CHAPTER 4

Managing GSS User Accounts Through a TACACS+ Server

This chapter describes how to configure the GSS, primary GSSM, or standby GSSM as a client of a Terminal Access Controller Access Control System Plus (TACACS+) server for separate authentication, authorization, and accounting (AAA) services. Configuring the GSS as a client of a TACACS+ server provides a higher level of security by allowing you to control who can access a GSS device, control which CLI commands are available for particular users, and to use the TACACS+ server to record the specific CLI commands and GUI pages accessed by a GSS user.

This chapter contains the following major sections:

TACACS+ Overview

TACACS+ security daemon running on a UNIX or Windows NT/Windows 2000 server.

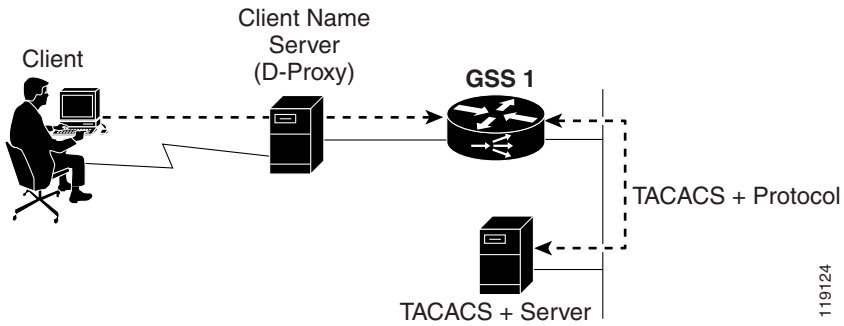
example of an AAA access control server.

TACACS+ uses TCP as the transport protocol for reliable delivery. Optionally, you can configure the GSS to encrypt all traffic transmitted between the GSS device and the TACACS+ server in the form of a shared secret.

When a user attempts to access a GSS device that is operating as a TACACS+ client, the GSS forwards the user authentication request to the TACACS+ server (containing the username and password). The TACACS+ server returns either a success or failure response depending on the information in the server's database.

Figure 4-1 shows a client GSS and a TACACS+ server configuration.

Figure 4-1 Simplified Example of Traffic Flow Between a GSS Client and a TACACS+ Server



The TACACS+ server provides the following AAA independent services to the GSS operating as a TACACS+ client:

Authentication—Identifies users attempting to access a GSS. Authentication frequently involves verifying a username with an assigned password. GSS users are authenticated against the TACACS+ server when remotely accessing a GSS through the console, Telnet, Secure Shell (SSH), FTP, or the primary GSSM GUI interfaces.

To successfully log in to a GSS from an SSH session, you must be configured on both the GSS and the TACACS+ server. To successfully log in from a Telnet or FTP session, you need only be configured on the TACACS+ server. In either case, if your remote login authentication attempt is denied, you are prohibited from accessing the GSS.

Authorization—Controls which GSS CLI commands a user can execute on a GSS or on a GSSM (primary or standby), providing per-command control and filtering. Authorization is performed after a user receives authentication by the TACACS+ server and begins to use the GSS. You also can assign a privilege level to a user accessing the primary GSSM GUI.

Accounting—Records the specific CLI commands and GUI pages accessed by a GSS user. Accounting enables system administrators to monitor the activities of GSS users, which is beneficial for administrating multi-user GSS devices. The information is contained in an accounting record that is sent to the TACACS+ server. Each record includes the username, the CLI command executed or the primary GSSM GUI page accessed, the primary GSSM GUI page action performed, and the time that the action was performed. You can import the log files from the TACACS+ server into a spreadsheet application.

