Cisco整合無線網路TACACS+組態

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[控制器中的TACACS+實作](#)
[驗證](#)
[Authorization](#)
[會計](#)
[WLC中的TACACS+組態](#)
[新增TACACS+身份驗證伺服器](#)
[新增TACACS+授權伺服器](#)
[新增TACACS+記帳伺服器](#)
[配置身份驗證順序](#)
[驗證設定](#)
[配置Cisco Secure ACS伺服器](#)
[網路設定](#)
[介面組態](#)
[使用者/組設定](#)
[Cisco Secure ACS中的記帳記錄](#)
[WCS中的TACACS+配置](#)
[使用虛擬域的WCS](#)
[配置Cisco Secure ACS以使用WCS](#)
[網路設定](#)
[介面組態](#)
[使用者/組設定](#)
[調試](#)
[從WLC為role1=ALL調試](#)
[從WLC調試多個角色](#)
[從WLC調試授權失敗](#)
[相關資訊](#)

簡介

本檔案將提供思科無線LAN控制器(WLC)和思科整合無線網路的思科無線控制系統(WCS)中的終端存取控制器存取控制系統Plus(TACACS+)組態範例。本文還提供一些基本的故障排除提示。

TACACS+是一種使用者端/伺服器通訊協定，可為嘗試取得路由器或網路存取伺服器管理存取的使

用者提供集中式安全。TACACS+提供以下AAA服務：

- 嘗試登入網路裝置的使用者的身份驗證
- 確定使用者應具有何種訪問級別的授權
- 用於跟蹤使用者所做的所有更改的記帳

有關AAA服務和TACACS+功能的詳細資訊，請參閱配置TACACS+。

請參閱TACACS+和RADIUS比較，以比較TACACS+和RADIUS。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解如何配置WLC和輕量型存取點(LAP)以進行基本操作
- 輕量型存取點通訊協定(LWAPP)和無線安全方法知識
- 基本知識RADIUS和TACACS+
- Cisco ACS配置基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於Windows的Cisco安全ACS版本4.0
- 執行版本4.1.171.0的Cisco無線LAN控制器。軟體版本4.1.171.0或更新版本支援WLC上的TACACS+功能。
- 運行版本4.1.83.0的Cisco無線控制系統。4.1.83.0或更高版本的軟體支援WCS上的TACACS+功能。

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

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

控制器中的TACACS+實作

驗證

可以使用使用使用者名稱和密碼的本地資料庫、RADIUS或TACACS+伺服器執行身份驗證。實施沒有完全模組化。身份驗證和授權服務相互關聯。例如，如果使用RADIUS/本機資料庫執行驗證，則不會使用TACACS+執行授權。它將使用與本地或RADIUS資料庫中的使用者關聯的許可權，例如只讀或讀取/寫入，而使用TACACS+執行身份驗證時，授權與TACACS+關聯。

在配置了多個資料庫的情況下，會提供CLI以指定後端資料庫的引用順序。

Authorization

授權是基於任務的，而不是基於每個命令的實際授權。這些任務將對映到多個頁籤，這些頁籤對應於當前在Web GUI上的七個選單欄專案。以下是選單欄專案：

- 監視
- WLAN
- 控制器
- 無線
- 安全性
- 管理
- 指令

此對映的原因是因為大多數客戶使用Web介面而不是CLI來配置控制器。

大廳管理員管理(LOBBY)的附加角色可供僅需要具有大廳管理員許可權的使用者使用。

使用者享有的任務是在TACACS+(ACS)伺服器中使用自訂屬性值(AV)配對進行設定。使用者可以獲得執行一項或多項任務的授權。最小授權僅監控，最大授權為ALL（授權執行所有七個頁籤）。 如果使用者無權執行特定任務，則仍允許使用者以只讀模式訪問該任務。如果啟用了身份驗證，且身份驗證伺服器無法訪問或無法授權，則使用者無法登入到控制器。

注意：若要使通過TACACS+的基本管理身份驗證成功，必須在WLC上配置身份驗證和授權伺服器。記帳配置是可選的。

會計

每當成功執行特定使用者啟動的操作時，都會發生記帳。變更的屬性將連同以下內容一起記錄在TACACS+記帳伺服器上：

- 進行更改的個人的使用者ID
- 使用者從其登入的遠端主機
- 執行命令的日期和時間
- 使用者的授權級別
- 一個字串，提供有關執行的操作和提供的值的資訊

如果計費伺服器無法訪問，使用者仍可以繼續會話。

注意：在軟體版本4.1或更早版本中，不會從WCS生成會計記錄。

WLC中的TACACS+組態

WLC軟體版本4.1.171.0和更新版本引入新的CLI和網路GUI變更，以便在WLC上啟用TACACS+功能。本節列出了介紹的CLI以供參考。Web GUI的相應更改將新增到「安全」頁籤下。

本檔案假設WLC的基本組態已完成。

若要在WLC控制器中設定TACACS+，需要完成以下步驟：

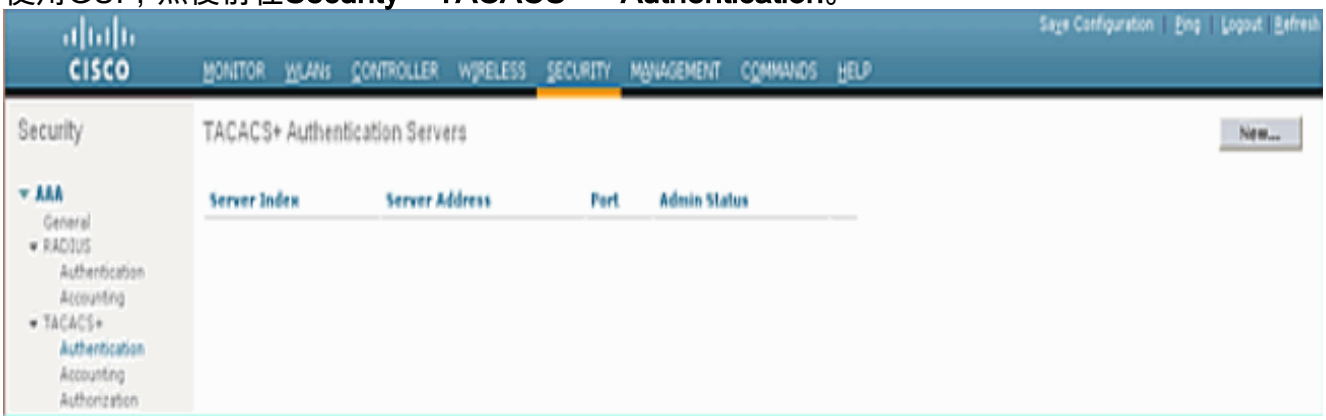
1. 新增TACACS+身份驗證伺服器
2. 新增TACACS+授權伺服器

3. 新增TACACS+記帳伺服器
4. 配置身份驗證順序

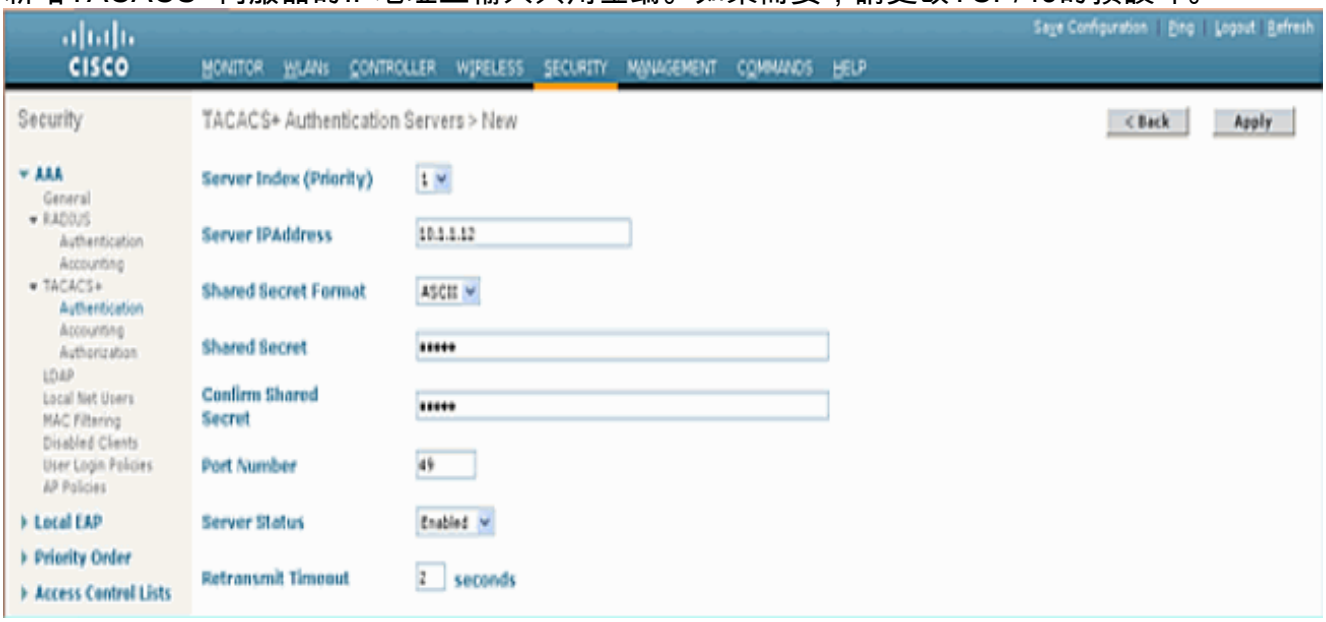
新增TACACS+身份驗證伺服器

完成以下步驟即可新增TACACS+驗證伺服器：

1. 使用GUI，然後前往**Security > TACACS+ > Authentication**。



2. 新增TACACS+伺服器的IP地址並輸入共用金鑰。如果需要，請更改TCP/49的預設埠。



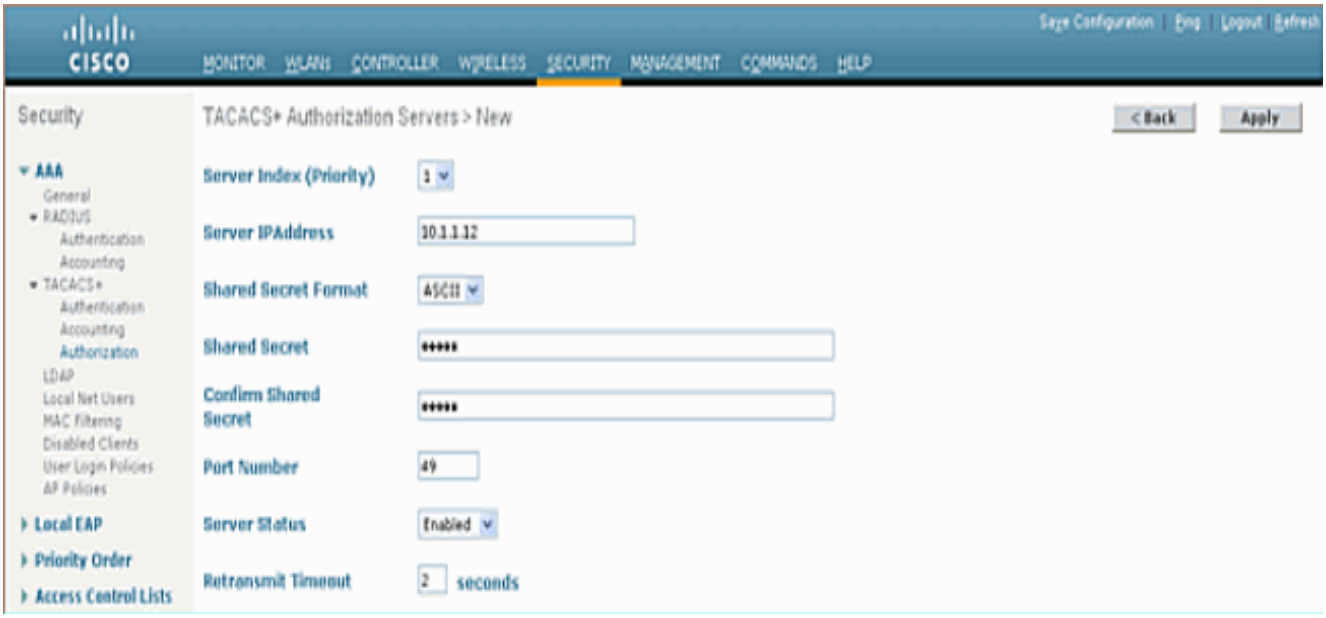
3. 按一下「**Apply**」。您可以使用**config tacacs auth add** <Server Index> <IP addr> <port> [ascii/hex] <secret>指令，從CLI完成**此操**作：

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

新增TACACS+授權伺服器

完成以下步驟即可新增TACACS+授權伺服器：

1. 在GUI上，前往**Security > TACACS+ > Authorization**。
2. 新增TACACS+伺服器的IP地址並輸入共用金鑰。如果需要，請更改TCP/49的預設埠。



3. 按一下「Apply」。您可以使用config tacacs atr add *<Server Index> <IP addr> <port> [ascii/hex] <secret>指令，從CLI完成*此操作：

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

新增TACACS+記帳伺服器

完成以下步驟即可新增TACACS+記帳伺服器：

1. 使用GUI，然後前往**Security > TACACS+ > Accounting**。
2. 新增伺服器的IP地址並輸入共用金鑰。如果需要，請更改TCP/49的預設埠。

3. 按一下「Apply」。您可以使用config tacacs acct add *<Server Index> <IP addr> <port> [ascii/hex] <secret>命令，在CLI中完成*以下操作：

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

配置身份驗證順序

此步驟說明當配置了多個資料庫時，如何配置AAA身份驗證順序。驗證順序可以是**local和RADIUS**，或者**local和TACACS**。驗證順序的預設控制器組態為*本機和RADIUS*。

完成以下步驟以設定驗證順序：

1. 在GUI中，轉至**Security > Priority Order > Management User**。
2. 選擇身份驗證優先順序。在本範例中，已選擇TACACS+。
3. 按一下**Apply**即可進行選擇。

您可以使用**config aaa auth mgmt *<server1> <server2>***指令，在CLI中完成以下操作：

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

驗證設定

本節介紹用於驗證WLC上的TACACS+組態的命令。以下是一些有用的**show**命令，可幫助確定配置是否正確：

- **show aaa auth** — 提供有關驗證順序的資訊。

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

- **show tacacs summary** — 顯示TACACS+服務和統計資訊的摘要。

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

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

Authorization Servers

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

Accounting Servers

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

- **show tacacs auth stats** — 顯示TACACS+驗證伺服器統計資訊。

```
(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 stats** — 顯示TACACS+授權伺服器統計資訊。

```
(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** — 顯示TACACS+記帳伺服器統計資訊。

```
(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
```

配置Cisco Secure ACS伺服器

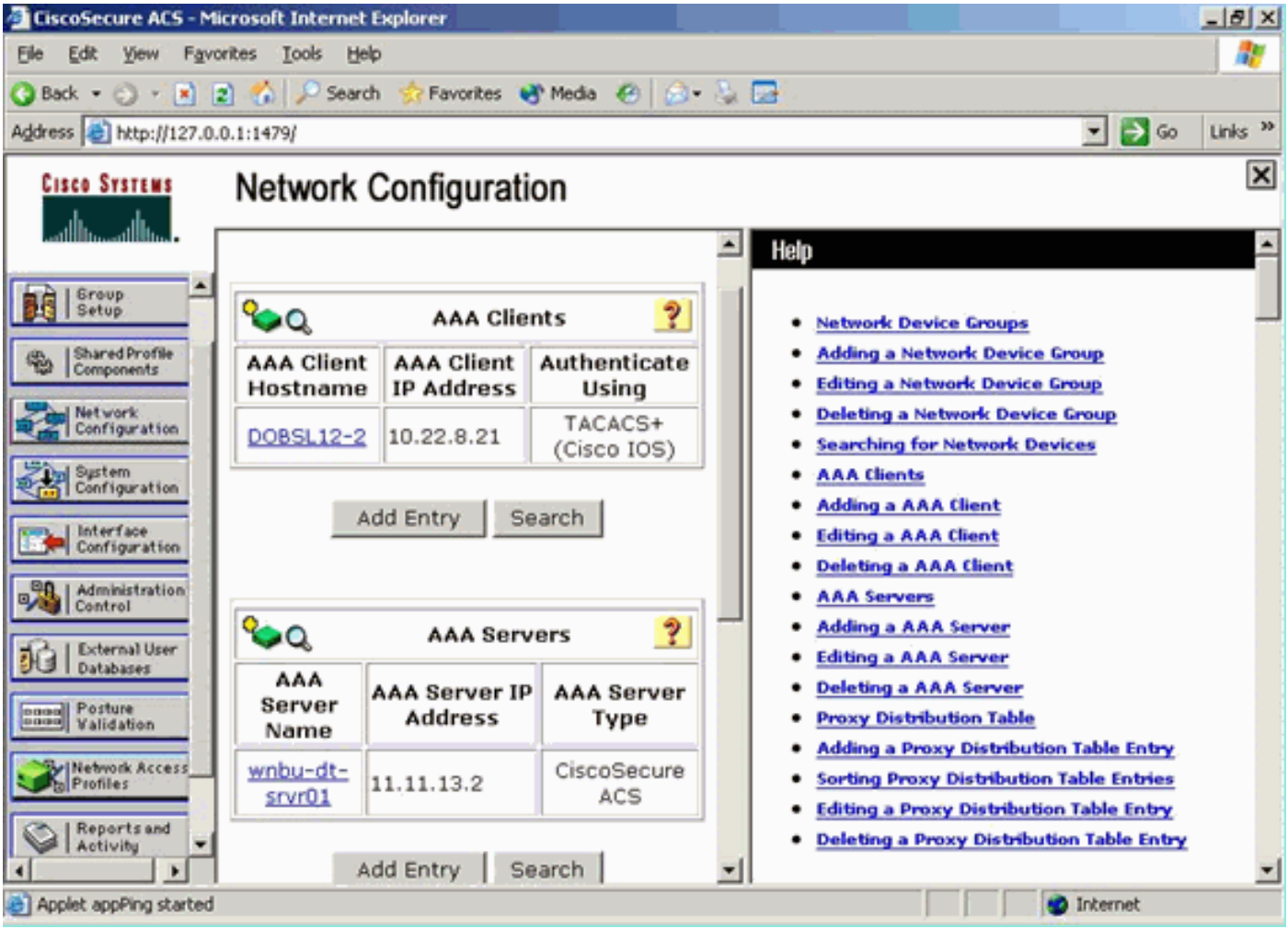
本節提供TACACS+ ACS伺服器中用於建立服務和自定義屬性以及將角色分配給使用者或組的步驟。

本節不介紹使用者和組的建立。假定根據需要建立使用者和組。有關如何建立使用者和使用者組的資訊，請參閱適用於Windows Server 4.0的Cisco Secure ACS使用手冊。

