

使用GUI進行登入身份驗證的Aironet接入點上的TACACS+配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[設定](#)

[網路圖表](#)

[配置TACACS+伺服器進行登入身份驗證 — 使用ACS 4.1](#)

[配置TACACS+伺服器進行登入身份驗證 — 使用ACS 5.2](#)

[為TACACS+身份驗證配置Aironet AP](#)

[驗證](#)

[ACS 5.2驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案將說明如何在Cisco Aironet存取點(AP)上啟用TACACS Plus(TACACS+)服務，以便使用TACACS+伺服器執行登入驗證。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解如何在Aironet AP上配置基本引數
- 瞭解如何配置TACACS+伺服器(如思科安全訪問控制伺服器(ACS))的知識
- TACACS+概念知識

有關TACACS+如何工作的資訊，請參閱[設定RADIUS和TACACS+伺服器的瞭解TACACS+](#)一節。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Aironet Cisco Aironet 1240/1140系列存取點

- 運行軟體版本4.1的ACS
- 運行軟體版本5.2的ACS

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](#)。

設定

本節介紹如何將Aironet AP和TACACS+伺服器(ACS)配置為基於TACACS+的登入身份驗證。

此配置示例使用以下引數：

- ACS的IP地址 — 172.16.1.1/255.255.0.0
- AP的IP地址 — 172.16.1.30/255.255.0.0
- AP和TACACS+伺服器上使用的共用金鑰 — 示例

以下是此示例在ACS上配置的使用者的憑據：

- 使用者名稱- User1
- 密碼 — Cisco
- 組 — AdminUsers

您需要配置TACACS+功能，以驗證嘗試通過Web介面或通過命令列介面(CLI)連線到AP的使用者。為了完成此配置，您必須執行以下任務：

1. [配置TACACS+伺服器進行登入身份驗證](#)。
2. [為Aironet AP配置TACACS+身份驗證](#)。

註：使用[Command Lookup Tool](#)(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：

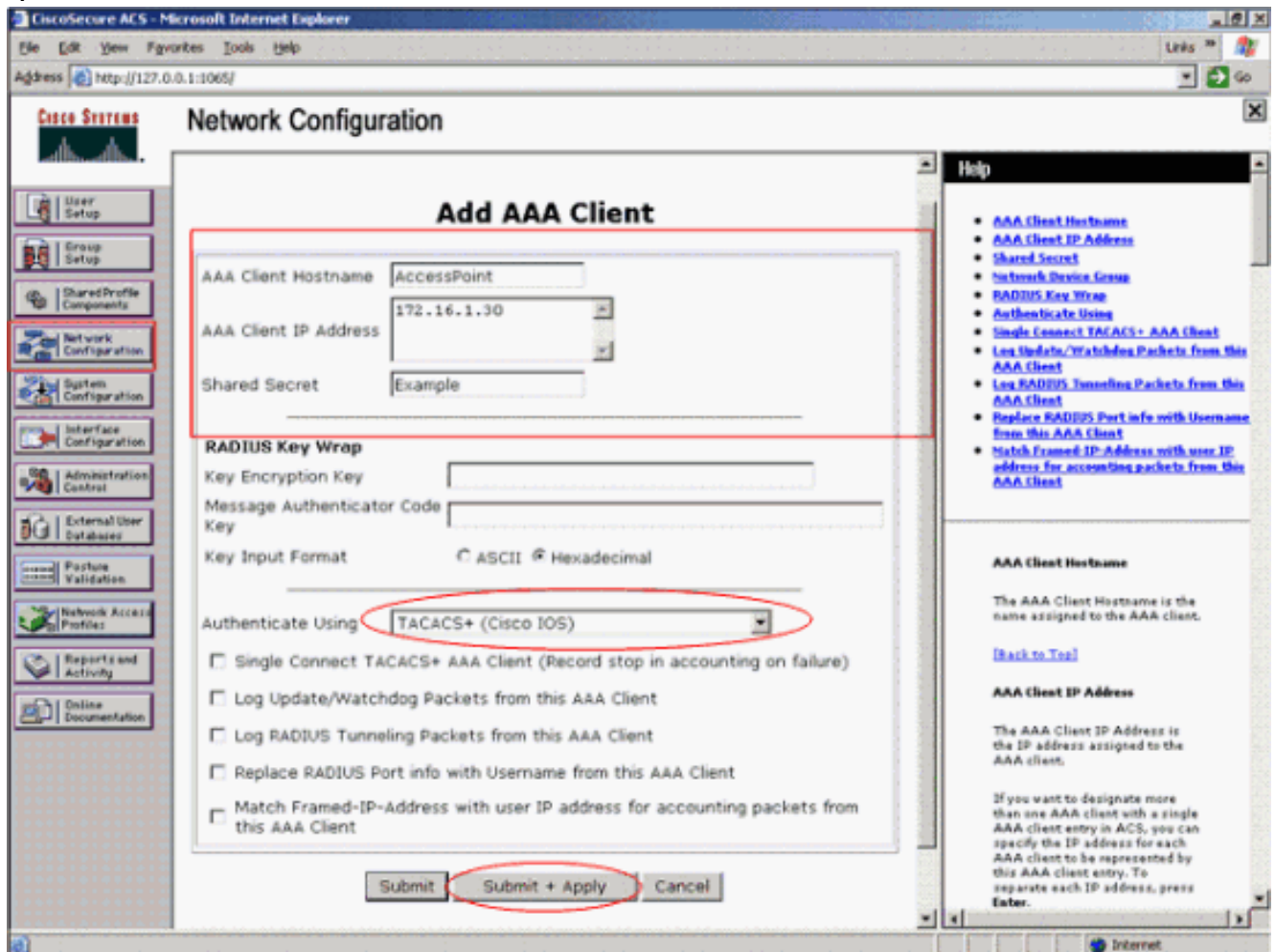


配置TACACS+伺服器進行登入身份驗證 — 使用ACS 4.1

第一步是設定TACACS+後台程式，以驗證嘗試訪問AP的使用者。必須設定ACS進行TACACS+身份驗證並建立使用者資料庫。您可以使用任何TACACS+伺服器。此示例使用ACS作為TACACS+伺服器。請完成以下步驟：

1. 完成以下步驟，以便將AP新增為身份驗證、授權和記帳(AAA)客戶端：在ACS GUI中，按一下**Network Configuration**頁籤。在AAA Clients下，按一下**Add Entry**。在「新增AAA客戶端」視窗中，輸入AP主機名、AP的IP地址和共用金鑰。此共用金鑰必須與您在AP上配置的共用金鑰相同。在「Authenticate Using」下拉選單中，選擇**TACACS+(Cisco IOS)**。按一下「**Submit + Restart**」以儲存組態。以下是範例

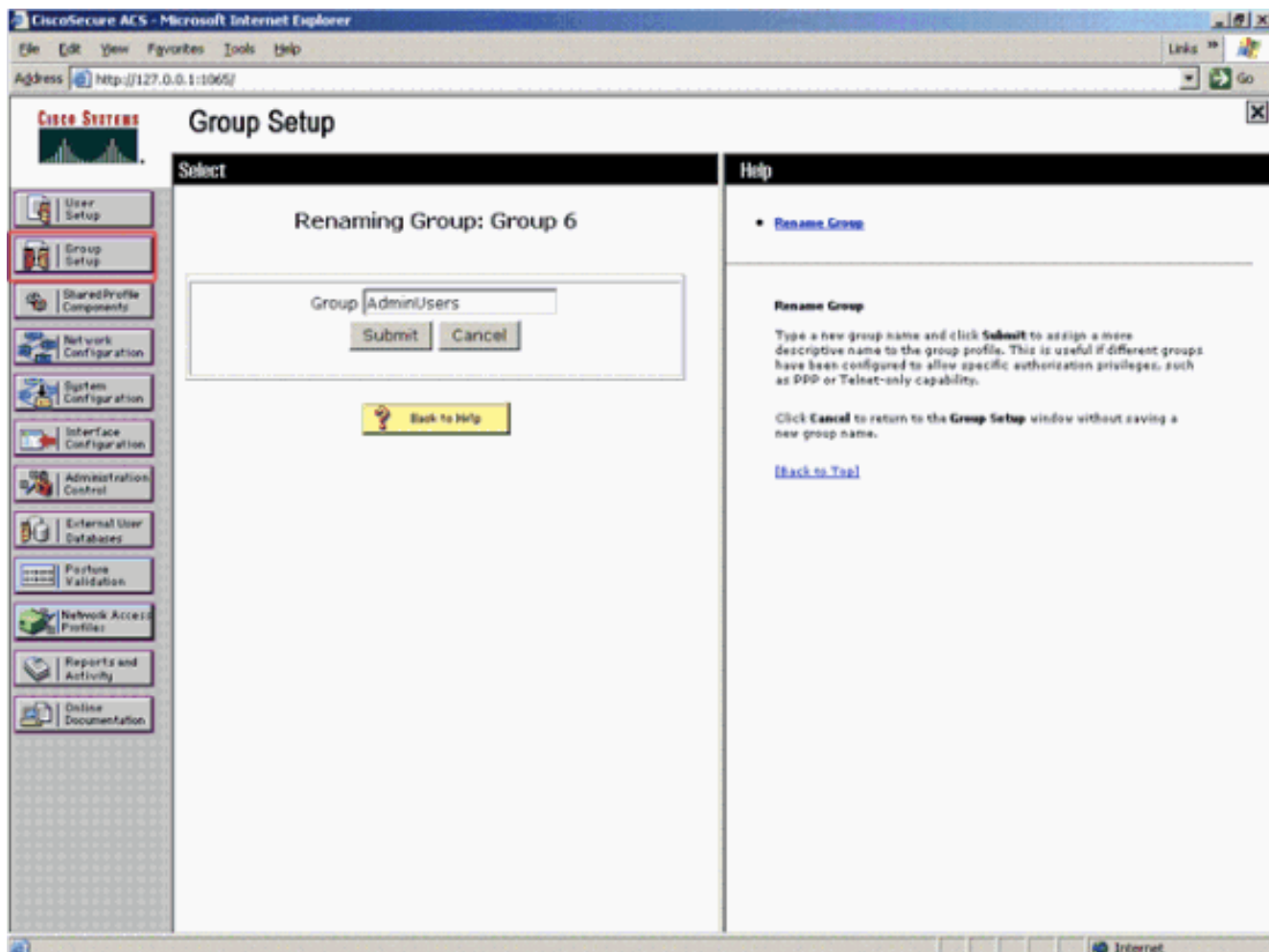
:



