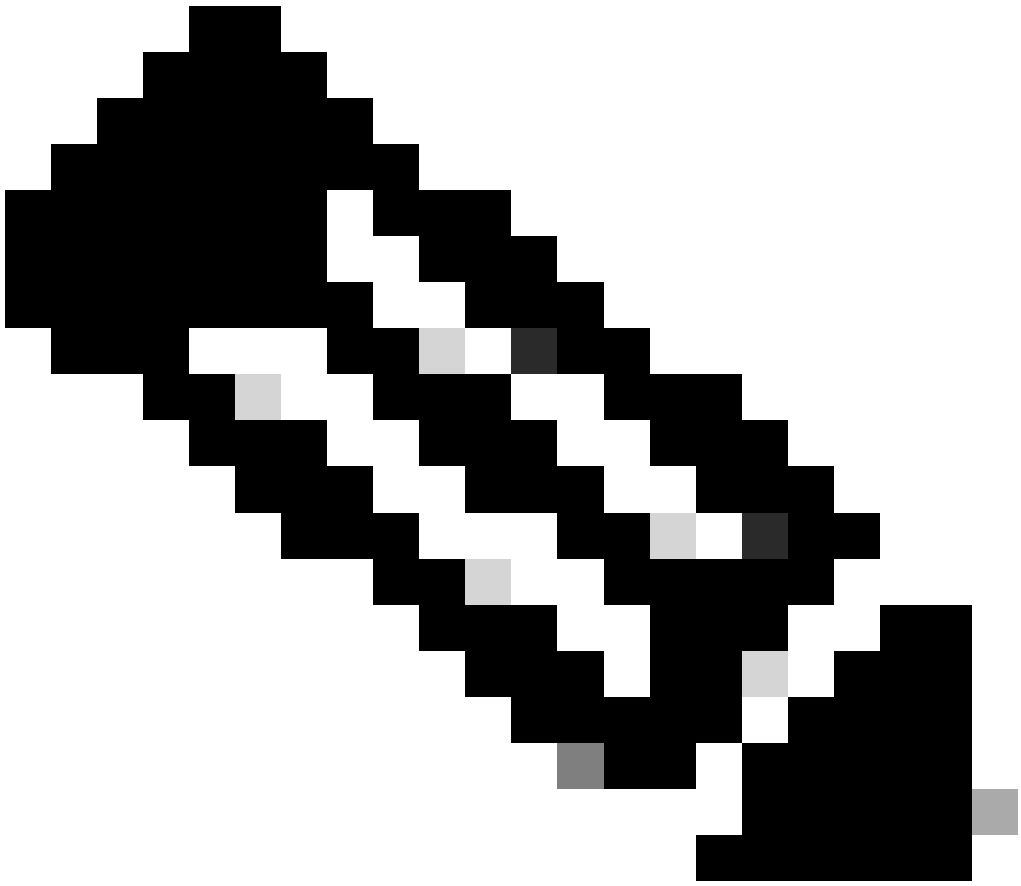


في هذا المثال، تمت إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS (ارجع إلى الخطوة 1. من القسم تكوين RADIUS ISE). لذلك، يحتاج تكوينه بسلطة إلى أن يتم تعديله لتكوين مصادقة TACACS، والذي يمكن فعله عندما تختار WLC في قائمة أجهزة الشبكة وانقر فوق الزر تحرير. وهذا يؤدي إلى فتح نموذج تكوين جهاز الشبكة كما هو موضح في هذه الصورة.



بمجرد فتح النافذة الجديدة، قم بالتمرير إلى قسم إعدادات مصادقة TACACS، وتمكين هذه الإعدادات، وإضافة السر المشترك الذي تم إدخاله أثناء الخطوة 1. من القسم تكوين TACACS+ WLC.

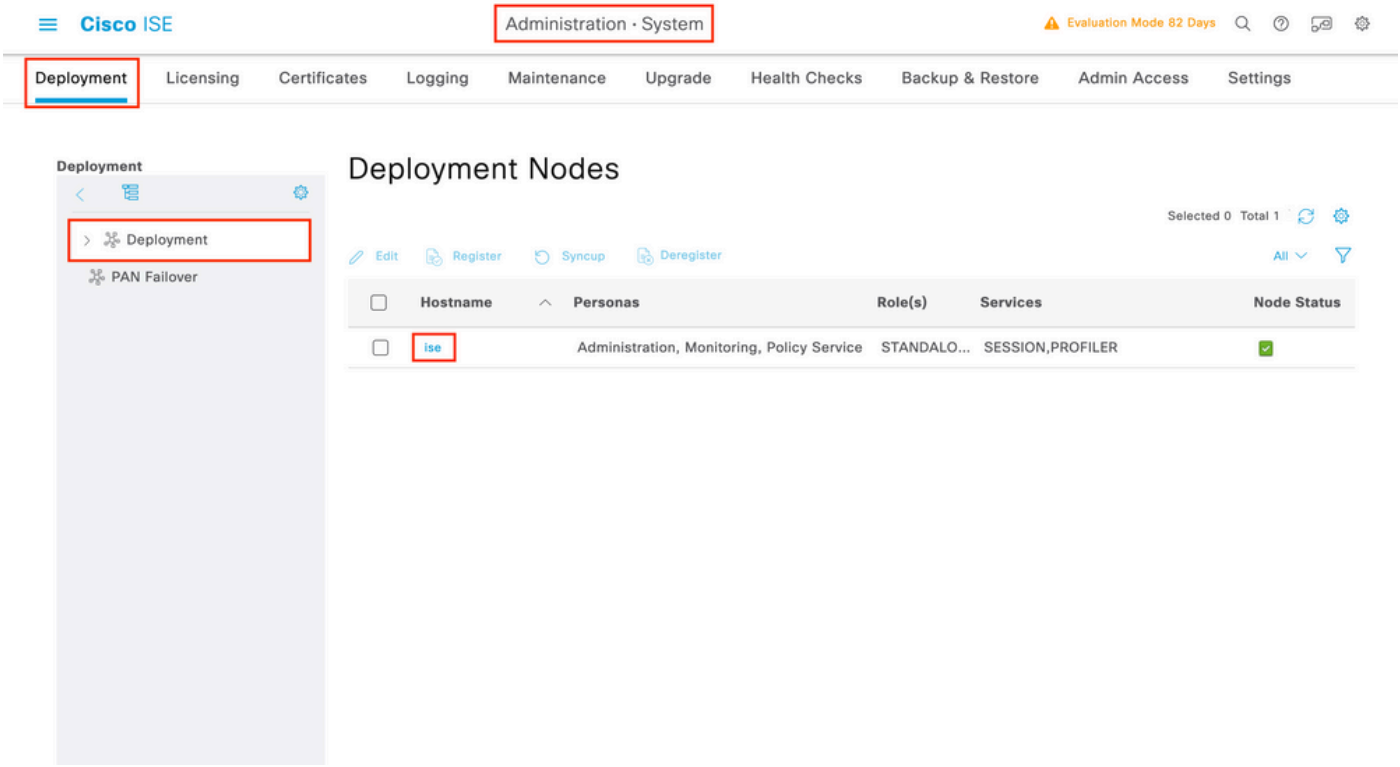
الخطوة 2. قم بتمكين ميزة "مسؤول الجهاز" للعقدة.



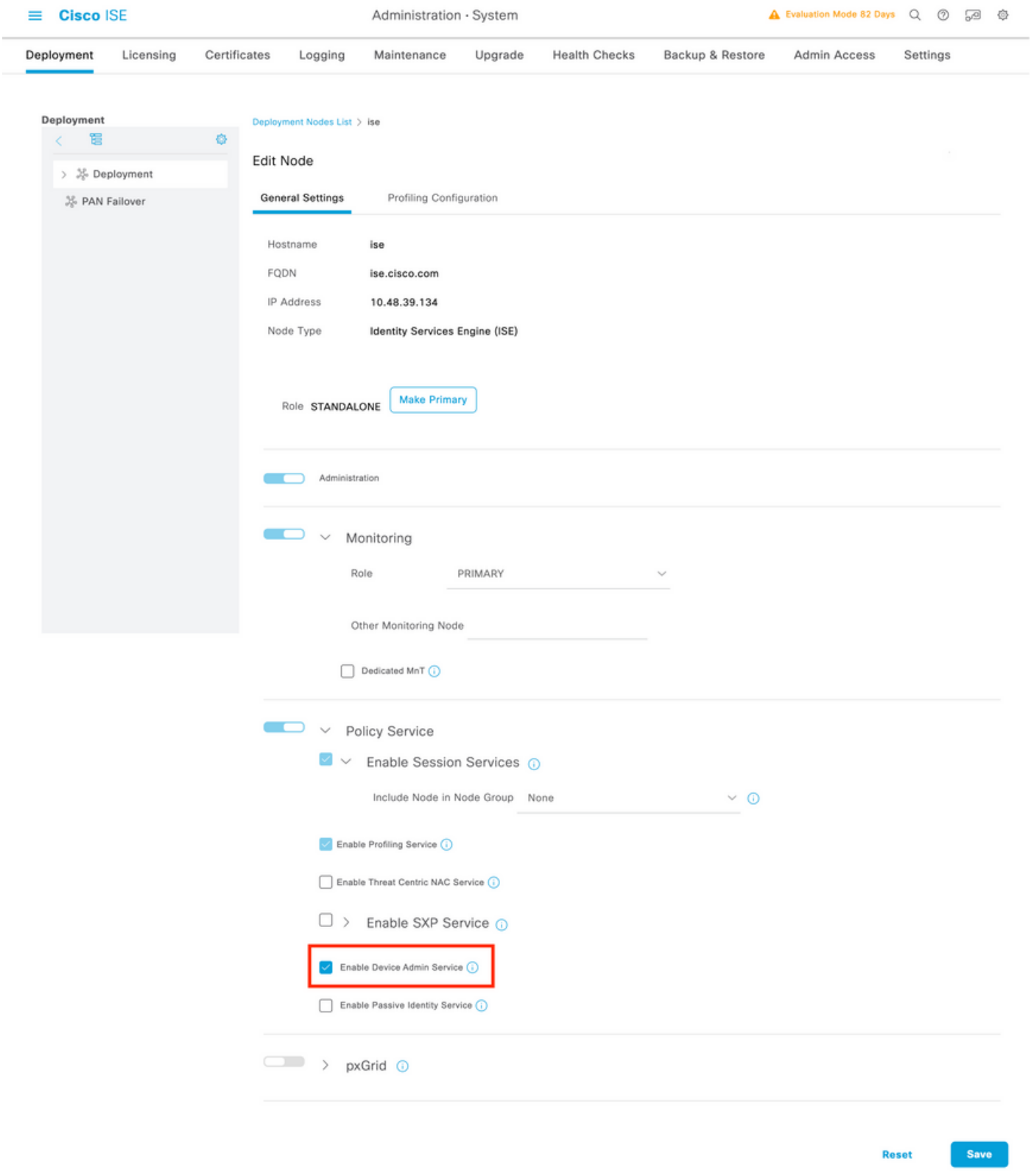
ةظحالم: لا ستخدام ISE كخادم TACACS+، يجب أن يكون لديك حزمة ترخيص إدارة الأجهزة، إما ترخيص Base أو ترخيص Mobility.

نم واجهة المستخدم الرسومية:

بمجرد تثبيت ترخيص إدارة الأجهزة، يجب عليك تمكين ميزة "إدارة الأجهزة" للعقدة لتتمكن من إستخدام ISE كخادم TACACS+. لذلك، قم بتحرير تكوين عقدة نشر ISE المستخدمة، والتي يمكن العثور عليها Administrator > Deployment أسفل، انقر فوق اسمها أو قم بذلك بمساعدة الزرEdit.



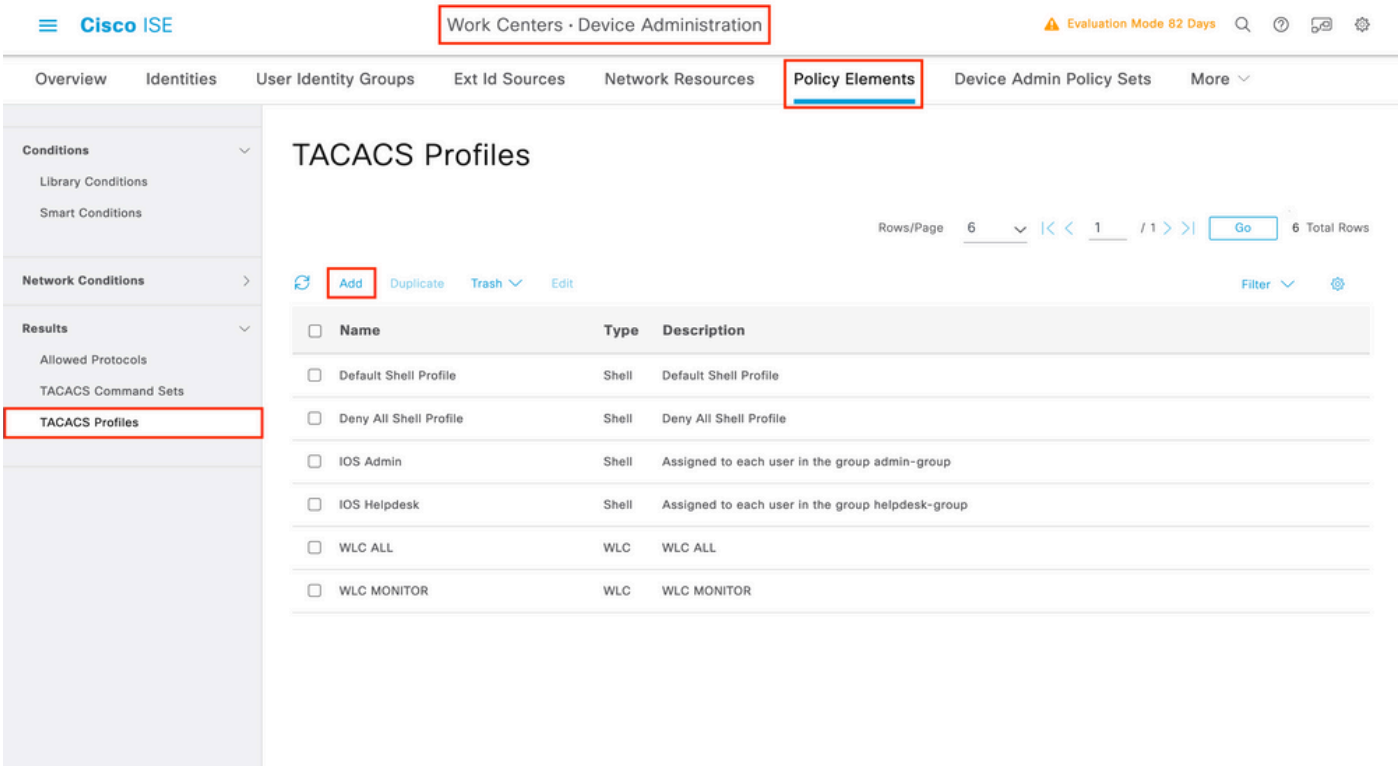
بمجرد فتح نافذة تكوين العقدة، تحقق من خيار تمكين خدمة إدارة الأجهزة ضمن قسم "خدمة النهج"، كما هو موضح في هذه الصورة.



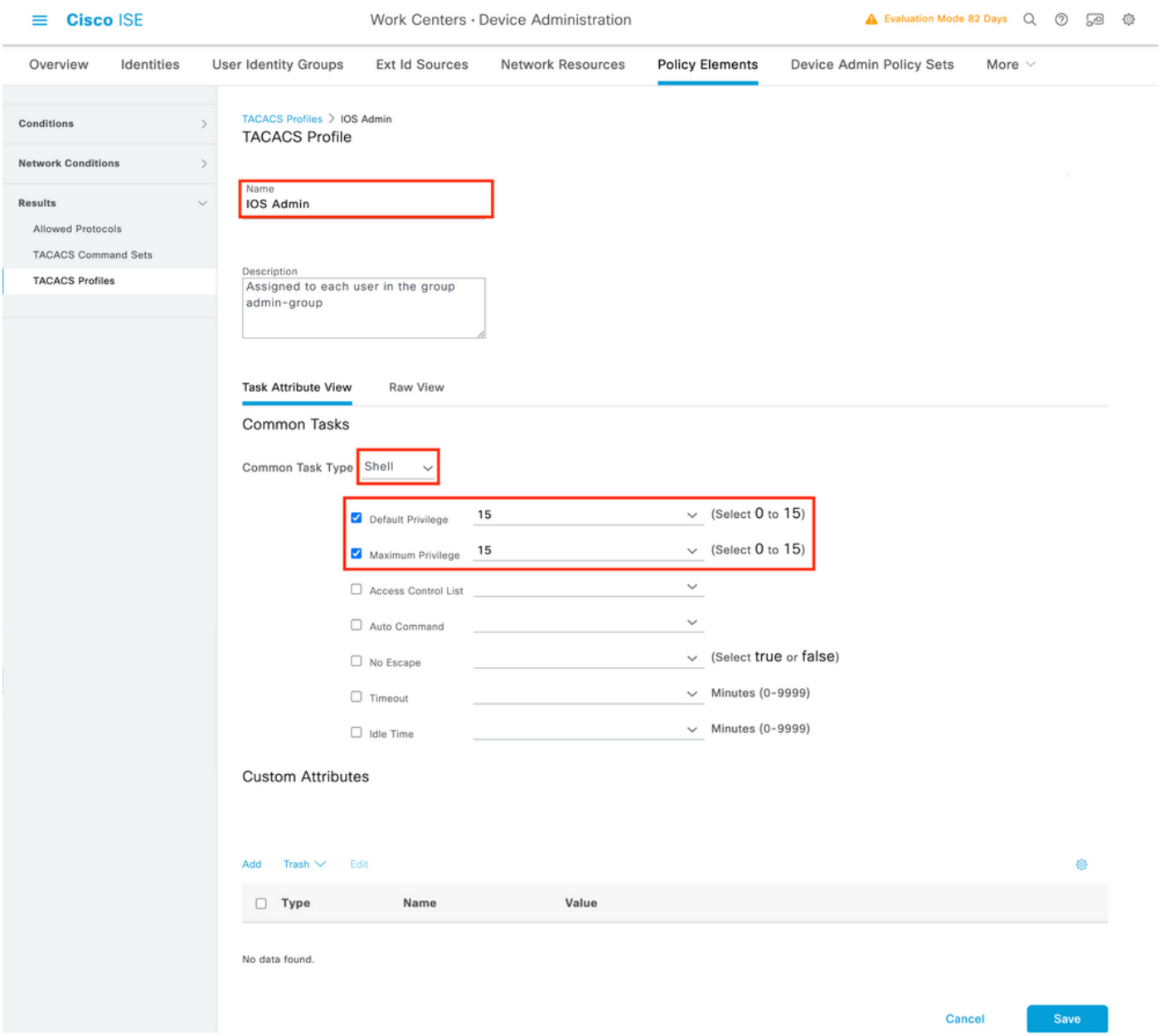
الخطوة 3. قم بإنشاء توصيفات TACACS، لإرجاع الامتياز.

<u>من واجهة المستخدم الرسومية:</u>

للحصول على حقوق الوصول للمسؤول، يلزمadminuser أن يكون مستوى الامتياز 15، والذي يسمح بالوصول إلى طبقة مطالبة exec. من ناحية أخرى، الhelpdeskuser يحتاج الأمر إلى وصول موجه أوامر EXEC إلى Shell وبالتالي يمكن تعيينه بمستوى امتياز أقل من 15. لتعيين مستوى الامتياز المناسب للمستخدمين، يمكن إستخدام ملفات تعريف التخويل. يمكن تكوين هذه العناصر من صفحةWork Centers > Device Administration > Policy Elements واجهة المستخدم الرسومية (ISE) أسفل علامة التبويبResults > TACACS Profiles كما هو موضح في الصورة التالية.



لتكوين ملف تعريف TACACS جديد، أستخدم الزر "إضافة" الذي يفتح نموذج تكوين ملف التعريف الجديد المماثل لذلك الموجود في الصورة. يجب أن يبدو هذا النموذج بهذا الشكل بشكل خاص لتكوين ملف التعريف الذي يتم تعيينه إلى adminuser (والذي هو، باستخدام مستوى امتيازات shell 15).



كرر العملية لملف helpdesk التعريف. ل هذا الأخير، التقصير امتياز، as maximum امتياز، كل ثبتت إلى 1.

الخطوة 4. إنشاء مجموعات مستخدمين على ISE.

هذا وه نفس معروض في الخطوة 3. من القسم تكوين RADIUS ISE من هذا المستند.

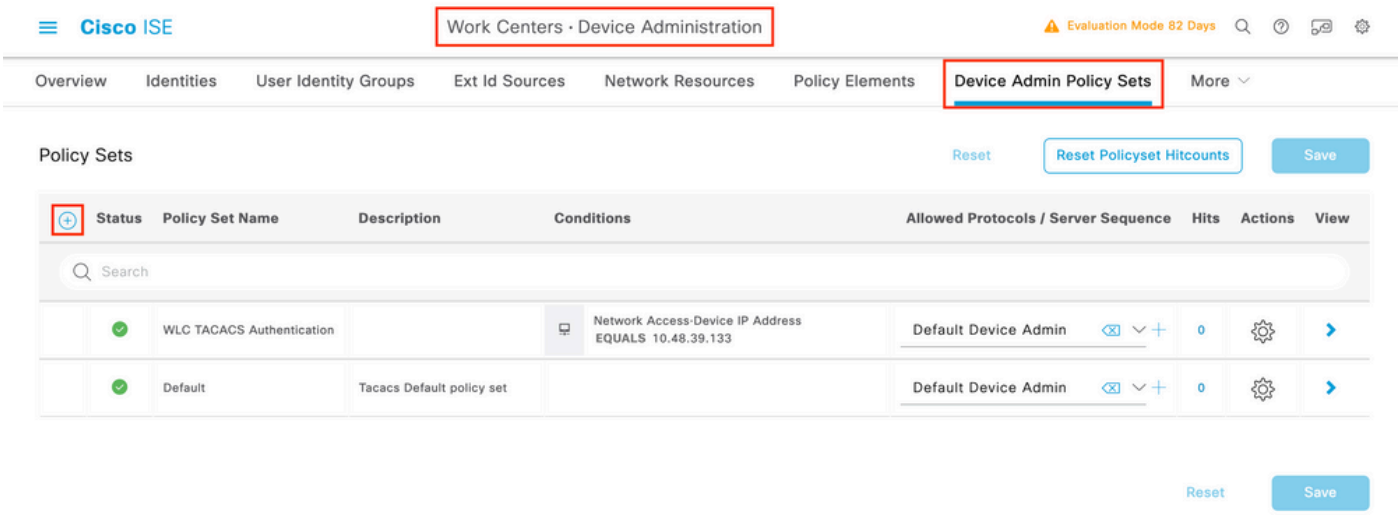
الخطوة 5. قم بإنشاء المستخدمين على ISE.

هذا وه نفس معروض في الخطوة 4. من القسم تكوين RADIUS ISE من هذا المستند.

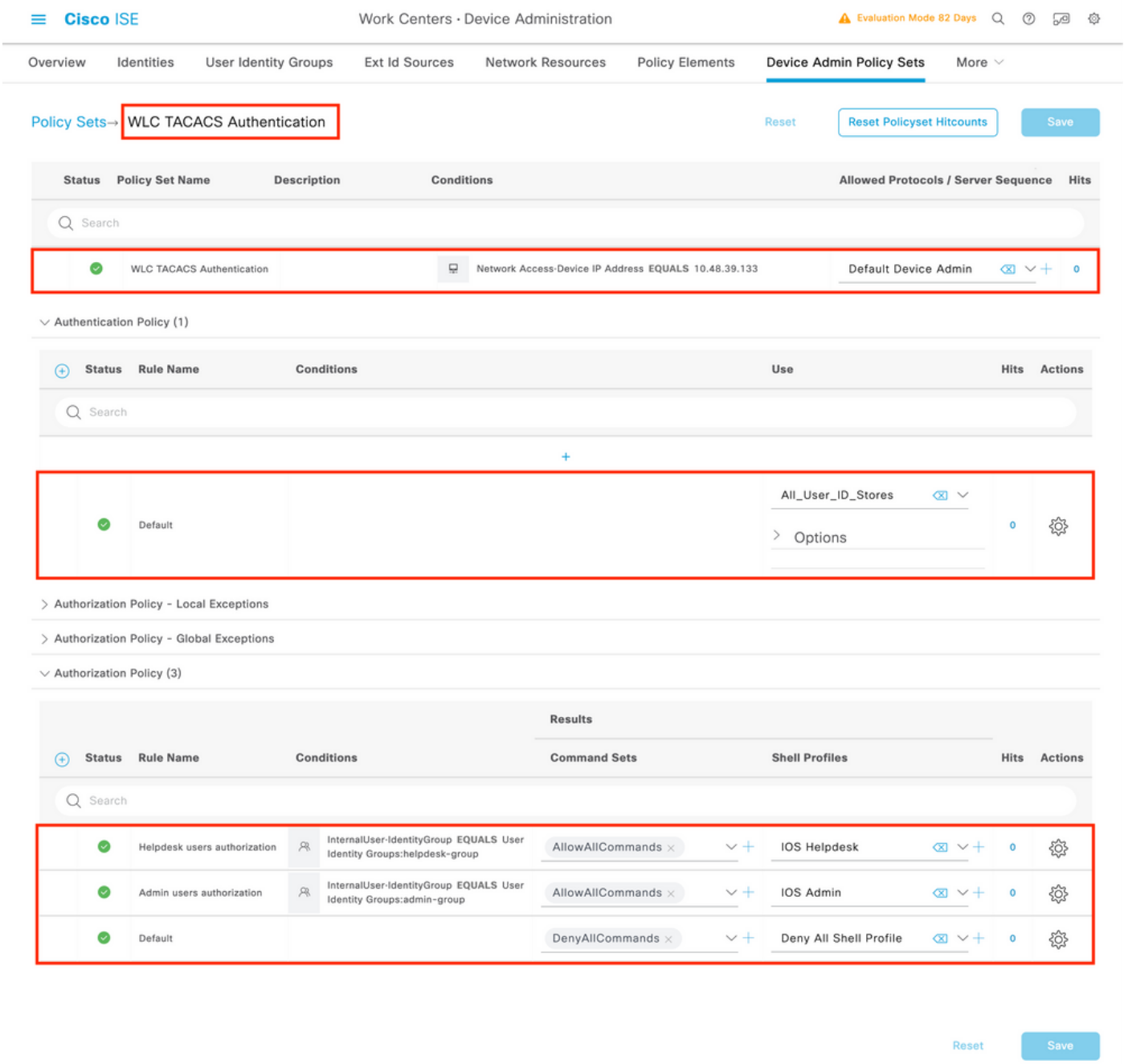
الخطوة 6. إنشاء مجموعة نهج مسؤول الجهاز.

من واجهة المستخدم الرسومية:

بالنسبة للوصول إلى RADIUS، بمجرد إنشاء المستخدمين، يظل من الضروري تعريف سياسات المصادقة والتفويض الخاصة بهم على ISE لمنحهم حقوق الوصول المناسبة. تستخدم مصادقة TACACS مجموعات نهج مسؤول الجهاز لهذه الغاية، والتي يمكن تكوينها من Work Centers > Device Administration > Device Admin Policy Sets GUI Pageكما هو موضح.



لإنشاء مجموعة سياسات لإدارة الأجهزة، أستخدم الزر "إضافة" المؤطر باللون الأحمر في الصورة السابقة، يؤدي هذا إلى إضافة عنصر إلى قائمة مجموعات النهج. قم بتوفير اسم للمجموعة التي تم إنشاؤها حديثًا، وشرط يجب تطبيقها تحته، والبروتوكولات/تسلسل الخادم المسموح به (هنا، Default Device Admin ما يكفي). أستخدم الزرSave لإنهاء إضافة مجموعة النهج واستخدام رأس السهم الموجود على يمينه للوصول إلى صفحة التكوين الخاصة به، كما يظهر على الصفحة المعروضة.



تقوم مجموعة النهج المحددة "مصادقة WLC TACACS" في هذا المثال بتصفية الطلبات بعنوان IP الذي يساوي المثال C9800 WLC عنوان IP.

كنهج مصادقة، تم ترك القاعدة الافتراضية لأنها تفي باحتياجات الاستخدام. تم إعداد قاعدتي تفويض:

- يتم تشغيل الخيار الأول عندما ينتمي المستخدم إلى المجموعةadmin-group المعرفة. وهو يسمح بجميع الأوامر (عبر القاعدة الافتراضيةPermit_all) ويعين الامتياز 15 (عبر ملف تعريف TACACSIOS_Admin المحدد).

- يتم تشغيل الخيار الثاني عندما ينتمي المستخدم إلى المجموعةhelpdesk-group المعرفة. وهو يسمح لك أمر (من خلال Permit_all القاعدة الافتراضية) ويعين امتياز 1 (من خلال ملف تعريف TACACSIOS_Helpdesk المعرف).

بعد اكتمال هذه الخطوة، يمكن إستخدام بيانات الاعتماد التي تم تكوينها ل adminuser المستخدمينhelpdesk للمصادقة في

عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عبر واجهة المستخدم الرسومية (GUI) أو باستخدام برنامج Telnet/SSH.

استكشاف الأخطاء وإصلاحها

إذا كان خادم RADIUS الخاص بك يتوقع إرسال سمة RADIUS لنوع الخدمة، فيمكنك الإضافة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) :

```
radius-server attribute 6 on-for-login-auth
```

أستكشاف أخطاء واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) أو وصول واجهة سطر الأوامر (CLI) عبر بروتوكول RADIUS/TACACS+ الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)

من أجل أستكشاف أخطاء وصول TACACS+ إلى واجهة المستخدم الرسومية (GUI) أو واجهة سطر الأوامر (CLI) الخاصةdebug tacacs بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وإصلاحها، قم بإصدار الأمر، بالإضافة إلى شاشة المحطة الطرفية الأولى ومشاهدة الإخراج المباشر عند إجراء محاولة تسجيل الدخول.

على سبيل المثال، يقوم تسجيل الدخول الناجح الذي يتبعه تسجيل الخروج من adminuser المستخدم بإنشاء هذا الإخراج.

<#root>

WLC-9800#

terminal monitor

```
WLC-9800#
```

debug tacacs

```
TACACS access control debugging is on
WLC-9800#
Dec 8 11:38:34.684: TPLUS: Queuing AAA Authentication request 15465 for processing
Dec 8 11:38:34.684: TPLUS(00003C69) login timer started 1020 sec timeout Dec 8 11:38:34.684: TPLUS: pro
```

