Account Management

This chapter provides recipes for managing users and their accounts. It includes the following sections:

Creating User Accounts for CLI Access

In MDS firmware versions prior to Release 2.0, a separate account was required for both SNMP (Simple Network Management Protocol) and CLI (command-line interface) access. After Release 2.0, a single username grants access to both CLI and SNMP.

Tip

- Use the admin account only during initial setup. After setup, create other user accounts. Each administrator should have their own individual account.
- Always change the admin password from the factory default value.
- Grant users the minimum amount of system rights or privileges required to perform their job.

To access the Cisco MDS 9000 switch via console, SSH, or Telnet, create a username with CLI access. To create a user with CLI access, follow these steps:

Step 1 Enter the configuration submode:

```
switch# config terminal
```

Step 2 Create the CLI user by using the following syntax: username <username> password <password> role <role>

```
switch(config)# username user1 password admin123 role network-admin
```

At this point the user (user1) can access the switch using the password **admin123** via console, SSH or Telnet.

Creating User Accounts for SNMP Access

To access the Cisco MDS 9000 switch using SNMP, create a user with SNMP access. To create a user with SNMP access, follow these steps:

Step 1 Enter the configuration submode:

```
switch# config terminal
```

Step 2 Create the SNMP user by using the following syntax: **snmp-server user <username> <role> auth <encryption method> <password>**

```
switch(config)# snmp-server user user1 network-admin auth md5 admin123
```

At this point, the user (user1) can access the switch using the password **admin123** via an SNMP based product such as Cisco's MDS 9000 Family Fabric Manager or Device Manager.

Tip

- Create a unique user account for each user to aid with troubleshooting and accounting, .
- Use both privacy and authentication passwords for increased security during SNMPv3 based sessions.

Creating an MDS 9000 Switch User Role

The Cisco MDS 9000 switch comes with two predefined roles:

- **Network-admin** is the role assigned to the predefined user called admin. The network-admin canperform any modification to the MDS 9000 platform. There are no restrictions on this user.
- **Network-operator** is a predefined read-only role. The network-operator cannot make modifications to the Cisco MDS 9000 switch. There are no predefined users assigned to this role.

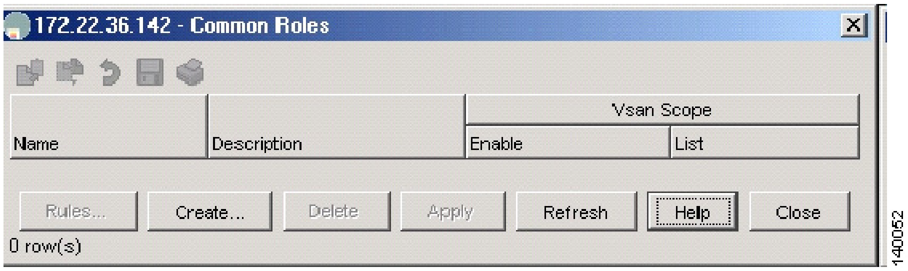
Tip

- Provide each user with a role that provides the minimum number of privileges required to perform their job.
- Leverage the read-only role of the network-operator for those users who do not require the ability to modify the Cisco MDS 9000 switch.
- Use the VSAN based role to allow administrators to have access to and complete control over their VSANs while having read-only or no access to other VSANs.

The following example shows how to create a role that provides the ability to only modify the zoning configuration on the switch.

Step 1 From the **Device Manager**, choose **Security > Common Roles**. (See Figure 1-1.)

Figure 1-1 Common Roles



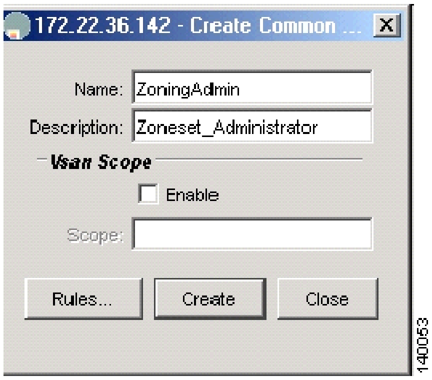
Name	Description	Vsan Scope	
		Enable	List

0 row(s)

Step 2 Click **Create**.

You see the Create Common Roles dialog box. (See Figure 1-2.)

Figure 1-2 Create Common Roles



Name: ZoningAdmin

Description: Zoneset_Administrator

Vsan Scope

□ Enable

Scope:

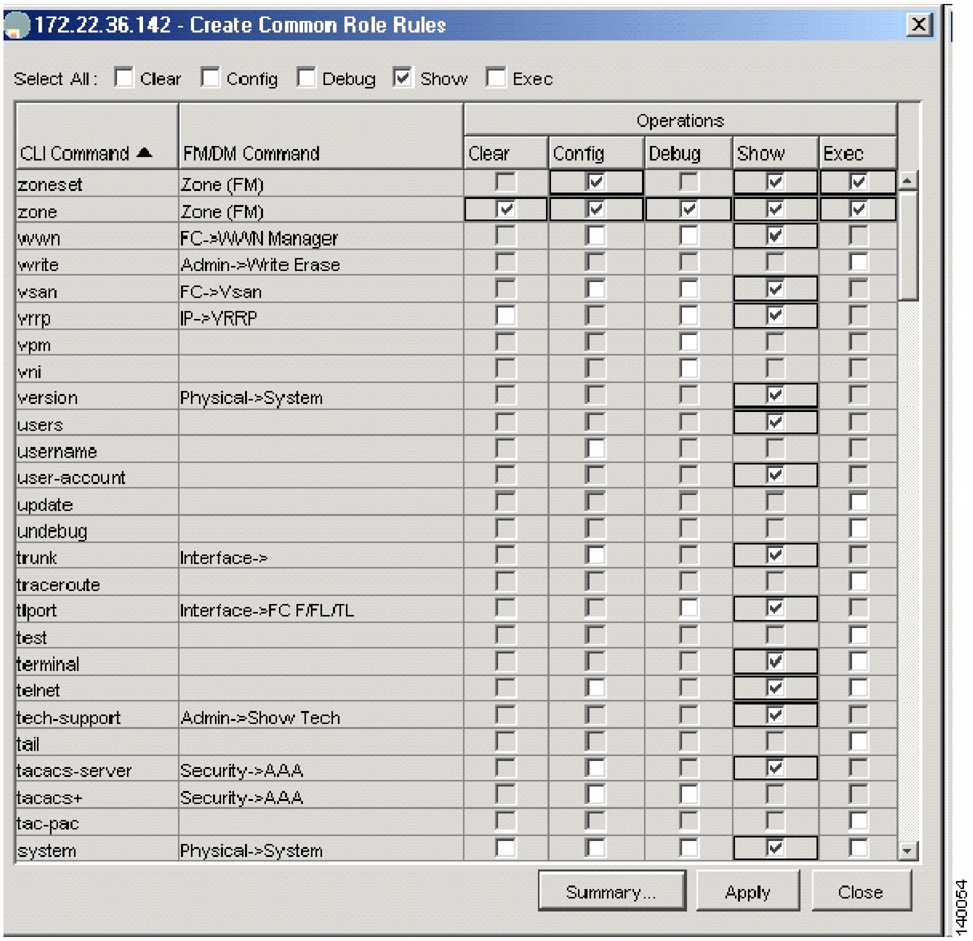
Step 3 Enter a name and description (without spaces) for the role.

Step 4 Optionally specify a VSAN scope to limit this specific role to a subset of VSANs. A zoning admin role can be created for zone admins who can only modify VSANs 1-10. This example does not specify a VSAN scope.

Step 5 Click **Rules**.

You see the Create Common Role Rules dialog box. (See Figure 1-3.)

Figure 1-3 Create Rules



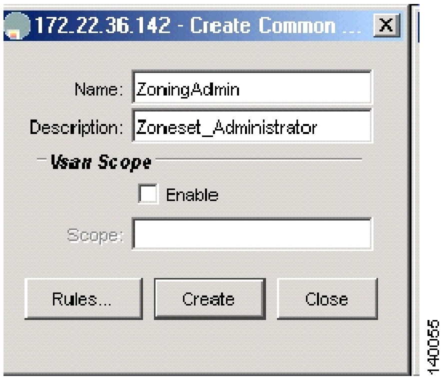
Select All: □ Clear □ Config □ Debug ☑ Show □ Exec

CLI Command ▲	FM/DM Command	Operations				
		Clear	Config	Debug	Show	Exec
zoneset	Zone (FM)	□	☑	□	☑	☑
zone	Zone (FM)	☑	☑	☑	☑	☑
wwn	FC->WWN Manager	□	□	□	☑	□
write	Admin->Write Erase	□	□	□	□	□
vsan	FC->Vsan	□	□	□	☑	□
vrrp	IP->VRRP	□	□	□	☑	□
vpm		□	□	□	□	□
vni		□	□	□	□	□
version	Physical->System	□	□	□	☑	□
users		□	□	□	☑	□
username		□	□	□	□	□
user-account		□	□	□	☑	□
update		□	□	□	□	□
undebug		□	□	□	□	□
trunk	Interface->	□	□	□	☑	□
traceroute		□	□	□	□	□
tlport	Interface->FC F/FL/TL	□	□	□	☑	□
test		□	□	□	□	□
terminal		□	□	□	☑	□
telnet		□	□	□	☑	□
tech-support	Admin->Show Tech	□	□	□	☑	□
tail		□	□	□	□	□
tacacs-server	Security->AAA	□	□	□	☑	□
tacacs+	Security->AAA	□	□	□	□	□
tac-pac		□	□	□	□	□
system	Physical->System	□	□	□	☑	□

Step 6 Check the **show** check box and all of the operations for the **zone** and **zoneset** commands. Also check the **copy** command so that the zoning admin can save the configuration.

Step 7 Click **Apply**. You see the Create Common Roles dialog box. (See Figure 1-4.)

Figure 1-4 Create Common Roles



Name: ZoningAdmin

Description: Zoneset_Administrator

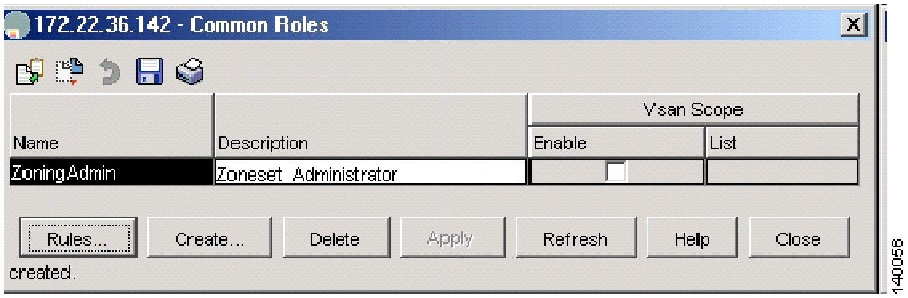
Vsan Scope

□ Enable

Scope:

Step 8 Click **Create** to display the Display Roles dialog box. (See Figure 1-5.)

Figure 1-5 Display Roles



172.22.36.142 - Common Roles

Name	Description	Vsan Scope	
		Enable	List
ZoningAdmin	Zoneset_Administrator	□	

created.

At this point, any user who is assigned to the role of ZoningAdmin can make zoning changes, or use the **copy running-configuration startup-configuration** command.

Step 9 To replicate this role to other systems, examine the startup-configuration for the relevant information, and enter the following CLI commands:

```
switch# config terminal
switch(config)#role name ZoningAdmin
switch(config-role)#  description Zoneset_Administrator
switch(config-role)#  rule 1 permit show
switch(config-role)#  rule 2 permit config feature zoneset
switch(config-role)#  rule 3 permit exec feature zoneset
switch(config-role)#  rule 4 permit clear feature zone
switch(config-role)#  rule 5 permit config feature zone
switch(config-role)#  rule 6 permit debug feature zone
switch(config-role)#  rule 7 permit exec feature zone
switch(config-role)#  rule 8 permit exec feature copy
```

Step 10 To create a user called **zoning_user** with the new role, enter the following commands on the switch:

```
switch# config terminal
switch(config)# username zoning_user password admin123 role ZoningAdmin
```

Configuring TACACS+ with Cisco Secure ACS

Cisco Secure ACS can enhance Cisco MDS 9000 switch management security, and provide centralized authentication, authorization, and accounting for users.

Tip We recommend using a TACACS+ server for both authentication, authorization, and accounting.

Authentication and Authorization with TACACS+

Configuring a Cisco MDS 9000 switch to use TACACS+ allows centralized account management of the switch. Centralized management means that an admin does not have to create and maintain usernames and passwords on individual switches. The Cisco Secure ACS server provides the authentication to a switch login as well as assigns the role to which the user is a member. A shared secret key provides encryption and authentication between the TACACS client (MDS 9500) and the TACACS+ server (Cisco Secure ACS).

In this procedure:

- The switch's IP address is 172.22.36.142
- The TACACS+ server's IP address is 172.22.36.10
- The TACACS+ shared secret key is WarEagle

Configuring Secure ACS Server

Prior to configuring the Cisco MDS 9000 switch, you must configure the Cisco Secure ACS server. To configure Secure ACS to allow the modification of advanced TACACS+ settings, follow these steps:

Step 1 Open Cisco MDS 9000 Family Device Manager. (See Figure 1-6.)

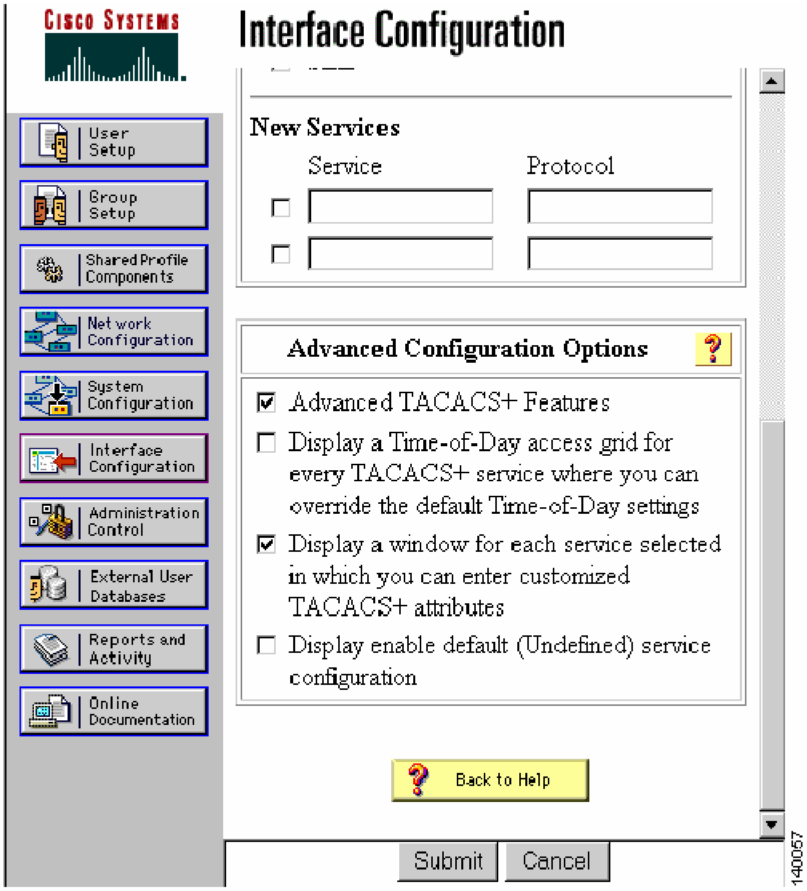
a. In the left pane of the main window, click **Interface Configuration**.

b. In the screen that opens, choose **TACACS+ (Cisco IOS)**.

c. Under **Advanced Configuration Options**, check **Advanced TACACS+ Features** and **Display a window...attributes.**

d. Click **Submit** to save the changes.

Figure 1-6 Secure ACS Configure Display



Interface Configuration

New Services

	Service	Protocol
□		
□		

Advanced Configuration Options

☑ Advanced TACACS+ Features

□ Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings

☑ Display a window for each service selected in which you can enter customized TACACS+ attributes

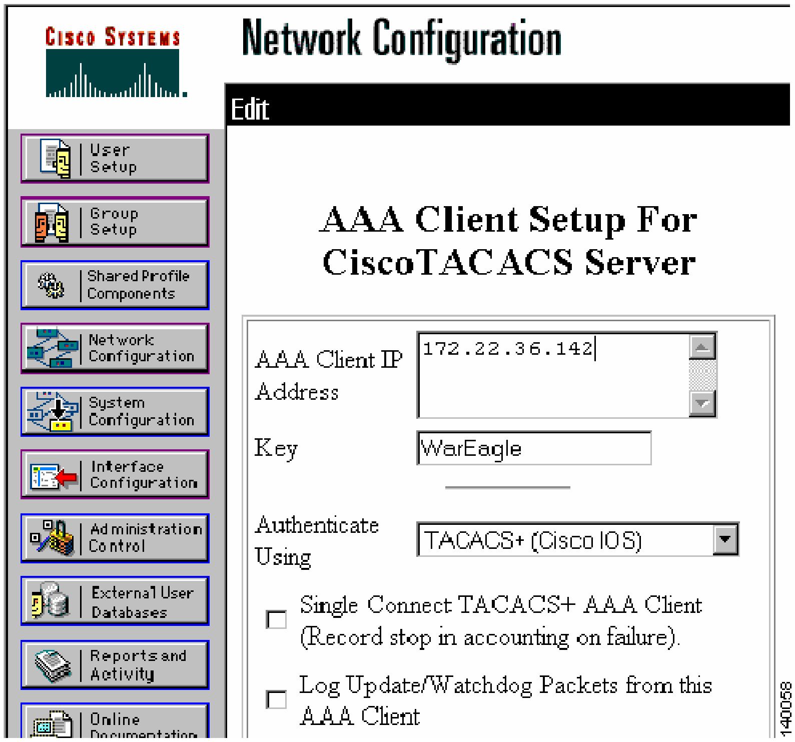
□ Display enable default (Undefined) service configuration

Step 2 Define the MD 9506 to the TACACS+ server so that the switch can be authenticated by the TACACS+. In the left pane, click **Network Configuration > Add Entry**. (See Figure 1-7.)

a. Enter the MDS 9506 switch's IP address (**172.22.36.142**) and shared secret key (**WarEagle**).

b. Click **Submit** to save the information.

Figure 1-7 Secure ACS Client Setup



Network Configuration

Edit

AAA Client Setup For CiscoTACACS Server

AAA Client IP Address	172.22.36.142
Key	WarEagle
Authenticate Using	TACACS+ (Cisco IOS)

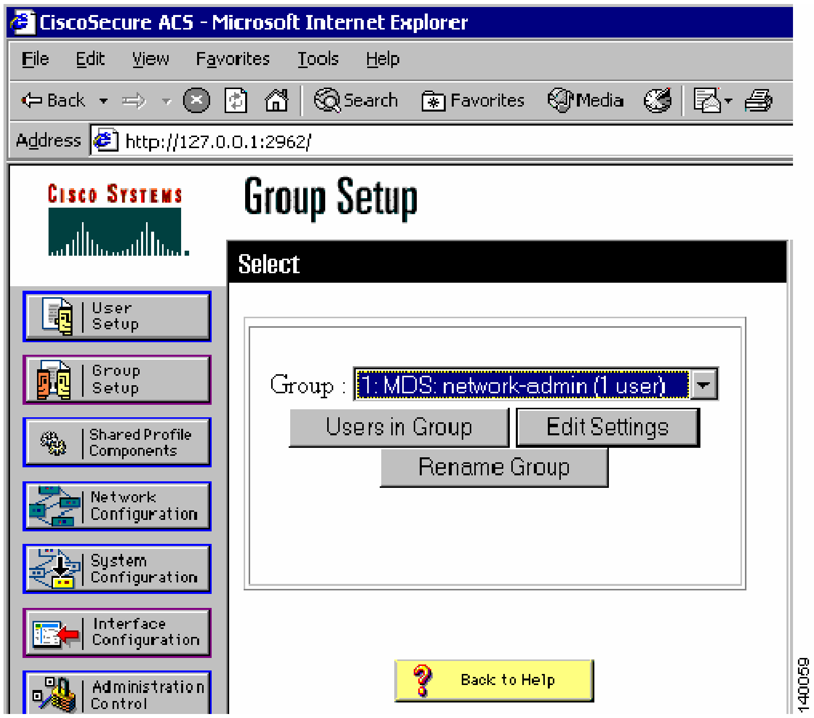
□ Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

□ Log Update/Watchdog Packets from this AAA Client

Step 3 Define a group by clicking **Group Setup**.

Groups provide an easy way to assign the same role to multiple users without having to modify the attributes of each user individually. (See Figure 1-8.)

Figure 1-8 Secure ACS: Group Setup


CiscoSecure ACS - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://127.0.0.1:2962/
Cisco Systems
Group Setup
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
Group : 1: MDS: network-admin (1 user)
Users in Group
Edit Settings
Rename Group
Back to Help
140059

Step 4 Chose an available group and click **Rename Group.** In the resulting box, choose a new name for this group.

Tip Use the same Secure ACS group name as the MDS role to ease creation of TACACS+ based users. Click **Submit** to save the name change.

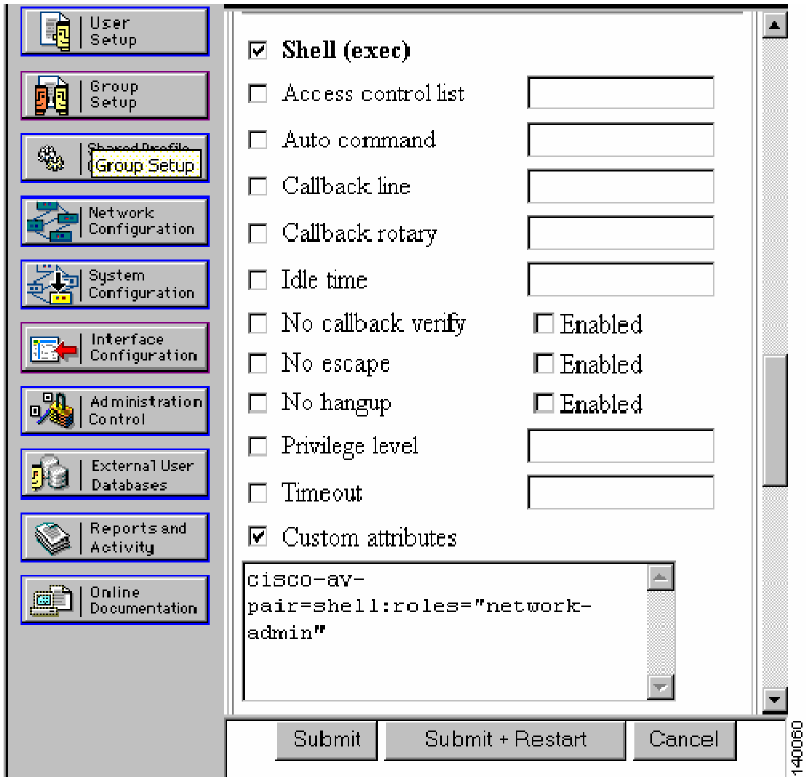
Step 5 In the left pane, click **Group Setup.**

Step 6 Choose the newly renamed group, and click **Edit Settings**.

Step 7 Scroll to the section labeled TACACS+ Settings, check **Shell** and **Custom attributes**.

Step 8 In the Custom attributes field, input the av-pair string corresponding to the role that is defined on the switch for users. The syntax is: `cisco-av-pair=shell:roles="<role>"` Click **Submit + Restart** to save and apply the configuration. (See Figure 1-9.)

Figure 1-9 ***Secure ACS Adding MDS Role***



☑ **Shell (exec)**

☐ Access control list

☐ Auto command

☐ Callback line

☐ Callback rotary

☐ Idle time

☐ No callback verify ☐ Enabled

☐ No escape ☐ Enabled

☐ No hangup ☐ Enabled

☐ Privilege level

☐ Timeout

☑ Custom attributes

```
cisco-av-
pair=shell:roles="network-
admin"
```

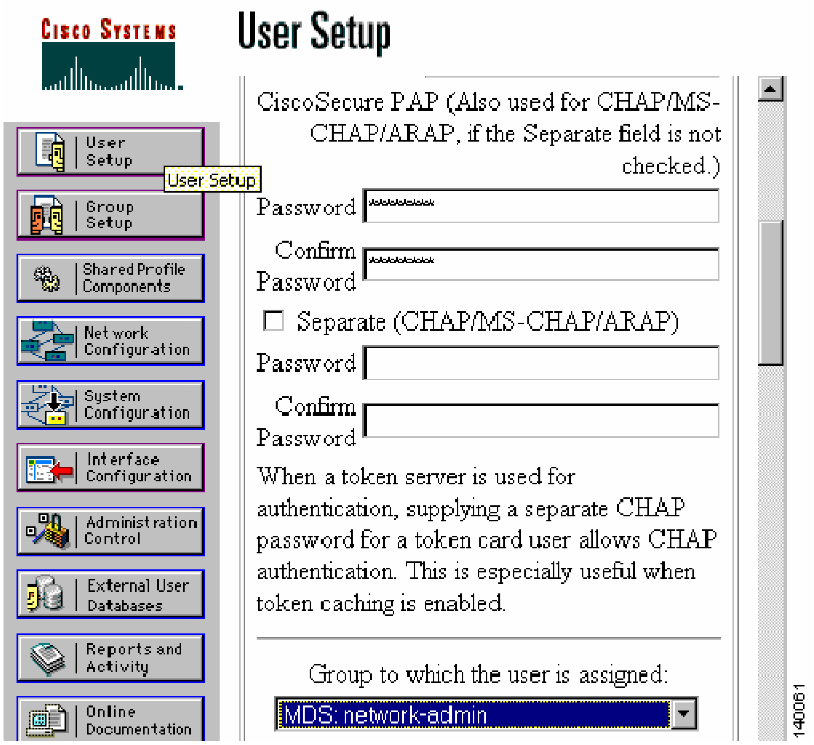
Step 9 Define a user by clicking **User Setup**.

Step 10 Enter a new or existing username and click **Add/Edit.**

Step 11 In the resulting window, enter a password in the Password and Confirm Password fields.

Step 12 Choose a group from **Group to which the user is assigned** as shown in Figure 1-10.

Figure 1-10 Secure ACS Creating TACACS+ User



User Setup

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. This is especially useful when token caching is enabled.

Group to which the user is assigned: MDS: network-admin

The Secure ACS server configuration is complete. You should now configure the Cisco MDS 9000 switch itself, using either the CLI or the SNMP.