此示例使用：AAA客戶端主機名**AccessPoint**地址**172.16.1.30/16**作為AAA客戶端IP地址共用金鑰示例

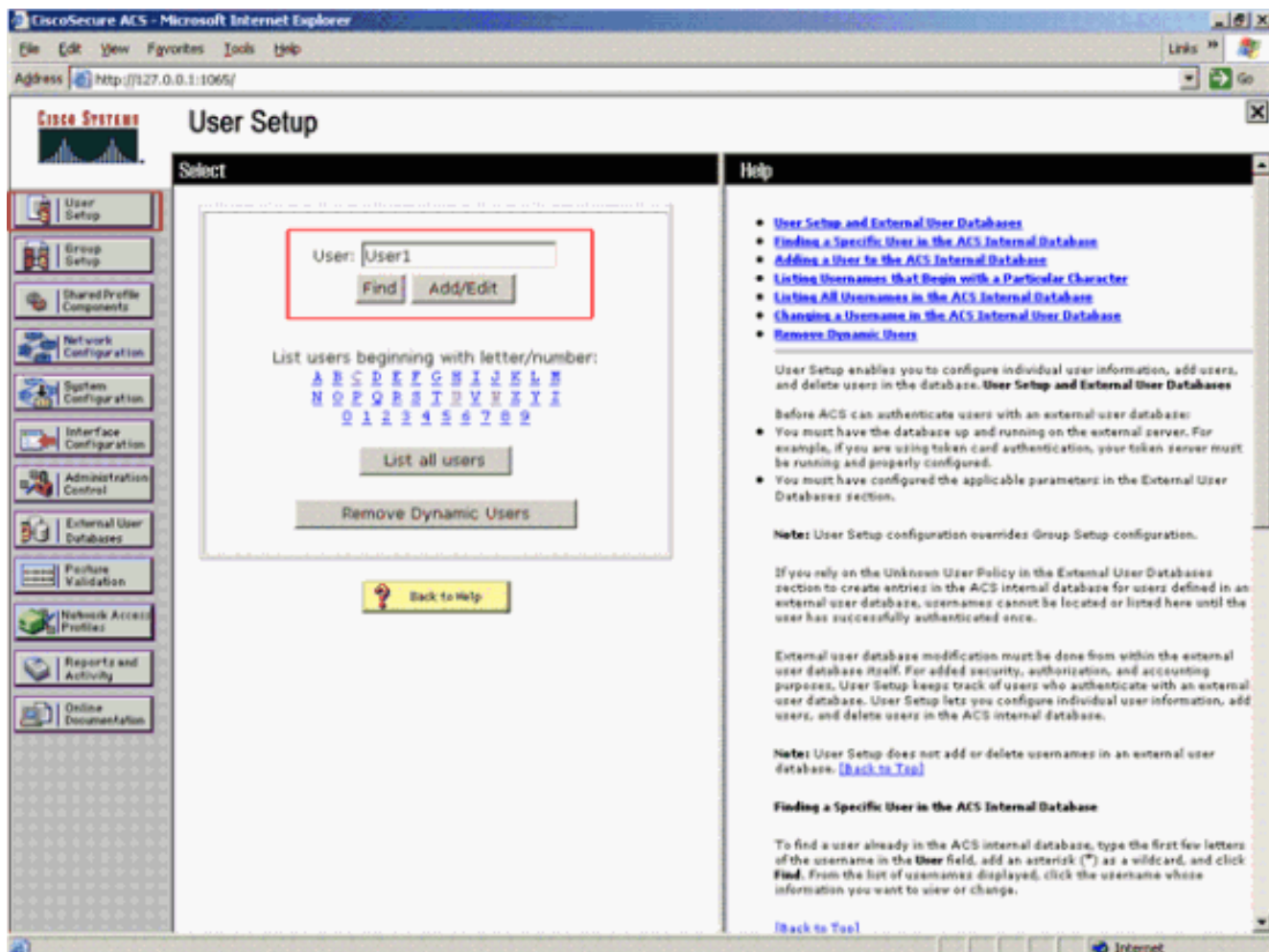
2. 完成以下步驟，建立包含所有管理(admin)使用者的組：從左側選單中按一下**Group Setup**。出現一個新視窗。在「組設定」視窗中，從下拉選單中選擇要配置的組，然後按一下**重新命名組**。此示例從下拉選單中選擇組6，並將該組重新命名為AdminUsers。按一下「**Submit**」。以下是範例

:



3. 完成以下步驟，即可將使用者新增到TACACS+資料庫：按一下**User Setup**頁籤。若要建立新使用者，請在「使用者」欄位中輸入使用者名稱，然後按一下**新增/編輯**。以下是建立**User1**的示例

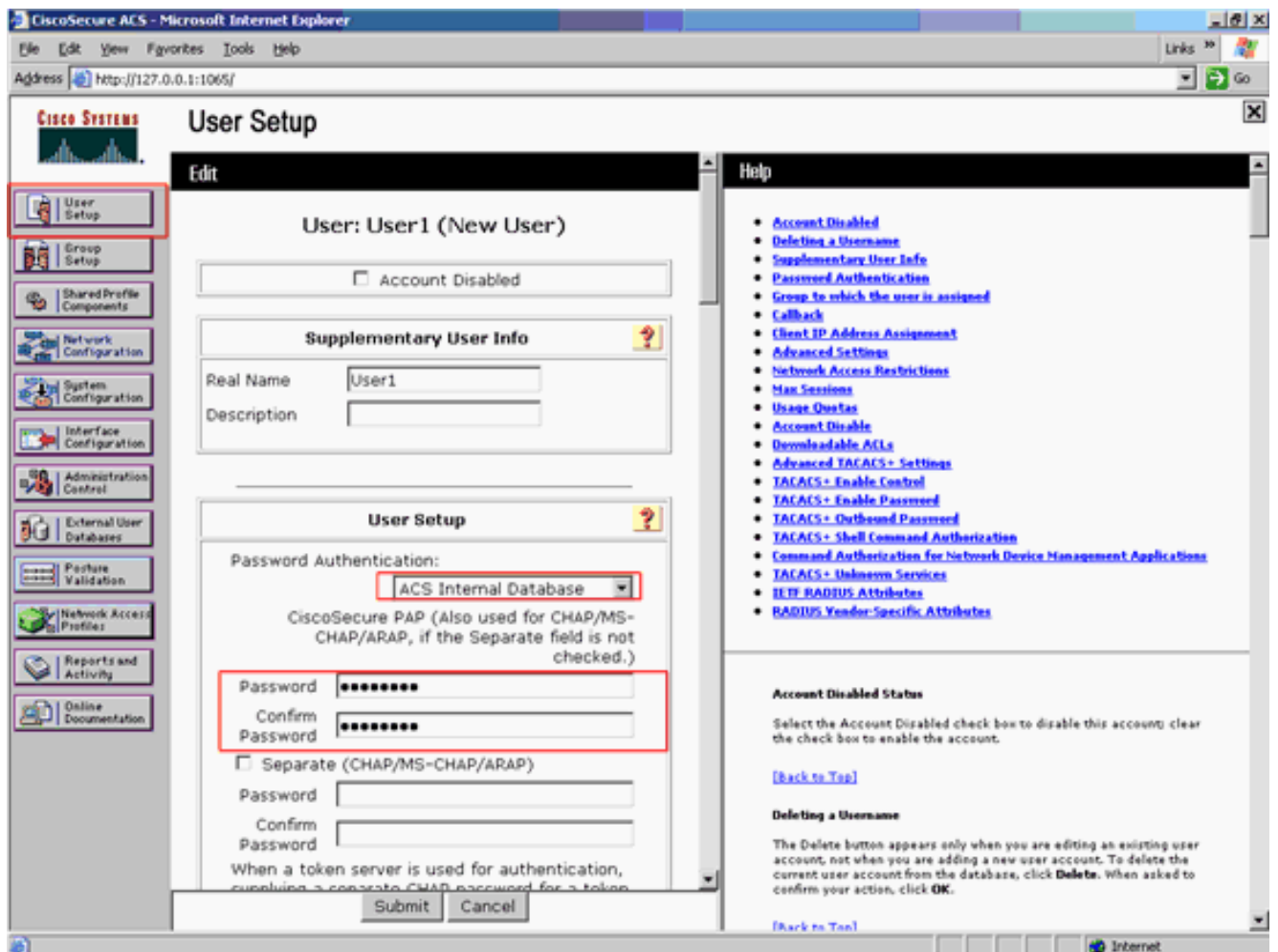
:



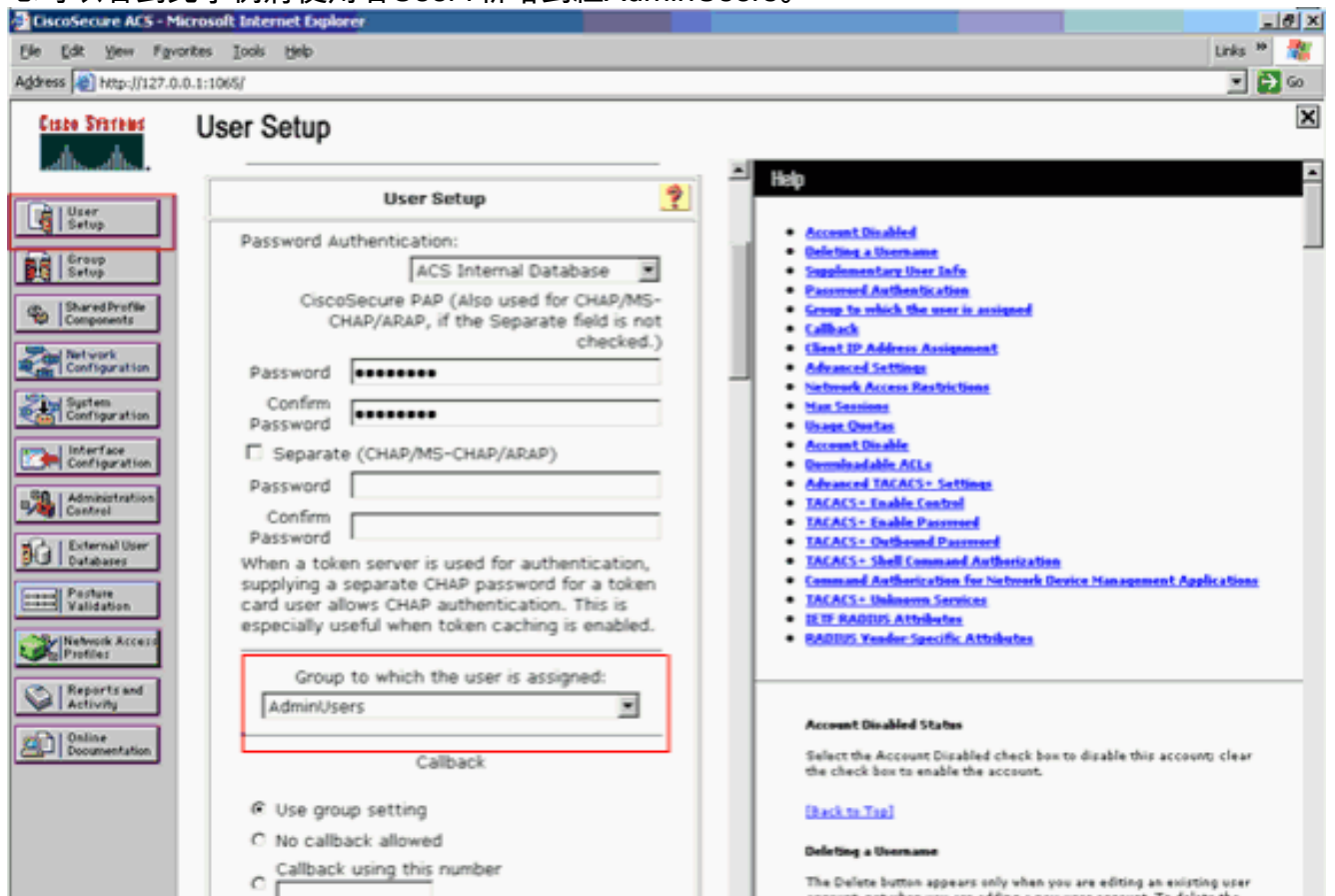
按一下「新增/編輯」後，將出現此使用者的「新增/編輯」視窗。

4. 輸入此使用者特定的憑據，然後按一下Submit以儲存配置。您可以輸入的憑證包括：補充使用者資訊使用者設定使用者分配到的組以下是範例

:



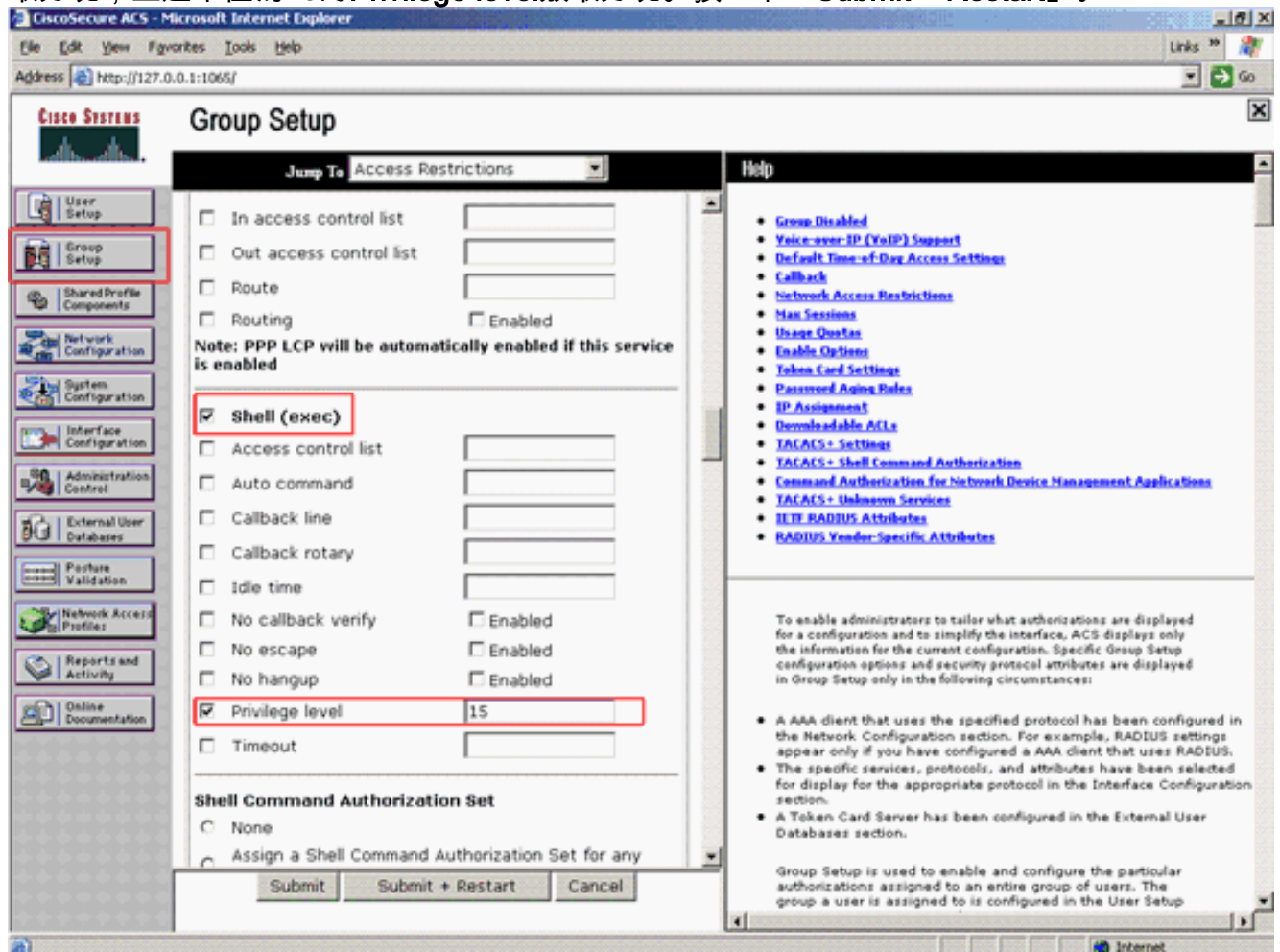
您可以看到此示例將使用者User1新增到組AdminUsers。



註：如果未建立特定組，則使用者將被分配到預設組。

5. 完成以下步驟以定義許可權級別：按一下Group Setup選項卡。選擇之前分配給此使用者的組

，然後按一下**編輯設定**。此示例使用組AdminUsers。在TACACS+設定下，選中**Shell(exec)**覈取方塊，並選中值為15的**Privilege level**覈取方塊。按一下「**Submit + Restart**」。



注意：必須為GUI和Telnet定義許可權級別15才能作為級別15訪問。否則，預設情況下，使用者只能作為級別1訪問。如果未定義許可權級別，且使用者嘗試在CLI上進入啟用模式（使用Telnet），AP將顯示以下錯誤消息：

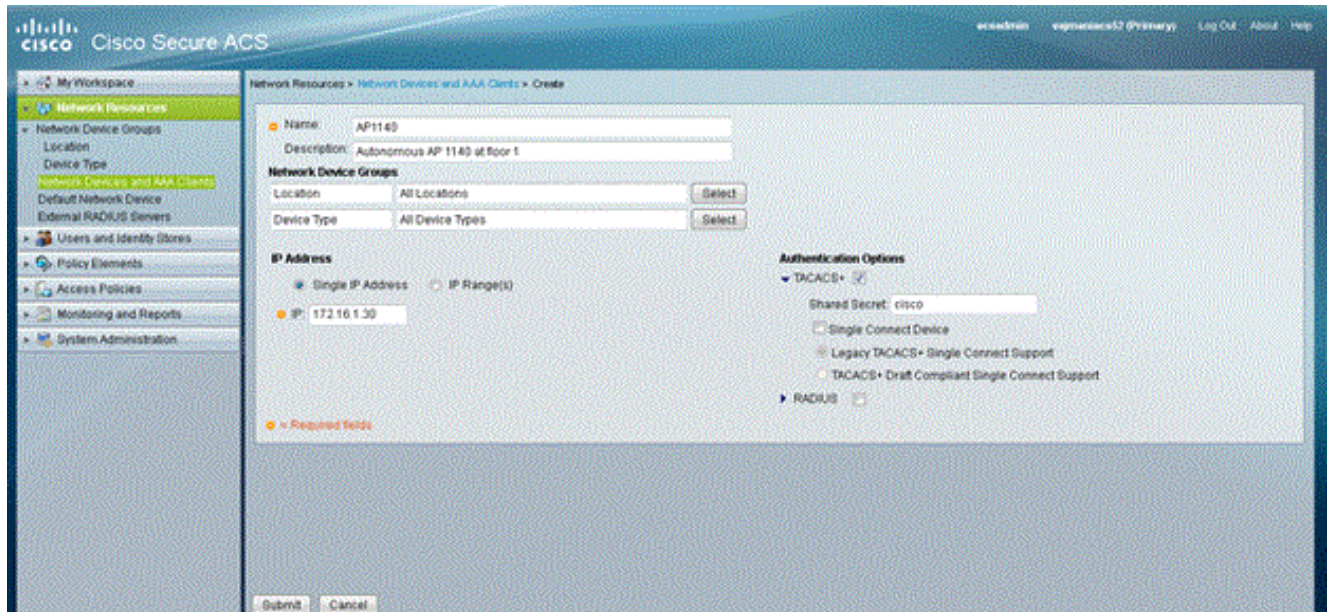
```
AccessPoint>enable
% Error in authentication
```

如果要向TACACS+資料庫新增更多使用者，請重複此過程中的步驟2到步驟4。完成這些步驟後，TACACS+伺服器即可驗證嘗試登入到AP的使用者。現在，您必須為TACACS+身份驗證配置AP。

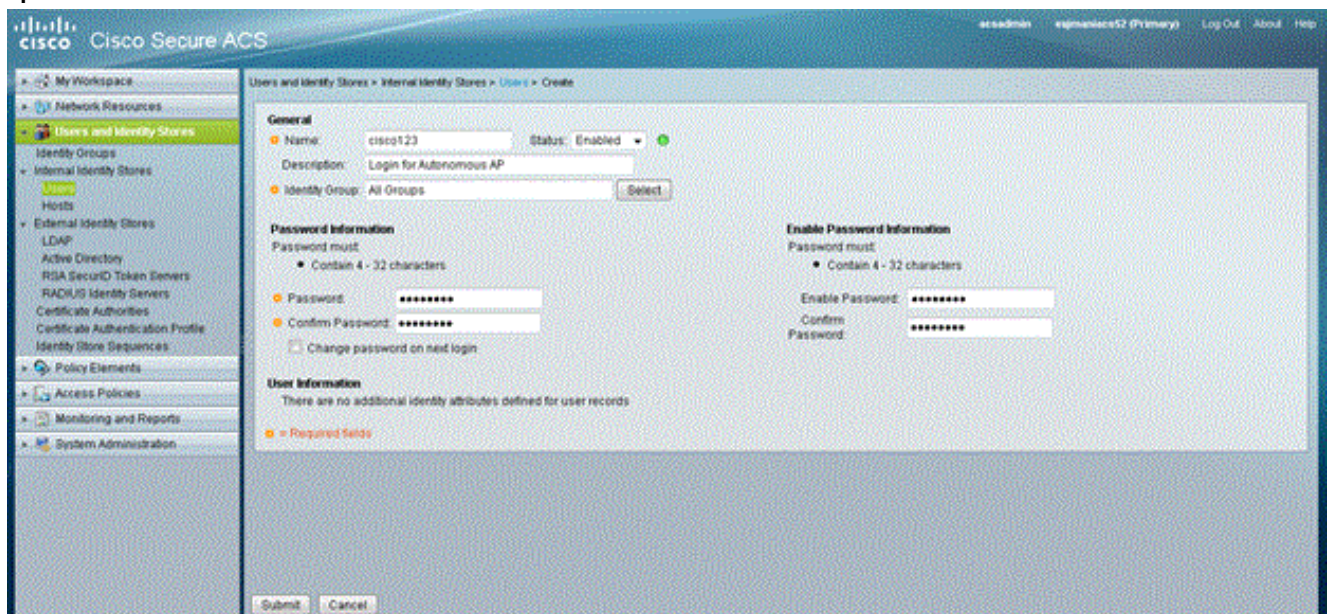
配置TACACS+伺服器進行登入身份驗證 — 使用ACS 5.2

第一步是在ACS中將AP新增為AAA客戶端，並為登入建立TACACS策略。

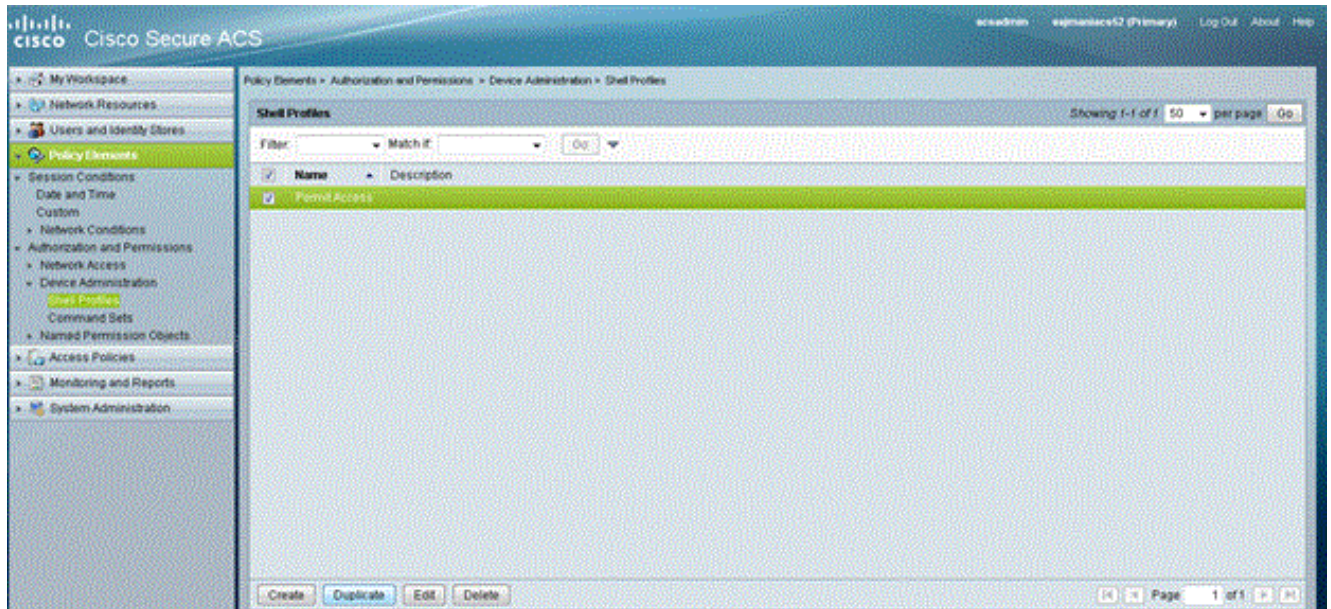
1. 完成以下步驟，以便將AP新增為AAA客戶端：在ACS GUI中，按一下**Network Resources**，然後按一下**Network Devices and AAA Clients**。在Network Devices下，按一下**Create**。在名稱中輸入AP的主機名，並提供有關AP的說明。如果定義了這些類別，請選擇**Location**和**Device Type**。由於只配置單個AP，請按一下**單個IP地址**。您可以通過按一下**IP Range(s)**新增多個AP的IP地址範圍。然後，輸入AP的IP地址。在**Authentication Options**下，選中**TACACS+**框，並輸入**Shared Secret**。以下是範例：



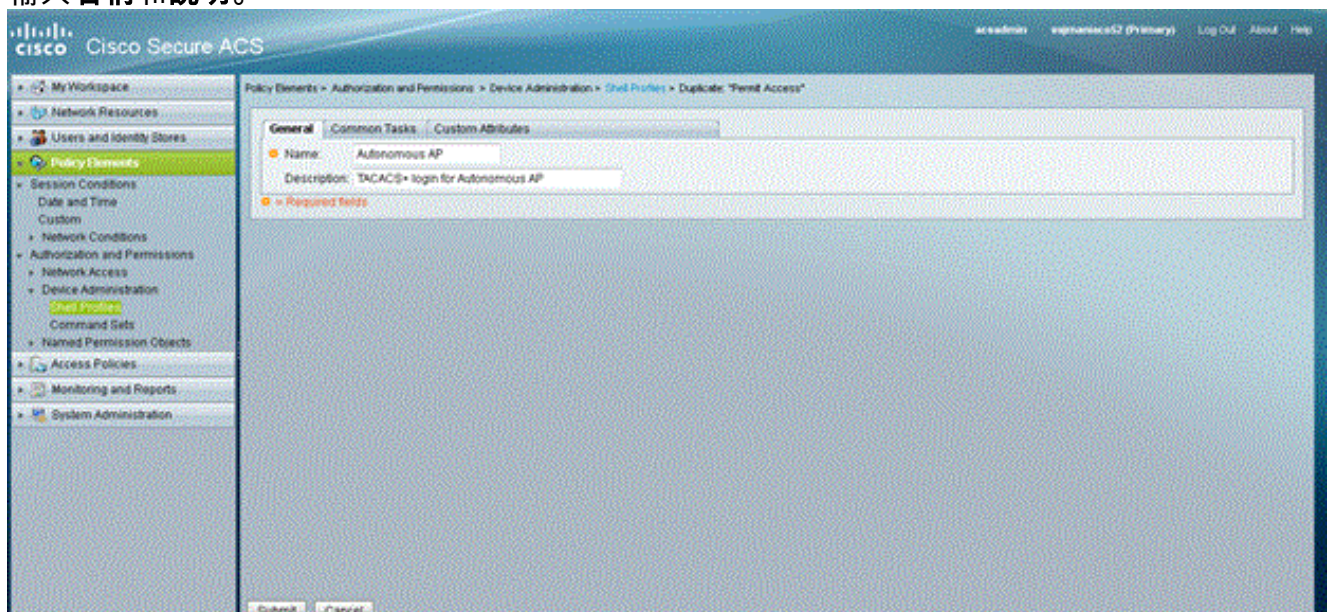
2. 下一步是建立登入使用者名稱和密碼：按一下**Users and Identity Stores**，然後按一下**Users**。按一下「**Create**」。在**Name**下提供使用者名稱，並提供說明。選擇**身份組**（如果有）。在**Password**文本框中輸入密碼，然後在**Confirm Password**下重新輸入。您可以在**Enable Password**下輸入密碼，以修改啟用密碼。重新輸入以確認。以下是範例：



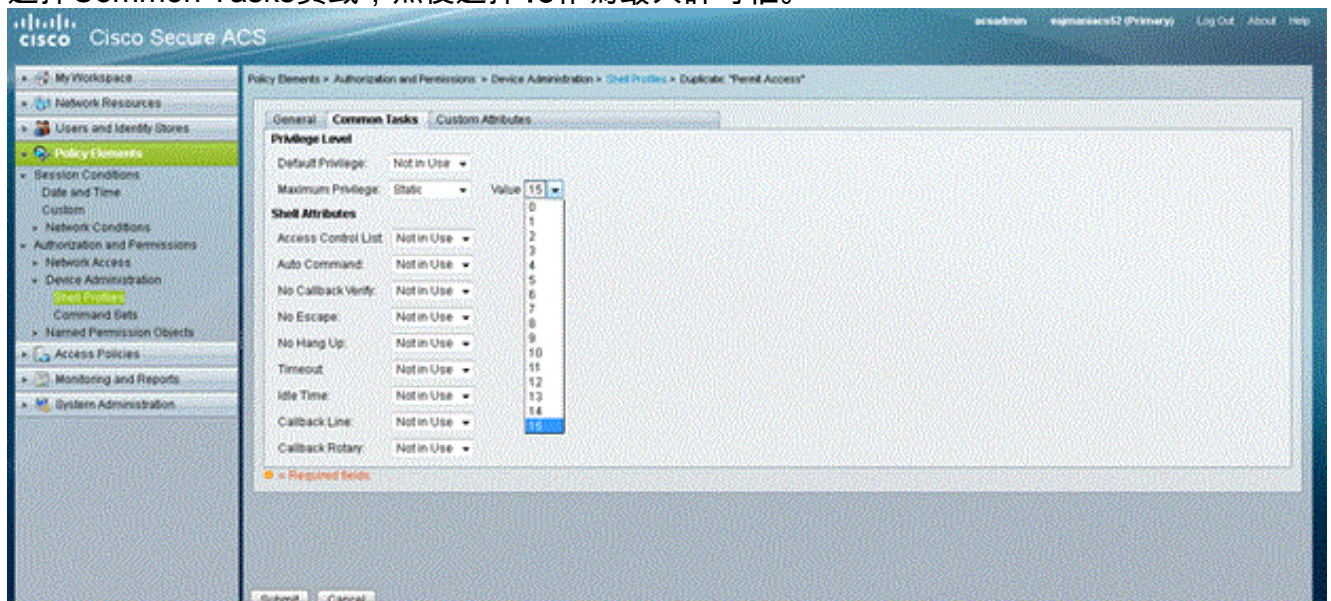
3. 完成以下步驟以定義許可權級別：按一下**Policy Elements > Authorizations and Permissions > Device Administration > Shell Profiles**。選中**Permit Access**釐取方塊，然後按一下**Duplicate**。



輸入名稱和說明。



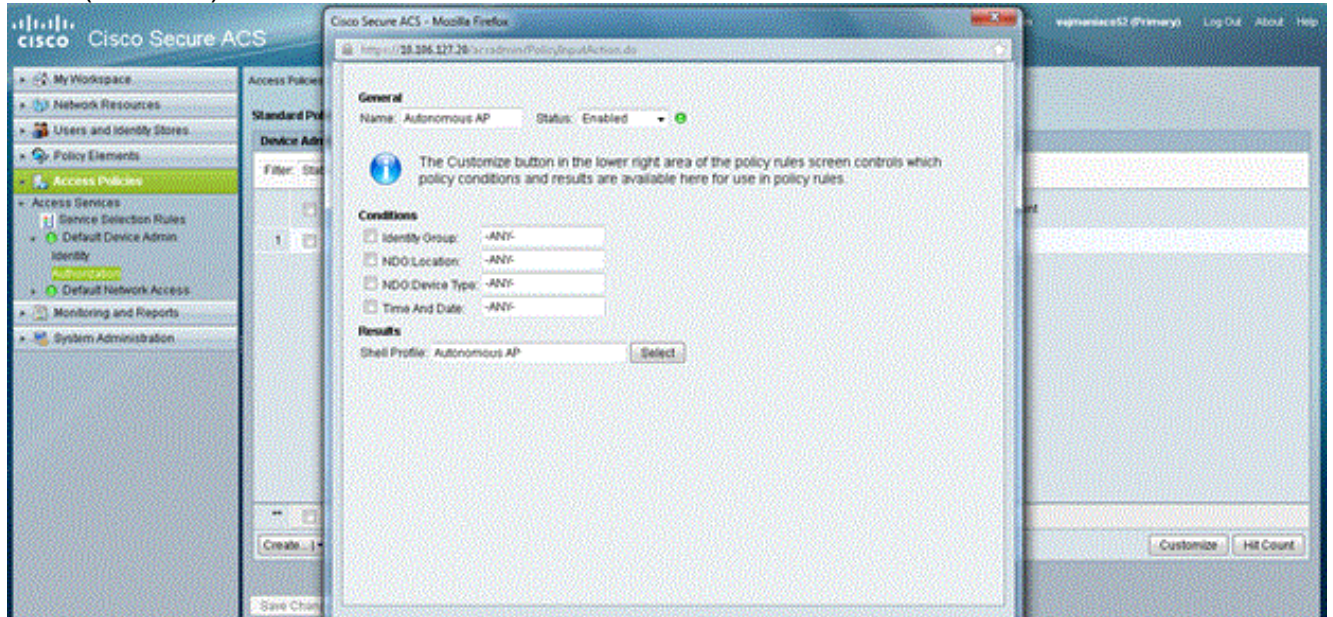
選擇 Common Tasks 頁籤，然後選擇 15 作為最大許可權。



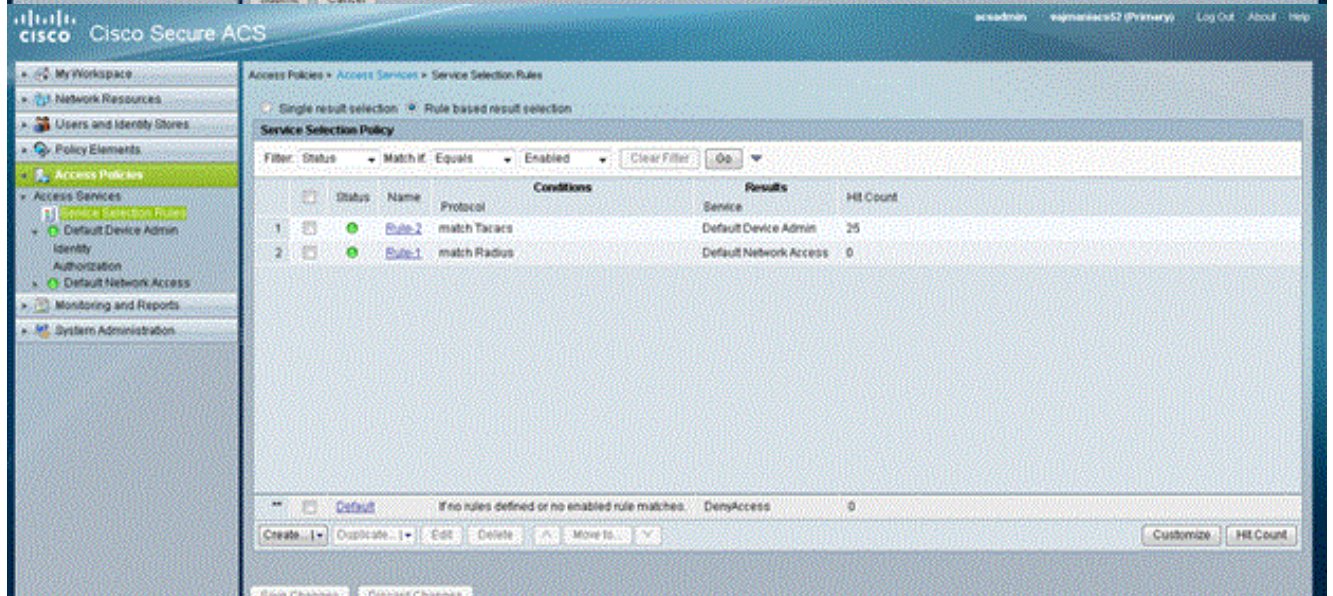
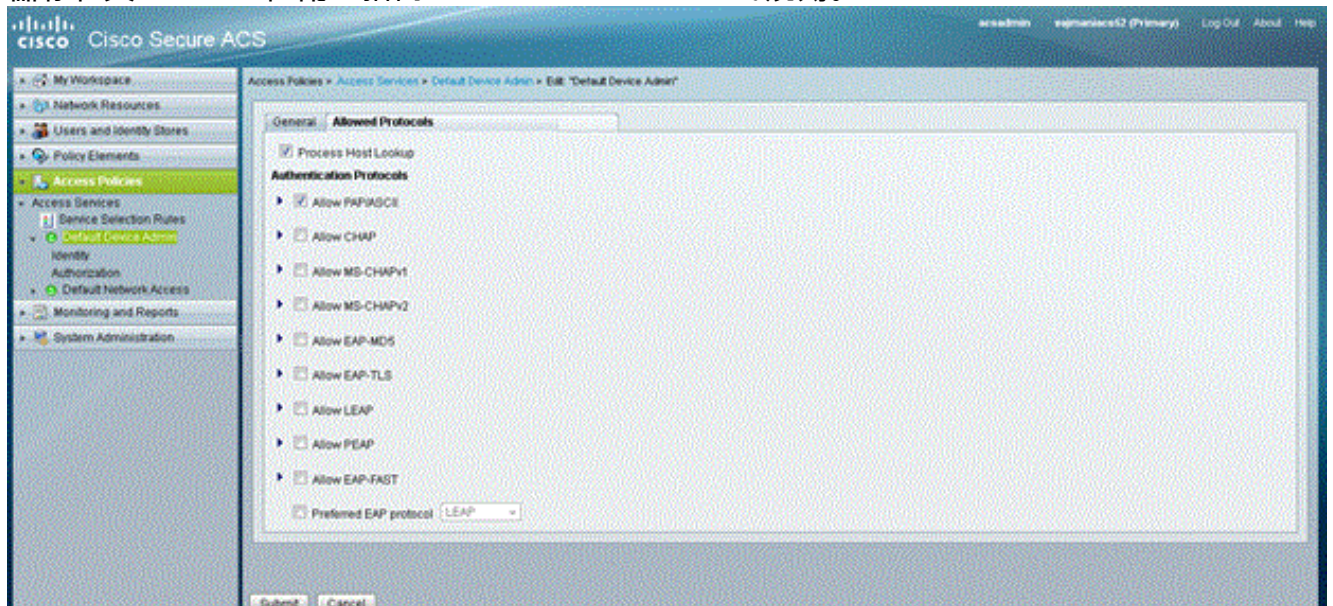
按一下「Submit」。

- 完成以下步驟以建立授權策略：按一下「Access Policies」>「Access Services」>「Default Device Admin」>「Authorization」。按一下 Create 以建立新的授權策略。此時會出現一個新

的彈出視窗，用於為授權策略建立規則。選擇特定使用者名稱和AAA客戶端(AP)的身份組、位置等 (如果有)。按一下Shell Profile的**Select**以選擇已建立的Autonomous AP的配置檔案。



完成此操作後，按一下**Save Changes**。按一下**Default Device Admin**，然後按一下**Allowed Protocols**。選中**Allow PAP/ASCII**，然後按一下**Submit**。按一下**Service Selection Rules**，確儲存在與TACACS匹配且指向Default Device Admin的規則。