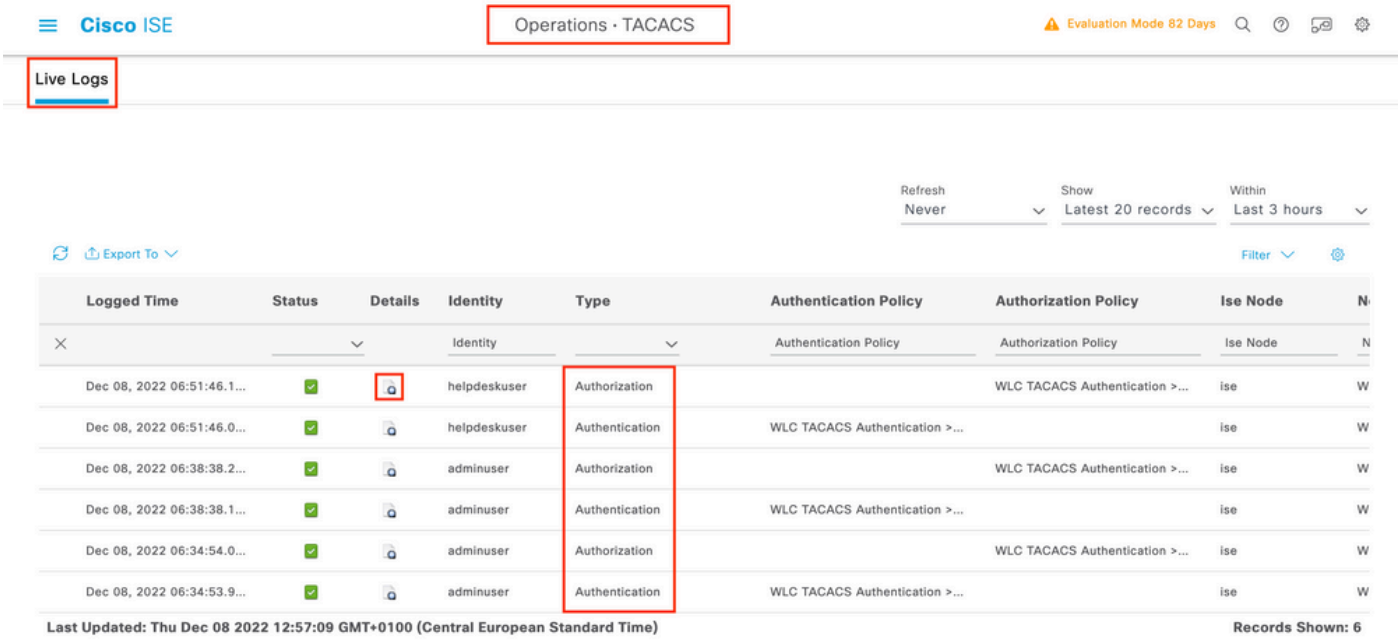
ويمكن ملاحظة أن خادم TACACS+ يرجع من هذه السجلات المتبقي الصحيح (وهو AV priv-lvl=15).

عندما تقوم بمصادقة RADIUS، يظهر إخراج تصحيح مماثل، والذي يتعلق بحركة مرور RADIUS.

الأمر debug aaa authenticationوبدل من ذلك،debug aaa authorization عرض قائمة الطرق التي يتم إختيارها بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عند محاولة المستخدم تسجيل الدخول.

أستكشاف أخطاء واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وإصلاحها التوافق مع معيار ISE لواجهة المستخدم الرسومية (GUI) عبر واجهة سطر الأوامر (TACACS+) للوصول إلى

من الصفحة Operations > TACACS > Live Logs، يمكن عرض كل مصادقة مستخدم تتم مع TACACS+ حتى آخر 24 ساعة. لتوسيع تفاصيل تفويض وأ مصادقة TACACS+، أستخدم زر التفاصيل المتعلق بهذا الحدث.



عند التوسيع، تبدوhelpdeskuser محاولة مصادقة ناجحة لهذه الطريقة كما يلي:

Cisco ISE

Overview

Request Type	Authentication
Status	Pass
Session Key	ise/459637517/243
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdeskuser
Authentication Policy	WLC TACACS Authentication >> Default
Selected Authorization Profile	IOS Helpdesk

Authentication Details

Generated Time	2022-12-08 06:51:46.077000 -05:00
Logged Time	2022-12-08 06:51:46.077
Epoch Time (sec)	1670500306
ISE Node	ise
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdeskuser
Network Device Name	WLC-9800
Network Device IP	10.48.39.133
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	tty5
Remote Address	10.61.80.151

Steps

13013	Received TACACS+ Authentication START Request
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - Network Access.Device IP Address
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
13045	TACACS+ will use the password prompt from global TACACS+ configuration
13015	Returned TACACS+ Authentication Reply
13014	Received TACACS+ Authentication CONTINUE Request (Step latency=3149ms)
15041	Evaluating Identity Policy
22072	Selected identity source sequence - All_User_ID_Stores
15013	Selected Identity Source - Internal Users
24210	Looking up User in Internal Users IDStore
24212	Found User in Internal Users IDStore
22037	Authentication Passed
15036	Evaluating Authorization Policy
15048	Queried PIP - Network Access.UserName
15048	Queried PIP - InternalUser.IdentityGroup
13015	Returned TACACS+ Authentication Reply

ومن هذا، يمكنك أن ترى أنه تمت مصادقة المستخدمhelpdeskuser بنجاح على جهازWLC-9800 الشبكة بمساعدة منWLC TACACS Authentication > Default المصادقة. علاوة على ذلك، تم تعيينIOS Helpdesk ملف تعريف التخويل لهذا المستخدم، وتم منح مستوى الامتياز 1.

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).