تكوين TACACS+ للشبكة اللاسلكية الموحدة من Cisco

المحتويات

المقدمة

يقدم هذا المستند مثالا لتكوين نظام التحكم في الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) في وحدة تحكم شبكة LAN اللاسلكية (WLC) من Cisco ونظام التحكم اللاسلكي (WCS) من

Cisco لشبكة Cisco اللاسلكية الموحدة. يزود هذا وثيقة أيضا بعض أساسي يتحرى طرف.

TACACS+ هو بروتوكول عميل/خادم يوفر أمانا مركزيا للمستخدمين الذين يحاولون الحصول على وصول الإدارة إلى موجه أو خادم وصول إلى الشبكة. يوفر TACACS+ خدمات AAA التالية:

- مصادقة المستخدمين الذين يحاولون تسجيل الدخول إلى أجهزة الشبكة
- التفويض لتحديد مستوى الوصول الذي يجب أن يتمتع به المستخدمون
- المحاسبة لتعقب كافة التغييرات التي يقوم بها المستخدم

ارجع إلى تكوين TACACS+ للحصول على مزيد من المعلومات حول خدمات AAA ووظائف TACACS+.

ارجع إلى مقارنة TACACS+ و RADIUS لمقارنة TACACS+ و RADIUS.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة كيفية تكوين نقاط الوصول في الوضع Lightweight (LAPs) و WLCs للتشغيل الأساسي
- معرفة ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) وطرائق الأمان اللاسلكية
- RADIUS للمعرفة الأساسية و TACACS+
- معرفة أساسية بتكوين Cisco ACS

المكونات المستخدمة

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

- Cisco Secure ACS ل Windows، الإصدار 4.0
- وحدة التحكم في شبكة LAN اللاسلكية من Cisco التي تشغل الإصدار 4.1.171.0. يتم دعم وظيفة TACACS+ على قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) على الإصدار 4.1.171.0 من البرنامج أو إصدار أحدث.
- نظام التحكم اللاسلكي من Cisco الذي يشغل الإصدار 4.1.83.0. وظيفة TACACS+ على WCS مدعومة على البرنامج الإصدار 4.1.83.0 أو إصدار أحدث.

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

تنفيذ TACACS+ في وحدة التحكم

المصادقة

يمكن إجراء المصادقة باستخدام خادم قاعدة بيانات محلية أو RADIUS أو TACACS+ يستخدم اسم مستخدم وكلمة مرور. التنفيذ ليس معياريا بالكامل. يتم ربط خدمات المصادقة والتفويض ببعضها البعض. على سبيل المثال، إذا تم

إجراء المصادقة باستخدام قاعدة بيانات RADIUS/محلية، فلا يتم إجراء التفويض باستخدام TACACS+. وسوف يستخدم الأذونات المرتبطة بالمستخدم في قاعدة البيانات المحلية أو RADIUS، مثل للقراءة فقط أو للقراءة والكتابة، بينما عند إجراء المصادقة باستخدام TACACS+، يتم ربط التفويض ب TACACS+.

في الحالات التي يتم فيها تكوين قواعد بيانات متعددة، يتم توفير واجهة سطر الأوامر (CLI) لإملاء التسلسل الذي يجب به إحالة قاعدة البيانات الخلفية.

الاعتماد

التفويض يستند إلى المهمة وليس إلى تفويض فعلي يستند إلى كل أمر. يتم تعيين المهام إلى علامات تبويب مختلفة تتوافق مع عناصر شريط القوائم السبعة الموجودة حاليا على واجهة المستخدم الرسومية (GUI) للويب. هذه هي عناصر شريط القوائم:

- جهاز عرض
- WLANs
- مراقب
- لاسلكي
- الأمان
- الذاتية المُحسنة

يستند السبب وراء هذا التعيين إلى حقيقة أن معظم العملاء يستخدمون واجهة الويب لتكوين وحدة التحكم بدلا من CLI (واجهة سطر الأوامر).

يتوفر دور إضافي لإدارة إدارة إدارة مجموعة الضغط (LOBBY) للمستخدمين الذين يحتاجون إلى امتيازات إدارة مجموعة الضغط فقط.

يتم تكوين المهمة التي يحق للمستخدم القيام بها في خادم ACS) +TACACS) باستخدام أزواج السمة-القيمة (AV) المخصصة. يمكن تخويل المستخدم لمهمة واحدة أو عدة مهام. الحد الأدنى للتخويل هو "مراقبة" فقط والحد الأقصى هو ALL (مصرح له بتنفيذ كافة علامات التبويب السبعة). إذا لم يكن المستخدم مؤهلا لمهمة معينة، يظل مسموحا للمستخدم بالوصول إلى تلك المهمة في وضع القراءة فقط. في حالة تمكين المصادقة وعدم إمكانية الوصول إلى خادم المصادقة أو عدم القدرة على التخويل، لا يمكن للمستخدم تسجيل الدخول إلى وحدة التحكم.

ملاحظة: لكي تنجح مصادقة الإدارة الأساسية عبر TACACS+، يجب تكوين خوادم المصادقة والتفويض على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تكوين المحاسبة إختياري.

محاسبة

تحدث عملية المحاسبة عندما يتم تنفيذ إجراء معين بدأه المستخدم بنجاح. يتم تسجيل السمات التي تم تغييرها في خادم محاسبة TACACS+ مع ما يلي:

- معرف المستخدم الخاص بالشخص الذي أجرى التغيير
- المضيف البعيد الذي تم تسجيل دخول المستخدم منه
- تاريخ ووقت تنفيذ الأمر
- مستوى تخويل المستخدم
- سلسلة توفر معلومات حول الإجراء الذي تم تنفيذه والقيم المقدمة

إذا أصبح خادم المحاسبة غير قابل للوصول، يظل بإمكان المستخدم متابعة الجلسة.

ملاحظة: لا يتم إنشاء سجلات المحاسبة من WCS في إصدار البرنامج 4.1 أو الأحدث.

تكوين TACACS+ في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

يقدم برنامج WLC الإصدار 4.1.171.0 وفيما بعد تغييرات جديدة في واجهة سطر الأوامر (CLI) وواجهة المستخدم الرسومية (GUI) للويب لتمكين وظائف TACACS+ على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). تم إدراج واجهة سطر الأوامر (CLI) التي تم إدخالها في هذا القسم كمرجع. تتم إضافة التغييرات المقابلة لواجهة المستخدم الرسومية (GUI) للويب ضمن علامة التبويب "الأمان".

يفترض هذا وثيقة أن التشكيل أساسي من ال WLC أتمت بالفعل.

in order to شكلت TACACS+ في ال WLC جهاز تحكم، أنت تحتاج أن يتم هذا steps:

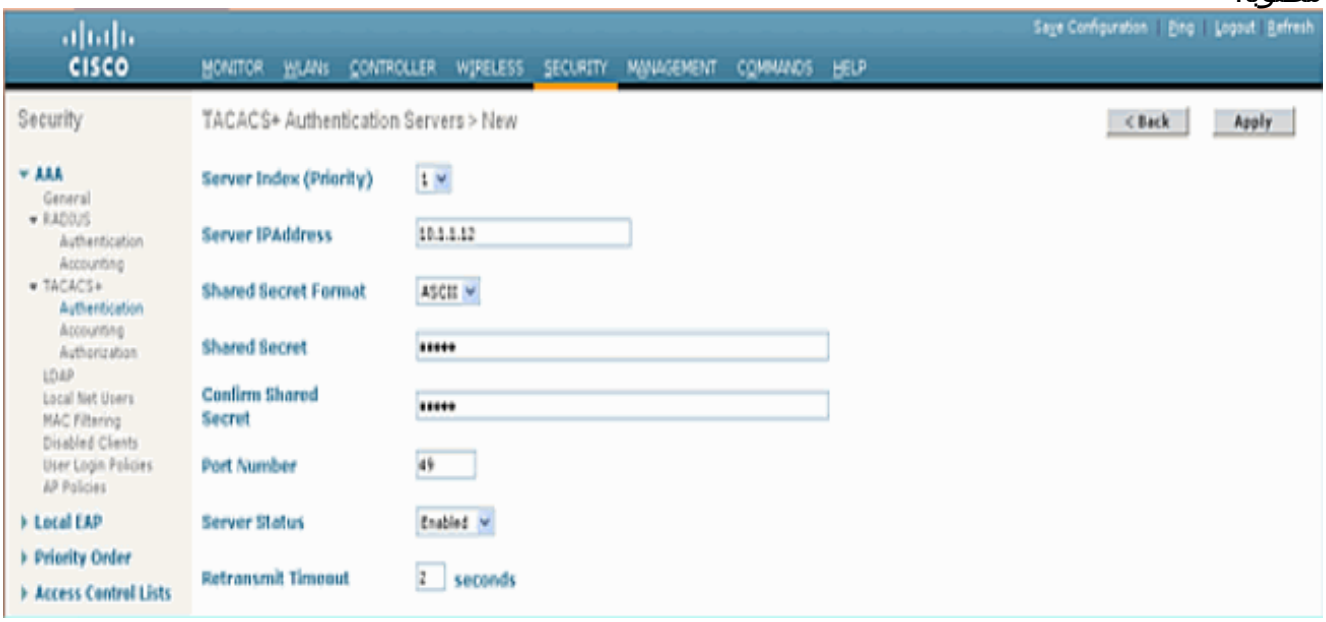
1. إضافة خادم مصادقة TACACS+
2. إضافة خادم تفويض TACACS+
3. إضافة خادم محاسبة TACACS+
4. تكوين ترتيب المصادقة

إضافة خادم مصادقة TACACS+

أكمل الخطوات التالية لإضافة خادم مصادقة TACACS+:

1. أستخدم واجهة المستخدم الرسومية، وانتقل إلى **الأمان > TACACS+ > المصادقة**.

2. قم بإضافة عنوان IP الخاص بخادم TACACS+ وأدخل المفتاح السري المشترك. قم بتغيير المنفذ الافتراضي ل TCP/49 إذا كان ذلك مطلوبا.



3. طقطقة **يطبق**.يمكنك تحقيق ذلك من CLI باستخدام الأمر **config tacacs auth add** *<server index> <ip*

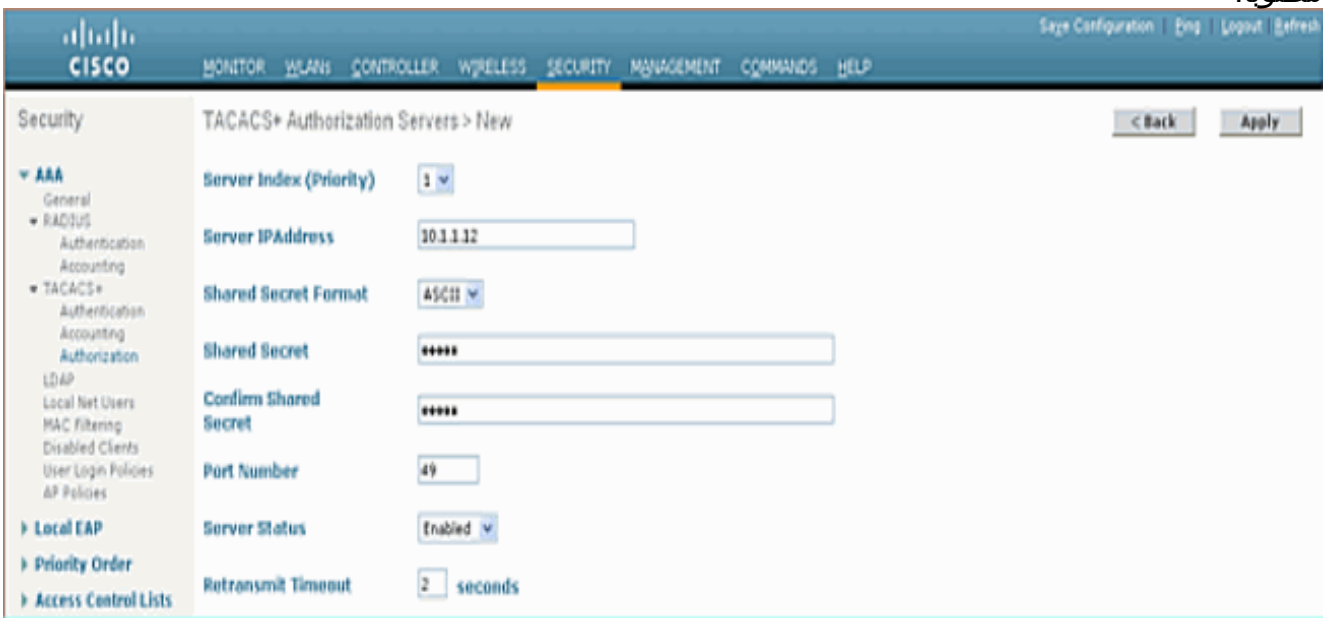
:*<addr> <port> [ascii/hex]* **<secret**

```
Cisco Controller) >config tacacs auth add 1 10.1.1.12 49 ascii cisco123)
```

إضافة خادم تفويض TACACS+

أكمل الخطوات التالية لإضافة خادم تفويض TACACS+:

1. من واجهة المستخدم الرسومية، انتقل إلى **الأمان > TACACS+ > التفويض**.
2. قم بإضافة عنوان IP الخاص بخادم TACACS+ وأدخل المفتاح السري المشترك. قم بتغيير المنفذ الافتراضي ل TCP/49 إذا كان ذلك مطلوبا.



3. طقطقة **يطبق**.يمكنك تحقيق ذلك من CLI باستخدام الأمر **config tacacs athr** *<server index> <ip addr>* :*<<port> [ascii/hex]* **<secret**

```
Cisco Controller) >config tacacs athr add 1 10.1.1.12 49 ascii cisco123)
```

إضافة خادم محاسبة TACACS+

أكمل الخطوات التالية لإضافة خادم محاسبة TACACS+:

1. أستخدم واجهة المستخدم الرسومية، وانتقل إلى **الأمان > TACACS+ > المحاسبة**.
2. قم بإضافة عنوان IP الخاص بالخادم وأدخل المفتاح السري المشترك. قم بتغيير المنفذ الافتراضي ل TCP/49 إذا كان ذلك مطلوبا.

3. طقطقة **يطبق**.يمكنك تحقيق ذلك من CLI باستخدام الأمر **config tacacs acct add** ***<server index> <ip*** ***<addr> <port> [ascii/hex]*** **<secret**>:

```
Cisco Controller) >config tacacs acct add 1 10.1.1.12 49 ascii cisco123)
```

تكوين ترتيب المصادقة

توضح هذه الخطوة كيفية تكوين ترتيب المصادقة والتفويض والمحاسبة (AAA) للمصادقة عند وجود قواعد بيانات متعددة تم تكوينها. يمكن أن يكون أمر المصادقة **محليا و RADIUS**، أو **محليا و TACACS**. تكوين وحدة التحكم الافتراضية لترتيب المصادقة هو *محلي و RADIUS*.

أتمت هذا steps in order to شكلت أمر المصادقة:

1. من واجهة المستخدم الرسومية، انتقل إلى **الأمان > ترتيب الأولوية > مستخدم الإدارة**.
2. حدد أولوية المصادقة.في هذا المثال، تم تحديد TACACS+.
3. طقطقة **يطبق** يقع in order to التحديد.

