

TACACS+ on an Aironet Access Point for Login Authentication Configuration Example

Document ID: 70149

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configure the TACACS+ Server for Login Authentication

Configure the Aironet AP for TACACS+ Authentication

Verify

Troubleshoot

Related Information

Introduction

This document explains how to enable TACACS Plus (TACACS+) services on a Cisco Aironet Access Point (AP) in order to perform login authentication with use of a TACACS+ server.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to configure basic parameters on Aironet APs
- Knowledge of how to configure a TACACS+ server like the Cisco Secure Access Control Server (ACS)
- Knowledge of TACACS+ concepts

For information on how TACACS+ works, refer to the *Understanding TACACS+* section of *Configuring RADIUS and TACACS+ Servers*.

Components Used

The information in this document is based on these software and hardware versions:

- Aironet 1240AG Series AP that runs Cisco IOS® Software Release 12.3(8)JEA
- ACS that runs software version 4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

This section explains how to configure the Aironet AP and the TACACS+ server (ACS) for TACACS+-based login authentication.

This configuration example uses these parameters:

- IP address of the ACS;72.16.1.1/255.255.0.0
- IP address of the AP;72.16.1.30/255.255.0.0
- Shared secret key that is used on the AP and the TACACS+ server **Example**

These are the credentials of the user that this example configures on the ACS:

- Username **User1**
- Password **Cisco**
- Group **AdminUsers**

You need to configure TACACS+ features to validate the users who try to connect to the AP either through the web interface or through the command-line interface (CLI). In order to accomplish this configuration, you must perform these tasks:

1. Configure the TACACS+ server for login authentication.
2. Configure the Aironet AP for TACACS+ authentication.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



Configure the TACACS+ Server for Login Authentication

The first step is to set up a TACACS+ daemon to validate the users who try to access the AP. You must set up the ACS for TACACS+ authentication and create a user database. You can use any TACACS+ server. This example uses the ACS as the TACACS+ server. Complete these steps:

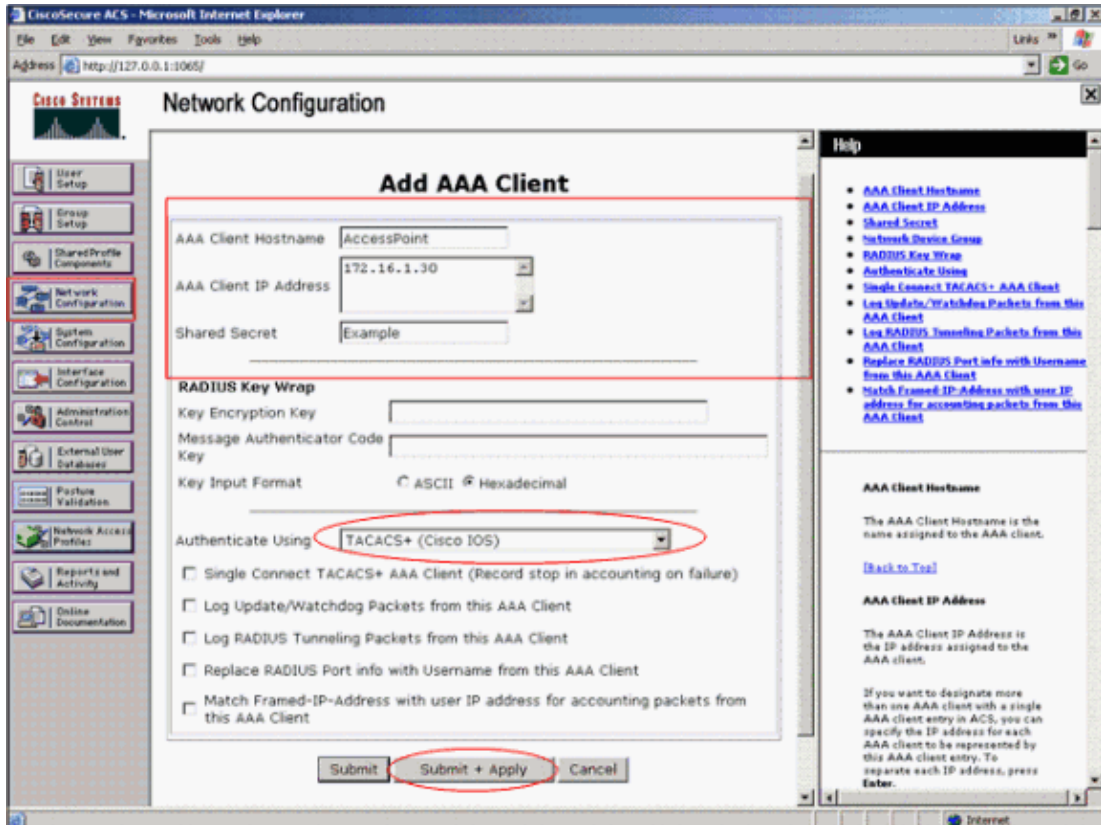
1. Complete these steps in order to add the AP as an authentication, authorization, and accounting (AAA) client:
 - a. From the ACS GUI, click the **Network Configuration** tab.