You can define a maximum of three TACACS+ servers for use with a GSS. The GSS periodically queries the first configured TACACS+ server with a TCP keepalive to ensure network connectivity and TACACS+ application operation. If the GSS determines that the TACACS+ server is down, the GSS

TACACS+ Configuration Quick Start

Table 4-1 TACACS+ Configuration Quick Start

Task and Command Example	
1.	
2.	gssm1.example.com# **config** gssm1.example.com(config)#
3.	address or hostname for the server. By default, the TCP port is 49. You can optionally define a different port number and, if required, a TACACS+ server encryption key. **tacacs-server host 192.168.1.102 port 9988 key SECRET-456**
4.	**tacacs-server timeout 60**
5.	**aaa authentication ssh**
6.	**aaa authorization commands**
7.	**aaa accounting commands**

Configuring a TACACS+ Server for Use with the GSS

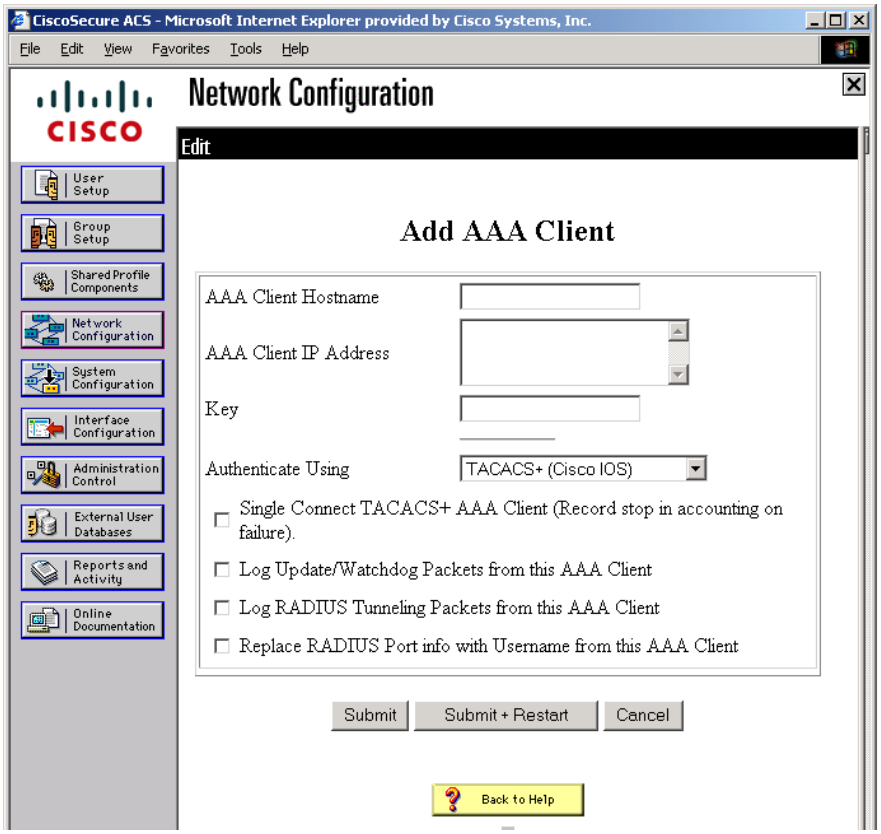
-
-
-

Note

Configuring Authentication Settings on the TACACS+ Server

1.