網路設定

完成以下步驟：

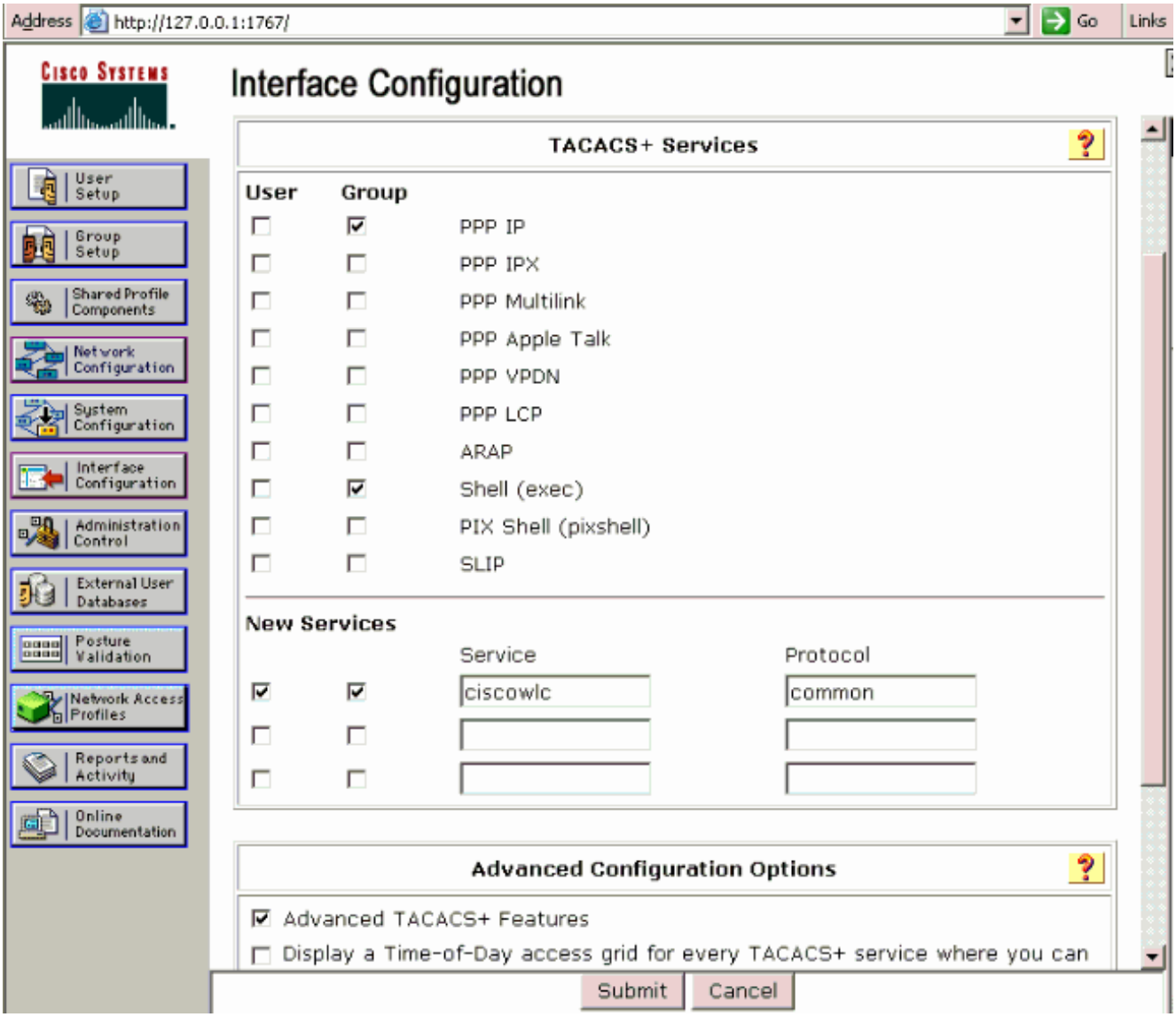
將控制器管理IP地址新增為AAA客戶端，身份驗證機製為TACACS+(Cisco IOS)。



介面組態

請完成以下步驟：

1. 在Interface Configuration選單中，選擇**TACACS+**(Cisco IOS)連結。
2. 啟用**New Services**。
3. 選中**User**和**Group**覈取方塊。
4. 輸入**ciscowlc**作為「服務」，輸入**common**作為「協定」。
5. 啟用**Advanced TACACS+功能**。

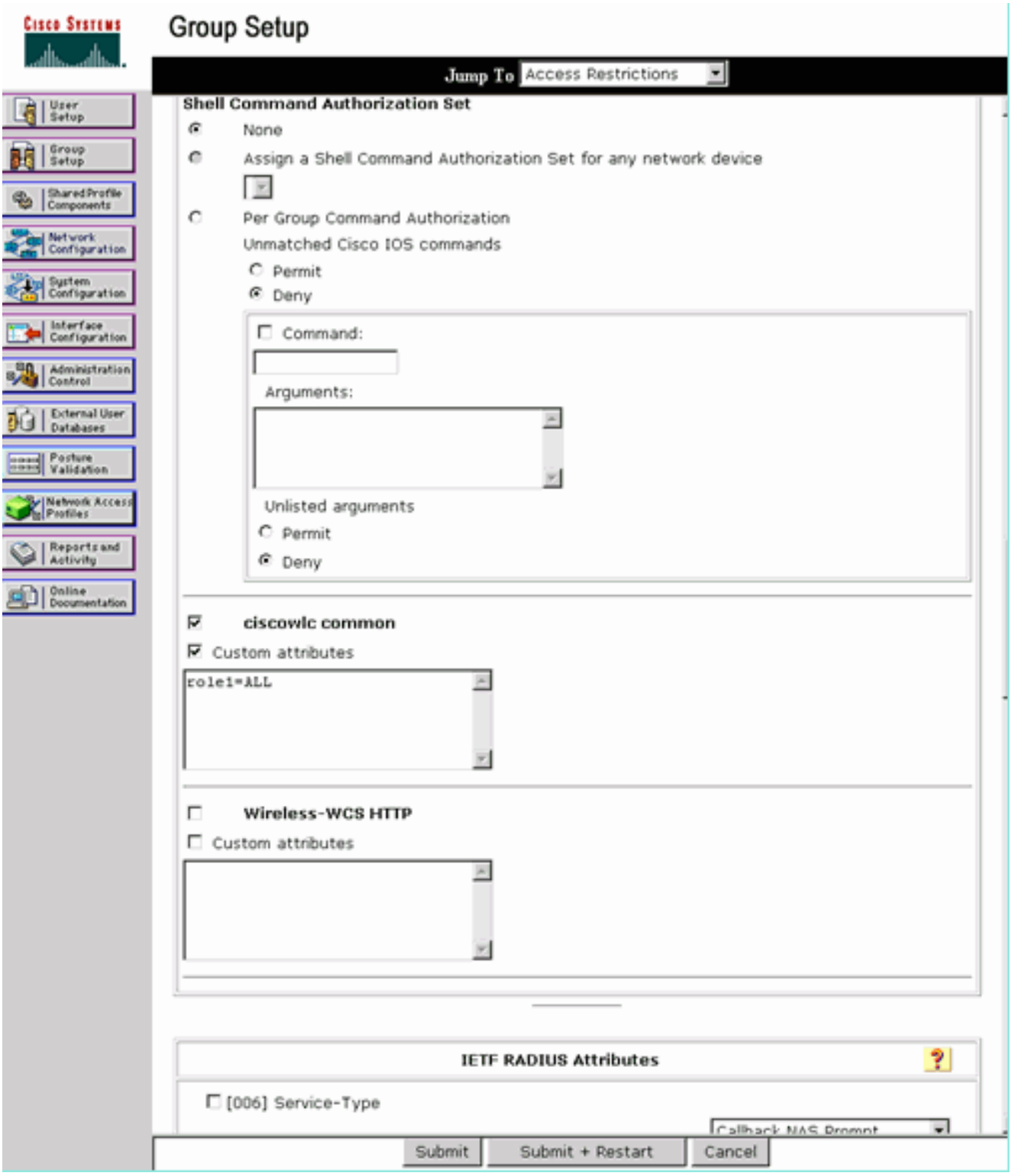


6. 按一下「**Submit**」以應用變更。

使用者/組設定

請完成以下步驟：

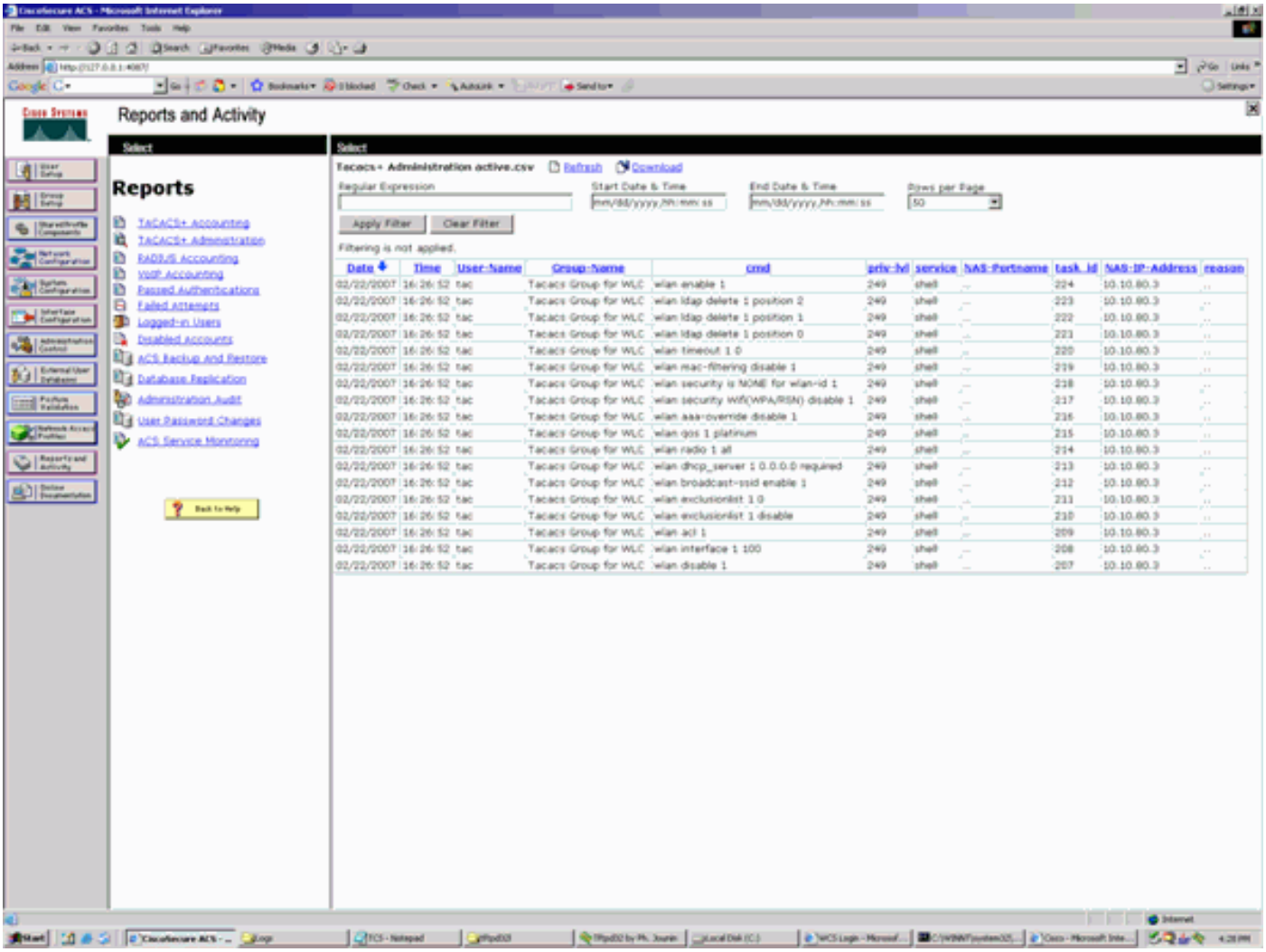
1. 選擇以前建立的使用者/組。
2. 前往**TACACS+設定**。
3. 勾選與「介面配置」部分中建立的*ciscowlc*服務對應的覈取方塊。
4. 選中**Custom attributes**覈取方塊。



5. 如果建立的使用者只需要訪問WLAN、SECURITY和CONTROLLER，請在Custom attributes下方的文本框中輸入此文本：**role1=WLAN role2=SECURITY role3=CONTROLLER**。如果使用者僅需要訪問SECURITY頁籤，請輸入以下文本：**role1=安全**。此角色對應控制器網路GUI中的七個功能表欄專案。選單欄專案包括MONITOR、WLAN、CONTROLLER、WIRELESS、SECURITY、MANAGEMENT和COMMAND。
6. 輸入使用者需要的role1、role2等角色。如果使用者需要所有角色，則應使用關鍵字**ALL**。大廳管理員角色應使用關鍵字**LOBBY**。

Cisco Secure ACS中的記帳記錄

WLC的TACACS+記帳記錄可在Cisco Secure ACS的「TACACS+報告和活動管理」中獲得：



WCS中的TACACS+配置

請完成以下步驟：

1. 從GUI使用根帳戶登入WCS。
2. 新增TACACS+伺服器。前往**Administration > AAA > TACACS+ > Add TACACS+ Server**。

3. 新增TACACS+伺服器詳細資訊，例如IP地址、埠號（49為預設值）和共用金鑰。

4. 在WCS中啟用TACACS+身份驗證以進行管理。前往**Administration > AAA > AAA Mode > Select TACACS+**。

使用虛擬域的WCS

虛擬域是WCS版本5.1中引入的一項新功能。WCS虛擬域由一組裝置和對映組成，並將使用者檢視限製為與這些裝置和對映相關的資訊。通過虛擬域，管理員可以確保使用者只能檢視他們負責的裝置和對映。此外，由於虛擬域的篩選器，使用者只能配置、檢視警報和生成其分配的網路部分的報告。管理員為每個使用者指定一組允許的虛擬域。只有其中一個可以在登入時對該使用者啟用。使用者可以通過從螢幕頂部的Virtual Domain下拉選單中選擇其他允許的虛擬域來更改當前虛擬域。現在，所有報告、警報和其他功能都按該虛擬域進行過濾。

如果系統中僅定義了一個虛擬域（根），且使用者在TACACS+/RADIUS伺服器的自定義屬性欄位中沒有任何虛擬域，則預設情況下會為使用者分配根虛擬域。

如果有多個虛擬域，且使用者沒有任何指定的屬性，則阻止使用者登入。為了允許使用者登入，虛擬域自定義屬性必須匯出到Radius/TACACS+伺服器。

「虛擬域自定義屬性」視窗允許您為每個虛擬域指定相應的協定特定資料。虛擬域層次結構邊欄上的「匯出」按鈕會預先格式化虛擬域的RADIUS和TACACS+屬性。您可以將這些屬性複製並貼上到ACS伺服器。這允許您僅將適用的虛擬域複製到ACS伺服器螢幕，並確保使用者僅有權訪問這些虛擬域。

若要將預先格式化的RADIUS和TACACS+屬性套用到ACS伺服器，請完成虛擬網域RADIUS和TACACS+屬性一節中說明的步驟。

配置Cisco Secure ACS以使用WCS

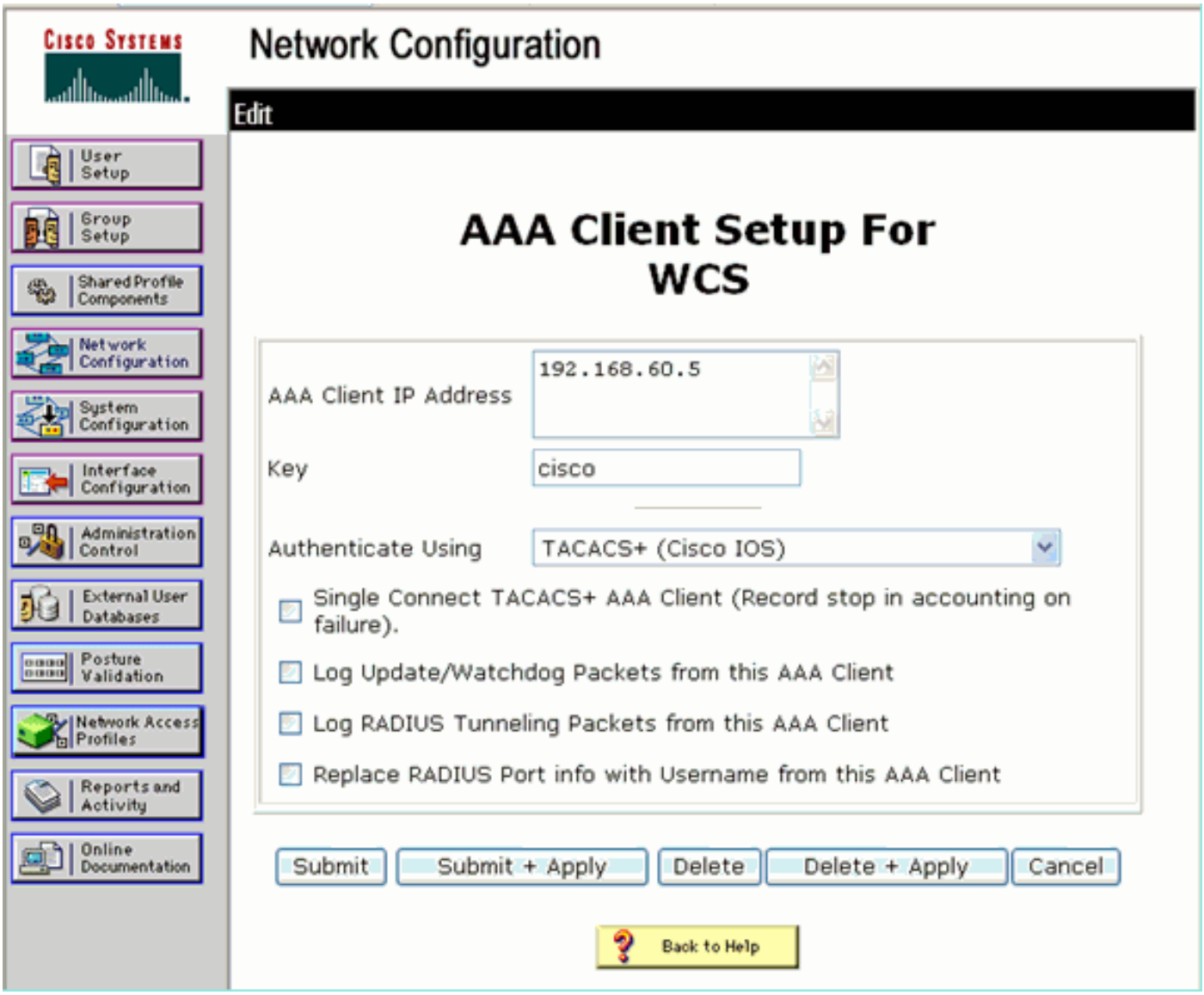
本節提供TACACS+ ACS伺服器中用於建立服務和自定義屬性以及將角色分配給使用者或組的步驟。

本節不介紹使用者和組的建立。假定根據需要建立使用者和組。

網路設定

完成以下步驟：

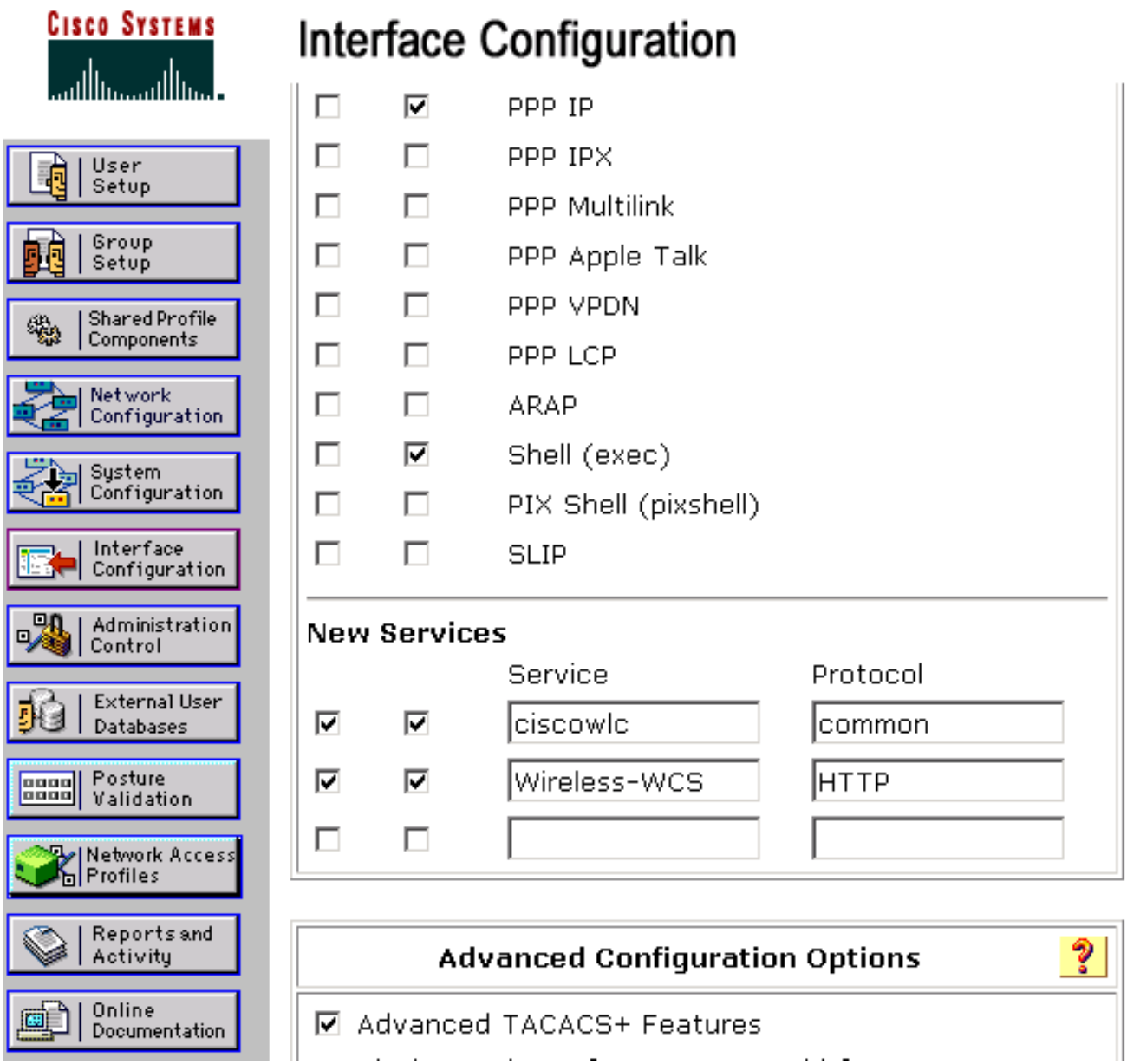
將WCS IP地址新增為AAA客戶端，身份驗證機製為TACACS+(Cisco IOS)。



介面組態

請完成以下步驟：

1. 在Interface Configuration選單中，選擇**TACACS+**(Cisco IOS)連結。
2. 啟用**New Services**。
3. 選中**User**和**Group**覈取方塊。
4. 輸入**Wireless-WCS**（適用於服務）和**HTTP**（適用於協定）。**注意：**HTTP必須採用CAPS格式。
5. 啟用**Advanced TACACS+功能**。

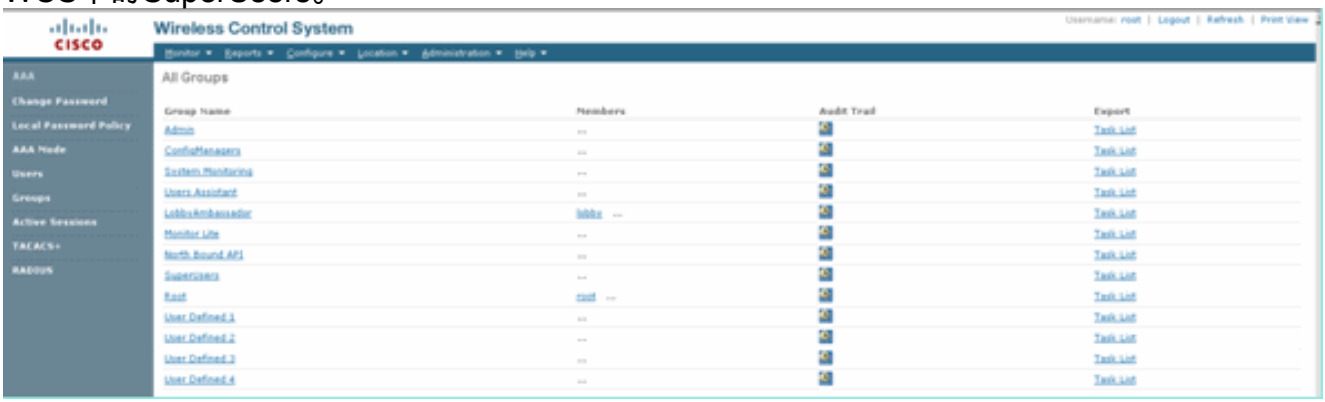


6. 按一下「**Submit**」以應用變更。

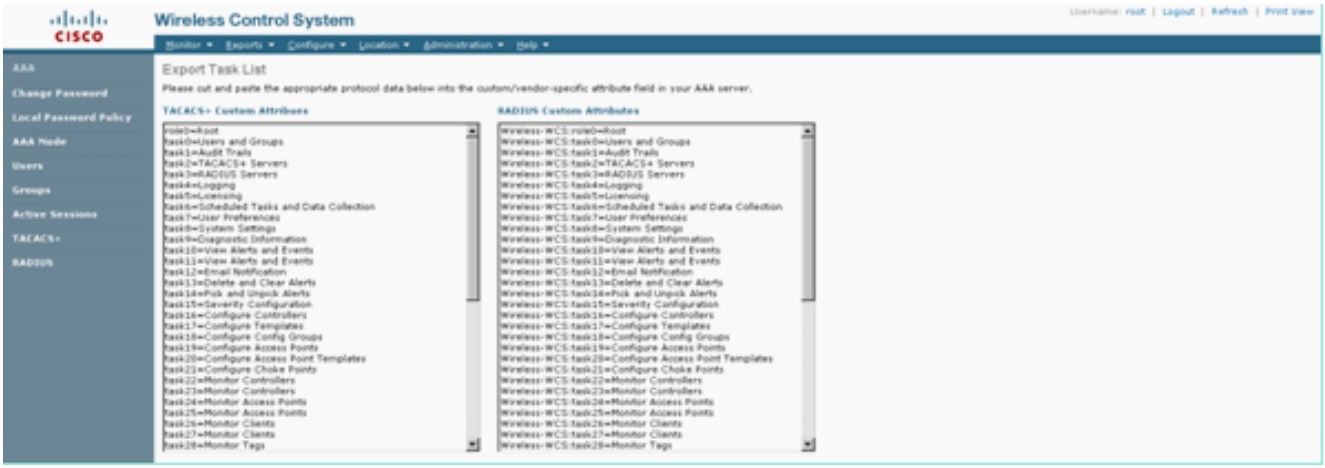
使用者/組設定

請完成以下步驟：

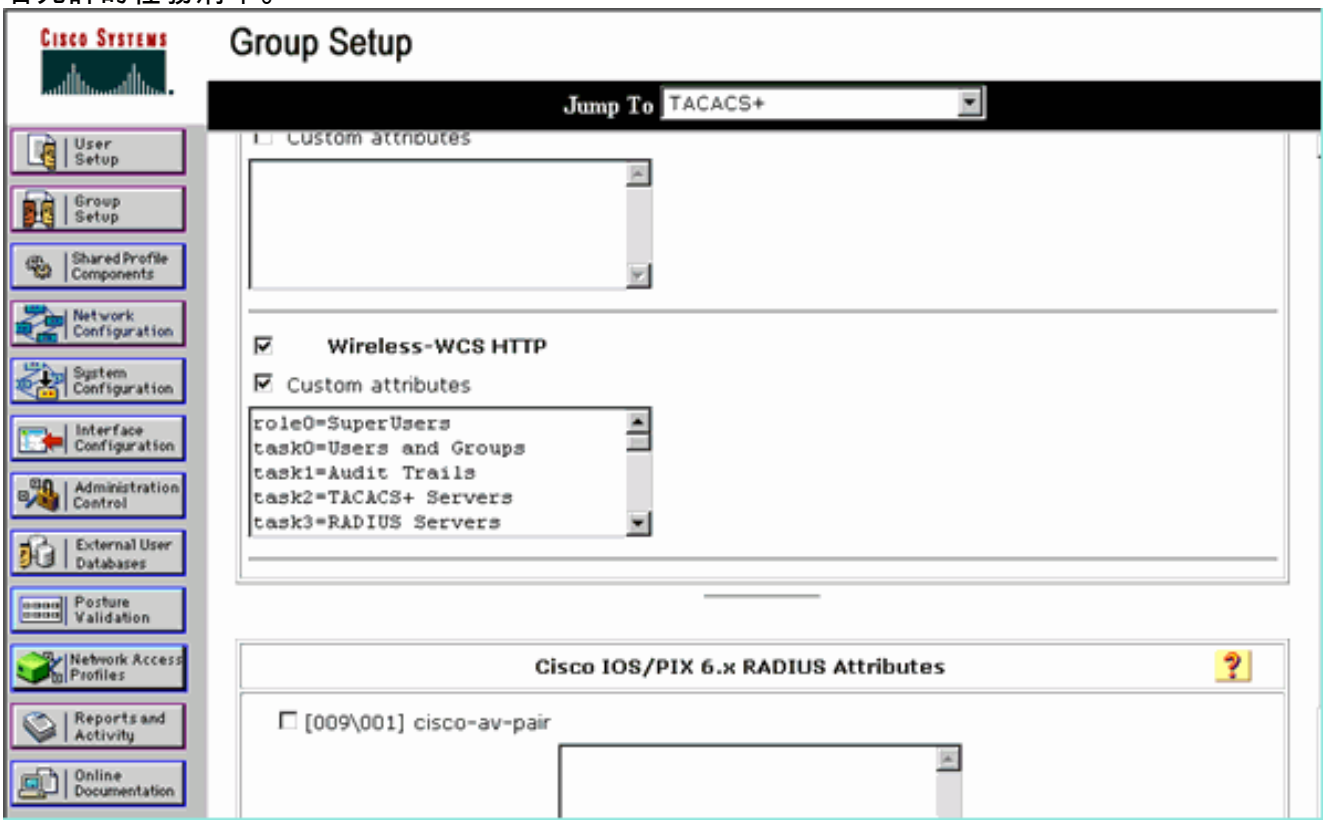
1. 在WCS GUI中，導航到**Administration > AAA > Groups**以選擇任何預配置的使用者組，例如WCS中的SuperUsers。



2. 為預配置的使用者組選擇Task List（任務清單），然後複製貼上到ACS。



3. 選擇以前建立的使用者/組並轉到**TACACS+設定**。
4. 在ACS GUI中，選中與之前建立的Wireless-WCS服務對應的覈取方塊。
5. 在ACS GUI中，選中**Custom attributes**框。
6. 在自定義屬性下面的文本框中，輸入從WCS複製的此角色和任務資訊。例如，輸入超級使用者允許的任務清單。



7. 然後，在ACS中使用新建立的使用者名稱/密碼登入WCS。

調試

從WLC為role1=ALL調試

```
(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
```

從WLC調試多個角色

```
(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
```

從WLC調試授權失敗

```
(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
```

相關資訊

- 適用於Web驗證的Cisco無線LAN控制器(WLC)和Cisco ACS 5.x(TACACS+)組態範例
- 設定TACACS+
- 如何在ACS 5.1中為管理員和非管理員使用者配置TACACS身份驗證和授權
- TACACS+ 和 RADIUS 比較
- 技術支援與文件 - Cisco Systems