- b. Under AAA Clients, click **Add Entry**.
- c. In the Add AAA Client window, enter the AP host name, the IP address of the AP, and a shared secret key.

This shared secret key must be the same as the shared secret key that you configure on the AP.

- d. From the Authenticate Using drop-down menu, select **TACACS+ (Cisco IOS)**.
- e. Click **Submit + Restart** in order to save the configuration.

Here is an example:



This example uses:

- ◆ The AAA Client Hostname **AccessPoint**
- ◆ The address **172.16.1.30/16** as the AAA Client IP Address
- ◆ The shared secret key **Example**

2. Complete these steps in order to create a group that contains all the administrative (admin) users:

- a. Click **Group Setup** from the menu on the left.

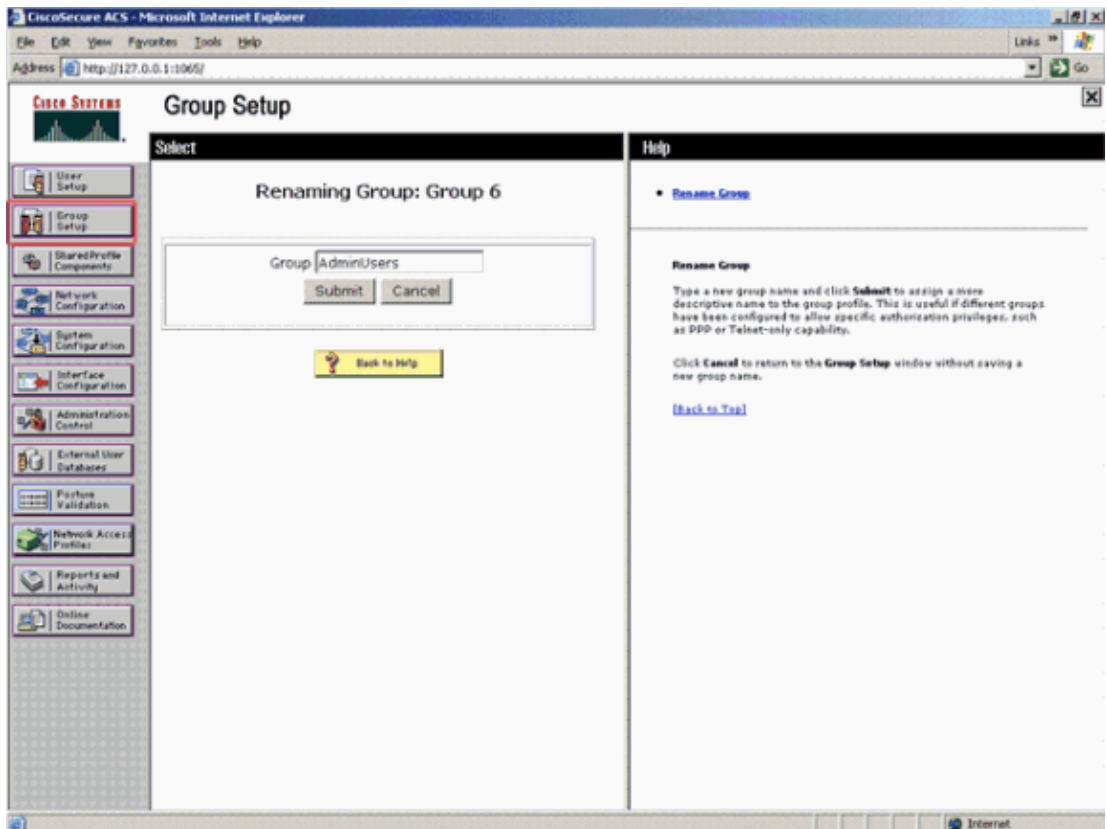
A new window appears.

- b. In the Group Setup window, select a group to configure from the drop-down menu and click **Rename Group**.

This example selects Group 6 from the drop-down menu and renames the group AdminUsers.

- c. Click **Submit**.

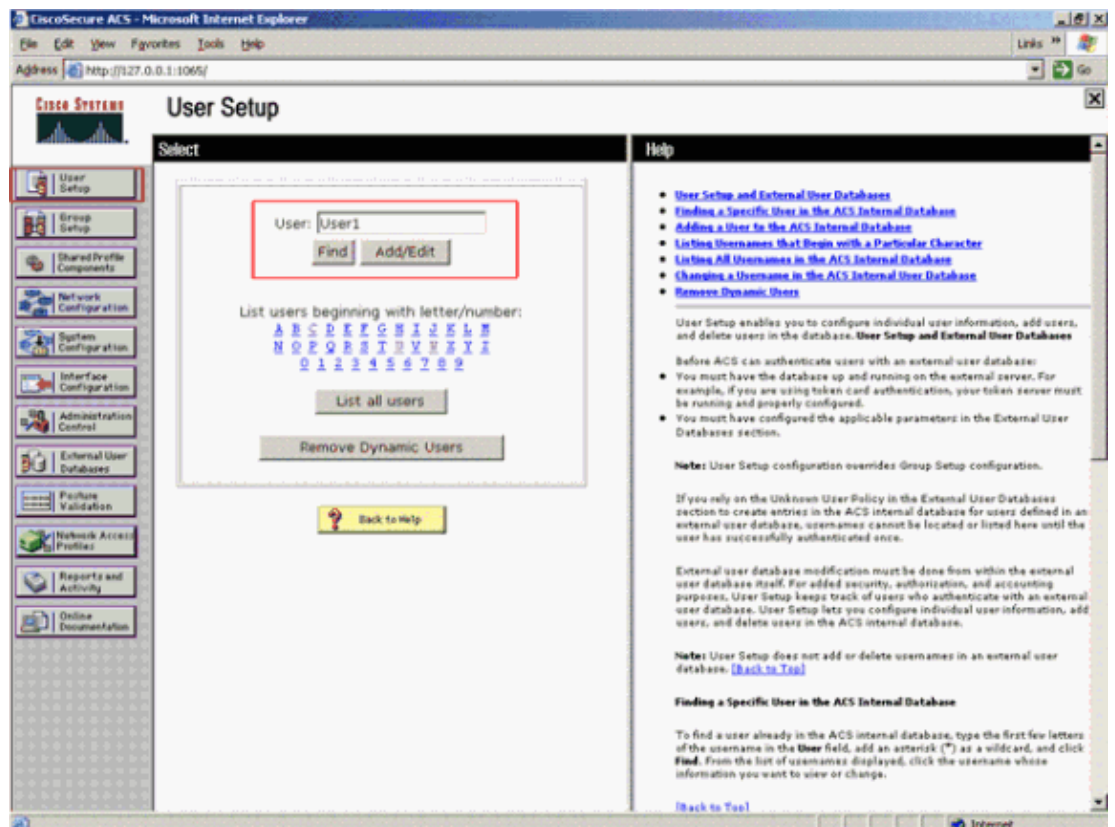
Here is an example:



3. Complete these steps in order to add the users to the TACACS+ database:

- a. Click the **User Setup** tab.
- b. In order to create a new user, enter the username in the User field and click **Add/Edit**.

Here is an example, which creates **User1**:



After you click Add/Edit, the Add/Edit window for this user appears.

4. Enter credentials that are specific to this user and click **Submit** in order to save the configuration.

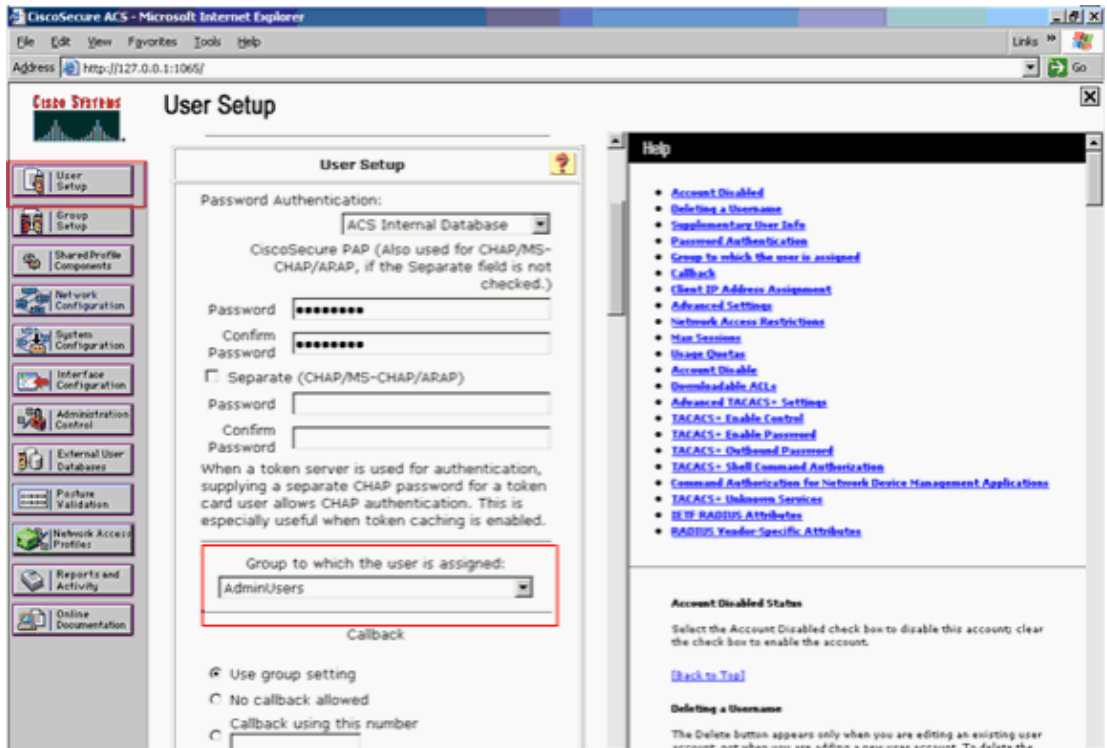
The credentials that you can enter include:

- ◆ Supplementary user information
- ◆ User setup
- ◆ The group to which the user is assigned

Here is an example:

The screenshot shows the CiscoSecure ACS User Setup interface. The browser window is titled "CiscoSecure ACS - Microsoft Internet Explorer" and the address bar shows "http://127.0.0.1:1065/". The main content area is titled "User Setup" and is in "Edit" mode for "User: User1 (New User)". The interface includes a navigation menu on the left with "User Setup" selected. The main form has three sections: "Account Disabled" (checkbox), "Supplementary User Info" (Real Name: User1, Description:), and "User Setup" (Password Authentication: ACS Internal Database, Password: , Confirm Password:). A red box highlights the "User Setup" section. The "Help" sidebar on the right lists various links such as "Account Disabled", "Deleting a Username", and "Supplementary User Info".

You can see that this example adds the user User1 to the group AdminUsers.



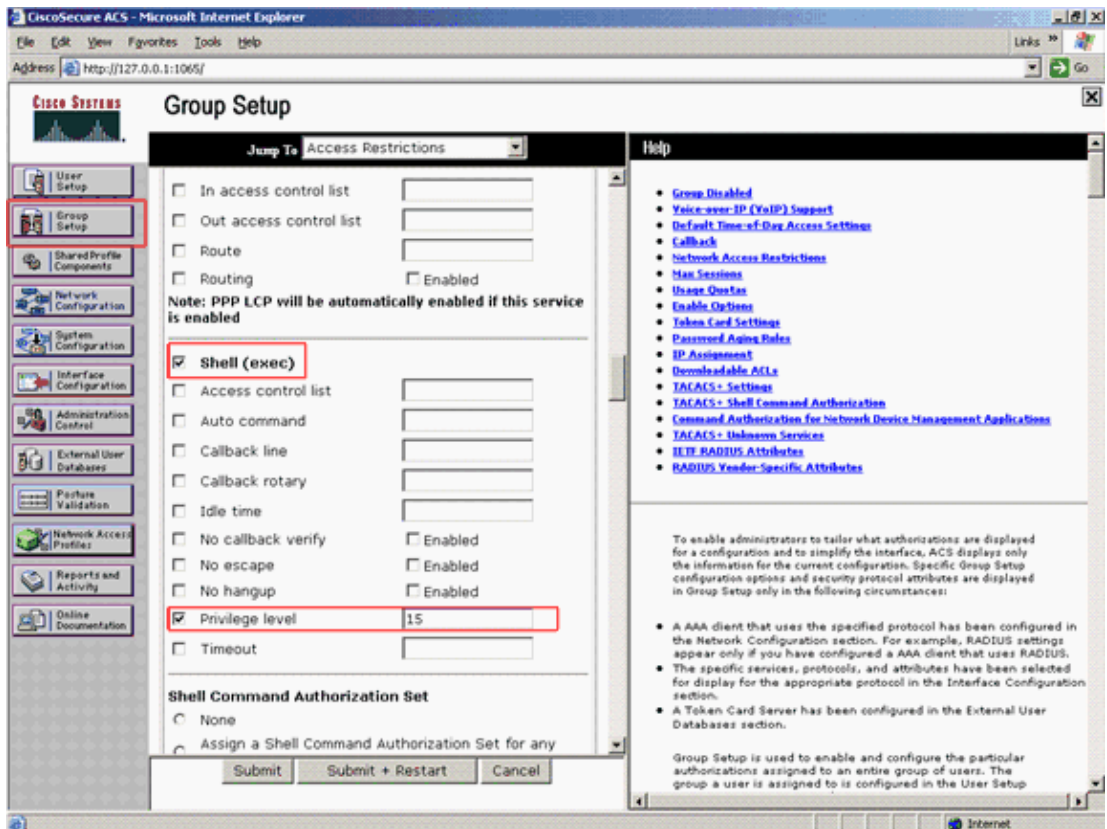
Note: If you do not create a specific group, the users are assigned to the default group.

5. Complete these steps in order to define the privilege level:

- a. Click the **Group Setup** tab.
- b. Select the group that you previously assigned to this user and click **Edit Settings**.

This example uses the group AdminUsers.

- c. Under TACACS+ Settings, check the **Shell (exec)** check box and check the **Privilege level** check box that has a value of 15.
- d. Click **Submit + Restart**.



Note: Privilege level 15 must be defined for the GUI and Telnet in order to be accessible as level 15. Otherwise, by default, the user can only access as level 1. If the privilege level is not defined and the user tries to enter enable mode on the CLI (with use of Telnet), the AP displays this error message:

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

Repeat Steps 2 through 4 of this procedure if you want to add more users to the TACACS+ database. After you have completed these steps, the TACACS+ server is ready to validate users who try to log in to the AP. Now, you must configure the AP for TACACS+ authentication.

Configure the Aironet AP for TACACS+ Authentication

You can use either CLI or GUI in order to enable the TACACS+ features on the Aironet AP. This section explains how to configure the AP for TACACS+ login authentication with use of the GUI.

Complete these steps in order to configure TACACS+ on the AP with use of the GUI:

1. Complete these steps in order to define the TACACS+ server parameters:

a. From the AP GUI, choose **Security > Server Manager**.

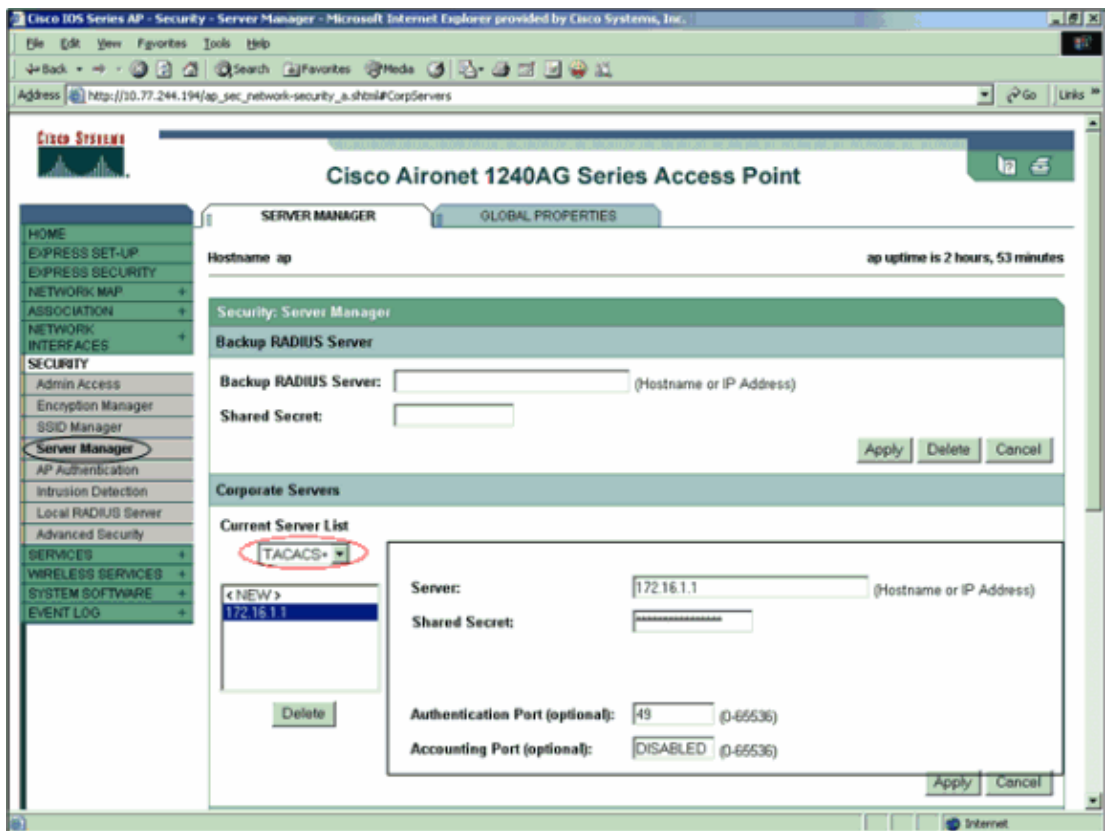
The Security: Server Manager window appears.

b. In the Corporate Servers area, select **TACACS+** from the Current Server List drop-down menu.

c. In this same area, enter the IP address, the shared secret, and the authentication port number of the TACACS+ server.

d. Click **Apply**.

Here is an example:

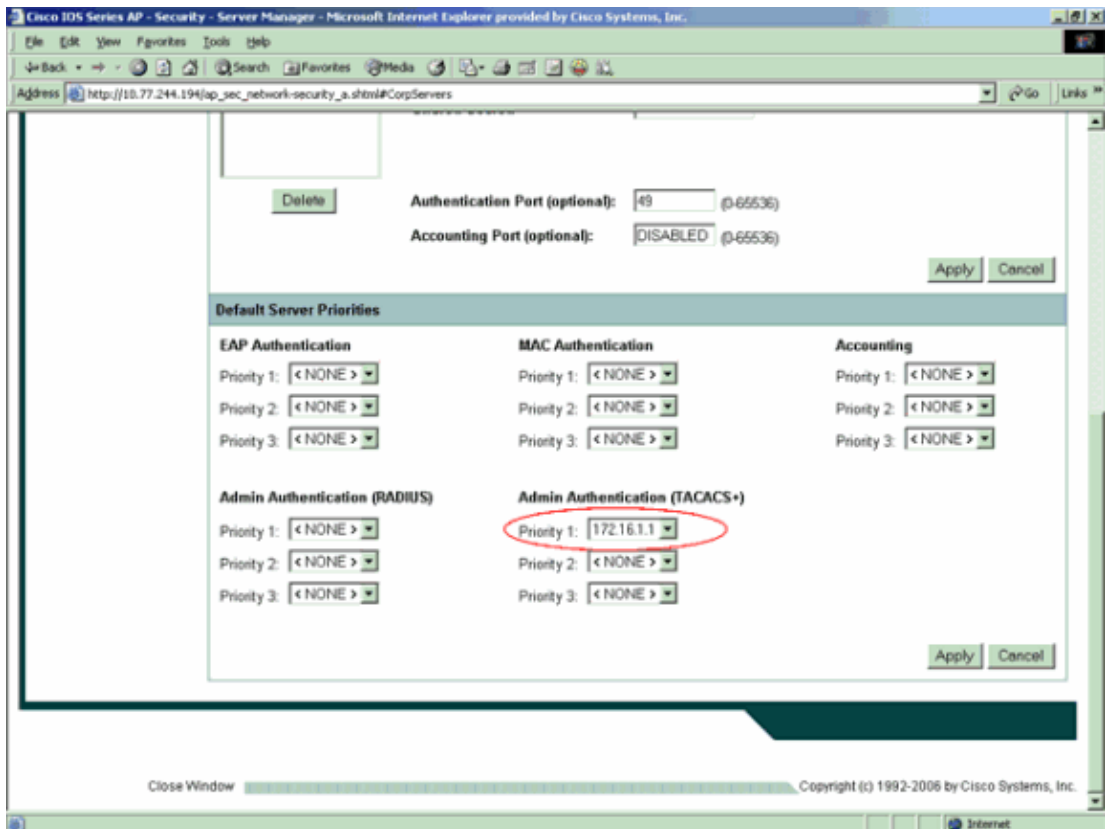


Note: By default, TACACS+ uses TCP port 49.

Note: The shared secret key that you configure on the ACS and the AP must match.

2. Choose **Default Server Priorities > Admin Authentication (TACACS+)**, select from the Priority 1 drop-down menu the TACACS+ server IP address that you have configured, and click **Apply**.

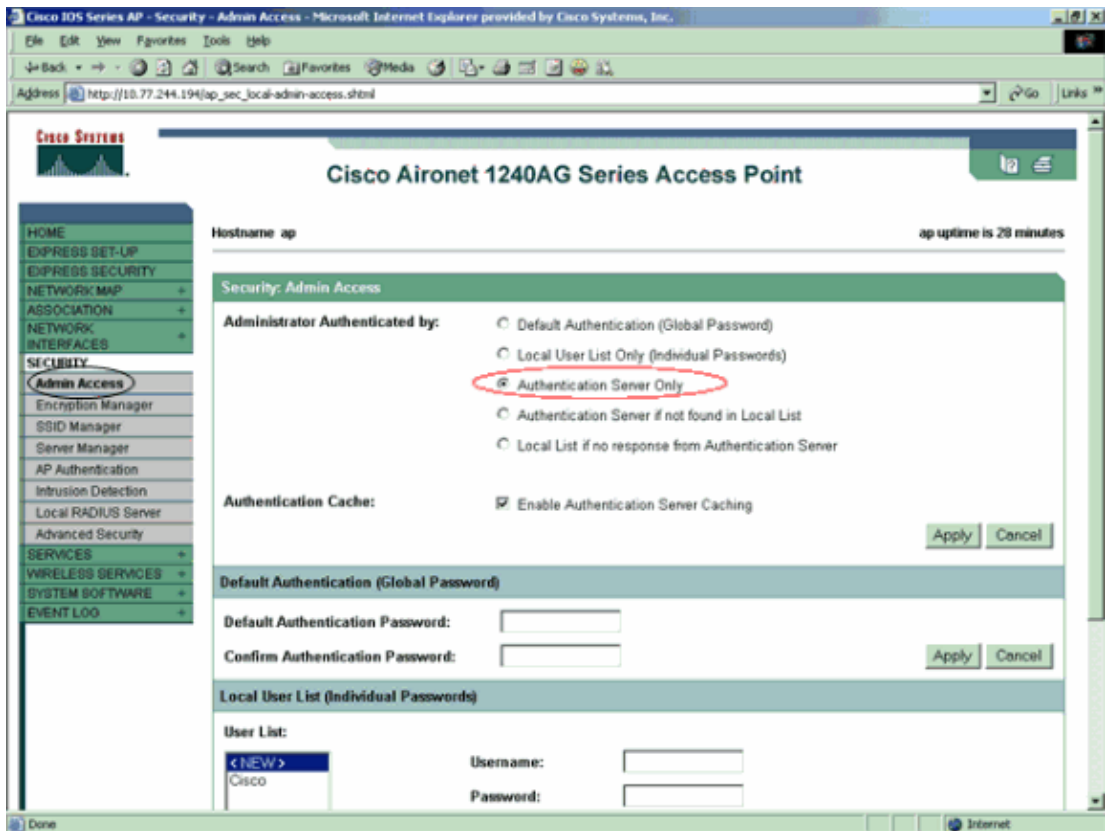
Here is an example:



3. Choose **Security > Admin Access** and, for Administrator Authenticated by:, choose **Authentication Server Only** and click **Apply**.

This selection ensures that users who try to log in to the AP are authenticated by an authentication server.

Here is an example:



This is the CLI configuration for the configuration example:

```

AccessPoint
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 BVI1
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/help/ea
ip radius source-interface BVI1
!
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

```

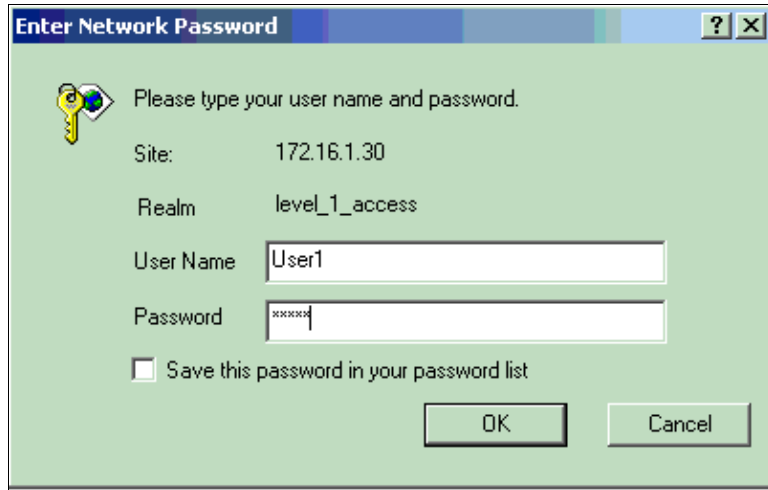
Note: You must have Cisco IOS Software Release 12.3(7)JA or later in order for all the commands in this configuration to work properly. An earlier Cisco IOS Software release might not have all these commands available.

Verify

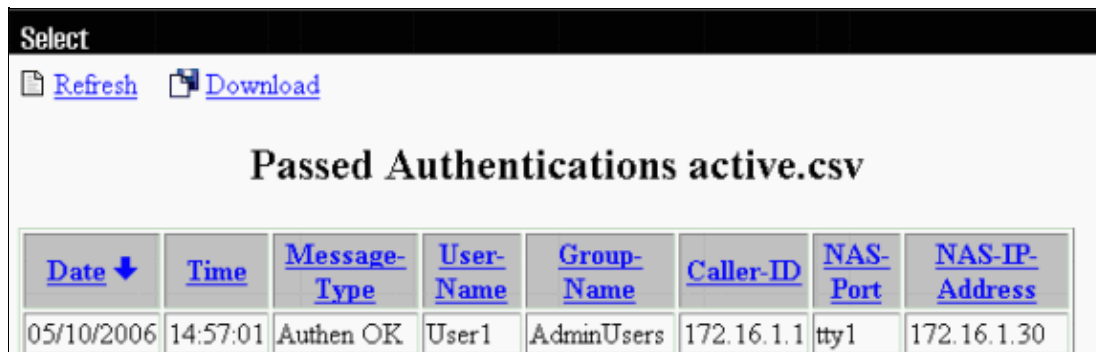
Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

In order to verify the configuration, try to log in to the AP with use of the GUI or the CLI. When you try to access the AP, the AP prompts you for a username and password.



When you provide the user credentials, the AP forwards the credentials to the TACACS+ server. The TACACS+ server validates the credentials on the basis of the information that is available in its database and provides access to the AP upon successful authentication. You can choose **Reports and Activity > Passed Authentication** on the ACS and use the Passed Authentication report in order to check for successful authentication for this user. Here is an example:



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

You can also use the **show tacacs** command in order to verify the correct configuration of the TACACS+ server. Here is an example:

```
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
```

Troubleshoot

You can use these debug commands on the AP in order to troubleshoot your configuration:

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug tacacs events** This command displays the sequence of events that happen during TACACS authentication. Here is an example of the output of this command:

```
*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** Use this command to troubleshoot HTTP authentication problems. The command displays the authentication method that the router attempted and authentication-specific status messages.
- **debug aaa authentication** This command displays information on AAA TACACS+ authentication.

If the user enters an username which does not exist on the TACACS+ server, the authentication fails. Here is **debug tacacs authentication** command output for a failed authentication:

```
*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)
```

You can choose **Reports and Activity > Failed Authentication** in order to see the failed authentication attempt on the ACS. Here is an example:

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

If you use a Cisco IOS Software release on the AP that is earlier than Cisco IOS Software Release 12.3(7)JA, you may hit a bug every time that you try to log in to the AP with use of HTTP. Cisco bug ID is CSCeb52431 (registered customers only) .

The Cisco IOS Software HTTP/AAA implementation requires the independent authentication of each separate HTTP connection. The wireless Cisco IOS Software GUI involves the reference of many dozens of separate files within a single web page (for example Javascript and GIF). So if you load a single page in the wireless Cisco IOS Software GUI, dozens and dozens of separate authentication/authorization requests can hit the AAA server.

For HTTP authentication, use RADIUS or local authentication. The RADIUS server is still subjected to the multiple authentication requests. But RADIUS is more scalable than TACACS+, and so it is likely to provide a less–adverse performance impact.

If you must use TACACS+ and you have a Cisco ACS, use the **single–connection** keyword with the **tacacs–server** command. Use of this keyword with the command spares the ACS most of the TCP connection setup/teardown overhead and is likely to reduce the load on the server to a certain extent.

For Cisco IOS Software Releases 12.3(7) JA and later on the AP, the software includes a fix. The remainder of this section describes the fix.

Use the AAA authentication cache feature in order to cache the information that the TACACS+ server returns. The authentication cache and profile feature allows the AP to cache the authentication/authorization responses for a user so that subsequent authentication/authorization requests do not need to be sent to the AAA server. In order to enable this feature with the CLI, use these commands:

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

For more information on this feature and the commands, refer to the *Configuring the Authentication Cache and Profile* section of *Administering the Access Point*.

In order to enable this feature on the GUI, choose **Security > Admin Access** and check the **Enable Authentication Server Caching** check box. Because this document uses Cisco IOS Software Release 12.3(7)JA, the document uses the fix, as the configurations illustrate.

Related Information

- **Configuring RADIUS and TACACS+ Servers**
 - **Field Notice: IOS Access Point Bombards TACACS+ Server with Requests**
 - **EAP Authentication with RADIUS Server**
 - **Wireless Product Support**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: May 21, 2006

Document ID: 70149