Figure 4-2 Add AAA Client Page of Cisco Secure ACS



Configuring Authorization Settings on the TACACS+ Server

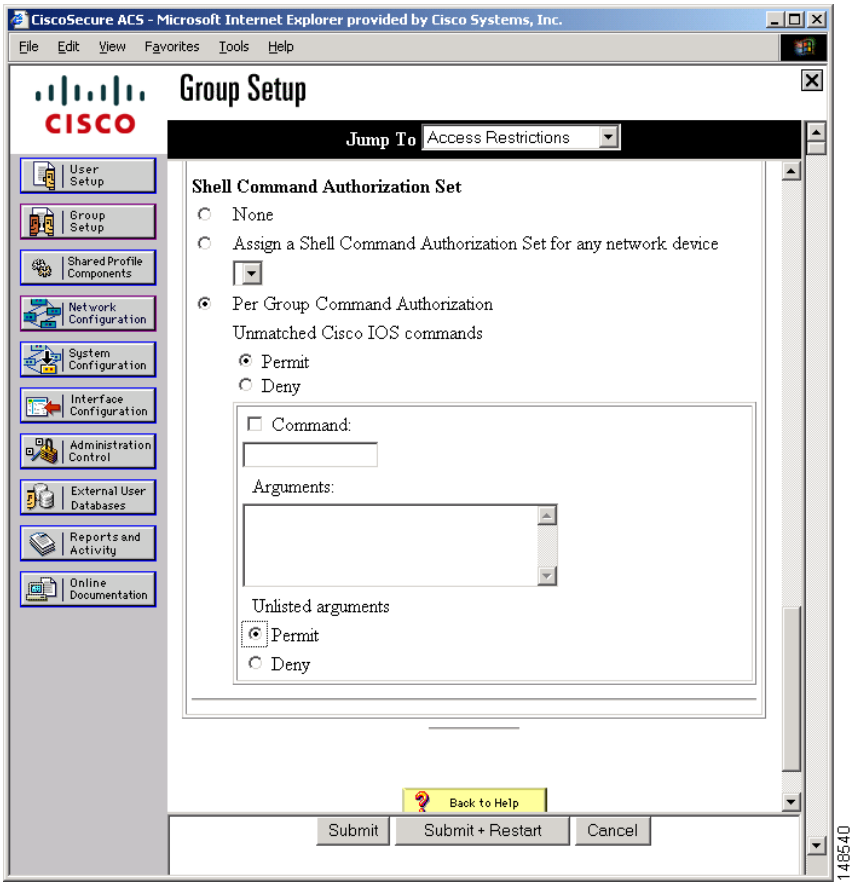
Note

1.

Edit Settings

Figure 4-3).

Figure 4-3 Shell Command Authorization Set Section of Group Setup Page



Per Group Command Authorization

Permit

a. **Command**

b. **Deny**

c.

6.

```
deny <arg1 … argN>
permit <arg1 … argN>
```

argument *argument*

8. Repeat Steps 5 through 7 for each CLI command that you want to restrict. Configure multiple commands by clicking the **Submit** button after each command. A new command configuration section appears for subsequent commands.

The following are examples of permitting and denying CLI commands:

To deny all CLI commands except the **show users**

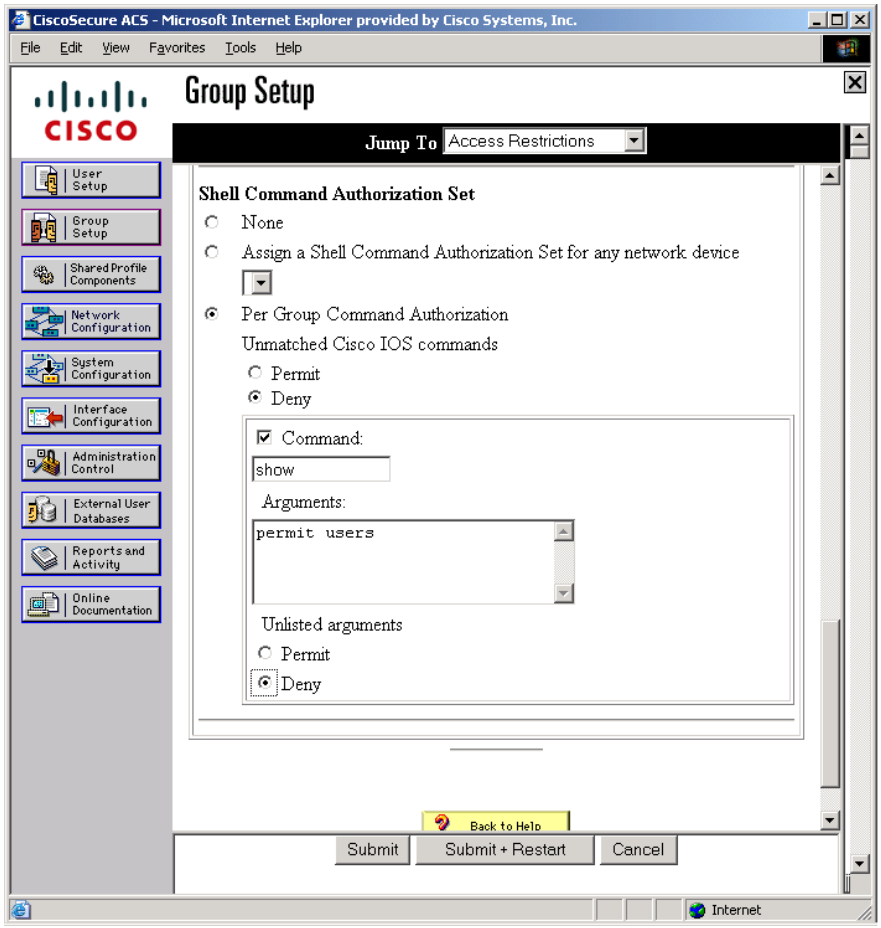
Deny

show

permit user

d.

Command Privileges Example—Deny All CLI Commands Except Specified Command



gss tech-report

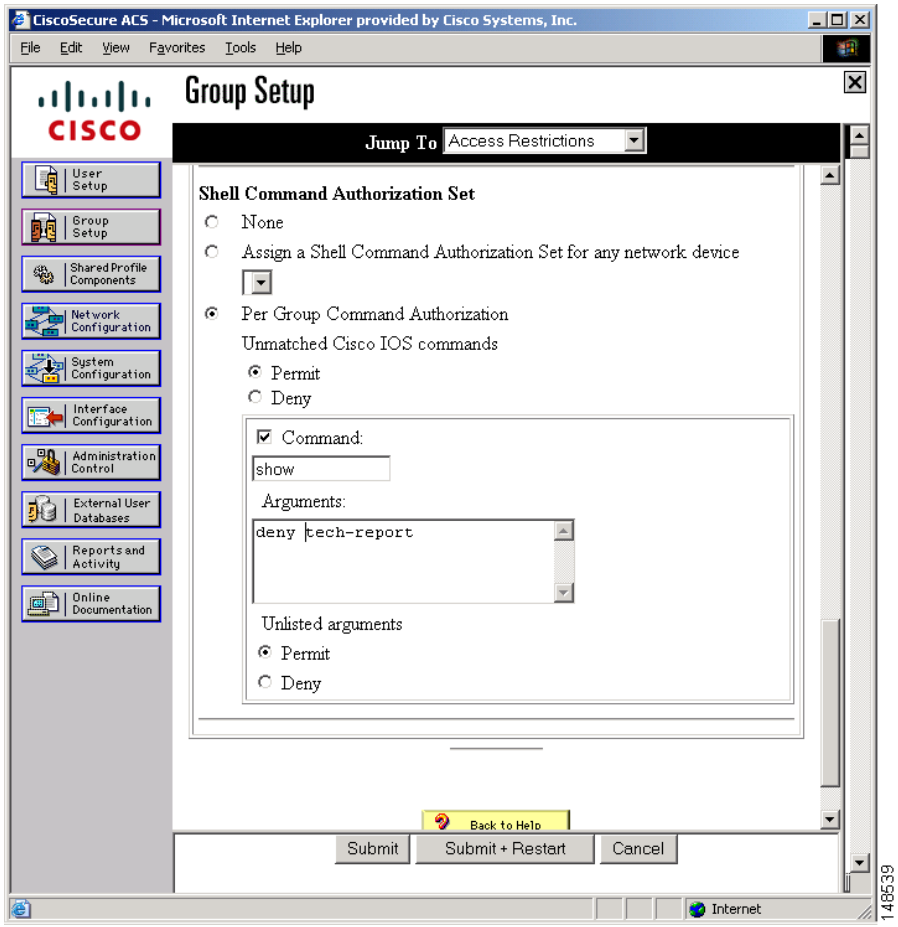
Permit

b.

c.

d.

Figure 4-5 Command Privileges Example—Permit All CLI Commands Except Specified Command



Enabling Custom User GUI Views When Authenticating a User from the TACACS+ Server

Configuring Primary GSSM GUI Privilege Level Authorization from the TACACS+ Server

-
-

"Privilege Levels for Using the Primary GSSM GUI" section in Chapter 3, Creating and Managing User Accounts for more information.

Primary GSSM GUI privileges assigned to a user from the TACACS+ server override the user privilege level defined from the primary GSSM GUI GSSM User Administration details page.

To specify a user privilege-level for accessing the primary GSSM GUI from the Cisco Secure ACS, perform the following steps:

If this is your first time enabling per-user CLI command authorization, access the Interface Configuration section of the Cisco Secure ACS interface and configure the following selections:

Access the TACACS+ (IOS) page. Click the **Shell (exec)**
Figure 4-6).

Figure 4-6 Interface Configuration Page—TACACS+ (IOS) Page

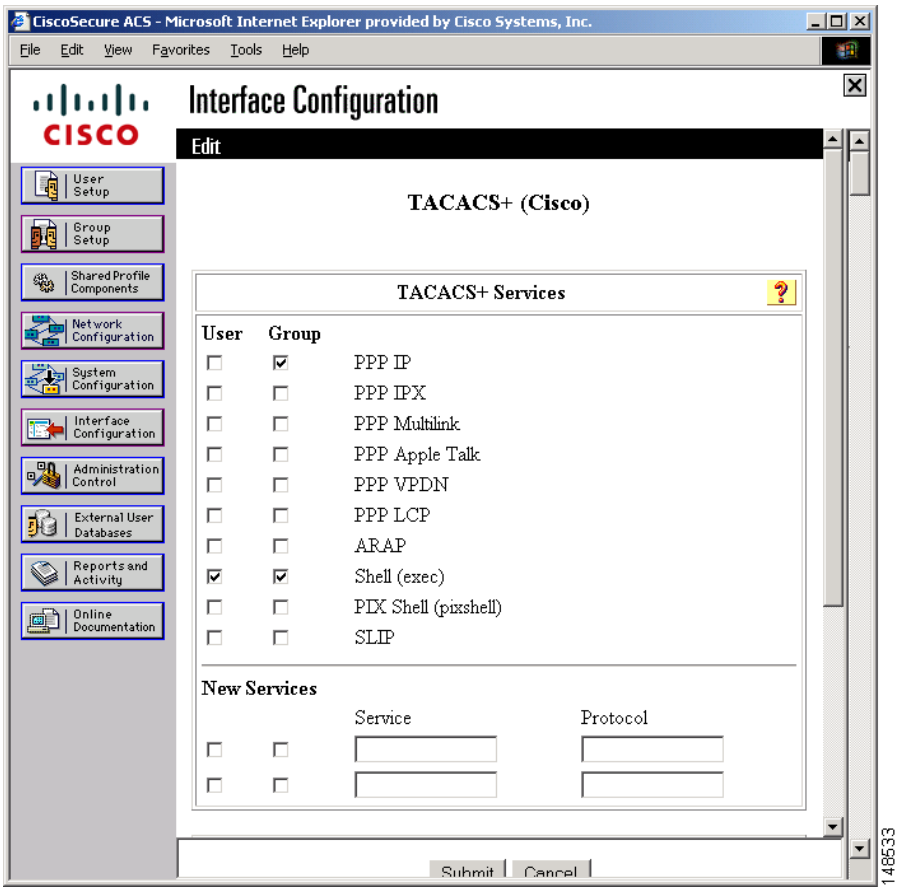
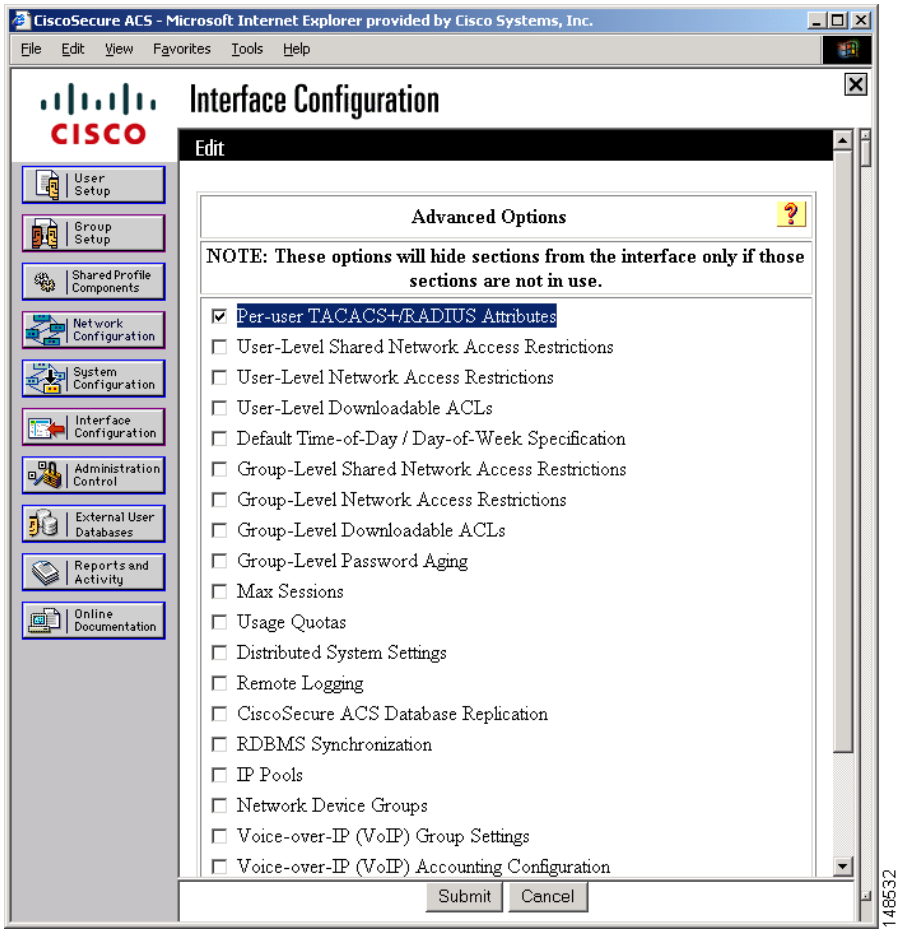


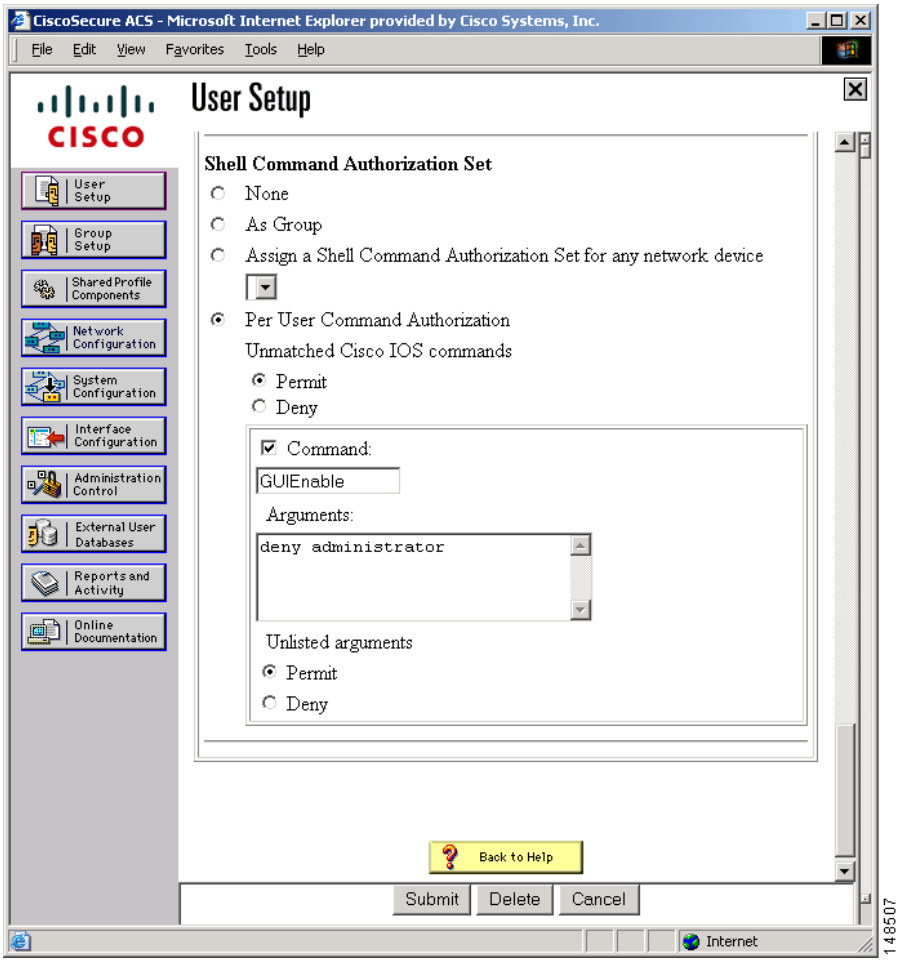
Figure 4-7 Interface Configuration Page—Advanced Options Page



Per User Command Authorization

Command **GuiEnable** Figure 4-8).

Figure 4-8 Assigning Operator-Level Privileges to a User from Cisco Secure ACS



Enabling Custom User GUI Views When Authenticating a User from the TACACS+ Server

-
-
-
-

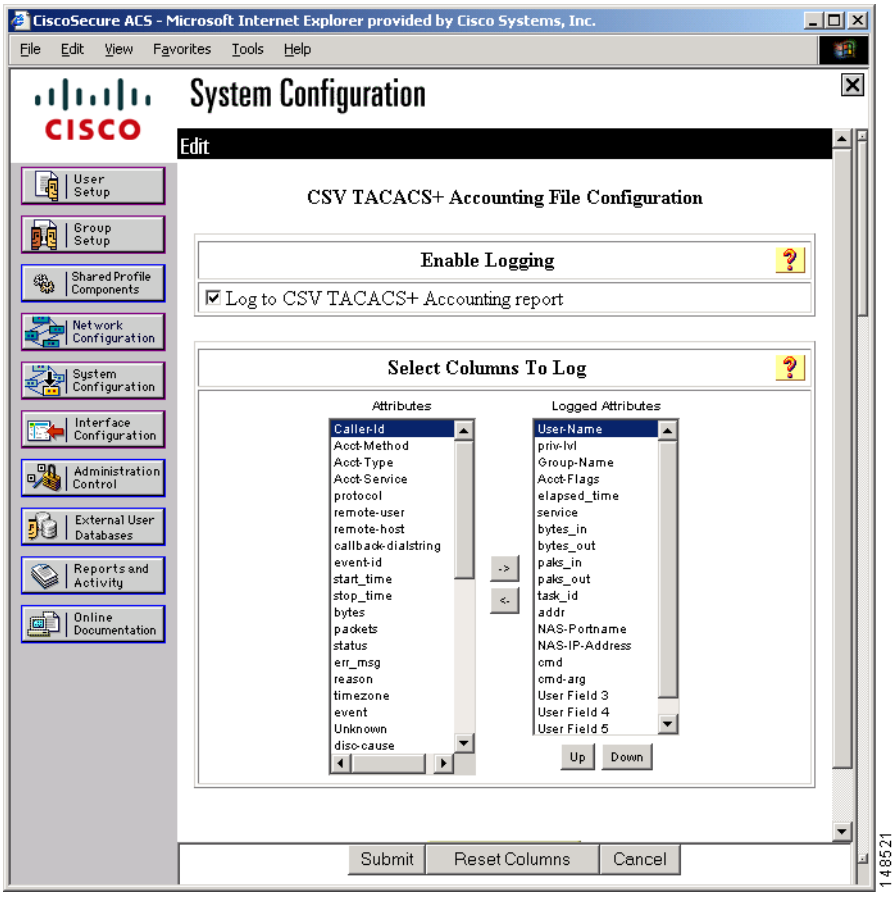
Note

Configuring Accounting Settings on the TACACS+ Server

1.