يمكنك تحقيق ذلك من CLI باستخدام الأمر ***<server1> <server2*** **<config aaa auth mgmt**>:

```
Cisco Controller) >config aaa auth mgmt tacacs local)
```

التحقق من التكوين

يصف هذا قسم الأمر يستعمل أن يدقق TACACS+ تشكيل على ال WLC. هذا بعض مفيد **عرض** أمر أن يساعد أن

يحدد ما إذا التشكيل صحيح:

- **show aaa auth**— يوفر معلومات حول ترتيب المصادقة.

```
Cisco Controller) >show aaa auth)
:Management authentication server order
local .....1
Tacacs .....2
```

- **show tacacs summary** — يعرض ملخصا لخدمات TACACS+ وإحصاءاته.

```
Cisco Controller) >show tacacs summary)
Authentication Servers

Idx  Server Address    Port    State     Tout
---  --------  ------  ---------------  ---
   Enabled   2      49         10.1.1.12    1

Authorization Servers

Idx  Server Address    Port    State     Tout
---  --------  ------  ---------------  ---
   Enabled   2      49         10.1.1.12    1

Accounting Servers

Idx  Server Address    Port    State     Tout
---  --------  ------  ---------------  ---
   Enabled   2      49         10.1.1.12    1
```

- **show tacacs auth stats**— يعرض إحصائيات خادم مصادقة TACACS+.

```
Cisco Controller) >show tacacs auth statistics)
:Authentication Servers

Server Index..... 1
Server Address..... 10.1.1.12
(Msg Round Trip Time..... 0 (1/100 second
First Requests..... 7
Retry Requests..... 3
Accept Responses..... 3
Reject Responses..... 0
Error Responses..... 0
Restart Responses..... 0
Follow Responses..... 0
GetData Responses..... 0
Encrypt no secret Responses..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 12
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **show tacacs athr status**—يعرض إحصائيات خادم تفويض TACACS+.

```
Cisco Controller) >show tacacs athr statistics)
:Authorization Servers

Server Index..... 1
Server Address..... 10.1.1.12
(Msg Round Trip Time..... 0 (1/100 second
First Requests..... 3
Retry Requests..... 3
Received Responses..... 3
Authorization Success..... 3
Authorization Failure..... 0
Challenge Responses..... 0
Malformed Msgs..... 0
```

```
Bad Athrenticator Msgs..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0
```

- **show tacacs acct stats**— يعرض إحصائيات خادم محاسبة TACACS+.

```
Cisco Controller) >show tacacs acct statistics)
:Accounting Servers

Server Index..... 1
Server Address..... 10.1.1.12
(Msg Round Trip Time..... 0 (1/100 second
First Requests..... 133
Retry Requests..... 0
Accounting Response..... 0
Accounting Request Success..... 0
Accounting Request Failure..... 0
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Timeout Requests..... 399
Unknowntype Msgs..... 0
Other Drops..... 0
```

تكوين خادم ACS الآمن من Cisco

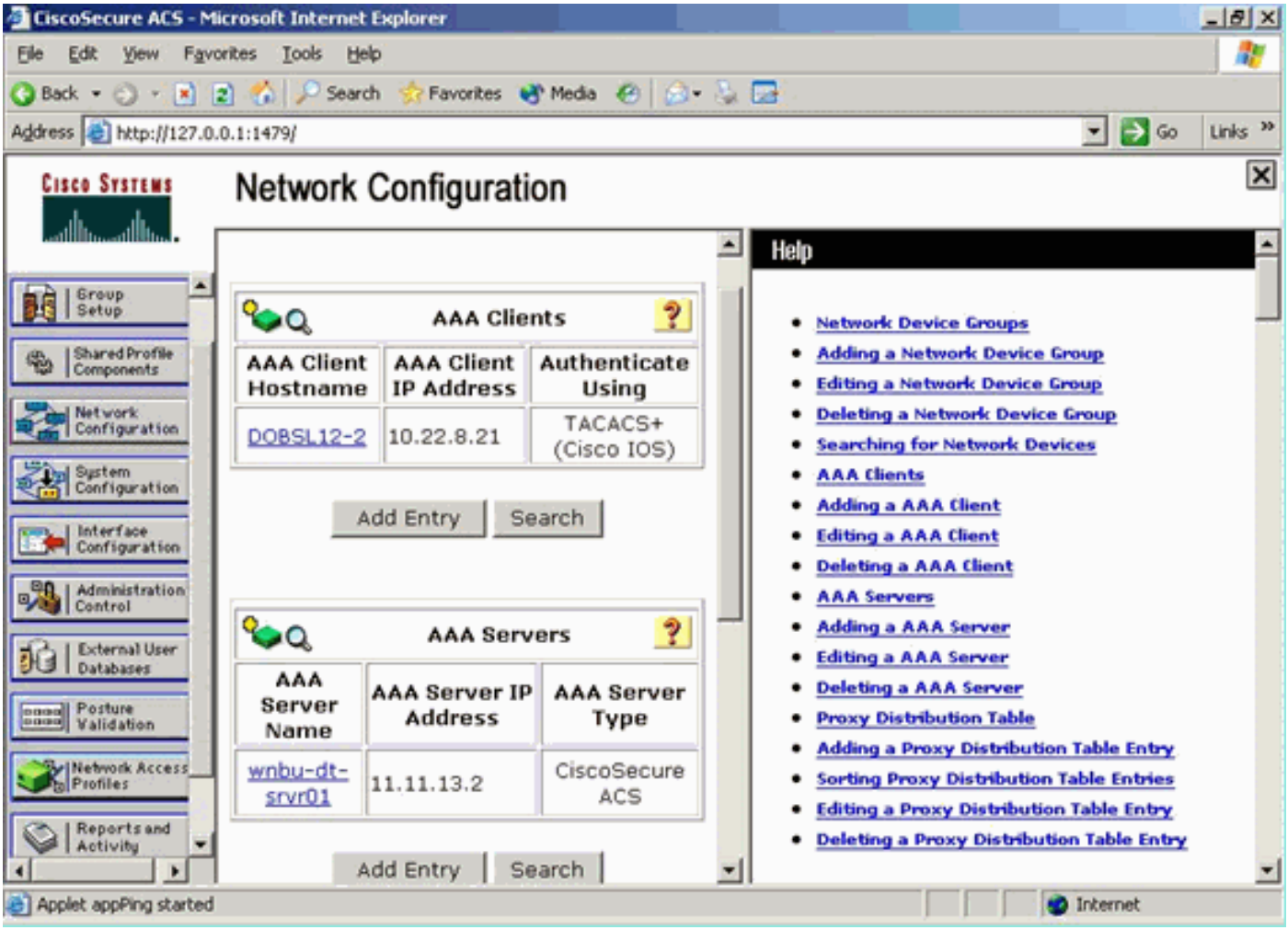
يوفر هذا القسم الخطوات المعنية بخادم TACACS+ ACS لإنشاء الخدمات والسمات المخصصة، وتعيين الأدوار للمستخدمين أو المجموعات.

لم يتم شرح إنشاء المستخدمين والمجموعة في هذا القسم. من المفترض أن المستخدمين والمجموعات يتم إنشاؤها حسب الحاجة. ارجع إلى دليل المستخدم ل Cisco Secure ACS ل Windows Server 4.0 للحصول على معلومات حول كيفية إنشاء مستخدمين ومجموعات مستخدمين.

تكوين الشبكة

أكمل هذه الخطوة:

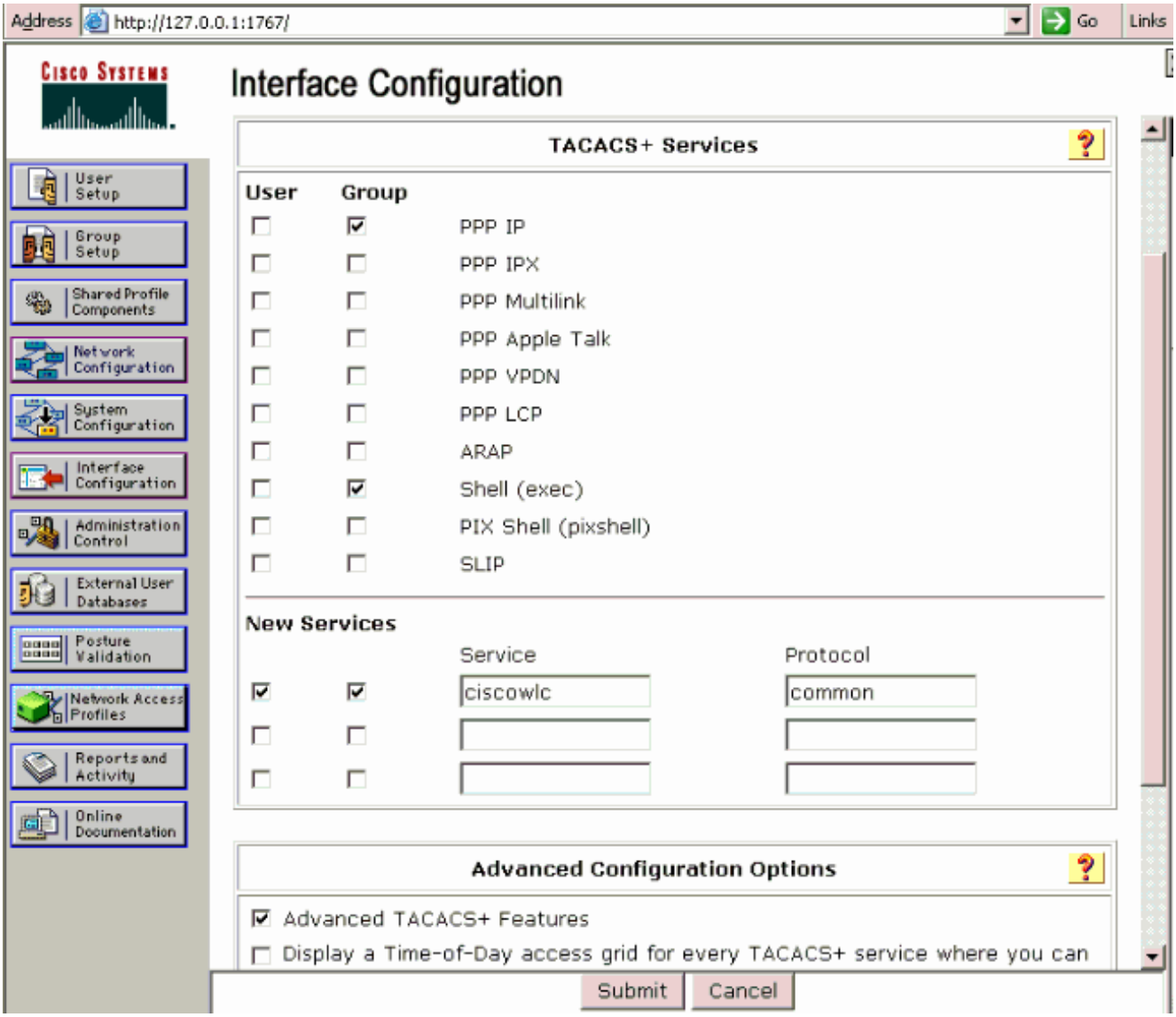
إضافة عنوان IP الخاص بإدارة وحدة التحكم كعميل AAA مع آلية المصادقة مثل Cisco IOS) +TACACS).



تكوين الواجهة

أكمل الخطوات التالية:

1. في قائمة تكوين الواجهة، حدد إرتباط Cisco IOS) **TACACS+**).
2. تمكين **الخدمات الجديدة**.
3. حدد خانتي الاختيار **المستخدم** و**المجموعة**.
4. أدخل **CiscoWLC** للخدمة و**شائع** للبروتوكول.
5. قم بتمكين **ميزات TACACS+ المتقدمة**.

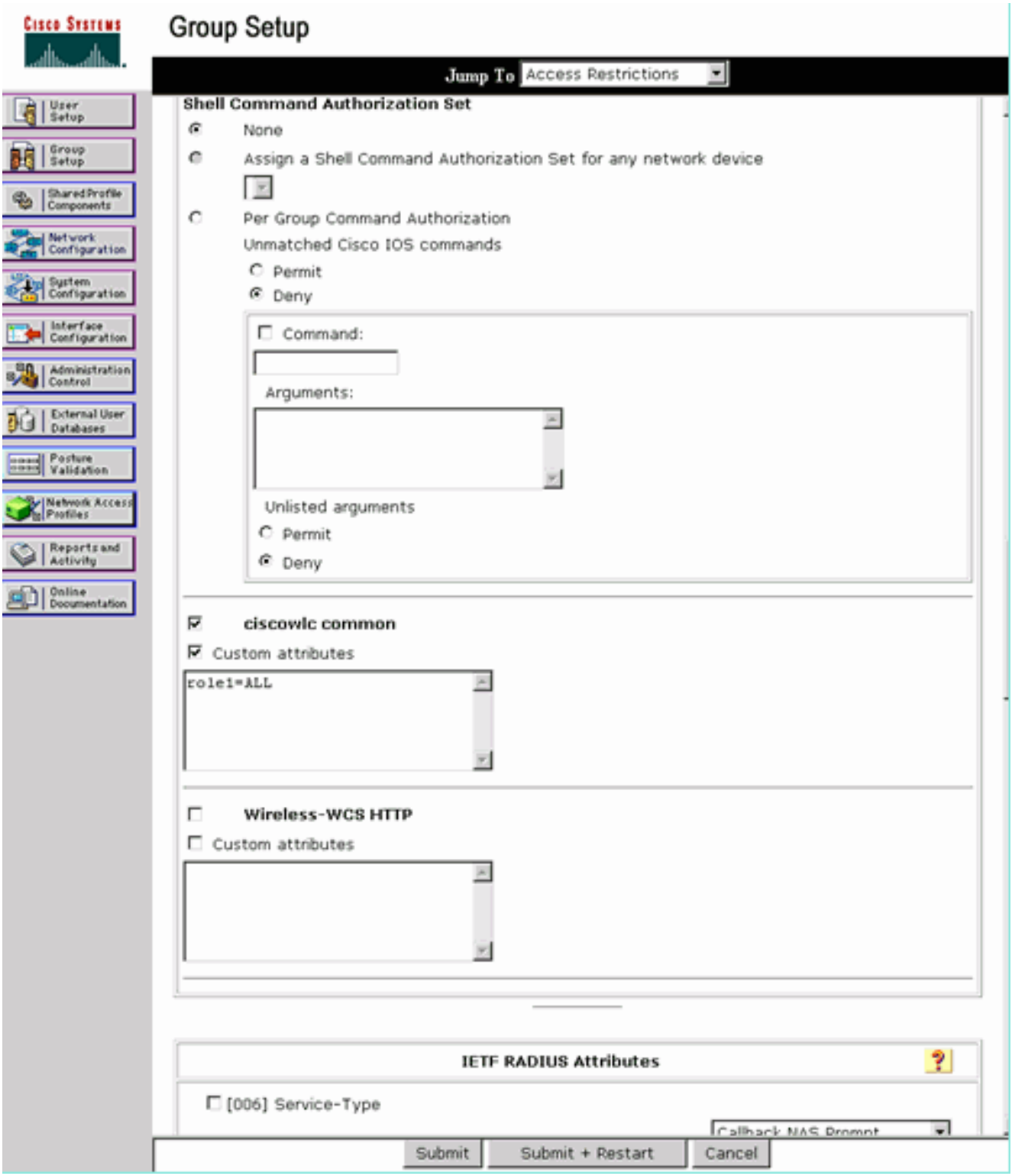


6. انقر فوق **إرسال** لتطبيق التغييرات.

إعداد المستخدم/المجموعة

أكمل الخطوات التالية:

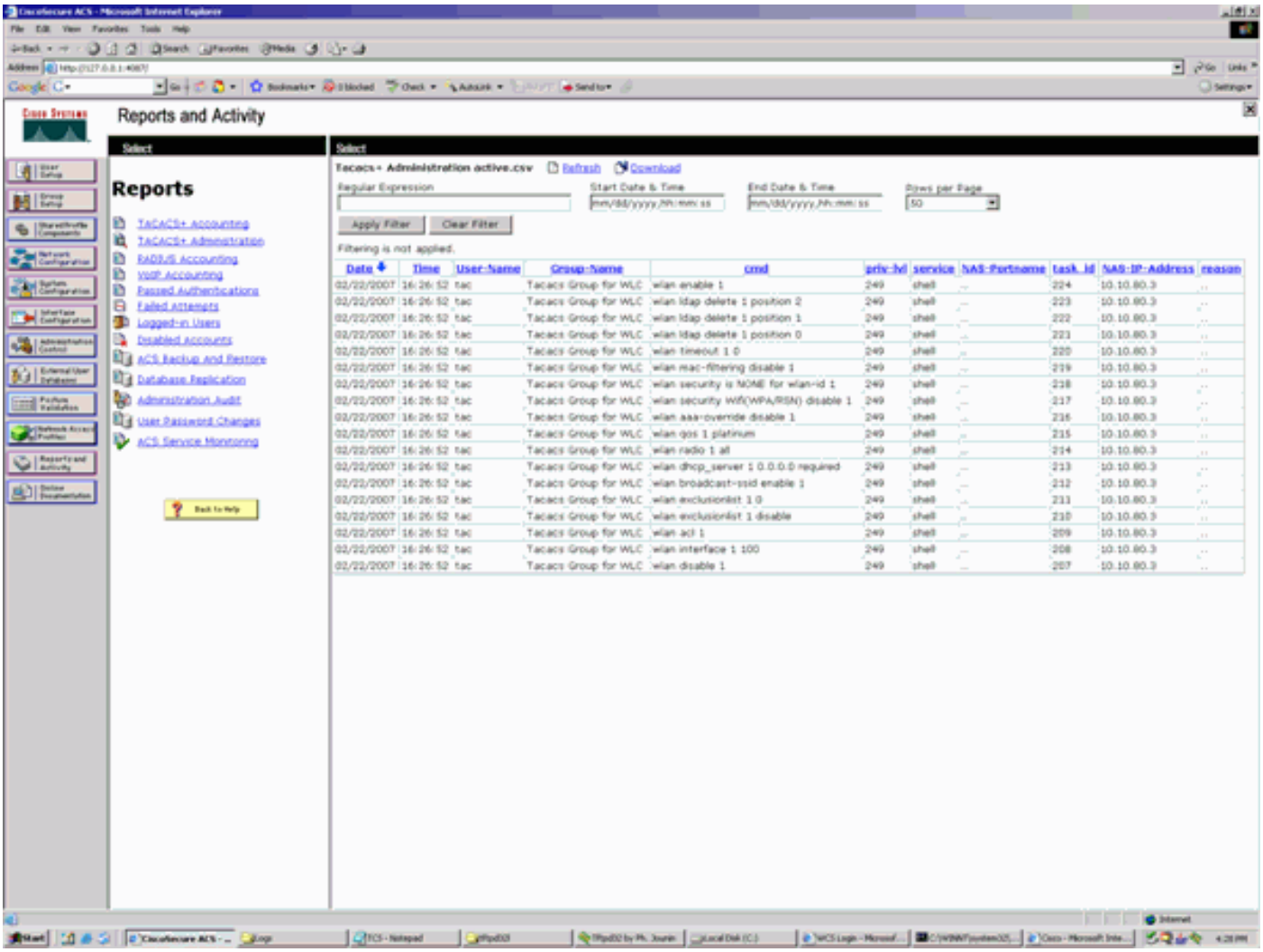
1. تحديد مستخدم/مجموعة تم إنشاؤها مسبقا.
2. انتقل إلى **إعدادات TACACS+**.
3. حدد خانة الاختيار التي تتوافق مع خدمة *CiscoWLC* التي تم إنشاؤها في قسم تكوين الواجهة.
4. حدد خانة الاختيار **سمات مخصصة**.



5. في مربع النص الموجود أسفل السمات المخصصة، أدخل هذا النص إذا كان المستخدم الذي أنشأه يحتاج إلى الوصول فقط إلى الشبكة المحلية اللاسلكية (WLAN) والأمان ووحدة التحكم: **role1=wlan role2=security**.إذا كان المستخدم بحاجة إلى الوصول إلى علامة التبويب "الأمان" فقط، فأدخل هذا النص: **role3=controller**.يتوافق الدور مع عناصر شريط القوائم السبعة في واجهة المستخدم الرسومية (GUI) الخاصة بويب لوحدة التحكم. عناصر شريط القائمة هي شاشة، شبكة محلية لاسلكية، وحدة تحكم، لاسلكي، أمان، إدارة وأمر. **role1=security**
6. أدخل الدور الذي يحتاج إليه المستخدم ل Role1 و Role2 وما إلى ذلك. إذا كان المستخدم بحاجة إلى كافة الأدوار، فيجب إستخدام الكلمة الأساسية **all** (**all**). بالنسبة لدور مسؤول ساحة الانتظار، يجب إستخدام **مجموعة** الضغط الرئيسية.

سجلات المحاسبة في ACS الآمن من Cisco

تتوفر سجلات محاسبة TACACS+ من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) في ACS الآمن من Cisco في إدارة التقارير والنشاط وفقا لمعيار TACACS+:

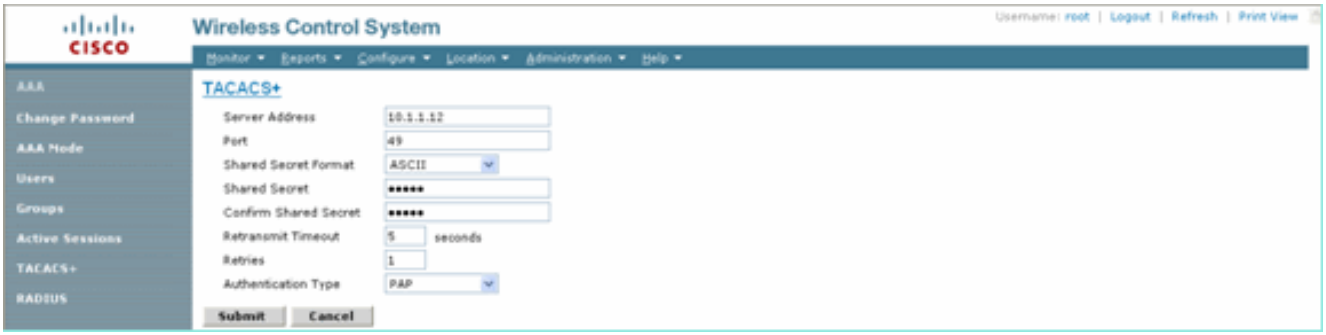


تكوين TACACS+ في WCS

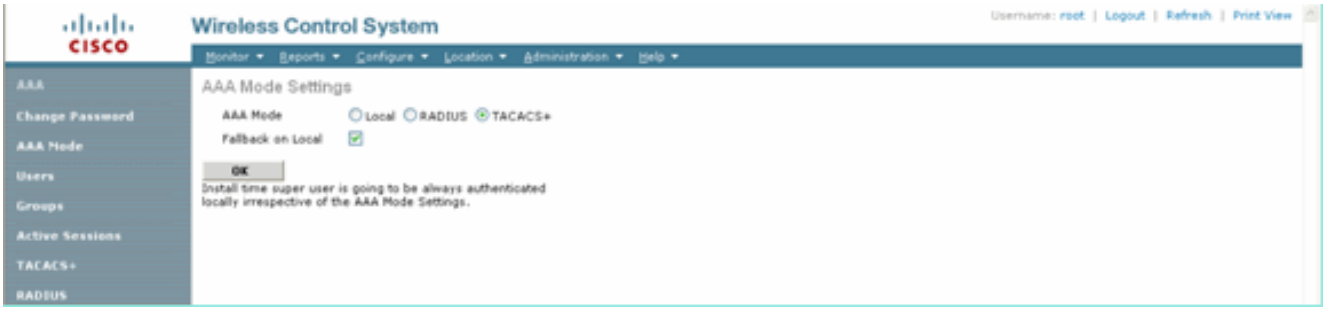
أكمل الخطوات التالية:

1. من ال login، gui إلى ال WCS مع الجذر حساب.
2. قم بإضافة خادم TACACS+. انتقل إلى **الإدارة > TACACS+ > AAA > إضافة خادم TACACS+**.

3. قم بإضافة تفاصيل خادم TACACS+، مثل عنوان IP ورقم المنفذ (49 افتراضيا) والمفتاح السري المشترك.



4. تمكين مصادقة TACACS+ للإدارة في WCS. انتقل إلى **الإدارة > AAA > وضع AAA > تحديد TACACS+**.



WCS باستخدام المجالات الظاهرية