Configuring TACACS+ on the Cisco MDS 9000 Switch

To configure TACACS+ on the switch, follow these steps:

Step 1 Enable TACACS+ by entering the following commands:

```
ca-9506# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ca-9506(config)# tacacs+ enable
```

Step 2 Define the TACACS+ server and the shared secret key to use with it.

```
ca-9506(config)# tacacs-server host 172.22.36.10 key WarEagle
```

Step 3 Define a group of authentication servers and add the TACACS+ server to the group.

```
ca-9506(config)# aaa group server tacacs+ tacacs-group1
ca-9506(config-tacacs+)# server 172.22.36.10
```

Step 4 Define the methods for the switch to perform authentication for Telnet/SSH/SNMP access.

```
ca-9506(config)# aaa authentication login default group tacacs-group1
```

The following **show** commands display the configuration:

```
ca-9506# show tacacs-server
timeout value:5
total number of servers:1

following TACACS+ servers are configured:
        172.22.36.10:
                available on port:49
                TACACS+ shared secret:********
ca-9506# show aaa authentication
         default: group tacacs-group1
         console: local
         iscsi: local
         dhchap: local

ca-9506# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin

user:seth
        expires on Fri Jun 18 23:59:59 2004
        roles:network-admin
account created through REMOTE authentication
Local login not possible
```

Note The user (seth) is not available locally on the switch, even though seth is a member of the network-admin group or role. This configuration means the user was authenticated by the TACACS+ server and not by the switch.

Accounting with TACACS+

Cisco Secure ACS server can be leveraged to provide a command history that captures which users performed which actions. This information is similar to the CLI **show accounting log** command. However, by placing logging on a remote system, the logs can be independently examined and are available in case the Cisco MDS 9000 switch is inaccessible. This configuration will build upon the configuration defined in Authentication and Authorization with TACACS+, page 1-5.

Configuring the Cisco MDS 9000 Switch

To configure the Cisco MDS 9000 switch to leverage a TACACS+ server for accounting, follow these steps:

Step 1 Configure the Cisco MDS 9000 switch to use the TACACS-group1 server group.

```
switch# conf t
switch(config)# aaa accounting default group  tacacs-group1 local
```

Step 2 Use the **local** keyword to indicate local logging on the switch if all servers listed in the server group are unavailable. If the server group is available, commands or events will **not** be logged locally.

Configuring Cisco Secure ACS

Because this procedure builds on the configuration defined in Authentication and Authorization with TACACS+, page 1-5, only small modifications need to be made.

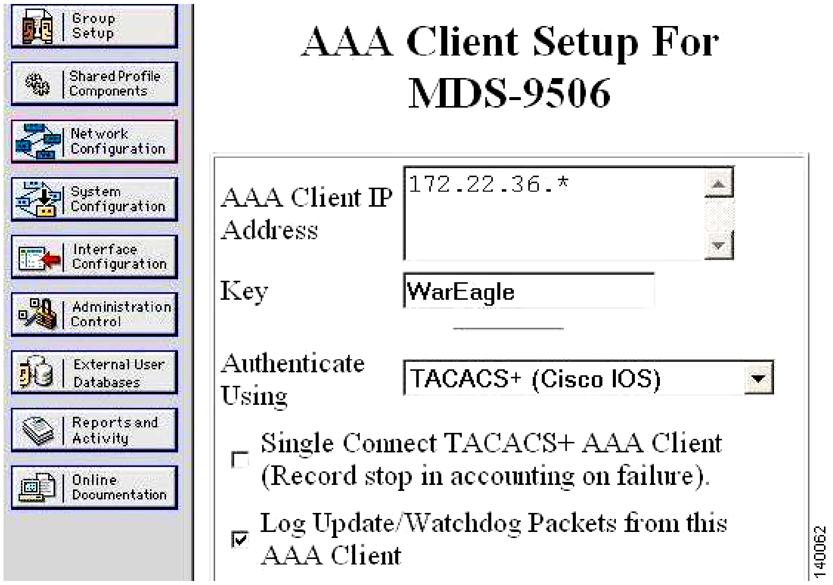
To configure the Secure ACS server to monitor for Update/Watchdog packets, modify the client configuration by following these steps:

Step 1 In Secure ACS, in the left pane, click **Network Configuration**. (See Figure 1-11.)

Step 2 Choose the client to be modified.

Step 3 Check the **Log Update/Watchdog Packets from this AAA Client** check box.

Figure 1-11 Enabling Accounting on the Secure ACS Server



AAA Client Setup For MDS-9506

AAA Client IP Address: 172.22.36.*

Key: WarEagle

Authenticate Using: TACACS+ (Cisco IOS)

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

☑ Log Update/Watchdog Packets from this AAA Client

To configure the Secure ACS to display commands, follow these steps:

Step 1 Click **System Configuration** in the left pane. (See Figure 1-12.)

Step 2 Click **Logging**.

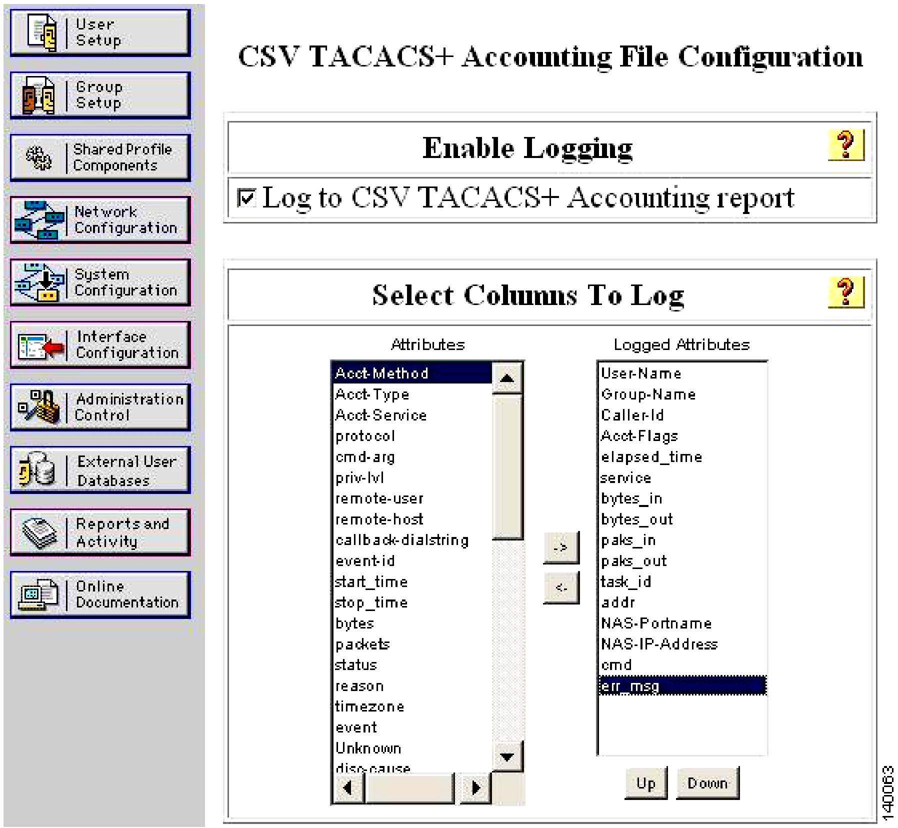
Step 3 Click **CSV TACACS+ Accounting.**

Step 4 Add the column **err_msg**

Step 5 Check the **Log to CSV TACACS+ Accounting report** box.

Step 6 Click **Submit**.

Figure 1-12 Add MDS Command Logging to Report



CSV TACACS+ Accounting File Configuration

Enable Logging

☑ Log to CSV TACACS+ Accounting report

Select Columns To Log

Attributes: Acct-Method, Acct-Type, Acct-Service, protocol, cmd-arg, priv-lvl, remote-user, remote-host, callback-dialstring, event-id, start_time, stop_time, bytes, packets, status, reason, timezone, event, Unknown, disc-cause

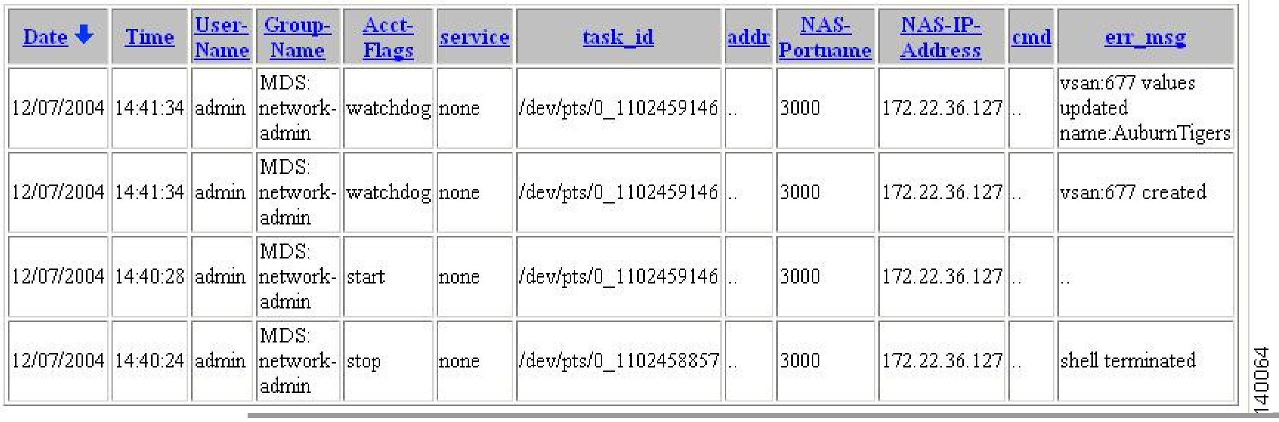
Logged Attributes: User-Name, Group-Name, Caller-Id, Acct-Flags, elapsed_time, service, bytes_in, bytes_out, paks_in, paks_out, task_id, addr, NAS-Portname, NAS-IP-Address, cmd, err_msg

Step 7 Click **Reports and Activity** in the left pane to view the accounting report. (See Figure 1-13.)

Step 8 Click **TACACS+ Accounting.**

Step 9 In the right pane, choose the day to view. The current day is called **TACACS+ Accounting active.csv**.

Figure 1-13 Secure ACS Accounting Log



Date ⬇	Time	User-Name	Group-Name	Acct-Flags	service	task_id	addr	NAS-Portname	NAS-IP-Address	cmd	err_msg
12/07/2004	14:41:34	admin	MDS: network-admin	watchdog	none	/dev/pts/0_1102459146	..	3000	172.22.36.127	..	vsan:677 values updated name:AuburnTigers
12/07/2004	14:41:34	admin	MDS: network-admin	watchdog	none	/dev/pts/0_1102459146	..	3000	172.22.36.127	..	vsan:677 created
12/07/2004	14:40:28	admin	MDS: network-admin	start	none	/dev/pts/0_1102459146	..	3000	172.22.36.127	..	..
12/07/2004	14:40:24	admin	MDS: network-admin	stop	none	/dev/pts/0_1102458857	..	3000	172.22.36.127	..	shell terminated

Providing Access Without a Password

In some instances, you may need to access the Cisco MDS 9000 switch without using a password, by using automated scripts or agents. Providing a null password or hard coding the password into the script or agent may be considered a weak security practice; however, leveraging the private/public key infrastructure associated with SSH maintains a solid and secure environment.