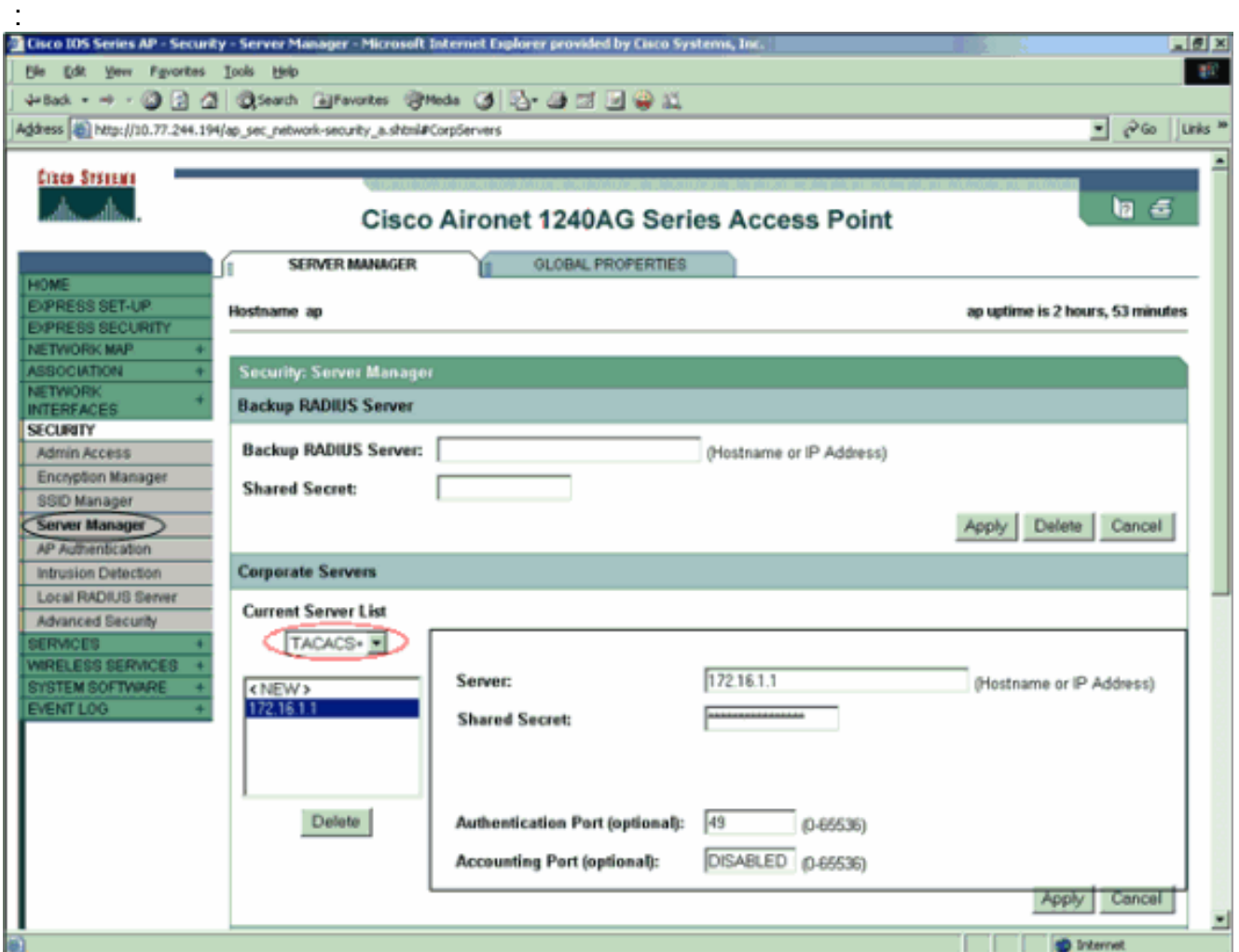


為TACACS+身份驗證配置Aironet AP

您可以使用CLI或GUI在Aironet AP上啟用TACACS+功能。本節介紹如何使用GUI為TACACS+登入身份驗證配置AP。

完成以下步驟，以便使用GUI在AP上設定TACACS+：

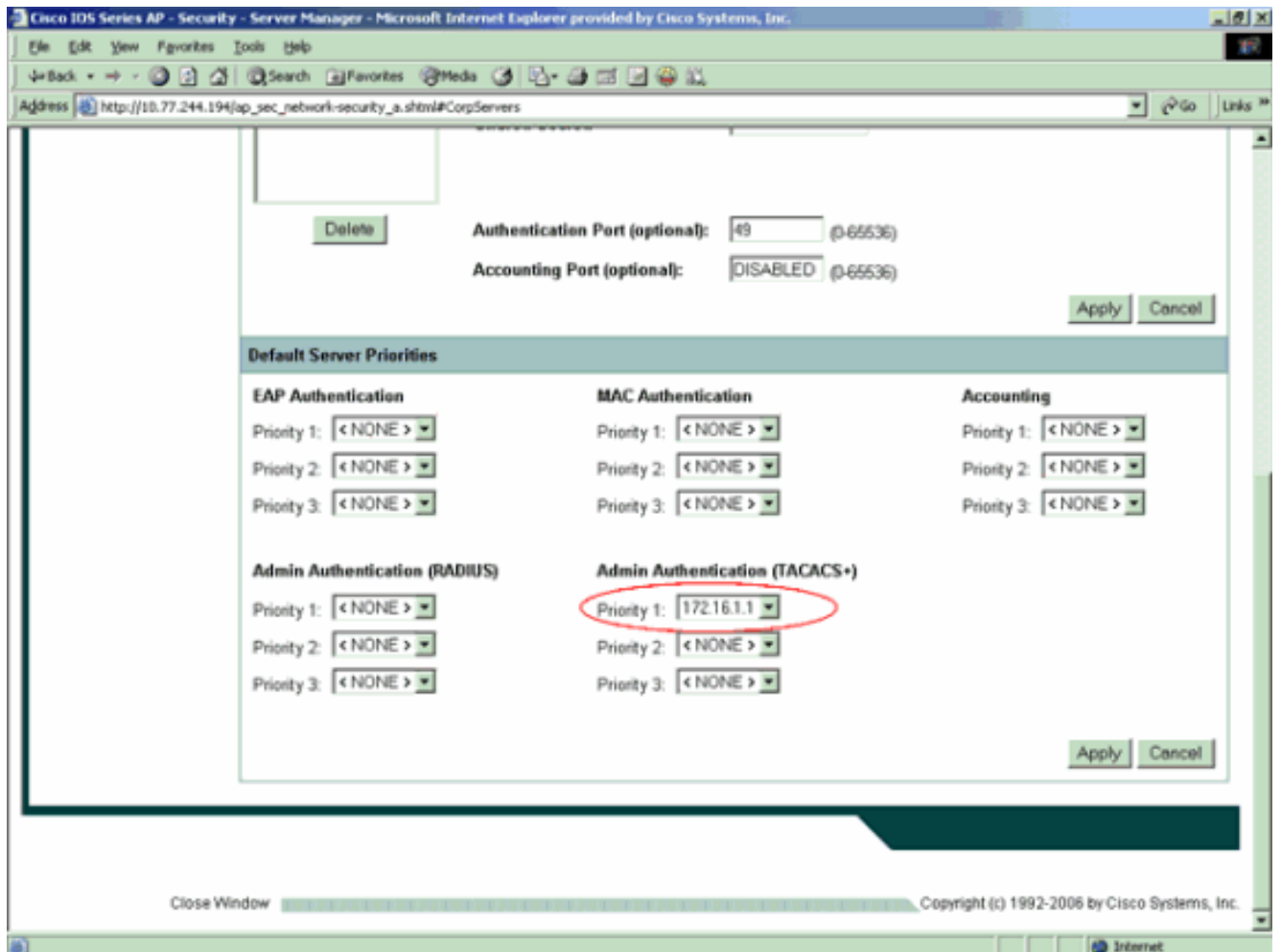
1. 完成以下步驟以定義TACACS+伺服器引數：在AP GUI中選擇**Security > Server Manager**。安全性：出現「Server Manager (伺服器管理器)」視窗。在Corporate Servers區域，從Current Server List下拉選單中選擇**TACACS+**。在此相同區域中，輸入TACACS+伺服器的IP地址、共用金鑰和身份驗證埠號。按一下「Apply」。以下是範例



注意：預設情況下，TACACS+使用TCP埠49。**注意：**您在ACS和AP上配置的共用金鑰必須匹配。

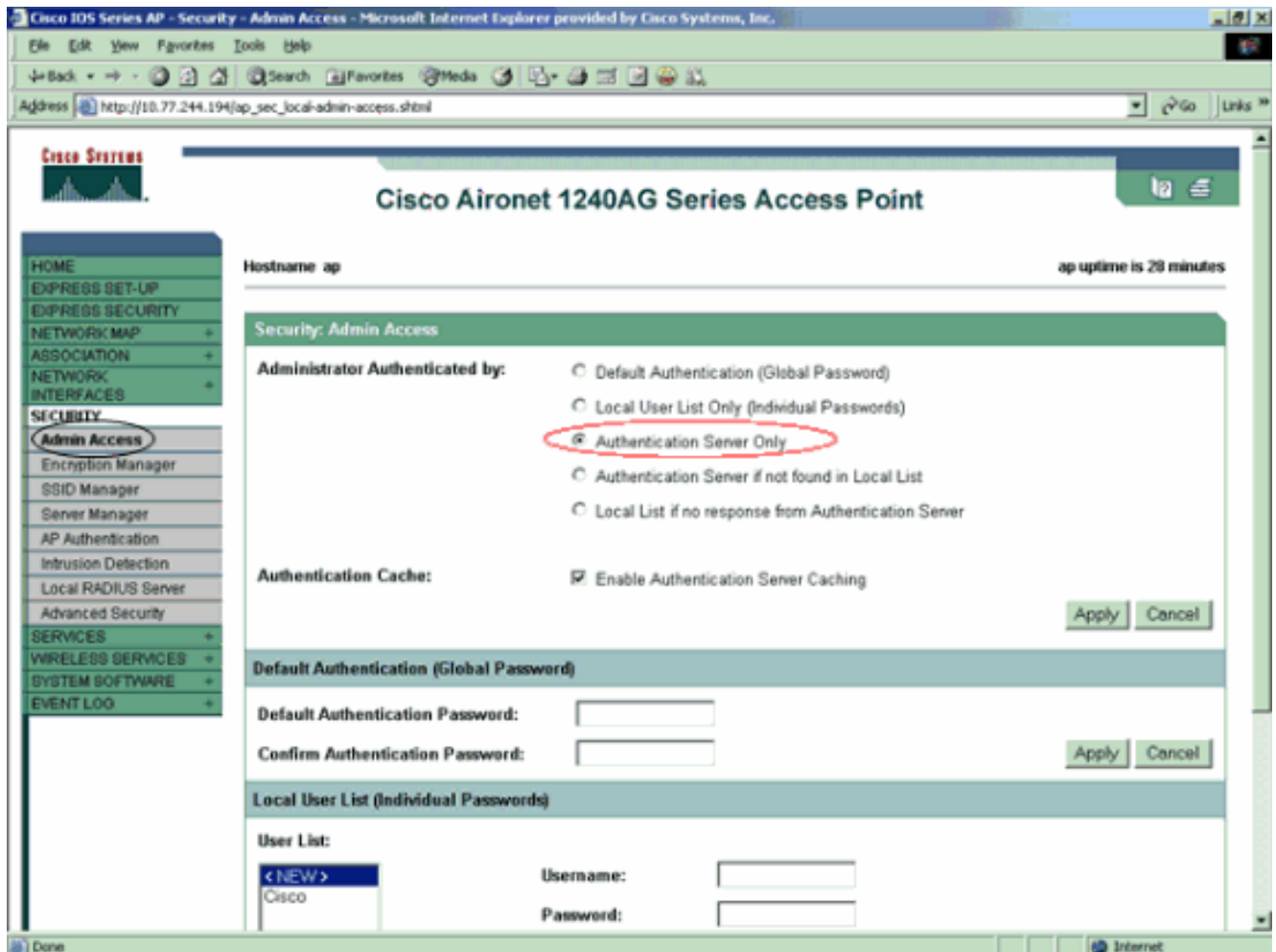
2. 選擇**Default Server Priorities > Admin Authentication(TACACS+)**，從Priority 1下拉選單中選擇已配置的TACACS+伺服器IP地址，然後按一下**Apply**。以下是範例

：



3. 選擇Security > Admin Access，對於Administrator Authenticated by:，選擇Authentication Server Only，然後按一下Apply。此選擇可確保嘗試登入到AP的使用者由身份驗證伺服器進行身份驗證。以下是範例

:



以下是組態範例的CLI組態：

接入點

```

AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
!--- Enable AAA. !! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
!--- Configure the server group tac_admin. server
172.16.1.1
!--- Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1

```

```

!--- Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BV11 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BV11 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end