المجال الظاهري هو ميزة جديدة قدمت مع WCS صيغة 5.1. يتكون مجال WCS الظاهري من مجموعة من الأجهزة والخرائط ويقيد عرض المستخدم للمعلومات المتعلقة بهذه الأجهزة والخرائط. من خلال مجال ظاهري، يمكن أن يضمن المسؤول أنه يمكن للمستخدمين عرض الأجهزة والخرائط المسؤولة عنها فقط. بالإضافة إلى ذلك، ونظرا لعوامل تصفية المجال الظاهري، يمكن للمستخدمين تكوين عمليات التنبيه وعرضها وإنشاء تقارير للجزء المعين فقط من الشبكة. يحدد المسؤول مجموعة من المجالات الظاهرية المسموح بها لكل مستخدم. يمكن تنشيط واحد فقط من هذه العناصر لذلك المستخدم عند تسجيل الدخول. يمكن للمستخدم تغيير المجال الظاهري الحالي عن طريق تحديد مجال ظاهري مختلف مسموح به من القائمة المنسدلة المجال الظاهري في أعلى الشاشة. تتم الآن تصفية جميع التقارير والتنبيهات والوظائف الأخرى بواسطة هذا المجال الظاهري.

في حالة وجود مجال ظاهري واحد فقط معرف (جذر) في النظام ولم يكن لدى المستخدم أي مجالات ظاهرية في حقول السمات المخصصة في خادم TACACS+/RADIUS، يتم تعيين المجال الظاهري الجذر بشكل افتراضي للمستخدم.

إذا كان هناك أكثر من مجال ظاهري واحد ولم يكن لدى المستخدم أي سمات محددة، فسيتم منع المستخدم من تسجيل الدخول. للسماح للمستخدم بتسجيل الدخول، يجب تصدير سمات المجال الظاهري المخصصة إلى خادم RADIUS/TACACS+.

يتيح لك إطار "السمات المخصصة للمجال الظاهري" الإشارة إلى البيانات المناسبة الخاصة بالبروتوكول لكل مجال ظاهري. يقوم زر التصدير الموجود على الشريط الجانبي للتدرج الهرمي للمجال الظاهري بتنسيق سمات RADIUS و TACACS+ للمجال الظاهري مسبقا. يمكنك نسخ ولصق هذه السمات في خادم ACS. وهذا يسمح لك بنسخ المجالات الظاهرية المطبقة فقط إلى شاشة خادم ACS ويضمن أن المستخدمين لديهم حق الوصول إلى هذه المجالات الظاهرية فقط.

من أجل تطبيق سمات RADIUS و TACACS+ المنسقة مسبقا على خادم ACS، أكمل الخطوات الموضحة في قسم سمات RADIUS و TACACS+ للمجال الظاهري.

تكوين مصدر المحتوى الإضافي الآمن من Cisco لاستخدام WCS

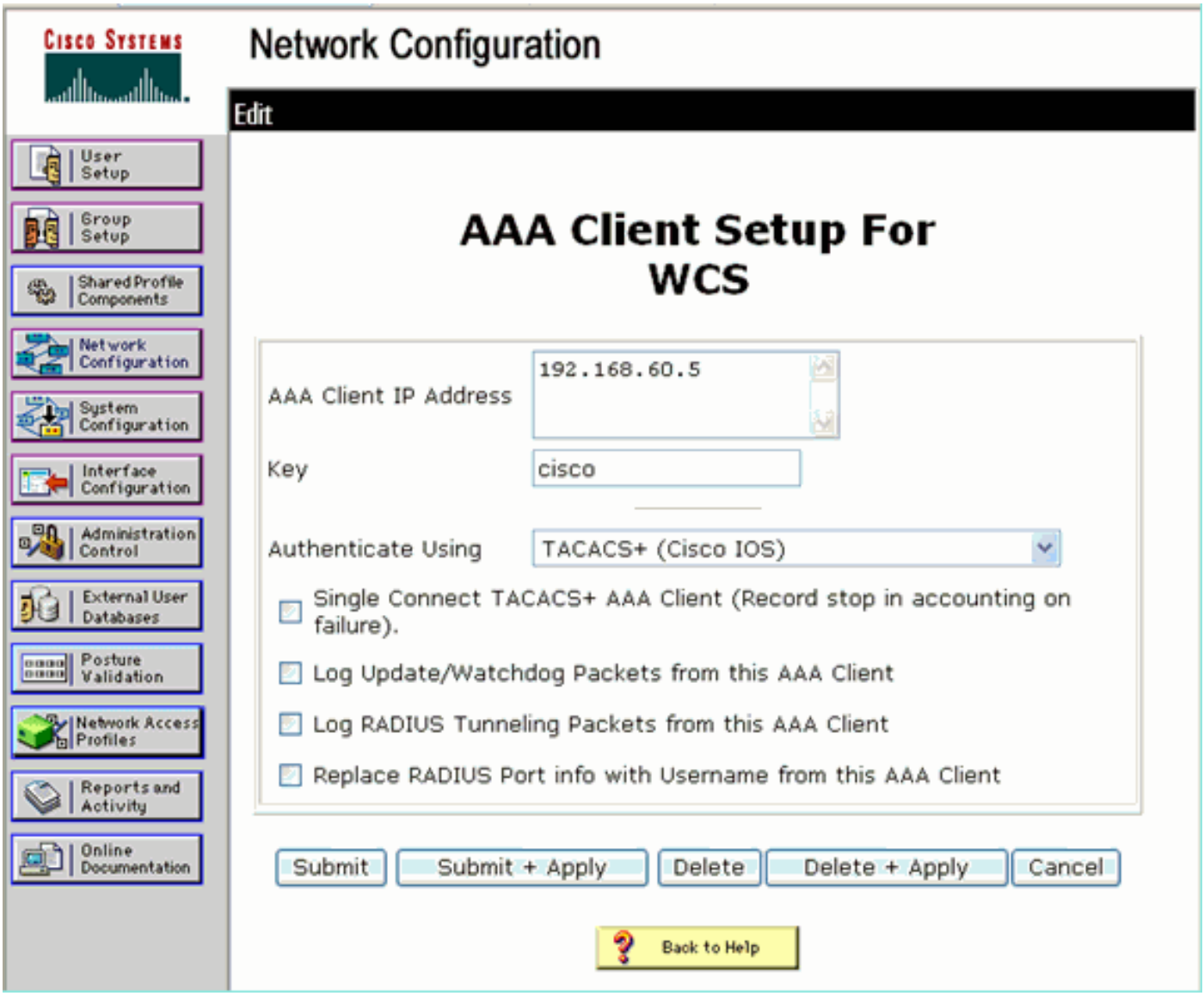
يوفر القسم الخطوات المعنية بخادم ACS +TACACS لإنشاء الخدمات والسمات المخصصة، وتخصيص الأدوار للمستخدمين أو المجموعات.

لم يتم شرح إنشاء المستخدمين والمجموعة في هذا القسم. من المفترض أن المستخدمين والمجموعات يتم إنشاؤها حسب الحاجة.

تكوين الشبكة

أكمل هذه الخطوة:

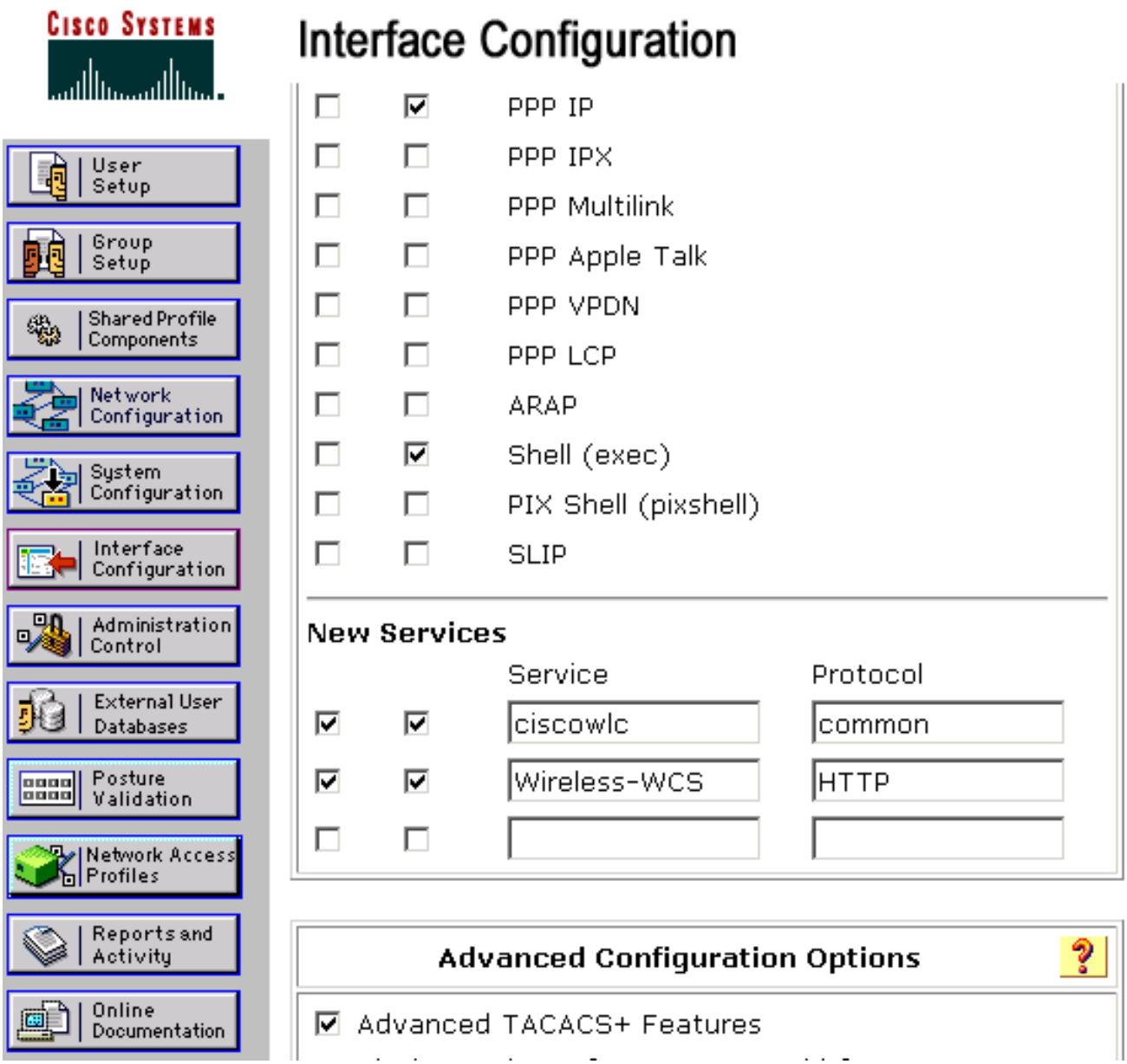
إضافة عنوان IP WCS كعميل AAA مع آلية المصادقة مثل Cisco IOS) +TACACS).



تكوين الواجهة

أكمل الخطوات التالية:

1. في قائمة تكوين الواجهة، حدد إرتباط Cisco IOS) **TACACS+**).
2. تمكين **الخدمات الجديدة**.
3. حدد خانتي الاختيار **المستخدم** و**المجموعة**.
4. أدخل **Wireless-WCS** للخدمة و**HTTP** للبروتوكول.**ملاحظة:** يجب أن يكون HTTP في CAPS.
5. قم بتمكين **ميزات TACACS+ المتقدمة**.



6. انقر فوق **إرسال** لتطبيق التغييرات.

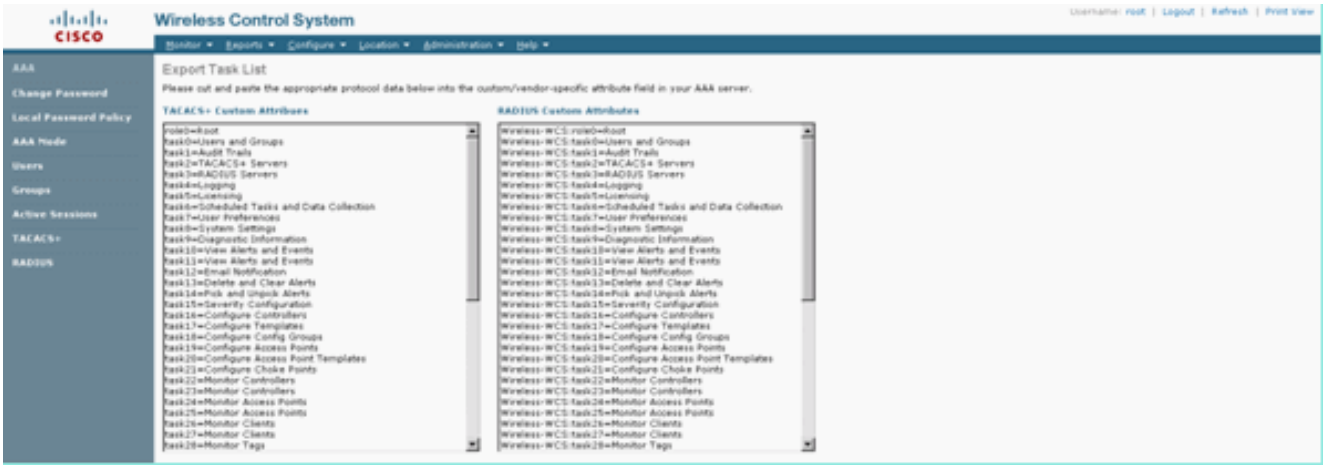
إعداد المستخدم/المجموعة

أكمل الخطوات التالية:

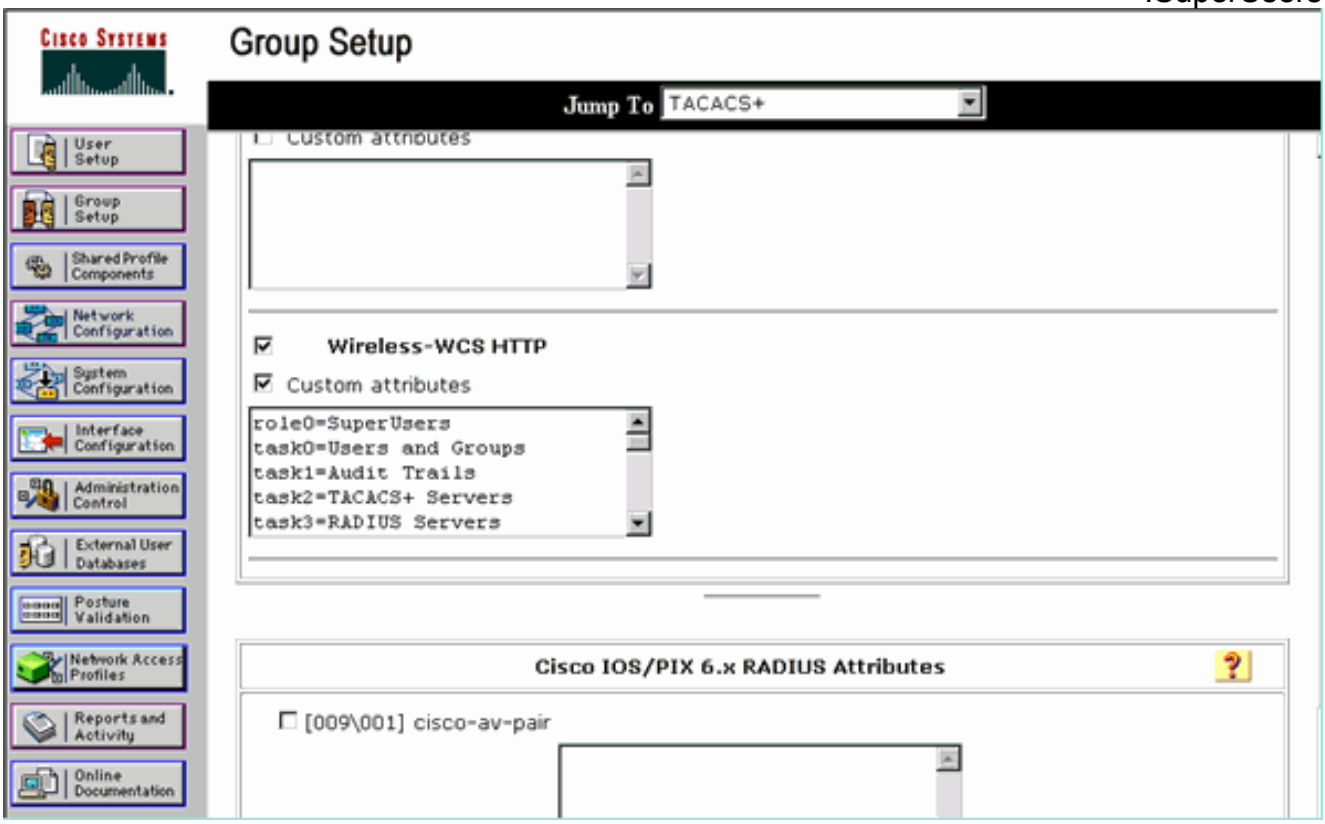
1. في واجهة المستخدم الرسومية (WCS)، انتقل إلى **الإدارة > AAA > مجموعات** لتحديد أي من مجموعات المستخدمين التي تم تكوينها مسبقا، مثل SuperUsers في عنصر التحكم في الشبكة المحلية اللاسلكية (WCS).

2. حدد قائمة المهام لمجموعات المستخدمين المكونة مسبقا ونسخ لصق إلى

.ACS



3. حدد مستخدما/مجموعة تم إنشاؤها مسبقا وانتقل إلى **إعدادات TACACS+**.
4. في واجهة المستخدم الرسومية (GUI) ل ACS، حدد خانة الاختيار التي تطابق خدمة Wireless-WCS التي تم إنشاؤها سابقا.
5. في واجهة المستخدم الرسومية (GUI) ل ACS، حدد مربع **السمات المخصصة**.
6. في مربع النص الموجود أسفل السمات المخصصة، أدخل معلومات المهمة والدور المنسوخة من WCS. على سبيل المثال، أدخل قائمة المهام المسموح بها من قبل SuperUsers.



7. بعد ذلك، login إلى ال WCS مع ال newly created username/كلمة في ال ACS.

تصحيح الأخطاء

تصحيح الأخطاء من WLC ل role1=all

```
Cisco Controller) >debug aaa tacacs enable)

Cisco Controller) >Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49)
```

```
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=2 session_id=5eaa857e
                                                          length=16 encrypted=0
                                Wed Feb 28 17:36:37 2007: TPLUS_AUTHEN_STATUS_GETPASS
                        Wed Feb 28 17:36:37 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:36:37 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:36:37 2007: tplus response: type=1 seq_no=4 session_id=5eaa857e
                                                          length=6 encrypted=0
Wed Feb 28 17:36:37 2007: tplus_make_author_request() from tplus_authen_passed returns rc=0
                        Wed Feb 28 17:36:37 2007: Forwarding request to 10.1.1.12 port=49
    Wed Feb 28 17:36:37 2007: author response body: status=1 arg_cnt=1 msg_len=0 data_len=0
                                                  [Wed Feb 28 17:36:37 2007: arg[0] = [9][role1=ALL
                        Wed Feb 28 17:36:37 2007: User has the following mgmtRole fffffff8
```

تصحيح الأخطاء من WLC للأدوار المتعددة

```
                                                  Cisco Controller) >debug aaa tacacs enable)

                        Wed Feb 28 17:59:33 2007: Forwarding request to 10.1.1.12 port=49
                                Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=2
                                                    session_id=b561ad88 length=16 encrypted=0
                                Wed Feb 28 17:59:34 2007: TPLUS_AUTHEN_STATUS_GETPASS
                        Wed Feb 28 17:59:34 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:59:34 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:59:34 2007: tplus response: type=1 seq_no=4 session_id=b561ad88
                                                          length=6 encrypted=0
        Wed Feb 28 17:59:34 2007: tplus_make_author_request() from tplus_authen_passed
                                                                  returns rc=0
                        Wed Feb 28 17:59:34 2007: Forwarding request to 10.1.1.12 port=49
    Wed Feb 28 17:59:34 2007: author response body: status=1 arg_cnt=4 msg_len=0 data_len=0
                                                  [Wed Feb 28 17:59:34 2007: arg[0] = [11][role1=WLAN
                                                [Wed Feb 28 17:59:34 2007: arg[1] = [16][role2=CONTROLLER
                                                  [Wed Feb 28 17:59:34 2007: arg[2] = [14][role3=SECURITY
                                                  [Wed Feb 28 17:59:34 2007: arg[3] = [14][role4=COMMANDS
                                Wed Feb 28 17:59:34 2007: User has the following mgmtRole 150
```

تصحيح الأخطاء من WLC لفشل التخويل

```
                                                  Cisco Controller) >debug aaa tacacs enable)

                        Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=2 session_id=89c553a1
                                                          length=16 encrypted=0
                                Wed Feb 28 17:53:04 2007: TPLUS_AUTHEN_STATUS_GETPASS
                        Wed Feb 28 17:53:04 2007: auth_cont get_pass reply: pkt_length=22
Wed Feb 28 17:53:04 2007: processTplusAuthResponse: Continue auth transaction
Wed Feb 28 17:53:04 2007: tplus response: type=1 seq_no=4 session_id=89c553a1
                                                          length=6 encrypted=0
        Wed Feb 28 17:53:04 2007: tplus_make_author_request() from tplus_authen_passed
                                                                  returns rc=0
                        Wed Feb 28 17:53:04 2007: Forwarding request to 10.1.1.12 port=49
  Wed Feb 28 17:53:04 2007: author response body: status=16 arg_cnt=0 msg_len=0 data_len=0
                                    Wed Feb 28 17:53:04 2007:User has the following mgmtRole 0
                                  Wed Feb 28 17:53:04 2007: Tplus authorization for tac failed status=16
```

معلومات ذات صلة

- مثال تكوين WLC (Cisco Wireless LAN Controller) و TACACS+ (Cisco ACS 5.x) لمصادقة الويب
- تكوين TACACS+
- كيفية تكوين مصادقة TACACS والتفويض للمستخدمين المسؤولين وغير المسؤولين في ACS 5.1

- مقارنة TACACS+ و RADIUS
- الدعم التقني والمستندات - Cisco Systems

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).