The procedure includes creating the appropriate key on a host and then adding it to a new user. Because SSH leverages a private/public key exchange, the Cisco MDS 9000 switch knows only the public key, while the host knows both the public and private keys.

Tip Assign logins without passwords to either a read-only role like network-operator or to a role with a minimal set of privileges.

Warning **Having only the public key does not cause the Cisco MDS 9000 switch to grant access to a user; the private key is required to be on the host. The private key should be guarded or treated like a password.**

To set up a read-only (network-operator) based account that only allows access if the user comes from a host that knows both the public and private keys, follow these steps:

Step 1 On the host, create a SSH rsa1 public/private key:

```
$ /usr/bin/ssh-keygen -t rsa1
Generating public/private rsa1 key pair.
Enter file in which to save the key (/users/testuser/.ssh/identity):
/users/setmason/.ssh/identity already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /users/testuser/.ssh/identity.
Your public key has been saved in /users/testuser/.ssh/identity.pub.
The key fingerprint is:
c2:4d:6d:26:21:9d:79:9b:c3:86:dc:a5:07:d2:62:d4 testuser@host
```

On the host, the file /users/testuser/.ssh/identity.pub is the SSH public key that is encrypted using the rsa1 algorithm. The contents of this file are used in the creation of the Cisco MDS 9000 switch user. In this example, the file looks like this:

```
$ cat /users/testuser/.ssh/identity.pub
1024 35
139198677264732164858153476357747926024656548233745027006381178621992083524037906211714241
450436547019604214530354070873624269283640613058470615170649963414635036859628344005142227
886318134122126153182906740418449098047827961768214148936752631482459130056603268404256522
191410368204629699075809390037814979061 testuser@host
```

Step 2 On the Cisco MDS 9000 switch, create all of the SSH keys, even though in this case the client is using rsa1.

```
172.22.36.11# conf t
Enter configuration commands, one per line.  End with CNTL/Z.

172.22.36.11(config)# ssh key rsa1
generating rsa1 key(1024 bits).....
generated rsa1 key
```

```
ca-9506(config)# ssh key dsa
generating dsa key(1024 bits).....
generated dsa key

ca-9506(config)# ssh key rsa
generating rsa key(1024 bits).....
generated rsa key
```

Step 3 Enable SSH on the Cisco MDS 9000 switch.

```
172.22.36.11(config)# ssh server enable
```

Step 4 On the Cisco MDS 9000 switch, create the user by pasting the contents of the identity.pub file after the sshkey parameter:

```
172.22.36.11# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
172.22.36.11(config)# username testuser role network-operator
warning: password for user:setmason not set. S/he cannot login currently
172.22.36.11(config)# username testuser sshkey 1024 35
139198677264732164858153476357747926024656548233745027006381178621992083524037906211714241
450436547019604214530354070873624269283640613058470615170649963414635036859628344005142227
886318134122126153182906740418449098047827961768214148936752631482459130056603268404256522
191410368204629699075809390037814979061 testuser@host
172.22.36.11(config)# end
```

Step 5 Use the following commands to list the user configuration:

```
172.22.36.11# show user-account testuser
user: testuser
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS/TACACS+ is possible
        ssh public key: 1024 35 139198677264732164858153476357747926024656548233
74502700638117862199208352403790621171424145043654701960421453035407087362426928
36406130584706151706499634146350368596283440051422278863181341221261531829067404
18449098047827961768214148936752631482459130056603268404256522191410368204629699
075809390037814979061 testuser@host
```

Step 6 Test the login process from the host:

```
$ ssh testuser@172.22.36.11
Warning: Remote host denied X11 forwarding.
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2004, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.
172.22.36.11#
```

If the same user tries logging in from another host that does not have both the private key file (/users/testuser/.ssh/identity) and the public key file (/users/testuser/.ssh/identity), the user will be denied access to the Cisco MDS 9000 switch. The fact that the public key has testuser@host at the end, does not tie it to a specific host, but allows an admin to determine which host it was generated from.

Tip A simple method to leverage this feature is to set up a scheduled backup, for example using cron, to back up the switch configuration on a nightly basis using SSH and TFTP.

Step 7 Set up the backup with the following commands on a host, provided the user has the privileges to issue the **copy** command:

```
#!/bin/sh
#####################################################
#
#/usr/local/bin/backup_mds_config.sh

# This is used for a cron entry. No arguments are
# allowed in cron.Absolute paths to commands must
# be specified to ssh for it to work properly
# ssh key exchange must be separately configured
# for the account "USER"
#
# Adjust the variables for your host and switch
######################################################

DIR=/mds_config
DATE=`date "+%m%d%y_%H%M%S"`
SWITCH_NAME=beat_bama
FILE=$SWITCH_NAME"_run_cfg_"$DATE
USER=cwilliams
COMMAND1="copy running-config startup-config’
COMMAND2="show startup-config"

#Copy running to startup-config
/usr/local/bin/ssh -l $USER $SWITCH_NAME $COMMAND1
#Backup MDS config to local file
/usr/local/bin/ssh -l $USER $SWITCH_NAME $COMMAND2 > $DIR/$FILE
```

The cron job that executes the script must be run by the user specified in the script. Configure the crontab for the user:

```
#Backup MDS config:
00  11  29 4 * /usr/local/bin/backup_mds_config.sh > /tmp/mds_log1
```