```

注意：您必須使用Cisco IOS軟體版本12.3(7)JA或更新版本，才能使此配置中的所有命令正常運行。早期的Cisco IOS軟體版本可能沒有這些命令可用。

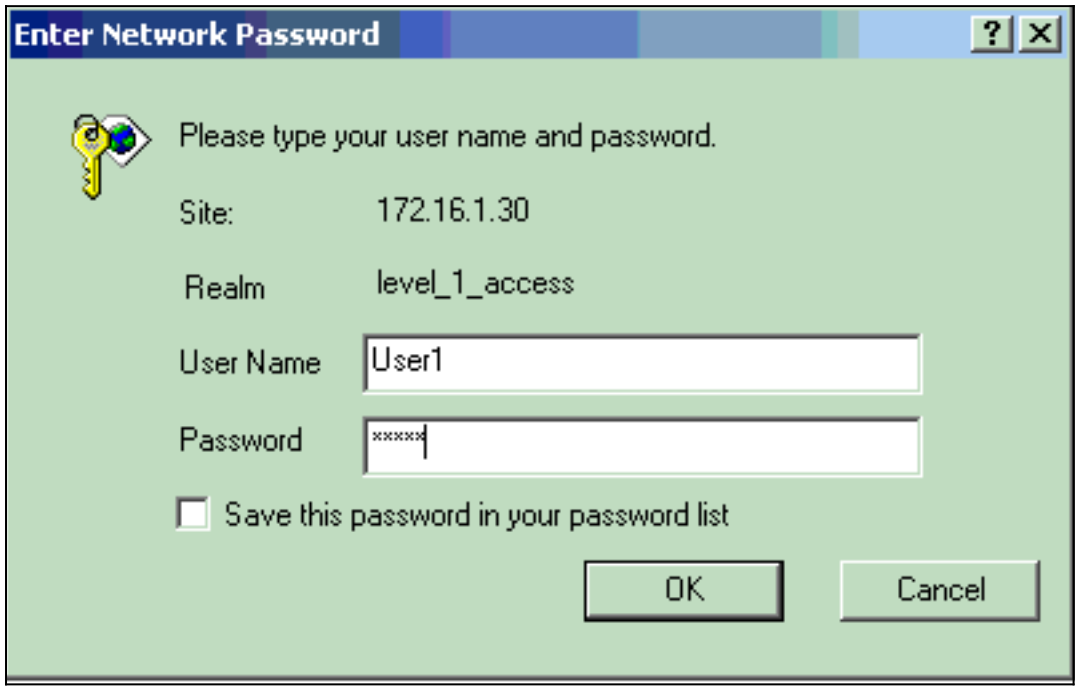
驗證

使用本節內容，確認您的組態是否正常運作。

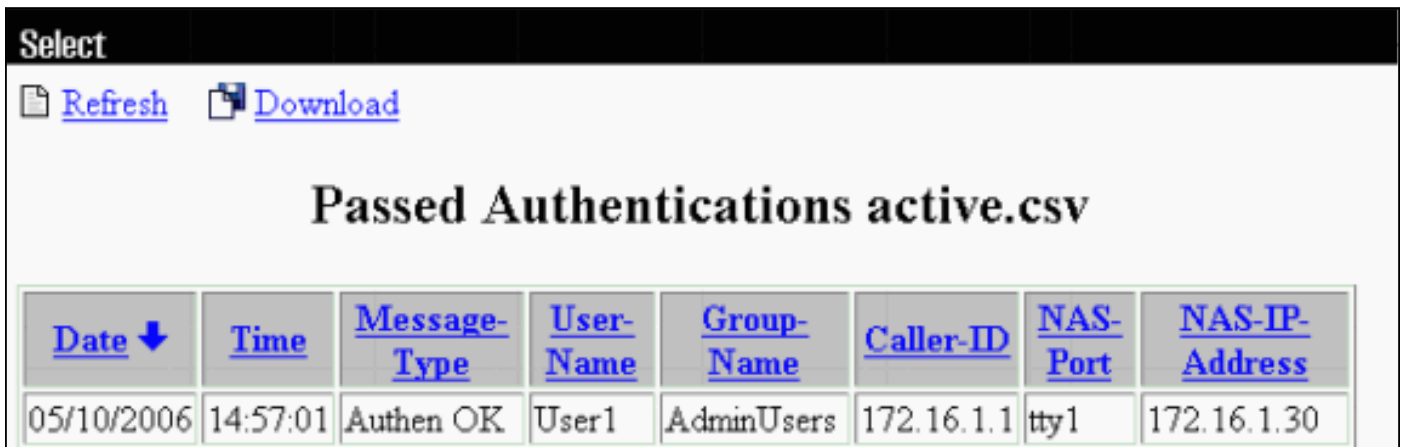
[輸出直譯器工具](#)(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

若要驗證設定，請嘗試使用GUI或CLI登入AP。當您嘗試訪問AP時，AP會提示您輸入使用者名稱和

密碼。



提供使用者認證時，AP會將認證轉送到TACACS+伺服器。TACACS+伺服器根據資料庫中提供的資訊驗證憑證，並在身份驗證成功後提供對AP的訪問。您可以在ACS上選擇**Reports and Activity > Passed Authentication**，並使用Passed Authentication報告檢查此使用者的身份驗證是否成功。以下是範例：



Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
05/10/2006	14:57:01	Authen OK	User1	AdminUsers	172.16.1.1	tty1	172.16.1.30

您還可以使用show tacacs命令來驗證TACACS+伺服器的正確配置。以下是範例：

```
AccessPoint#show tacacs

Tacacs+ Server          : 172.16.1.1/49
  Socket opens:         348
  Socket closes:        348
  Socket aborts:         0
  Socket errors:         0
  Socket Timeouts:      0
  Failed Connect Attempts: 0
  Total Packets Sent:    525
  Total Packets Recv:    525
```

[ACS 5.2驗證](#)

您可以驗證來自ACS 5.2的登入憑證失敗/通過嘗試：

1. 按一下**Monitoring and Reports > Launch Monitoring and Report Viewer**。將開啟一個包含儀表板的新彈出視窗。
2. 按一下「**Authentications-TACACS-Today**」。這顯示失敗/通過嘗試的詳細資訊。

疑難排解

您可以在AP上使用以下debug指令對組態進行疑難排解：

附註：使用 **debug** 指令之前，請先參閱[有關 Debug 指令的重要資訊](#)。

- **debug tacacs events** — 此命令顯示TACACS身份驗證期間發生的事件序列。以下是此指令輸出的範例：

```
*Mar 1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar 1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
*Mar 1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar 1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0
*Mar 1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar 1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

- **debug ip http authentication** — 使用此命令排除HTTP身份驗證問題。命令顯示路由器嘗試的身份驗證方法和身份驗證特定的狀態消息。
- **debug aaa authentication** — 此命令顯示有關AAA TACACS+身份驗證的資訊。

如果使用者輸入的使用者名稱不在TACACS+伺服器上，則身份驗證失敗。以下是**debug tacacs authentication**命令輸出中的身份驗證失敗：

```
*Mar 1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar 1 00:07:26.624: TPLUS: Using server 172.16.1.1
*Mar 1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2
```



```

*Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading
*Mar 1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar 1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar 1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.689: TPLUS: Received authen response status FAIL (3)

```

可以選擇 **Reports and Activity > Failed Authentication** 以檢視ACS上的身份驗證嘗試失敗。以下是範例：

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	CS user unknown

如果您在AP上使用低於Cisco IOS軟體版本12.3(7)JA的Cisco IOS軟體版本，則每次嘗試使用HTTP登入AP時都可能會碰到錯誤。思科錯誤ID為[CSCeb52431](#)(僅限[註冊](#)客戶)。

Cisco IOS軟體HTTP/AAA實施要求對每個單獨的HTTP連線進行獨立身份驗證。無線Cisco IOS軟體GUI涉及在單一網頁內引用多個獨立的檔案(例如Javascript和GIF)。因此，如果您在無線Cisco IOS軟體GUI中載入單一頁面，AAA伺服器可能會收到幾十個不同的驗證/授權要求。

對於HTTP身份驗證，請使用RADIUS或本地身份驗證。RADIUS伺服器仍要承受多個驗證要求。但RADIUS的可擴充性高於TACACS+，因此可能會提供較小的效能影響。

如果必須使用TACACS+且您有思科ACS，請將**single-connection**關鍵字與**tacacs-server**命令一起使用。將此關鍵字與命令一起使用會使ACS省去大部分TCP連線建立/拆卸開銷，並可能會在一定程度上降低伺服器上的負載。

對於AP上的Cisco IOS軟體版本12.3(7)JA及更高版本，軟體包含修復。本節的其餘部分將介紹修復程式。

使用AAA驗證快取功能可快取TACACS+伺服器傳回的資訊。身份驗證快取和配置檔案功能允許AP快取使用者的身份驗證/授權響應，以便無需將後續身份驗證/授權請求傳送到AAA伺服器。若要使用CLI啟用此功能，請使用以下命令：

```

cache expiry
cache authorization profile

```

```
cache authentication profile
aaa cache profile
```

有關此功能和命令的更多資訊，請參閱[管理接入點](#)的[配置身份驗證快取和配置檔案](#)部分。

要在GUI上啟用此功能，請選擇**Security > Admin Access**，並選中**Enable Authentication Server Caching**覈取方塊。由於本檔案使用Cisco IOS軟體版本12.3(7)JA，因此本檔案會使用[設定](#)所述的修正程式。

[相關資訊](#)

- [設定RADIUS和TACACS+伺服器](#)
- [公告：IOS接入點通過請求來轟炸TACACS+伺服器](#)
- [使用RADIUS伺服器的EAP身份驗證](#)
- [無線產品支援](#)
- [技術支援與文件 - Cisco Systems](#)