CSV TACACS+ Accounting

Figure 4-9 CSV TACACS+ Accounting File Logging Page of Cisco Secure ACS



Log to CSV TACACS+ Accounting report

-> **Up** **Down**

Submit

Identifying the TACACS+ Server Host on the GSS

tacacs-server host

tacacs-server host

Note

tacacs-server timeout

tacacs-server host

tacacs-server host

aaa

authorization commands

tacacs-server host

aaa authorization commands

tacacs-server host *ip_or_host* [*port*] [**key** *encryption_key*

ip_or_host

port

encryption_key

```
tacacs-server host 192.168.1.100 port 8877 key SECRET-123
tacacs-server host 192.168.1.101 key SECRET-456
tacacs-server host 192.168.1.102 port 9988 key SECRET-789
```

```
no tacacs-server host 192.168.1.101
```

```
no tacacs-server host 192.168.1.101 port 49
```

```
no tacacs-server host 192.168.1.101 port 8877
```

```
no tacacs-server host 192.168.1.101 key SECRET-123
```

```
no tacacs-server host 192.168.1.101 port 8877 key SECRET-123
```

Disabling TACACS+ Server Keepalives on the GSS

```
no tacacs-server keepalive-enable
```

```
tacacs-server keepalive-enable
```

Specifying the TACACS+ Server Timeout on the GSS

Specifying TACACS+ Authentication of the GSS

Note

{**ftp** | | | } [ ]

The keywords for this global configuration command are as follows:

- —Enables the TACACS+ authentication service for a File Transfer Protocol (FTP) remote access connection.
- —Enables the TACACS+ authentication service for a primary GSSM GUI connection.
- —Enables the TACACS+ authentication service for the login service, using either a direct connection to the GSS console port or through a Telnet remote access connection.
- —Enables the TACACS+ authentication service for a Secure Shell (SSH) remote access connection.
- —(Optional) Used when you want the GSS to fall back to local authentication if TACACS+ authentication fails for an FTP, GUI, or SSH connection. The option is always enabled for the login (console port or Telnet) access method.

For example, to enable TACACS+ authentication for an SSH remote access connection that can revert back to local authentication, enter:

Use the form of the command to disable the TACACS+ authentication function. For example, to disable TACACS+ authentication for an SSH remote access connection, enter:

Specifying TACACS+ Authorization of the GSS

Specifying TACACS+ Accounting on the GSS

- **commands—**
  commands

  gui

  no aaa accounting

Inserting Header Information Into an Authentication Request

- lient hostname in the rem_addr field of the TACACS+ authentication packet which gets displayed in the CallerId field on the access control server (ACS). This is the default setting.
- —Instructs the GSS to insert the client source IP address in the rem_addr field of the TACACS+ authentication packet which gets displayed in the CallerId field on the ACS.

Note When you use the keyword and the GSS cannot resolve the client source IP address to the client hostname, the GSS inserts the client source IP address.

The form of the command is not permitted.

For example, to instruct the GSS to insert the client source IP address into the remote address header, enter:

Use the , , and commands to display the command setting.

Showing TACACS+ Statistics on the GSS

You can display a summary of the TACACS configuration on your GSS device by using the use the command.

For example, to display the current TACACS+ configuration, enter:

```
                  show tacacs
Current tacacs server configuration
tacacs-server timeout 5
tacacs-server callerId-info-type hostname
tacacs-server keepalive-enable
tacacs-server host 1192.168.1.100 port 49
aaa authentication ftp
```

```
gss1.example.com#


    Server 192.168.1.100:49   ONLINE
                   PASS   FAIL   ERROR
    Authentication  321    4      0
    Authorization   782    48     0
    Accounting      535    0      0

    Server 192.168.1.101:49   ONLINE
                   PASS   FAIL   ERROR
    Authentication  17     1      0
    Authorization   39     3      0
    Accounting      12     0      0
```

Field	Description

```
gss1.example.com#
Are you sure? (yes/no)
```

Hardware Installation Guide

```
GSS-1.31
LILO:GSS-1.31 DISABLETACACS=1


Mounting other Filesystems:  [  OK  ]
*** Disabling TACACS Authentication and Authorization
Building Properties
```

4.