鎖定與金鑰：動態存取清單

目錄

簡介

使用鎖鑰型存取，可以設定動態存取清單，透過使用者驗證程式，將每個使用者對特定來源/目的地主機的存取授予該清單。使用者可以動態地通過Cisco IOS®防火牆進行訪問，而不會影響安全限制。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。在本例中，實驗環境由運行Cisco IOS®軟體版本12.3(1)的2620路由器組成。 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

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

欺騙注意事項

鎖鑰型存取允許外部事件在Cisco IOS防火牆中開啟一個開口。如果存在此開啟，路由器容易受到源地址欺騙。為了防止發生這種情況，請使用身份驗證或加密的IP加密來提供加密支援。

欺騙是所有現有訪問清單都存在的一個問題。鎖鑰型存取無法解決此問題。

由於鎖鑰型存取會引入通過網路防火牆的潛在路徑，因此需要考慮動態存取。另一個主機（偽裝經過身份驗證的地址）可在防火牆後獲得訪問許可權。使用動態存取時，未經授權的主機（偽裝您的已驗證位址）可能會透過防火牆獲得存取許可權。鎖鑰型存取不會造成位址詐騙問題。此處問題只是使用者關心的問題。

效能

在這兩種情況下效能會受到影響。

- 每個動態訪問清單強制在矽交換引擎(SSE)上重建訪問清單。 這會導致SSE交換路徑暫時變慢。
- 動態存取清單需要閒置逾時工具（即使逾時保留為預設值）。 因此，動態訪問清單無法進行SSE交換。這些專案會在通訊協定快速交換路徑中處理。

觀察邊界路由器配置。遠端使用者在邊界路由器上建立訪問清單條目。訪問清單會動態地增大和縮小。當空閒超時或最大超時時間到期後，將從清單中動態刪除條目。大型訪問清單會降低資料包交換效能。

使用鎖鑰型存取的時機

以下是使用鎖鑰型存取的兩個範例：

- 當您希望遠端主機能夠通過Internet訪問您網際網路中的主機時。鎖鑰型存取會針對個別主機或網路限制透過防火牆進行的存取。
- 當您希望網路中的主機子集訪問受防火牆保護的遠端網路上的主機時。透過鎖鑰型存取，您可以僅啟用所需的一組主機以透過TACACS+或RADIUS伺服器進行驗證，從而取得存取許可權。

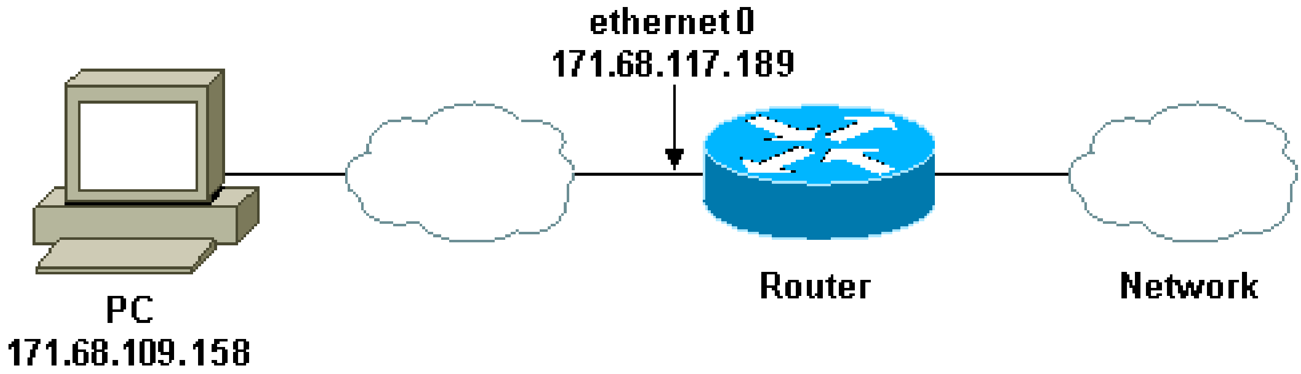
鎖鑰型存取作業

此程式描述鎖鑰型存取操作。

1. 使用者開啟與為鎖鑰型存取而設定的邊界路由器的Telnet作業階段。
2. Cisco IOS軟體接收Telnet封包。它執行使用者身份驗證過程。使用者必須通過身份驗證才能允許訪問。驗證程式由路由器或中央存取伺服器（例如TACACS+或RADIUS伺服器）完成。

示例配置和故障排除

網路圖表



思科建議您使用TACACS+伺服器進行驗證查詢程式。TACACS+提供驗證、授權及計費服務。它還提供了協定支援、協定規範和一個集中式安全資料庫。

您可以在路由器上或在TACACS+或RADIUS伺服器上驗證使用者身分。

附註： 除非另有說明，否則這些命令是全域性的。

在路由器上，您需要使用者的**使用者名稱**進行本地身份驗證。

```
username test password test
```

vty線路上存在**login local**會導致使用此使用者名稱。

```
line vty 0 4
login local
```

如果不信任使用者發出**access-enable**命令，則可以執行下列兩種操作之一：

- 按使用者將超時與使用者關聯。

  ```
  username test autocommand access-enable host
  timeout 10
  ```

  或
- 強制Telnet的所有使用者都具有相同的超時。

  ```
  line vty 0 4
  login local
  autocommand access-enable host timeout 10
  ```

注意：語法**中**的10是訪問*列*表的空閒超時。動態存取清單中的絕對逾時會將其覆寫。

定義使用者（任何使用者）登入到路由器並發出**access-enable**命令時應用的擴展訪問清單。過濾器中的此「孔」的最大絕對時間設定為15分鐘。15分鐘後，無論是否有人使用它，這個洞都會關閉。名稱**testlist**必須存在，但並不重要。通過配置源地址或目標地址來限制使用者有權訪問的網路（此處使用者不受限制）。

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

定義阻止所有內容所需的訪問清單，但Telnet到路由器的功能除外（為了開啟孔，使用者需要Telnet到路由器）。 這裡的IP地址是路由器的乙太網IP地址。

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

結尾有隱含的**deny all**（未在此處輸入）。

將此訪問清單應用於使用者進入的介面。

```
interface ethernet1
       ip access-group 120 in
```

你完了。

路由器上的過濾器現在看起來是這樣的：

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

訪問您的內部網路的使用者在Telnet到路由器之前看不到任何內容。

注意：這**里**10是存*取*清單的閒置逾時。動態存取清單中的絕對逾時會將其覆寫。

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test

Connection closed by foreign host.
```

過濾器如下所示。

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

根據來源IP位址，此使用者對應的篩選器中有一個洞。當別人這麼做時，你會看到*兩個洞*。

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
```

```
        permit ip host 171.68.109.158 any log
     20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

這些使用者能夠從其源IP地址獲得對任何目標IP地址的完全IP訪問。

使用TACACS+

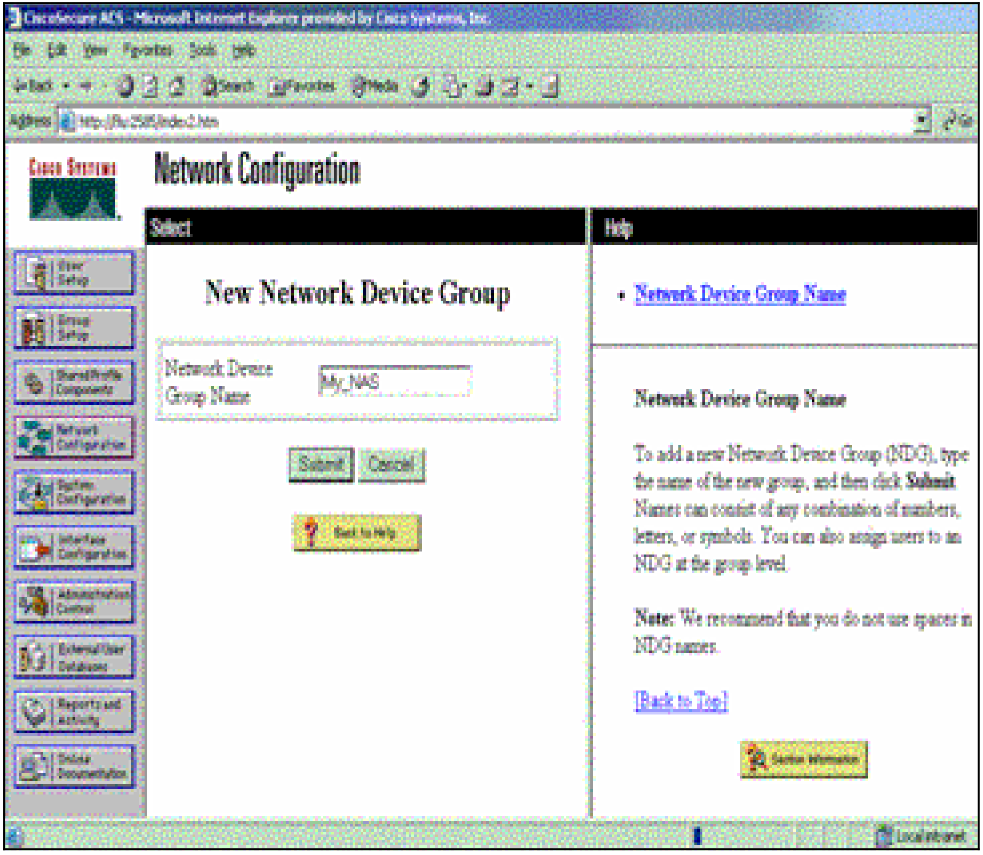
設定TACACS+

設定TACACS+伺服器以強制在TACACS+伺服器上完成驗證和授權，以便使用TACACS+，如下輸出所示：

```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

完成以下步驟，在適用於Windows的Cisco Secure ACS上配置TACACS+:

1. 開啟Web瀏覽器。輸入ACS伺服器的地址，格式為**http://*<IP_address or DNS_name>***:2002。（此示例使用預設埠2002。）以管理員身份登入。
2. 按一下「**Network Configuration**」。按一下**Add Entry**以建立包含網路訪問伺服器(NAS)的網路裝置組。 輸入組的名稱，然後按一下**Submit**。



Network Configuration

New Network Device Group

Network Device Group Name: My_NAS

- Network Device Group Name

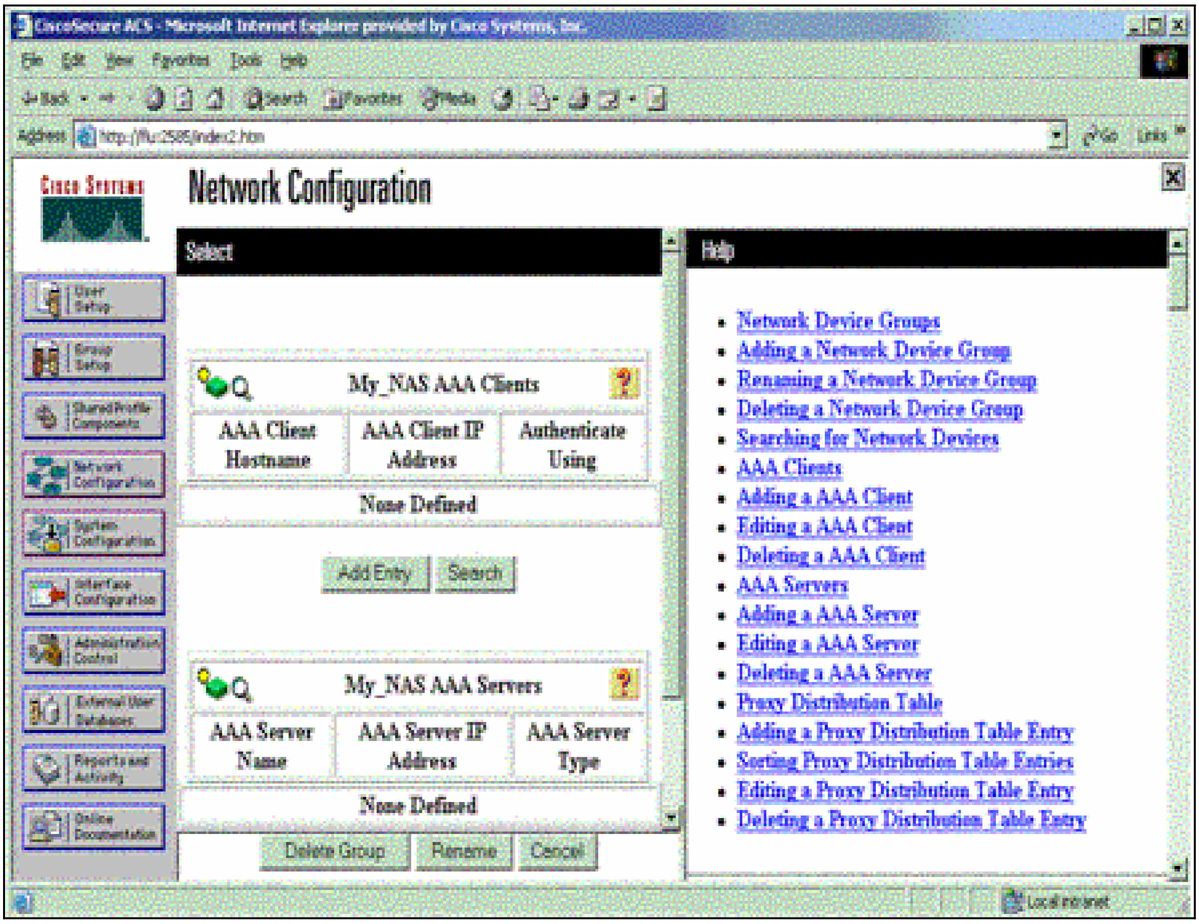
Network Device Group Name

To add a new Network Device Group (NDG), type the name of the new group, and then click **Submit**. Names can consist of any combination of numbers, letters, or symbols. You can also assign users to an NDG at the group level.

Note: We recommend that you do not use spaces in NDG names.

[Back to Top]

3. 按一下**Add Entry**新增身份驗證、授權和記帳(AAA)客戶端(NAS)。



Network Configuration

My_NAS AAA Clients

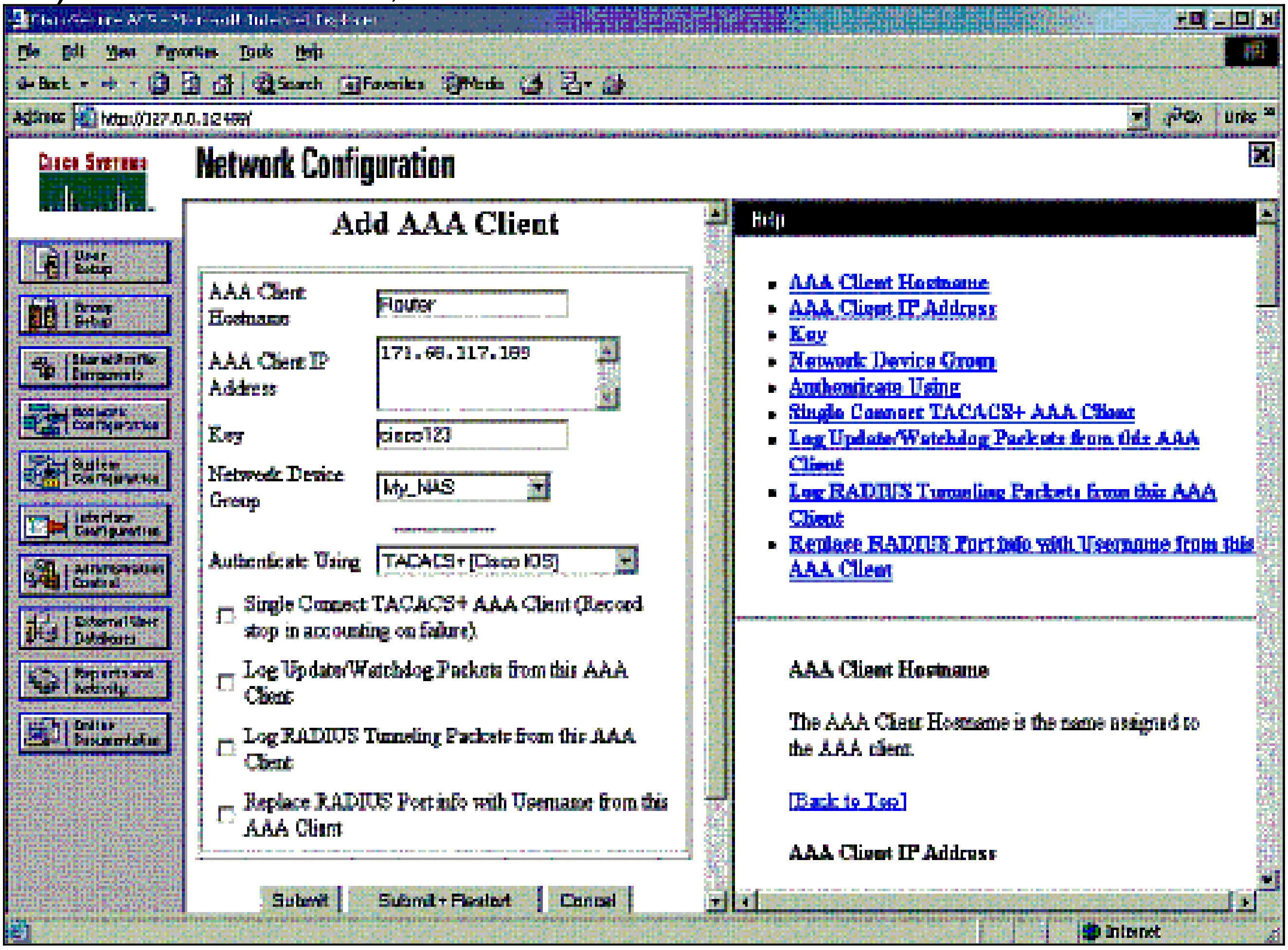
AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

My_NAS AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
None Defined		

- Network Device Groups
- Adding a Network Device Group
- Renaming a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

4. 輸入用於加密AAA伺服器和NAS之間通訊的主機名、IP地址和金鑰。選擇**TACACS+(Cisco IOS)**作為驗證方法。完成後，按一下**Submit +Restart**應用更改。



Network Configuration

Add AAA Client

AAA Client Hostname: Router

AAA Client IP Address: 171.68.117.189

Key: cisco123

Network Device Group: My_NAS

Authenticate Using: TACACS+ (Cisco IOS)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

□ Log RADIUS Tunneling Packets from this AAA Client

□ Replace RADIUS Port info with Username from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

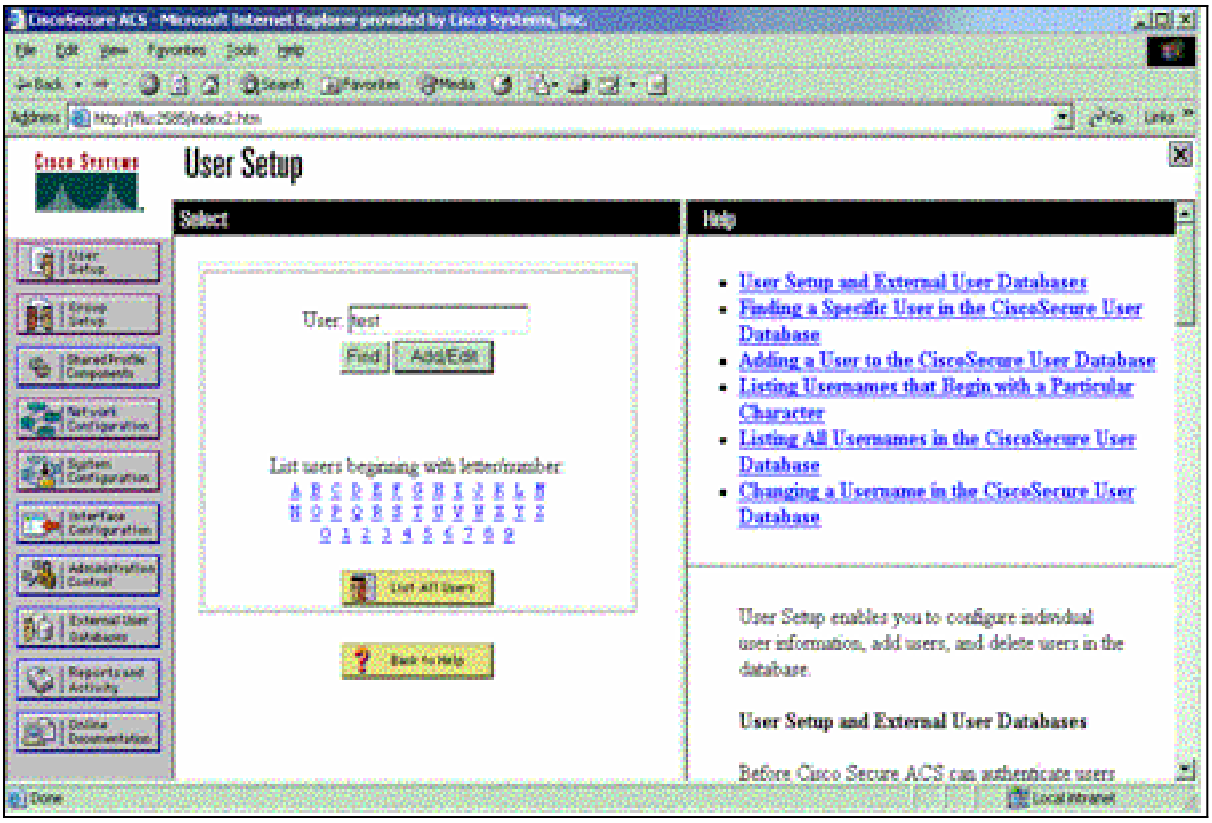
AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

[Back to Top]

AAA Client IP Address

5. 按一下**User Setup**，輸入使用者ID，然後按一下**Add/Edit**。



User Setup

Select

User: test

Find Add/Edit

List users beginning with letter/number:

A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

List All Users

Back to Help

Help

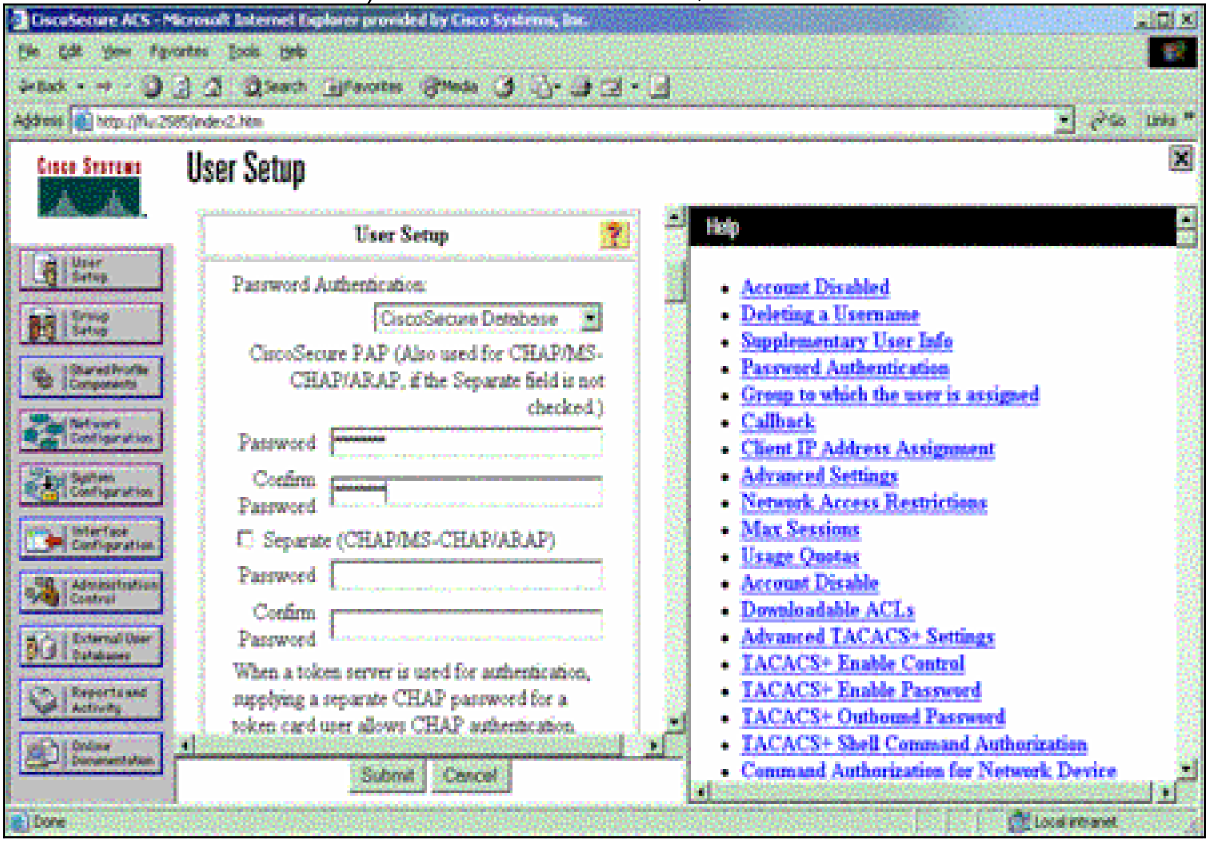
- User Setup and External User Databases
- Finding a Specific User in the CiscoSecure User Database
- Adding a User to the CiscoSecure User Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the CiscoSecure User Database
- Changing a Username in the CiscoSecure User Database

User Setup enables you to configure individual user information, add users, and delete users in the database.

User Setup and External User Databases

Before Cisco Secure ACS can authenticate users

6. 選擇一個資料庫以對使用者進行身份驗證。（在本示例中，使用者是「test」使用者，ACS的內部資料庫用於身份驗證）。 輸入使用者的密碼，並確認密碼。



User Setup

User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password ********

Confirm Password ********

□ Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

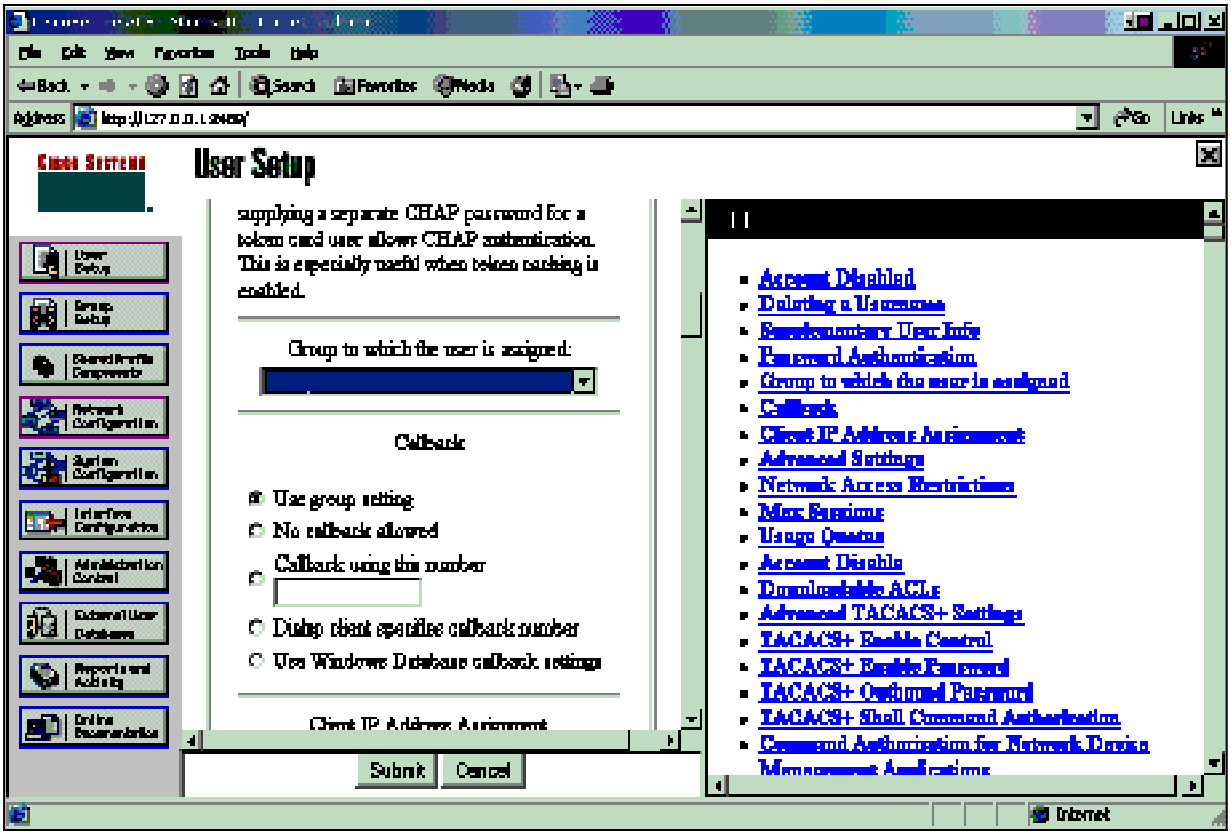
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication.

Submit Cancel

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device

7. 選擇使用者分配到的組，並選中**使用組設定**。按一下「**Submit**」。



User Setup

supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Callback

● Use group setting

○ No callback allowed

○ Callback using this number

○ Dialup client specifies callback number

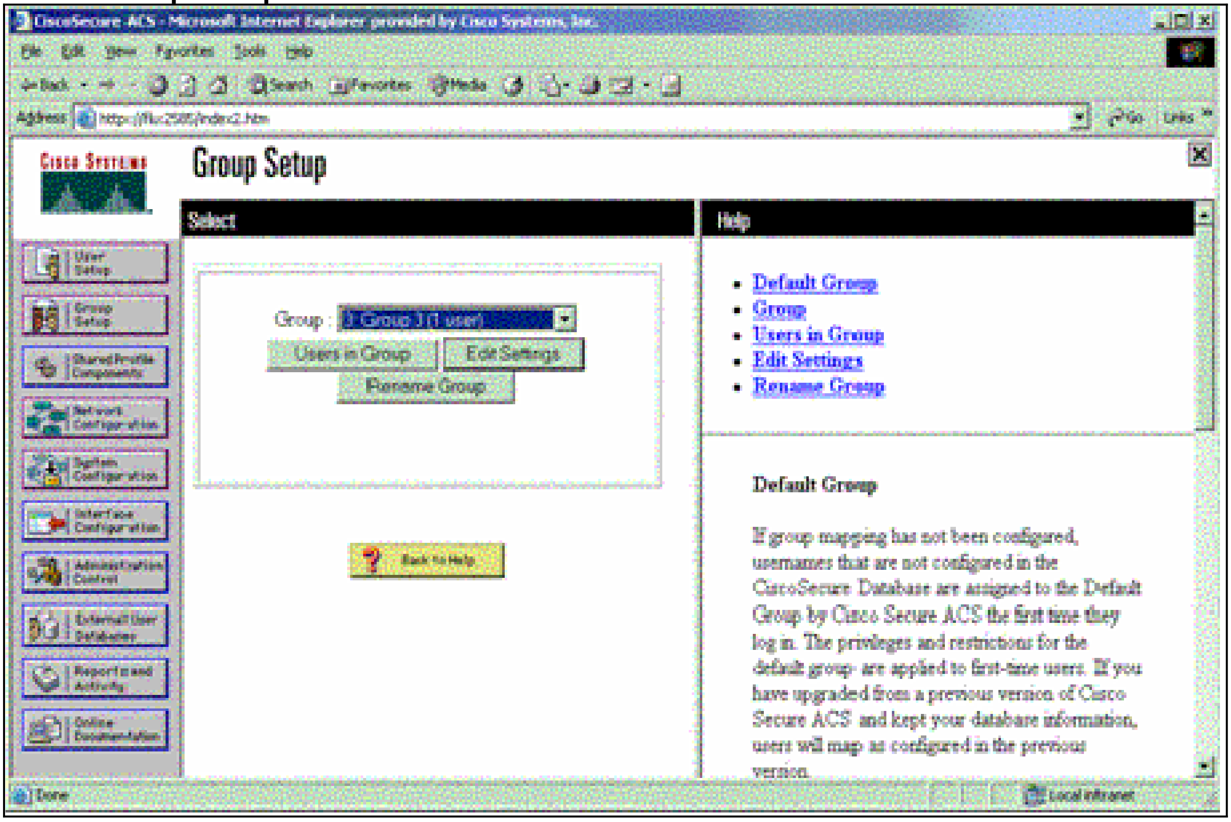
○ Use Windows Database callback settings

Client IP Address Assignment

Submit Cancel

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications

8. 按一下Group Setup。選擇在步驟7中為使用者分配的組。按一下**編輯設定**。



Group Setup

Select

Group : 1: Group 1 (1 user)

Users in Group Edit Settings

Rename Group

Back to Help

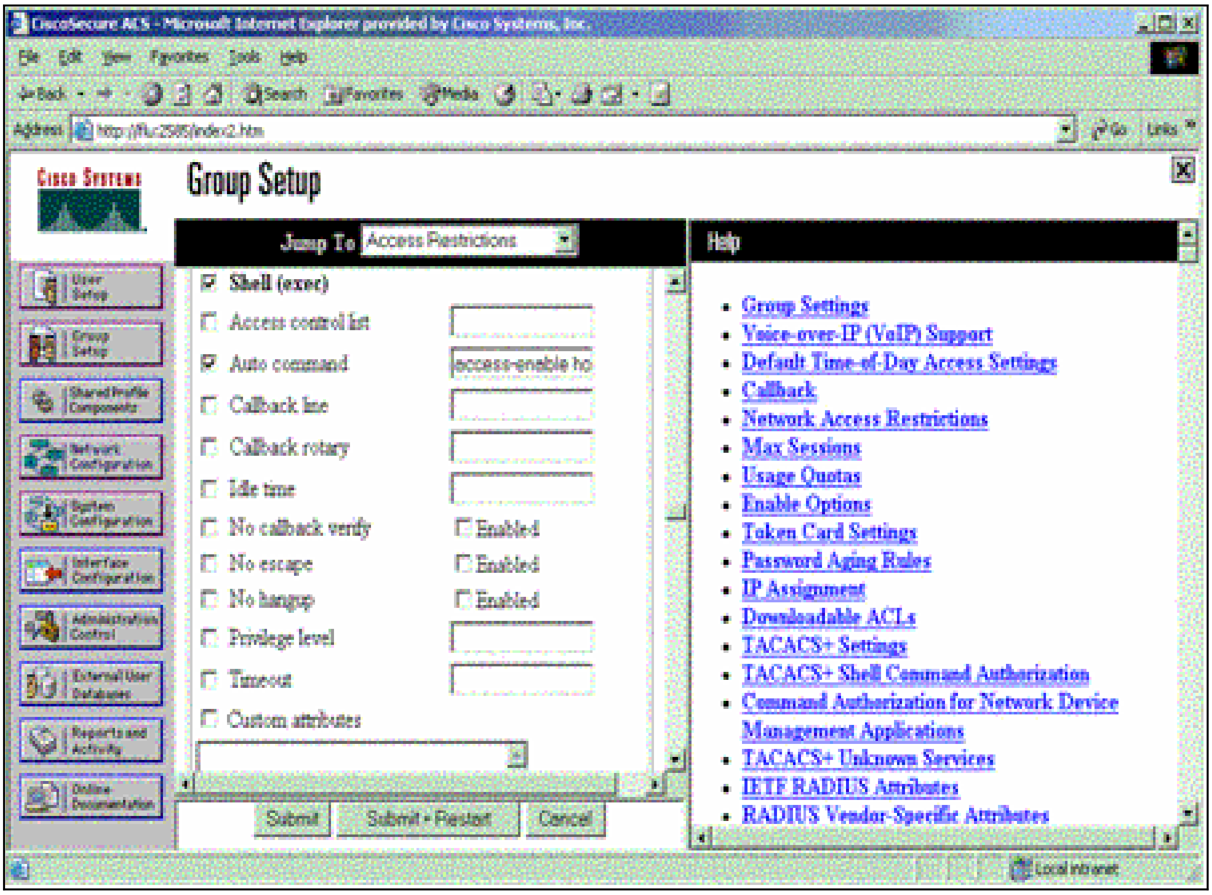
Help

- Default Group
- Group
- Users in Group
- Edit Settings
- Rename Group

Default Group

If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.

9. 向下滾動到「TACACS+設定」部分。選中**Shell exec**覈取方塊。選中**Auto**命令對應的框。輸入要在成功授權使用者後執行的auto — 命令。(此示例使用**access-enable host timeout 10**命令。) 按一下**Submit+Restart**。



Group Setup

☑ Shell (exec)
□ Access control list
☑ Auto command access-enable ho
□ Callback line
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
□ Privilege level
□ Timeout
□ Custom attributes

- Group Settings
- Voice-over-IP (VoIP) Support
- Default Time-of-Day Access Settings
- Callback
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Enable Options
- Token Card Settings
- Password Aging Rules
- IP Assignment
- Downloadable ACLs
- TACACS+ Settings
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

疑難排解TACACS+

在NAS上使用這些**debug**命令來排除TACACS+故障。

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 authentication** — 顯示有關TACACS+身份驗證過程的資訊。僅在某些版本的軟體中可用。如果不可用，請僅使用**debug tacacs**。
- **debug tacacs authorization** — 顯示有關TACACS+授權進程的資訊。僅在某些版本的軟體中可用。如果不可用，請僅使用**debug tacacs**。
- **debug tacacs events** — 顯示來自TACACS+幫助程式進程的資訊。僅在某些版本的軟體中可用。如果不可用，請僅使用**debug tacacs**。

使用以下命令排除AAA故障：

- **debug aaa authentication** — 顯示有關AAA/TACACS+身份驗證的資訊。
- **debug aaa authorization** — 顯示有關AAA/TACACS+授權的資訊。

此處的**debug**輸出範例顯示ACS TACACS+伺服器上的驗證和授權程式成功。

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
=======================================================
Router#
 AAA/BIND(00000009): Bind i/f
```

```
AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication start request id 9
TPLUS: Authentication start packet created for 9()
TPLUS: Using server 10.48.66.53
TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
 AAA/AUTHOR/EXEC(00000009): processing AV
   autocmd=access-enable host timeout 10
 AAA/AUTHOR/EXEC(00000009): Authorization successful
```

使用RADIUS

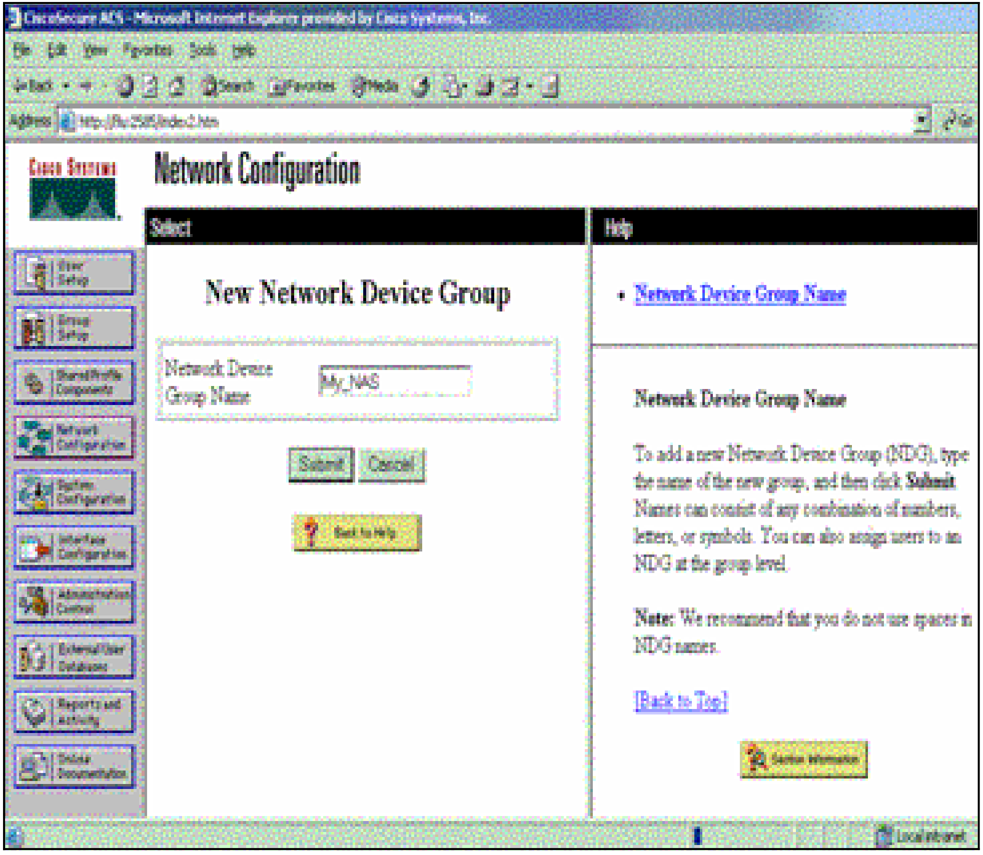
設定RADIUS

若要使用RADIUS，請設定RADIUS伺服器，以強制在RADIUS伺服器上完成驗證，並將授權引數(autocommand)以廠商專屬屬性26向下傳送，如下所示：

```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

完成以下步驟，在適用於Windows的Cisco Secure ACS上配置RADIUS:

1. 開啟Web瀏覽器並輸入ACS伺服器的地址，格式為**http://*<IP_address or DNS_name>***:2002。（此示例使用預設埠2002。）以管理員身份登入。
2. 按一下「**Network Configuration**」。按一下**Add Entry**以建立包含NAS的網路裝置組。輸入組的名稱，然後按一下**Submit**。



New Network Device Group

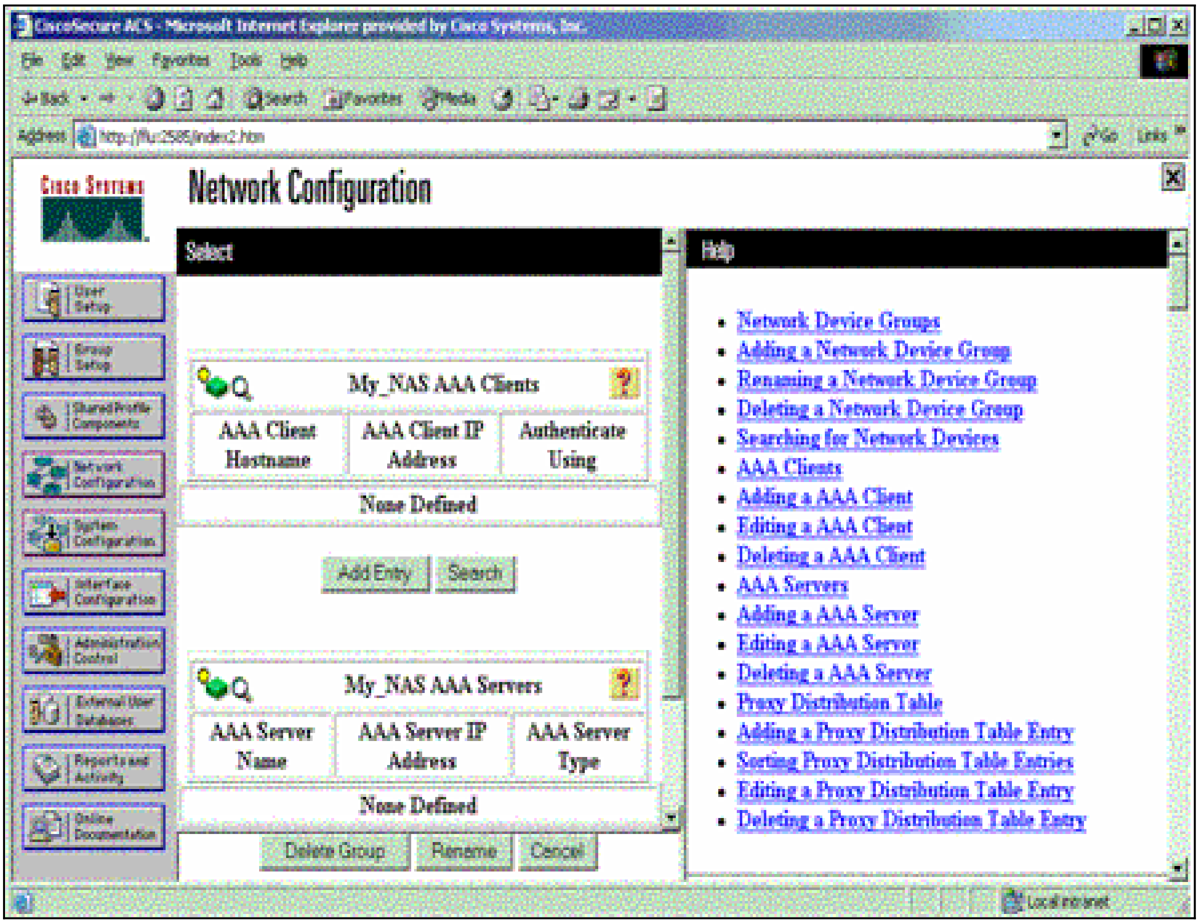
Network Device Group Name: My_NAS

Network Device Group Name

To add a new Network Device Group (NDG), type the name of the new group, and then click **Submit**. Names can consist of any combination of numbers, letters, or symbols. You can also assign users to an NDG at the group level.

Note: We recommend that you do not use spaces in NDG names.

3. 按一下**Add Entry**新增AAA客戶端(NAS)。



Network Configuration

My_NAS AAA Clients

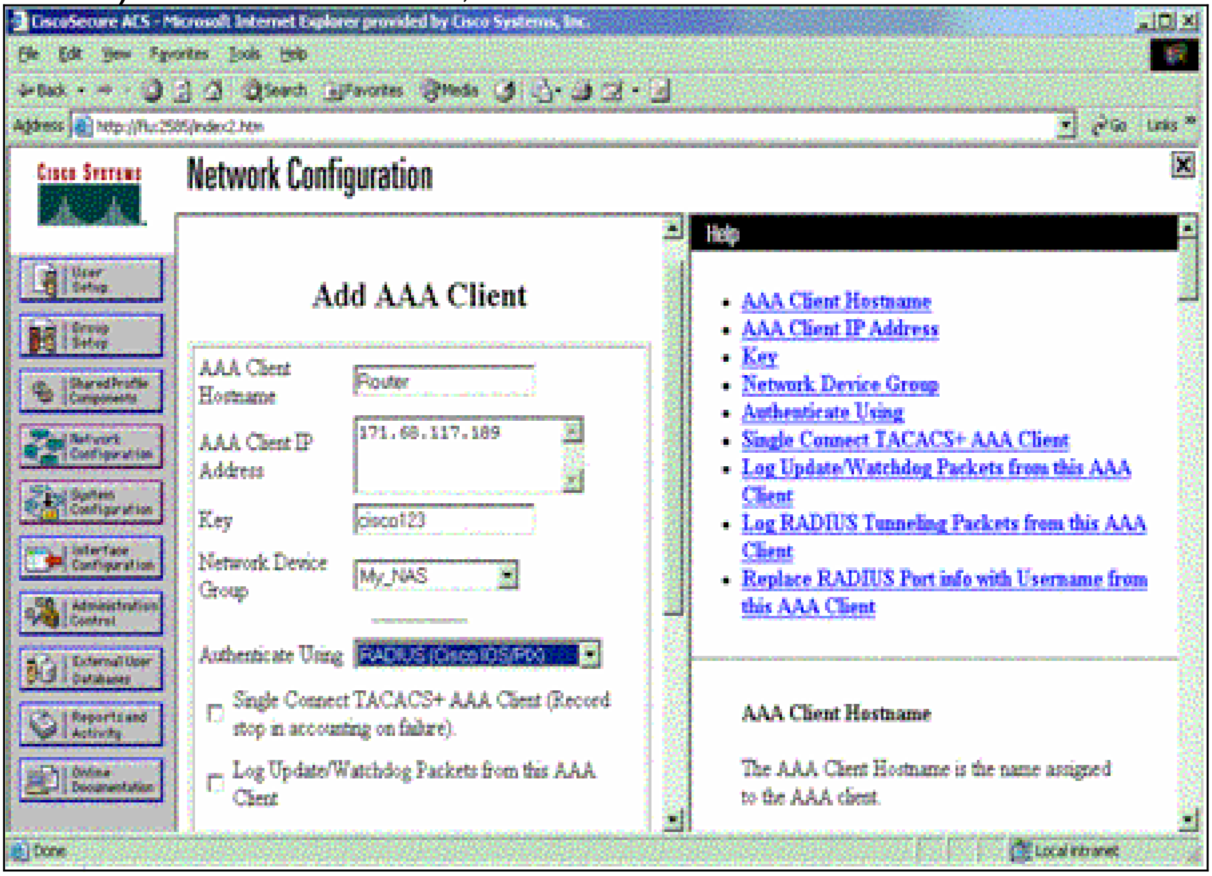
AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

My_NAS AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
None Defined		

- Network Device Groups
- Adding a Network Device Group
- Renaming a Network Device Group
- Deleting a Network Device Group
- Searching for Network Devices
- AAA Clients
- Adding a AAA Client
- Editing a AAA Client
- Deleting a AAA Client
- AAA Servers
- Adding a AAA Server
- Editing a AAA Server
- Deleting a AAA Server
- Proxy Distribution Table
- Adding a Proxy Distribution Table Entry
- Sorting Proxy Distribution Table Entries
- Editing a Proxy Distribution Table Entry
- Deleting a Proxy Distribution Table Entry

4. 輸入用於加密AAA伺服器和NAS之間通訊的主機名、IP地址和金鑰。選擇**RADIUS(Cisco IOS/PIX)**作為驗證方法。完成後，按一下**Submit +Restart**應用更改。



Network Configuration

Add AAA Client

AAA Client Hostname: Router

AAA Client IP Address: 171.68.117.189

Key: cisco123

Network Device Group: My_NAS

Authenticate Using: RADIUS (Cisco IOS/PIX)

□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

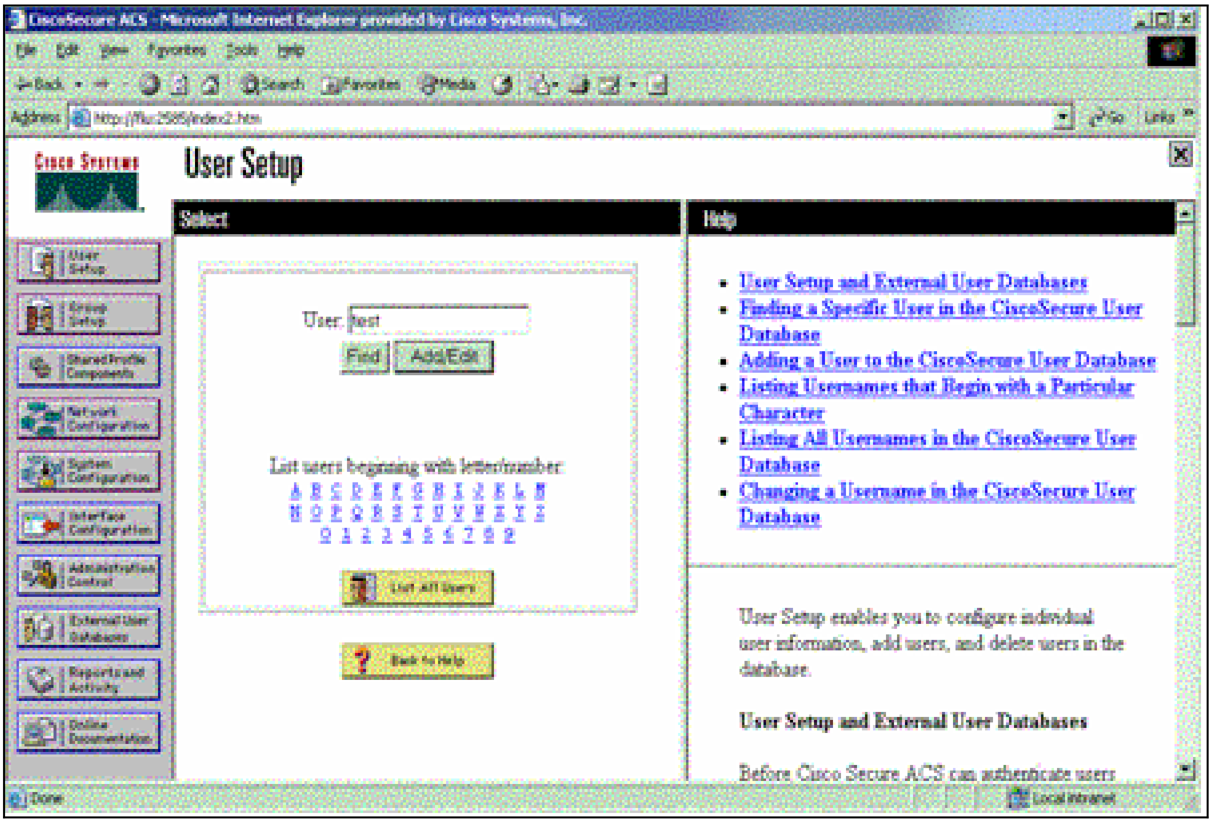
□ Log Update/Watchdog Packets from this AAA Client

- AAA Client Hostname
- AAA Client IP Address
- Key
- Network Device Group
- Authenticate Using
- Single Connect TACACS+ AAA Client
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

AAA Client Hostname

The AAA Client Hostname is the name assigned to the AAA client.

5. 按一下**User Setup**，輸入使用者ID，然後按一下**Add/Edit**。



User Setup

Select

User: test

List users beginning with letter/number:
A B C D E F G H I J K L M
N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9

Help

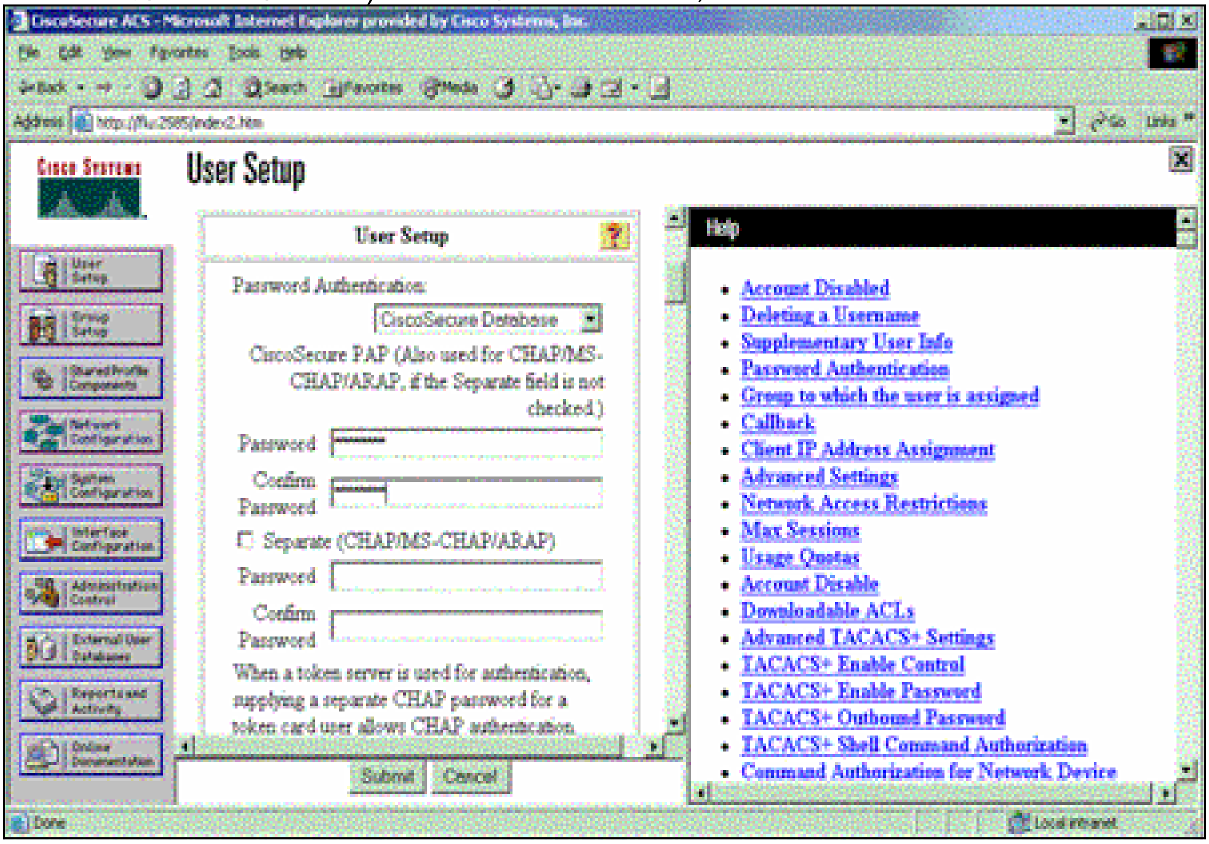
- User Setup and External User Databases
- Finding a Specific User in the CiscoSecure User Database
- Adding a User to the CiscoSecure User Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the CiscoSecure User Database
- Changing a Username in the CiscoSecure User Database

User Setup enables you to configure individual user information, add users, and delete users in the database.

User Setup and External User Databases

Before Cisco Secure ACS can authenticate users

6. 選擇一個資料庫以對使用者進行身份驗證。（在本示例中，使用者是「test」使用者，ACS的內部資料庫用於身份驗證）。 輸入使用者的密碼，並確認密碼。



User Setup

User Setup

Password Authentication:

CiscoSecure Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password ********

Confirm Password ********

□ Separate (CHAP/MS-CHAP/ARAP)

Password

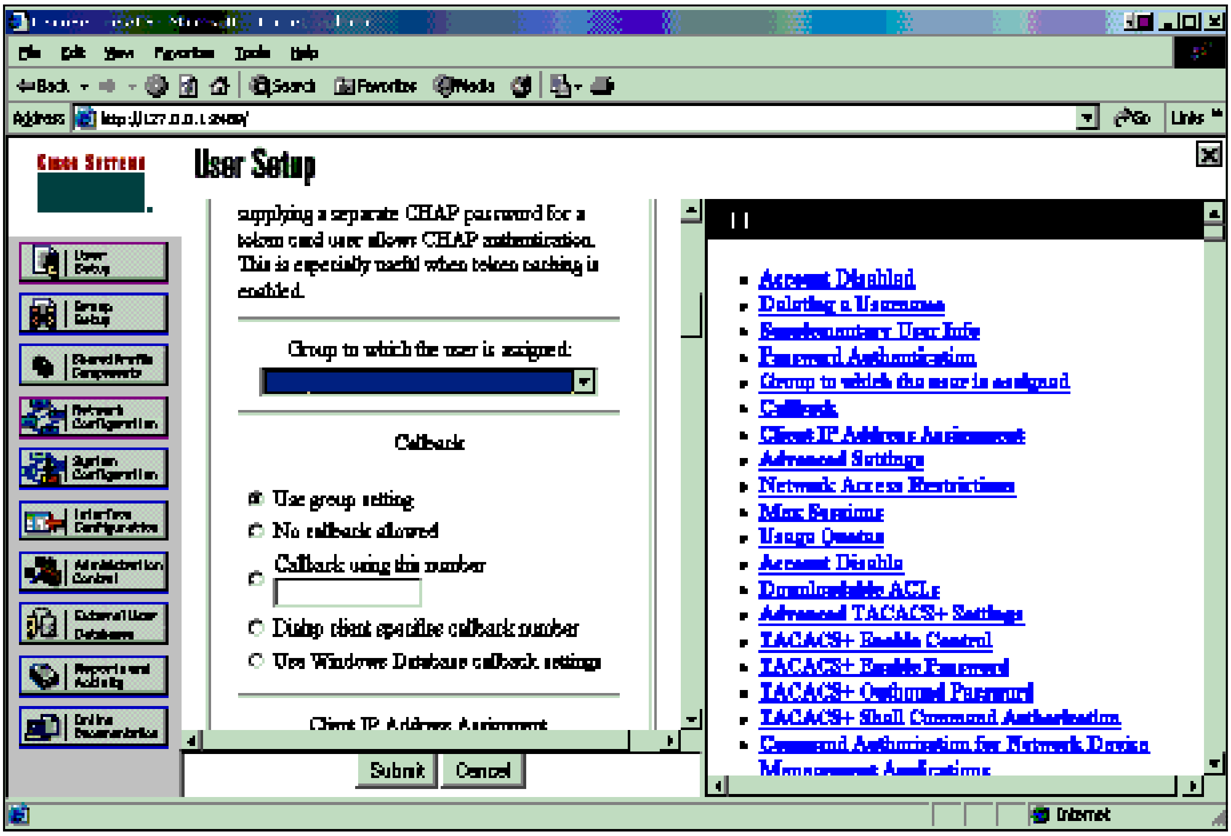
Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication.

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device

7. 選擇使用者分配到的組，並選中**使用組設定**。按一下「**Submit**」。



supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

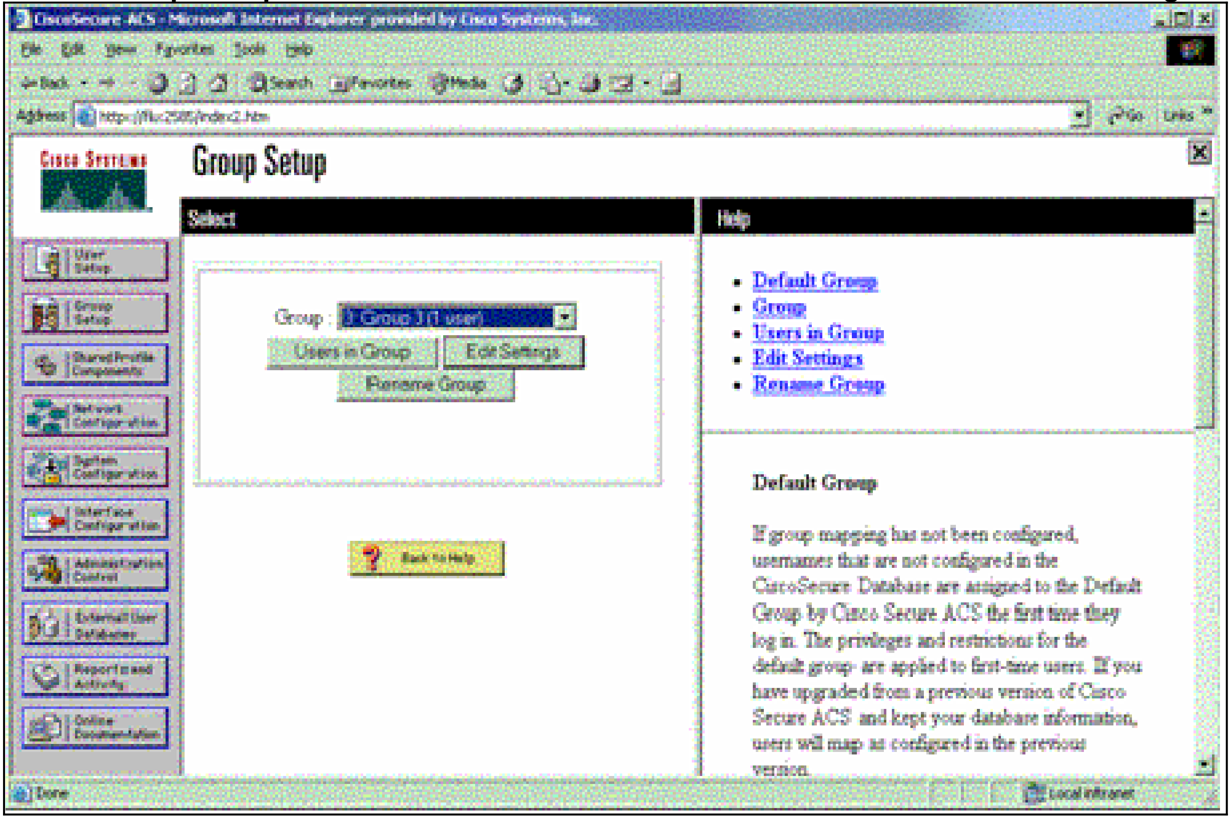
Callback

● Use group setting
○ No callback allowed
○ Callback using this number
○ Dialup client specifies callback number
○ Use Windows Database callback settings

Client IP Address Assignment

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications

8. 按一下Group Setup，然後選擇在上一步中分配給使用者的組。按一下「Edit Settings」。



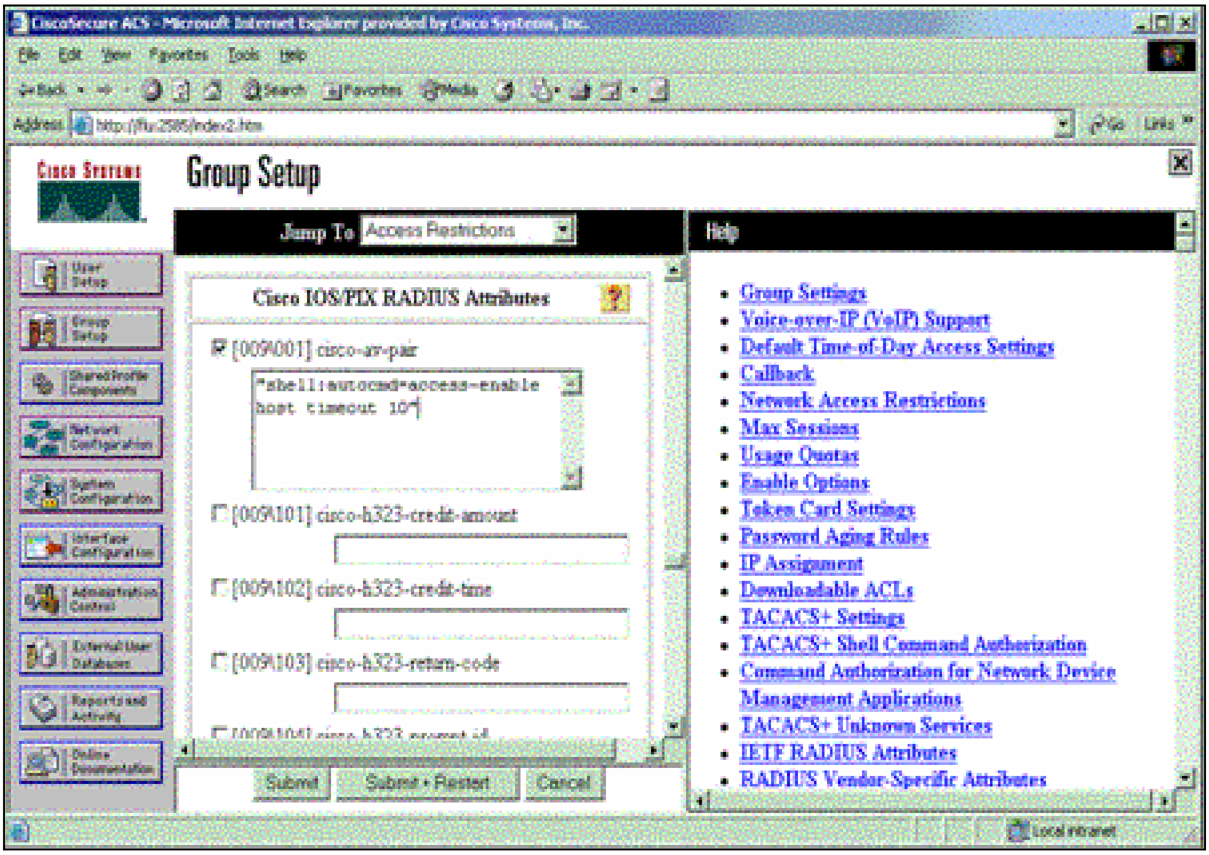
Group : 1: Group 1 (1 user)

- Default Group
- Group
- Users in Group
- Edit Settings
- Rename Group

Default Group

If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version.

9. 向下滾動到Cisco IOS/PIX RADIUS屬性部分。選中**cisco-av-pair**覈取方塊。輸入要在成功授權使用者後執行的**shell**命令。(此示例使用**shell:autocmd=access-enable host timeout 10**。) 按一下**Submit+Restart**。



Group Setup

Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

```
"shell:autocmd=access-enable
host timeout 10"
```

□ [009\101] cisco-h323-credit-amount

□ [009\102] cisco-h323-credit-time

□ [009\103] cisco-h323-return-code

CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://ftu:2585/index2.htm
Go Links
Cisco Systems
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Jump To Access Restrictions
Submit
Submit + Restart
Cancel
Help
Group Settings
Voice-over-IP (VoIP) Support
Default Time-of-Day Access Settings
Callback
Network Access Restrictions
Max Sessions
Usage Quotas
Enable Options
Token Card Settings
Password Aging Rules
IP Assignment
Downloadable ACLs
TACACS+ Settings
TACACS+ Shell Command Authorization
Command Authorization for Network Device Management Applications
TACACS+ Unknown Services
IETF RADIUS Attributes
RADIUS Vendor-Specific Attributes
Local intranet

RADIUS疑難排解

在NAS上使用這些**debug**命令來排除RADIUS問題。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug radius** — 顯示與RADIUS關聯的資訊。

使用以下命令排除AAA故障：

- **debug aaa authentication** — 顯示有關AAA/TACACS+身份驗證的資訊。
- **debug aaa authorization** — 顯示有關AAA/TACACS+授權的資訊。

這裡的**debug**輸出範例顯示為RADIUS設定的ACS上的驗證和授權程式成功。

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=======================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                       [tty]
 RADIUS(00000003): Storing nasport 66 in rad_db
```

```
RADIUS/ENCODE(00000003): dropping service type,
  "radius-server attribute 6 on-for-login-auth" is off
RADIUS(00000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(00000003): acct_session_id: 1
RADIUS(00000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
  BE B5 07 BD E9 05 5B 5D
RADIUS:  User-Name           [1]   7   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port            [5]   6   66
RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
  Access-Accept, len 93
RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
  68 4B C3 FC 25 21 47 CD
RADIUS:  Vendor, Cisco       [26]  51
RADIUS:   Cisco AVpair       [1]   45
  "shell:autocmd=access-enable host timeout 10"
RADIUS:  Class               [25]  22
RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
RADIUS:   31 2F 36 36                 [1/66]
RADIUS(00000003): Received from id 21645/1
AAA/AUTHOR/EXEC(00000003): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

相關資訊

- Cisco IOS鎖定與金鑰型安全
- TACACS/TACACS+ 支援頁面
- IOS 文件中的 TACACS+
- RADIUS 支援頁面
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems