锁和钥匙动态访问列表

目录

简介

“锁和密匙”访问允许设置动态访问列表，通过用户身份验证进程为每个用户授予访问特定源主机/目的地主机的权限。在不会对安全限制造成任何损害的情况下，将会动态地允许用户透过 Cisco IOS® 防火墙进行访问。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备创建的。在本例中，实验室环境包括一个运行 Cisco IOS® 软件版本 12.3(1) 的 2620 路由器。 本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

欺骗注意事项

锁和密钥访问允许外部事件在 Cisco IOS 防火墙中放置一个开口。在此开口存在之后，路由器容易遭受源地址欺骗。为了防止发生这种情况，请使用带身份验证或加密的 IP 加密来提供加密支持。

欺骗是所有现有访问列表都存在的一个问题。锁和密钥访问不能解决此问题。

由于锁和密钥访问引入了通过网络防火墙的潜在路径，因此，您需要考虑动态访问。欺骗您的身份验证地址的另一个主机会在防火墙的后面获得访问权限。采用动态访问时，一个欺骗您的身份验证地址的未授权主机可能会在防火墙的后面获得访问权限。锁和密钥访问不会导致这种地址欺骗问题。在这里，该问题仅确定为用户需要关心的问题。

性能

在这两种情况下，性能会受到影响。

- 每个动态访问列表都会在硅交换引擎 (SSE) 上强制进行访问列表重建。 这会导致 SSE 交换路径瞬间变慢。
- 动态访问列表需要空闲超时设备（即使超时保留为默认设置）。 因此，动态访问列表不能进行 SSE 交换。将在协议快速交换路径中对这些条目进行处理。

注意边界路由器配置。远程用户会在边界路由器上创建访问列表条目。访问列表会动态扩展和收缩。在空闲超时或最大超时时间段过后，将从列表中动态删除条目。大型访问列表会降低数据包交换性能。

何时使用锁和密钥访问

下面列出了使用锁和密钥访问时的两个示例：

- 当您希望远程主机能够通过 Internet 访问互联网络中的主机时。锁和密钥访问会基于单个主机或网络来限制越过防火墙的访问。
- 当您希望网络上的一部分主机访问受防火墙保护的远程网络上的主机时。通过锁和密钥访问，您可以仅启用所需的一组主机，以便通过让它们通过 TACACS+ 或 RADIUS 服务器进行身份验证来获取访问权限。

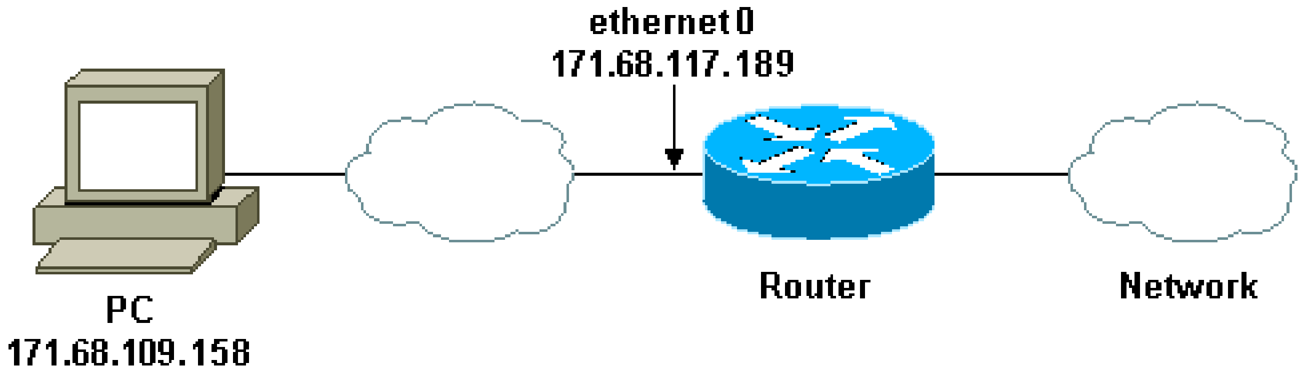
锁和密钥访问操作

下面的过程描述了锁和密钥访问操作。

1. 用户打开与针对锁和密钥访问而配置的边界路由器之间的 Telnet 会话。
2. Cisco IOS 软件接收 Telnet 数据包。该软件执行用户身份验证过程。在能够进行访问之前，用户必须通过身份验证。身份验证过程是由路由器或中央接入服务器（如 TACACS+ 或 RADIUS 服务器）完成的。

示例配置和故障排除

网络图



Cisco 建议您使用 TACACS+ 服务器来完成身份验证查询过程。TACACS+ 提供身份验证、授权和记帐服务。它还提供协议支持、协议规范和集中式安全数据库。

您可以在路由器上或使用 TACACS+ 或 RADIUS 服务器对用户进行身份验证。

注意： 除非另有说明，否则这些命令是全局命令。

在路由器上，对于要进行本地身份验证的用户，您需要一个 **username。**

```
username test password test
```

vty 行上存在 **login local 会导致使用此用户名。**

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

如果您不信任用户发出 **access-enable 命令，则可以执行以下两个操作之一：**

- 基于每个用户将超时与用户进行关联。

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

  或
- 强制所有远程登录的用户具有相同超时。

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

注意：语**法**中的10是访问列表的空闲超时。它将由动态访问列表中的绝对超时覆盖。

定义在用户（任何用户）登录到路由器中并发出 **access-enable 命令时应用的扩展访问列表。**过滤器中此“开口”的最大绝对时间已设置为 15 分钟。15 分钟后，无论是否有人使用，此开口都会关闭。需要存在名称 **testlist，但它并不十分重要。**通过配置源地址或目标地址来限制用户有权访问的网络（此时该用户不受限制）。

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

定义阻止除能够远程登录路由器（以便打开用户远程登录路由器所需的开口）之外的所有功能所需的访问列表。 此处的 IP 地址是路由器的以太网 IP 地址。

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

末尾处有一个隐式 **deny all 语句（不在此处输入）。**

将此访问列表应用于用户进入的接口。

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

您已完成此过程。

这是该过滤器当前在路由器上呈现的内容：

```
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)
```

访问您的内部网络的用户在远程登录到路由器之前，看不到任何内容。

注意：此**处**的10是 访问列表的空闲超时。它将由动态访问列表中的绝对超时覆盖。

```
%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.
```

该过滤器如下所示。

```
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)
```

基于源 IP 地址，过滤器中有一个用于此用户的开口。当其他人执行此操作时，您会看到*两个开口*。

```
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)
```

这些用户能够从其*源 IP 地址对任何目标 IP 地址进行全面 IP 访问。*

使用 TACACS+

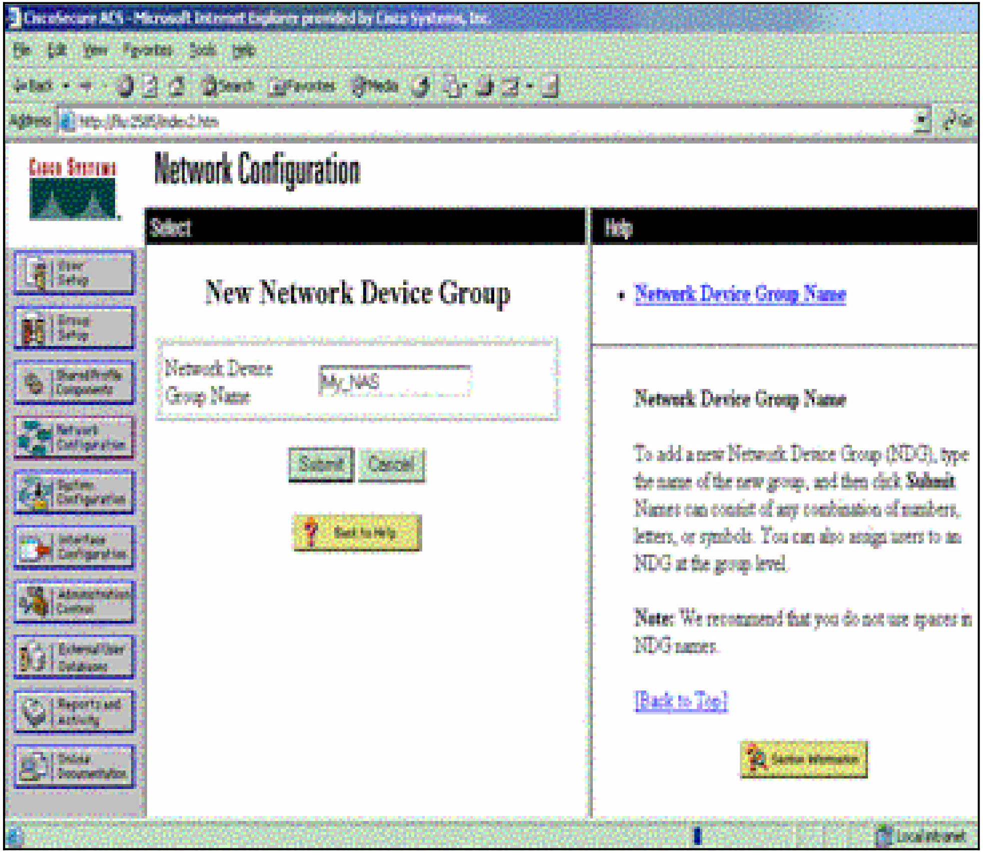
配置 TACACS+

配置 TACACS+ 服务器以强制在 TACACS+ 服务器上进行身份验证和授权，以便使用 TACACS+，如以下输出所示：

```
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
```

完成以下步骤以在 Cisco Secure ACS for Windows 上配置 TACACS+：

1. 打开 Web 浏览器。输入ACS服务器的地址，格式为**http:// *<IP_address or DNS_name>*:2002**。（本示例使用默认端口2002。）以管理员身份登录。
2. 单击 **Network Configuration**。单击 **Add Entry 以创建一个包含网络接入服务器 (NAS) 的网络设备组。** 为该组输入名称，然后单击 **Submit**。



Network Device Group Name: My_NAS

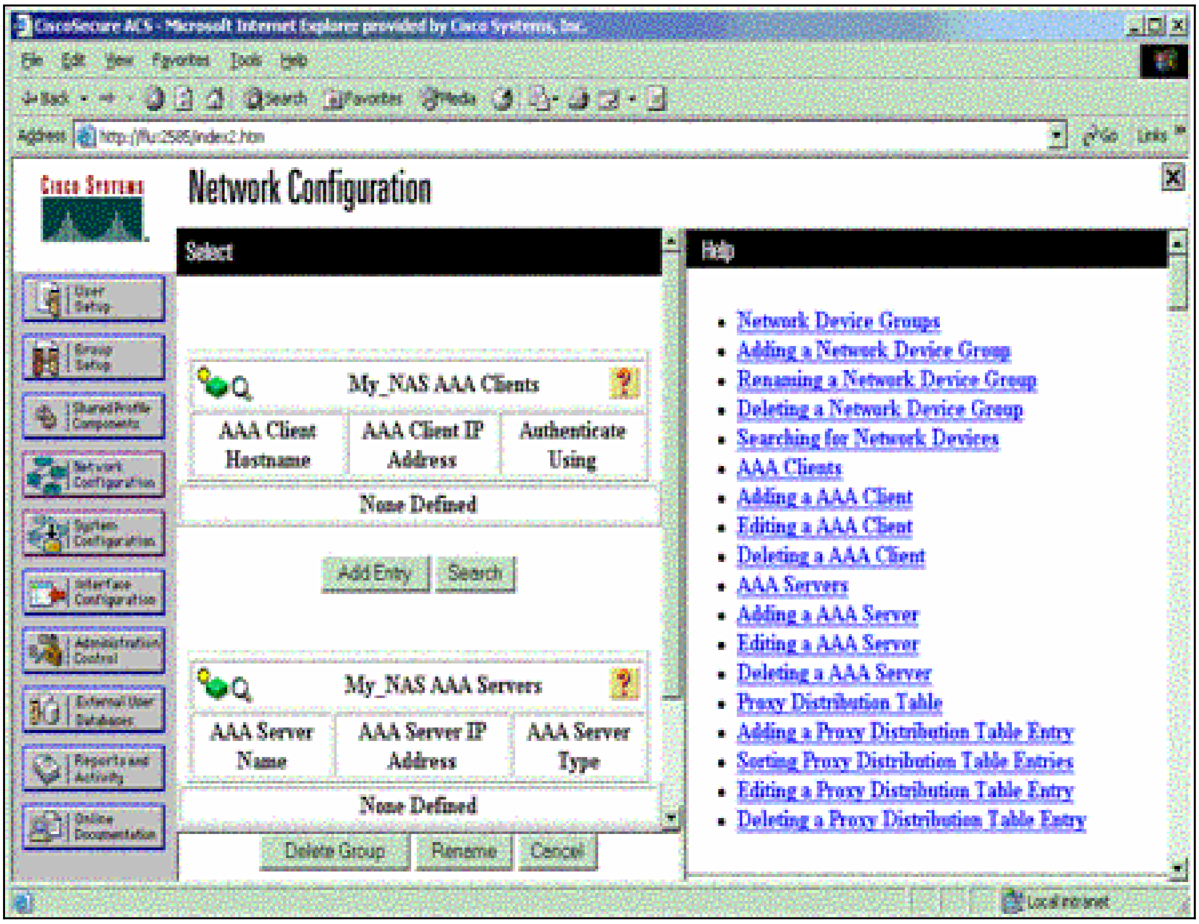
- Network Device Group Name

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.

3. 单击 **Add Entry 以添加身份验证、授权和记帐 (AAA) 客户端 (NAS)。**



Network Configuration

Select

My_NAS AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

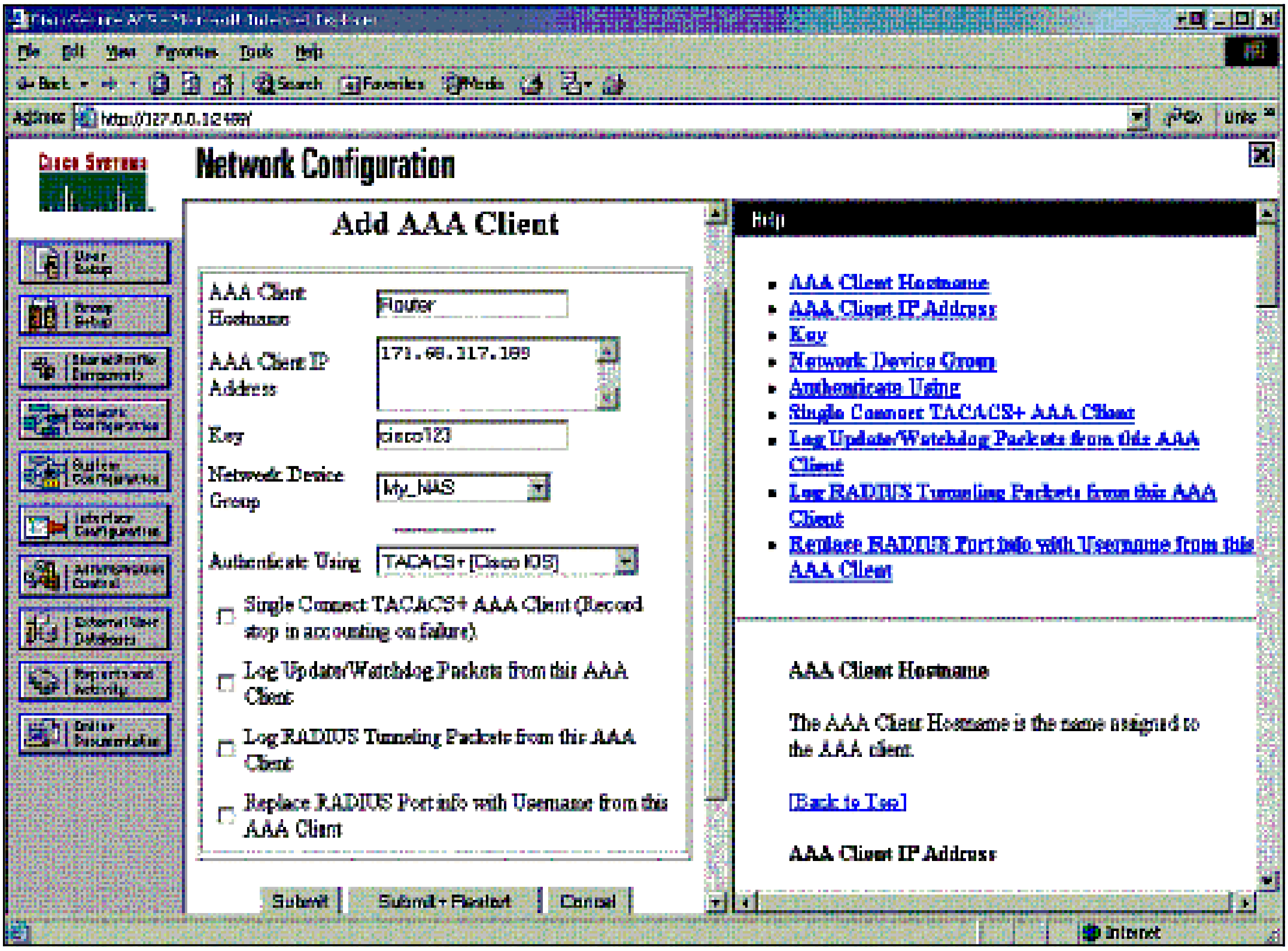
My_NAS AAA Servers

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

Help

- 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. 输入主机名、IP 地址以及用于对 AAA 服务器与 NAS 之间的通信进行加密的密钥。选择 **TACACS+ (Cisco IOS) 作为身份验证方法。**完成后，单击 **Submit + Restart 应用所做的更改**。



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

Help

- 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

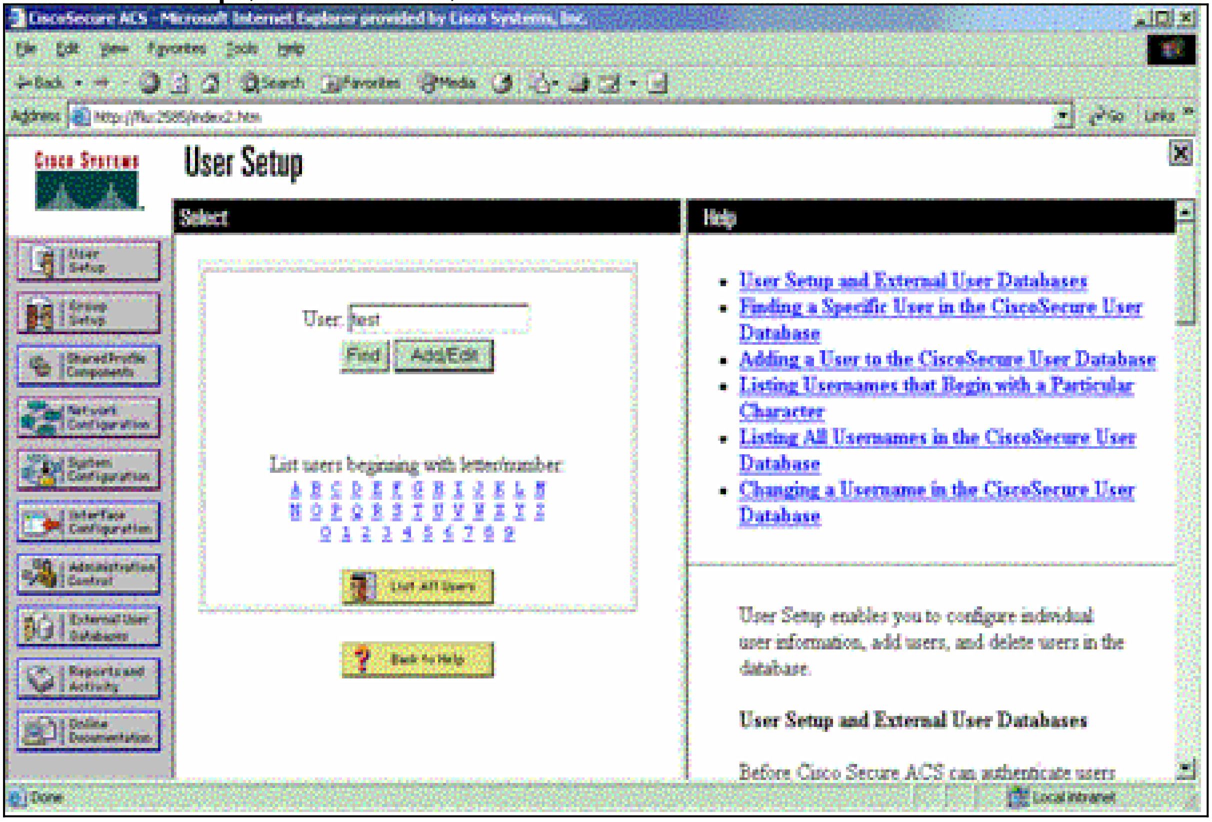
AAA Client Hostname

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

[Back to Top]

AAA Client IP Address

5. 单击 **User Setup**，输入用户 ID，然后单击 **Add/Edit**。


CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://fu:2585/index2.htm
Go Links
User Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Done
Local intranet

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

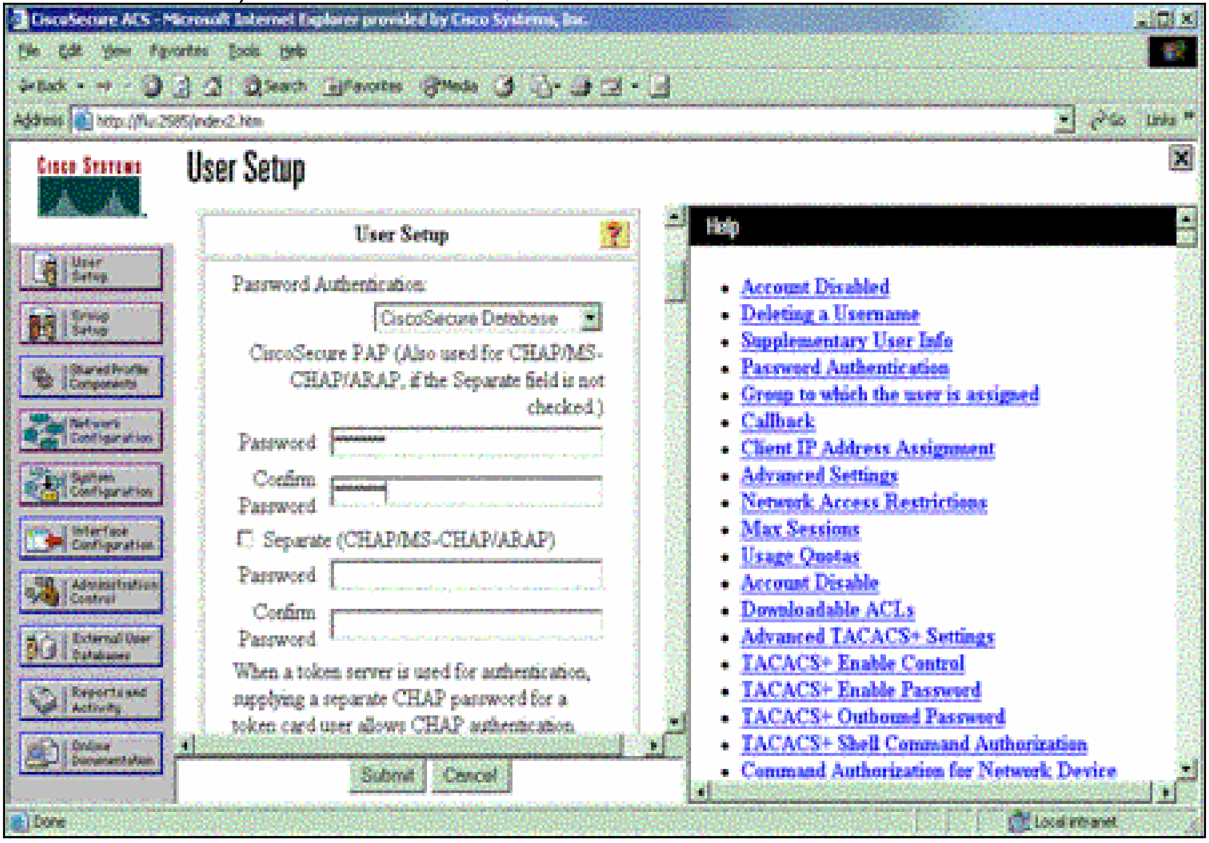
- User Setup and External User Databases
- Finding a Specific User in the CiscoSecure User Database
- Adding a User to the CiscoSecure User Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the CiscoSecure User Database
- Changing a Username in the CiscoSecure 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. 选择用于对用户进行身份验证的数据库。（在此示例中，用户为“test”，并将 ACS 的内部数据库用于身份验证）。 输入用户密码，并确认该密码。


CiscoSecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc.
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://fu:2585/index2.htm
Go Links
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Done
Local intranet

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

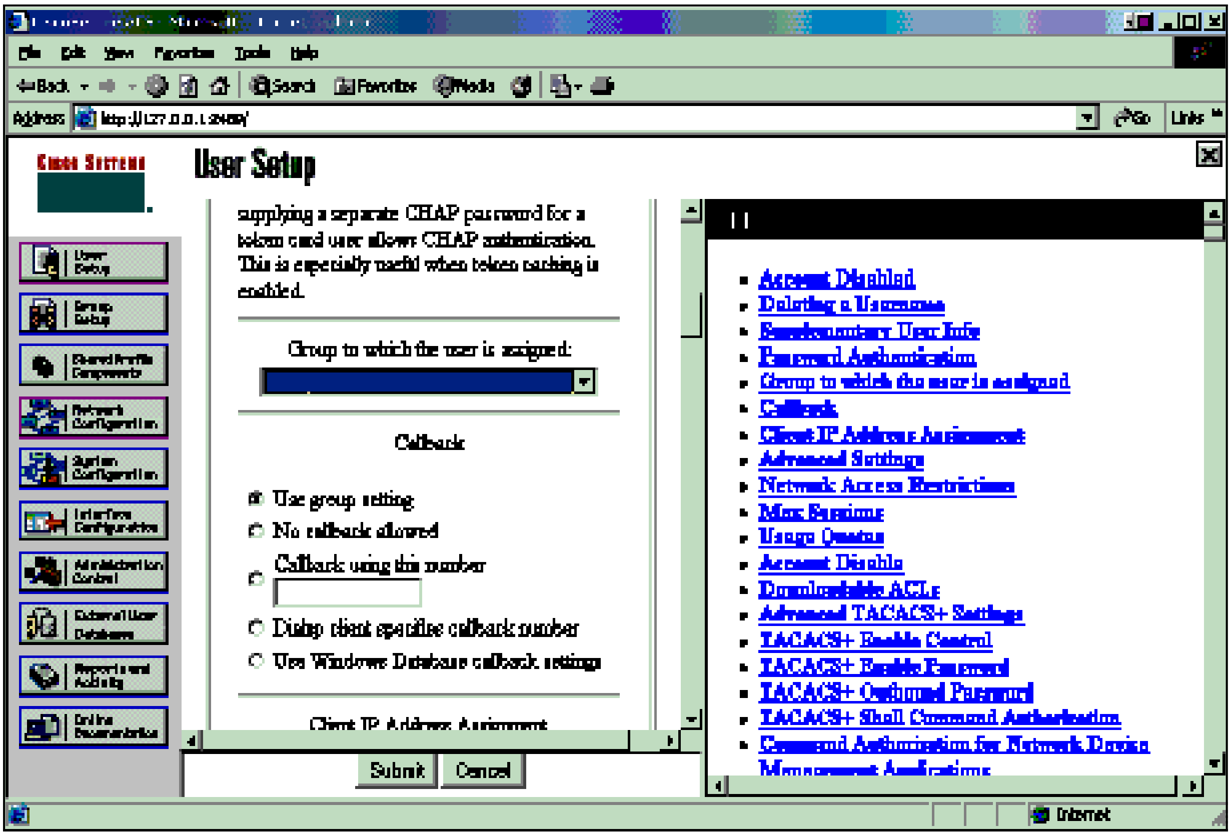
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication.

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. 选择将用户分配到的组，然后选中 **Use group setting**。单击“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:

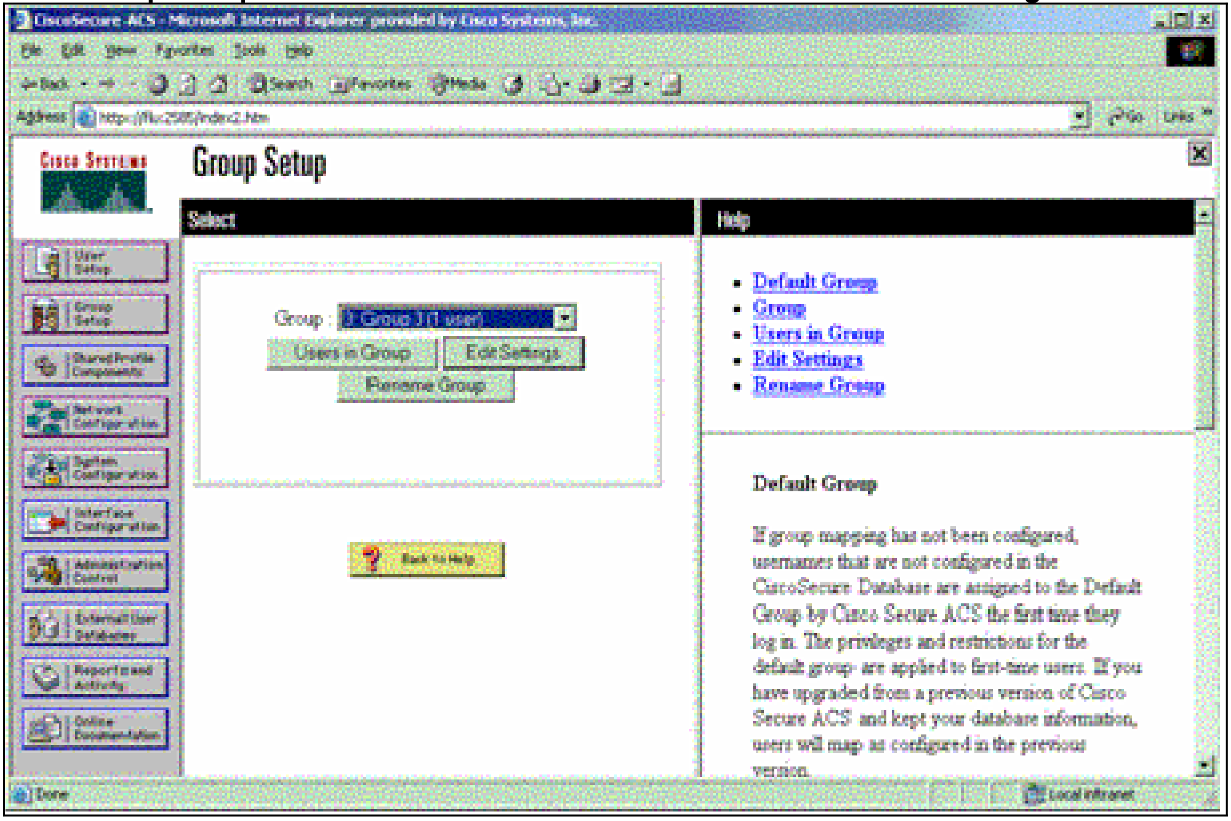
Callback

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

Client IP Address Assignment

- 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. 单击 Group Setup。选择在步骤 7 中将用户分配到的组。单击 Edit Settings。



Group Setup

Select

Group : 1: Group 1 (1 user)

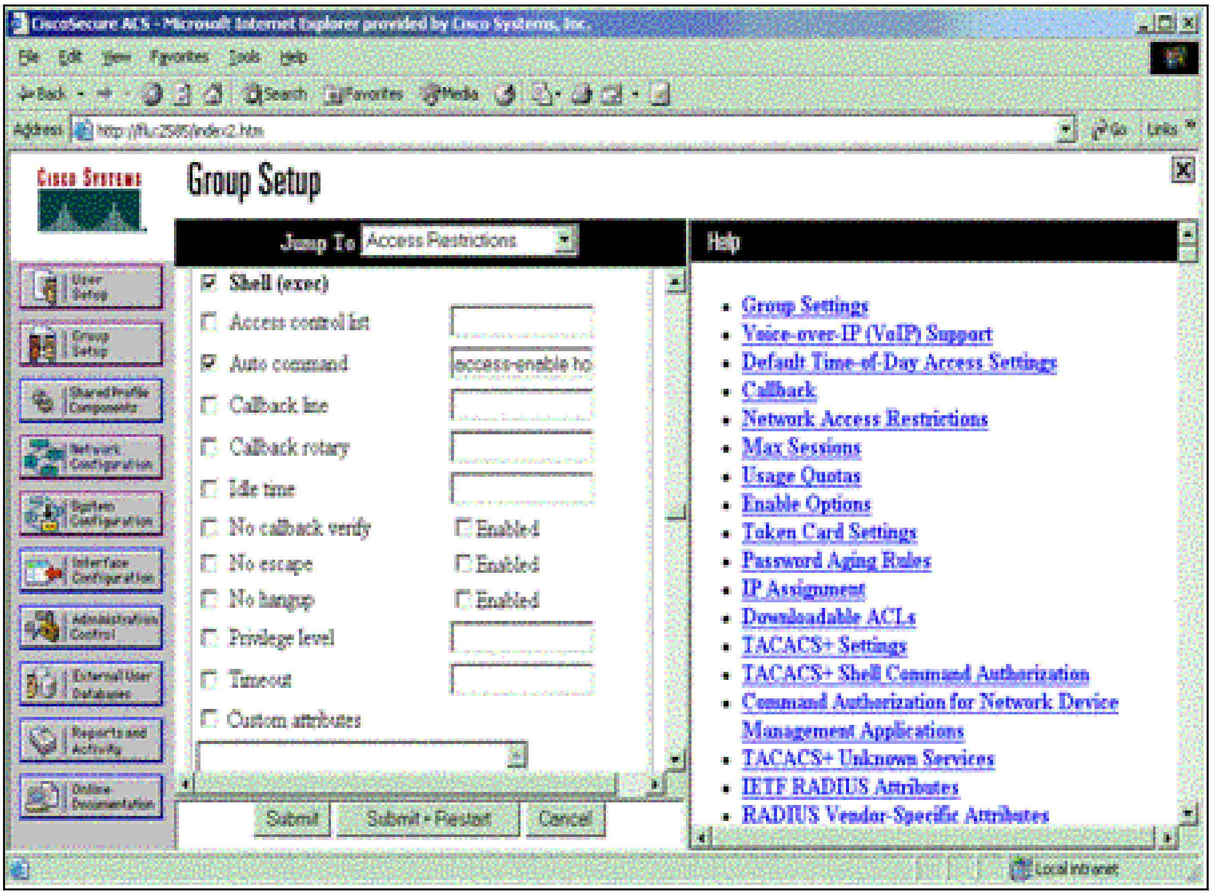
Help

- 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. 向下滚动到 TACACS+ Settings 部分。选中 Shell exec 所对应的框。选中 Auto command 所对应的框。输入在对用户成功进行身份验证时要执行的自动命令。（此示例使用 access-enable host timeout 10 命令。）单击 Submit+ Restart。



Group Setup

Jump To Access Restrictions

☑ 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

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

TACACS+ 故障排除

在 NAS 上使用以下 **debug 命令对 TACACS+ 问题进行故障排除。**

注意：在使用debug命令之前，请参阅有关Debug命令**的**重要信息。

- **debug tacacs authentication — 显示有关 TACACS+ 身份验证过程的信息。**仅在某些软件版本中提供。如果未提供，请仅使用 **debug tacacs。**
- **debug tacacs authorization — 显示有关 TACACS+ 身份验证过程的信息。**仅在某些软件版本中提供。如果未提供，请仅使用 **debug tacacs。**
- **debug tacacs events — 显示来自 TACACS+ 帮助程序进程的信息。**仅在某些软件版本中提供。如果未提供，请仅使用 **debug tacacs。**

使用以下命令对 AAA 问题进行故障排除：

- **debug aaa authentication — 显示有关 AAA/TACACS+ 身份验证的信息。**
- **debug aaa authorization - 显示有关 AAA/TACACS+ 授权的信息。**

此处的示例 debug 输出显示了 ACS TACACS+ 服务器上的成功身份验证和授权过程。

```
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

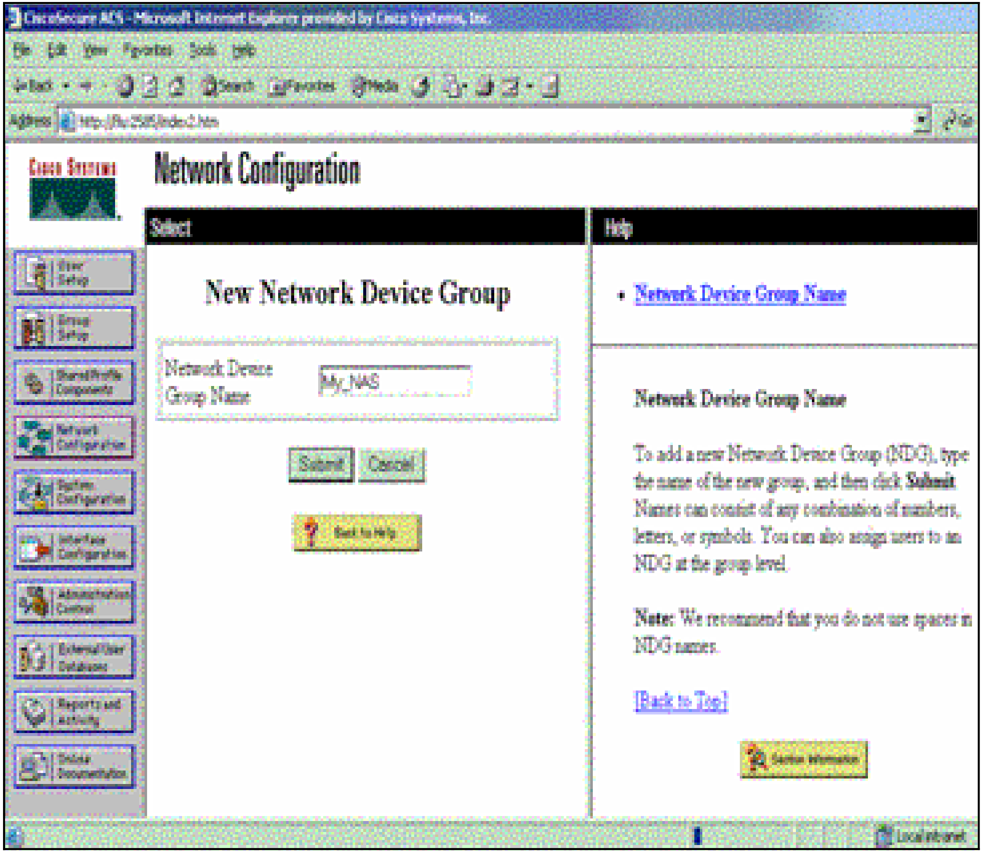
配置 RADIUS

为了使用 RADIUS，可将 RADIUS 服务器配置为强制在 RADIUS 服务器上进行身份验证，并在供应商特定属性 26 中向下发送授权参数（自动命令），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
```

完成以下步骤以在 Cisco Secure ACS for Windows 上配置 RADIUS：

1. 打开Web浏览器并输入ACS服务器的地址，格式为**http://*<IP_address or DNS_name>*:2002**。（本示例使用默认端口2002。）以管理员身份登录。
2. 单击 **Network Configuration**。单击 **Add Entry 以创建一个包含 NAS 的网络设备组。**为该组输入名称，然后单击 **Submit**。



New Network Device Group

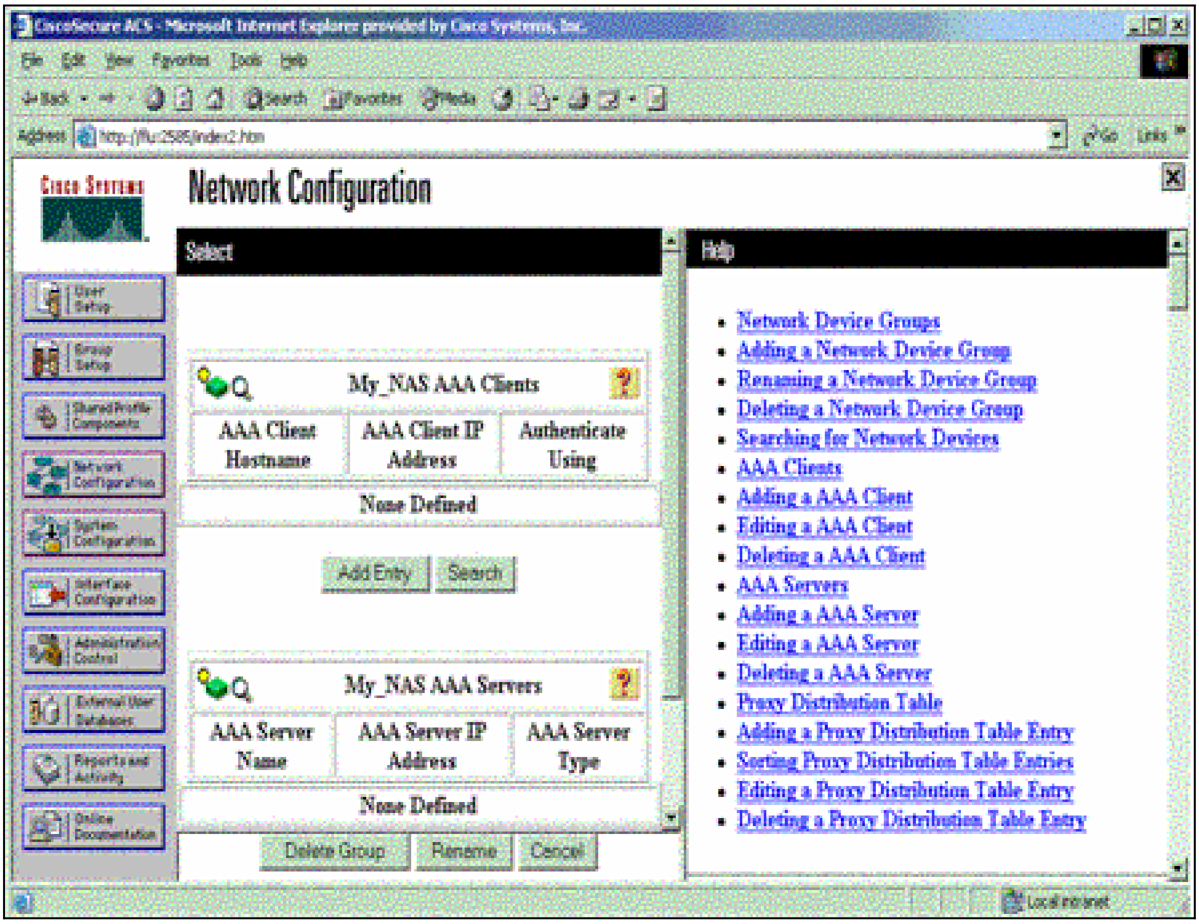
Network Device Group Name: My_NAS

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. 单击 **Add Entry 以添加 AAA 客户端 (NAS)。**



Network Configuration

Select

My_NAS AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry　Search

My_NAS AAA Servers

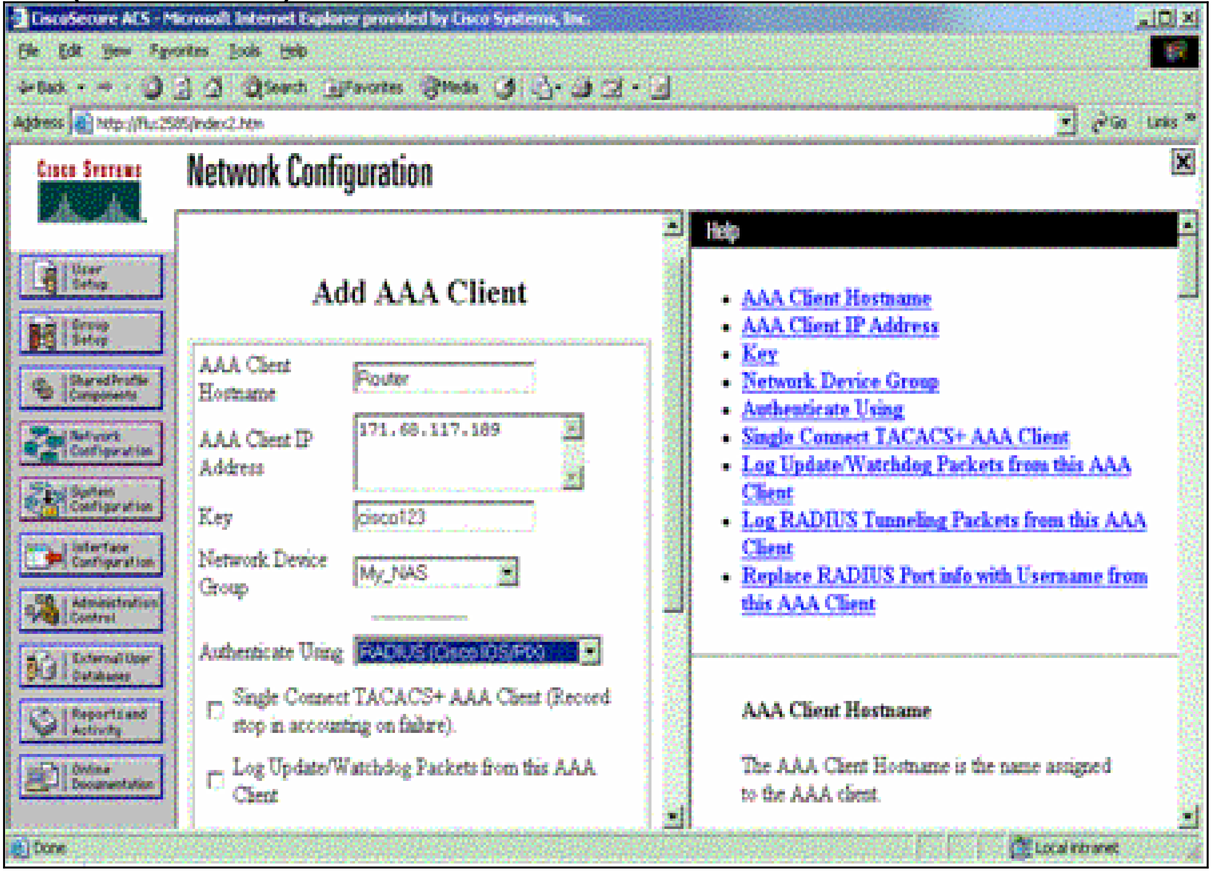
AAA Server Name	AAA Server IP Address	AAA Server Type
None Defined		

Delete Group　Rename　Cancel

Help

- 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. 输入主机名、IP 地址以及用于对 AAA 服务器与 NAS 之间的通信进行加密的密钥。选择 **RADIUS (Cisco IOS/PIX) 作为身份验证方法。**完成后，单击 **Submit + Restart 应用所做的更改。**



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

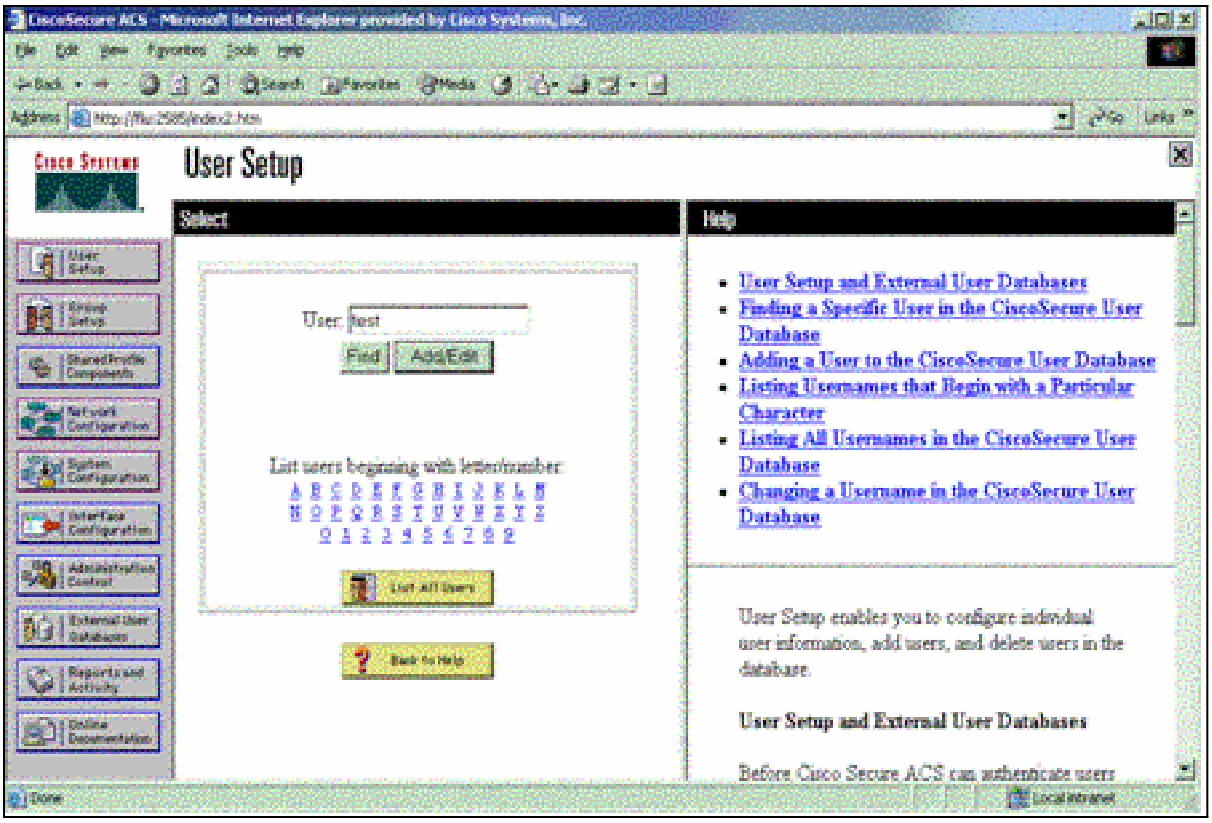
Help

- 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. 单击 **User Setup**，输入用户 ID，然后单击 **Add/Edit**。



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

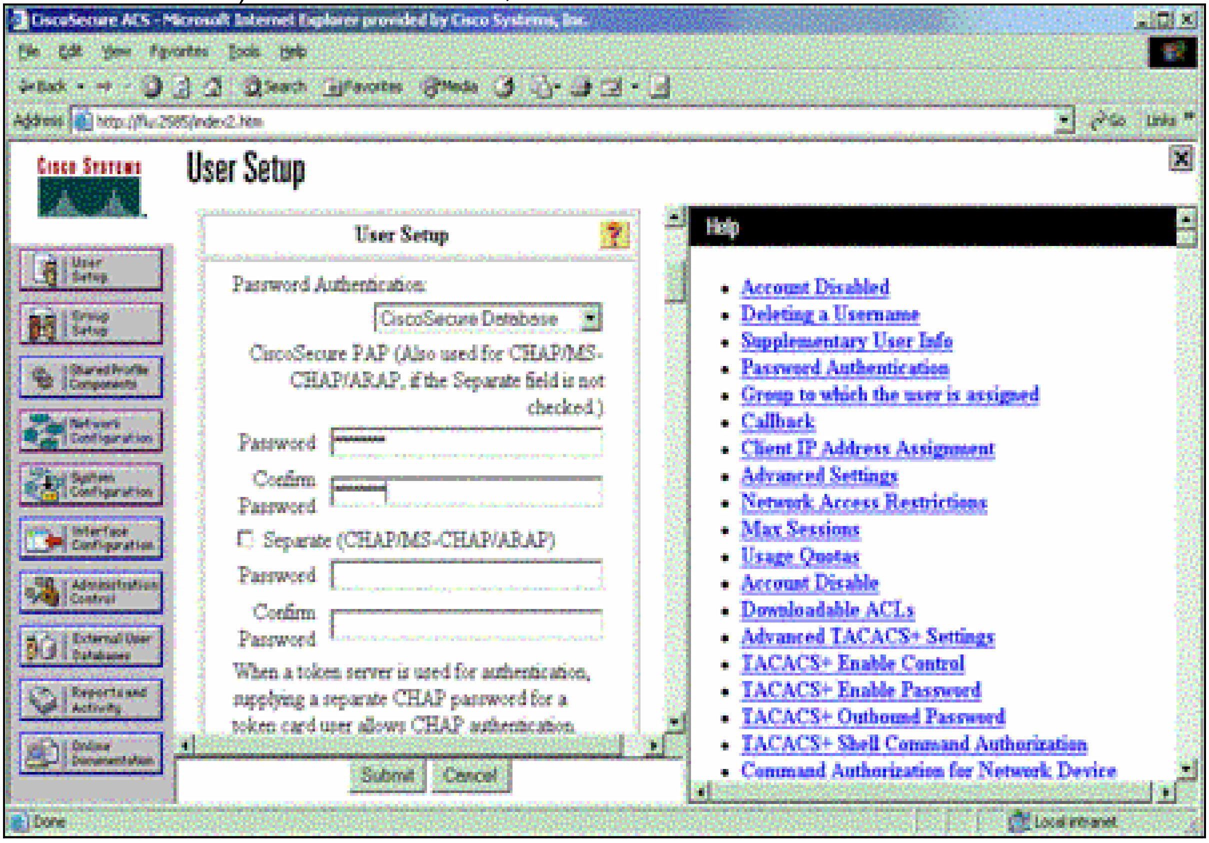
- User Setup and External User Databases
- Finding a Specific User in the CiscoSecure User Database
- Adding a User to the CiscoSecure User Database
- Listing Usernames that Begin with a Particular Character
- Listing All Usernames in the CiscoSecure User Database
- Changing a Username in the CiscoSecure 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. 选择用于对用户进行身份验证的数据库。（在此示例中，用户为“test”，并将 ACS 的内部数据库用于身份验证）。 输入用户密码，并确认该密码。



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)

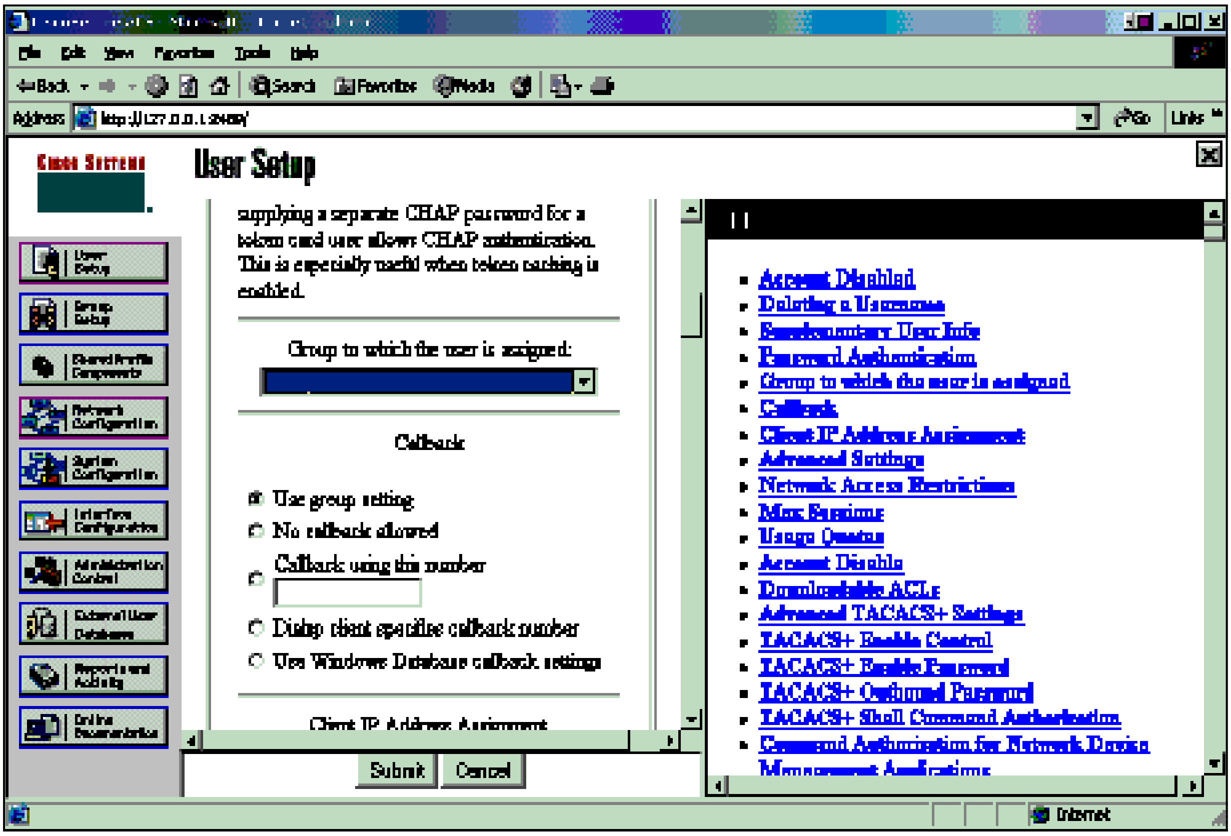
Password

Confirm Password

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

- 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. 选择将用户分配到的组，然后选中 **Use group setting**。单击“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:

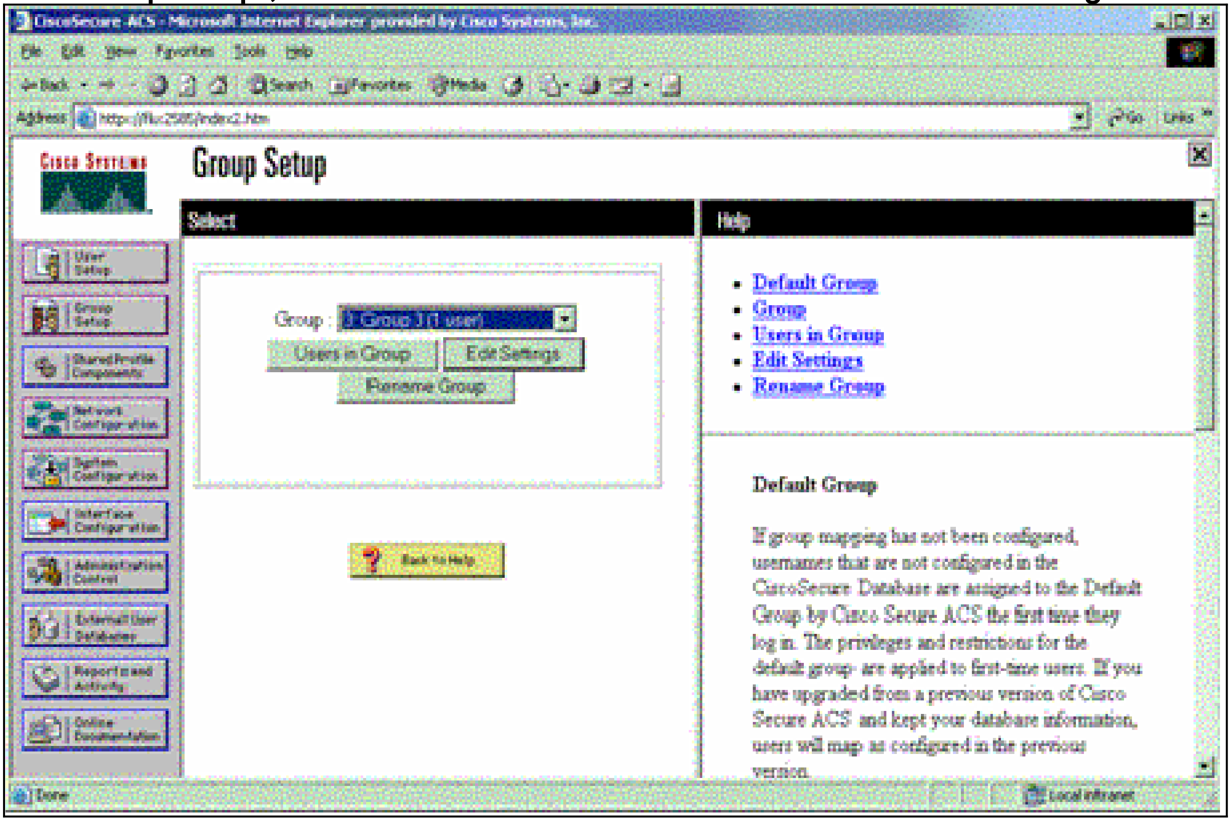
Callback

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

Client IP Address Assignment

- 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. 单击 **Group Setup，然后选择在上一步中将用户分配到的组。**单击 **Edit Settings。**



Group Setup

Select

Group : 1 Group 1 (1 user)

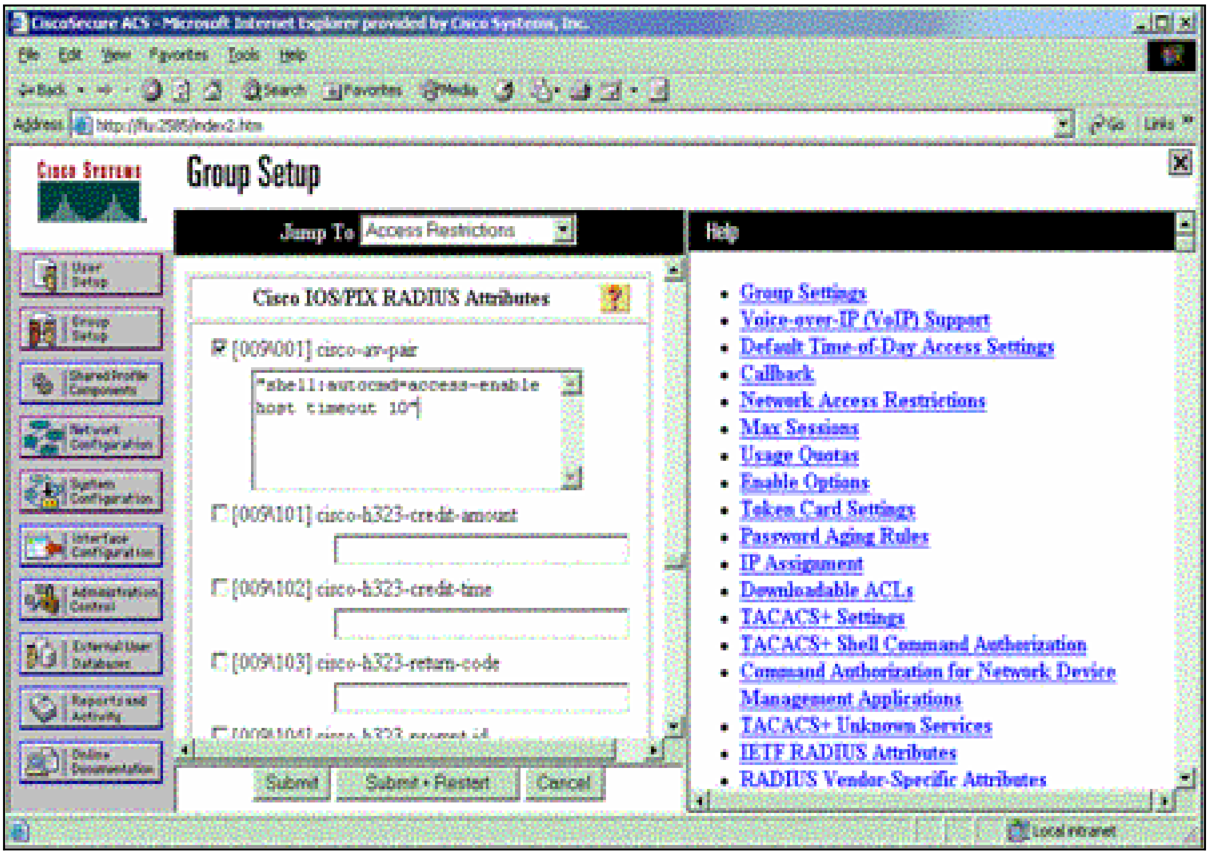
Help

- 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. 向下滚动到 Cisco IOS/PIX RADIUS Attributes 部分。选中 **cisco-av-pair** 所对应的框。输入在对用户成功进行身份验证时要执行的 **shell 命令。**(本示例使用**shell:autocmd=access-enable host timeout 10。**) 单击 **Submit+ Restart。**



Group Setup

Jump To Access Restrictions

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

☐ [009\104] cisco-h323-prompt-id

RADIUS 故障排除

在 NAS 上使用以下 **debug 命令对 RADIUS 问题进行故障排除。**

注意：在使用debug命令之前，请参阅有关Debug命令**的**重要信息。

- **debug radius -显示信息与RADIUS相关。**

使用以下命令对 AAA 问题进行故障排除：

- **debug aaa authentication — 显示有关 AAA/TACACS+ 身份验证的信息。**
- **debug aaa authorization - 显示有关 AAA/TACACS+ 授权的信息。**

此处的示例 debug 输出显示了为 RADIUS 配置的 ACS 上的成功身份验证和授权过程。

```
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
```

相关信息

- Cisco IOS 锁和密钥安全
- TACACS/TACACS+支持页面
- IOS 文档中的 TACACS+
- RADIUS 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems