CHAPTER 28

Configuring RADIUS and TACACS+

The authentication, authorization, and accounting (AAA) mechanism verifies the identity of, grants access to, and tracks the actions of users managing a switch. All Cisco MDS 9000 Family switches use Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols to provide solutions using remote AAA servers.

Based on the user ID and password combination provided, switches perform local authentication or authorization using the local database or remote authentication or authorization using AAA server(s). A preshared secret key provides security for communication between the switch and AAA servers. This secret key can be configured for all AAA server or for only a specific AAA server. This security mechanism provides a central management capability for AAA servers.

This chapter includes the following sections:

Switch Management Security

Management security in any switch in the Cisco MDS 9000 Family provides security to all management access methods including the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

CLI Security Options

You can access the CLI using the console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console or Telnet and SSH), you can configure one or more of the following security control options: local, remote (RADIUS or TACACS+), or none.

- Remote security control
  - Using Remote Authentication Dial-In User Services (RADIUS). See the "Configuring RADIUS" section on page 28-5.
  - Using Terminal Access Controller Access Control System plus (TACACS+). See the "Configuring TACACS+" section on page 28-10.
- Local security control. See the "Local AAA Services" section on page 28-19.

These security mechanisms can also be configured for the following scenarios:

- iSCSI authentication (see the "Authentication Mechanism" section on page 35-23).
- Fibre Channel Security Protocol (FC-SP) authentication (see the Chapter 31, "Configuring FC-SP and DHCHAP")

SNMP Security Options

The SNMP agent supports security features for SNMPv1,SNMPv 2c, and SNMPv3. Normal SNMP security mechanisms apply to all applications that use SNMP (for example, Cisco MDS 9000 Fabric Manager).

CLI security options also apply to the Cisco MDS Fabric Manager and Device Manager.

See Chapter 27, "Configuring SNMP".

Refer to the *Cisco MDS 9000 Family Fabric Manager Configuration Guide* for information on the Cisco MDS Fabric or Device Managers.

Switch AAA Functionalities

Using the CLI or an SNMP application, you can configure authentication, authorization, and accounting (AAA) switch functionalities on any switch in the Cisco MDS 9000 Family.

Authentication

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. Cisco MDS 9000 Family switches allow you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

Note When you log in to a Cisco MDS switch successfully using the Fabric Manager or Device Manager via Telnet or SSH and if that switch is configured for AAA server-based authentication, a temporary SNMP user entry is automatically created with an expiry time of one day. The SNMPv3 protocol data units (PDUs) with your Telnet/SSH login name as the SNMPv3 user are authenticated by the switch. The management station can temporarily use the Telnet/SSH login name as the SNMPv3 `auth` and `priv` passphrase. This temporary SNMP login is only allowed if you have one or more active MDS Shell sessions. If you do not have an active session at any given time, your login is deleted and you will not be allowed to perform SNMP v3 operations.

Authorization

By default, two roles exist in all Cisco MDS switches:

- Network operator (**`network-operator`**)—Has permission to view the configuration only. The operator cannot make any configuration changes.
- Network administrator (**`network-admin`**)— Has permission to execute all commands and make configuration changes. The administrator can also create and customize up to 64 additional roles.

If you use a SAN Volume Controller (SVC) setup, two more default roles exist in all Cisco MDS switches:

- SVC administrator (**svc-admin**)— Has permission to view the entire configuration and make SVC-specific configuration changes within the `switch(svc)` prompt.
- SVC operator (**svc-operator**)—Has permission to view the entire configuration. The operator cannot make any configuration changes.

Note Refer to the *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide* for more information on SVC.

These four default roles cannot be changed or deleted. You can create additional roles and configure the following options:

- Configure role-based authorization by assigning user roles locally or using remote AAA servers.
- Configure user profiles on a remote AAA server to contain role information. This role information is automatically downloaded and used when the user is authenticated through the remote AAA server.

Note If a user only belongs to one of the newly-created roles and that role is subsequently deleted, then the user immediately defaults to the network-operator role.

Accounting

The accounting feature tracks and maintains a log of every management session used to access the switch. This information can be used to generate reports for troubleshooting and auditing purposes. Accounting logs can be stored locally or sent to remote AAA servers.

Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over AAA servers:

- It is easier to manage user password lists for each switch in the fabric.
- AAA servers are already deployed widely across enterprises and can be easily adopted.
- Easier to manage.
- Accounting log for all switches in the fabric can be centrally managed.
- Easier to manage user role mapping for each switch in the fabric.

Remote Authentication Guidelines

When you prefer using remote AAA servers, follow these guidelines:

- A minimum of one AAA server should be IP reachable.
- Be sure to configure a desired local AAA policy as this policy is used if all AAA servers are not reachable.
- AAA servers are easily reachable if an overlay Ethernet LAN is attached to the switch (see Chapter 37, “Configuring IP Storage”). This is the recommended method.
- SAN networks connected to the switch should have at least one gateway switch connected to the Ethernet LAN reaching the AAA servers.

Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups. A server group is a set of remote AAA servers implementing the same AAA protocol. The purpose of a server group is to provide for fail-over servers in case a remote AAA server fails to respond. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fails to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Cisco MDS switch encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Service Configuration Options

AAA configuration in Cisco MDS 9000 Family switches is service based. You can have separate AAA configurations for the following services

- Telnet or SSH login (Cisco MDS Fabric Manager and Device Manager login).
- Console login.
- iSCSI authentication (see the “Authentication Mechanism” section on page 35-23).
- FC-SP authentication (see Chapter 31, “Configuring FC-SP and DHCHAP”).
- Accounting.

In general, server group, local, and none are the three options that can be specified for any service in an AAA configuration. Each option is tried in the order specified. If all the methods fail, local is tried.

Caution Cisco MDS SAN-OS does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric username exists on an AAA server and is entered during login, the user is not logged in.

Note Even if local is not specified as one of the options, it is tried when all other configured options fail.

Table 28-1 provides the related CLI command for each AAA service configuration option.

Table 28-1 AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
Telnet or SSH login (Cisco MDS Fabric Manager and Device Manager login)	**aaa authentication login default**
Console login	**aaa authentication login console**
iSCSI authentication	**aaa authentication iscsi default**
FC-SP authentication	**aaa authentication dhchap default**
Accounting	**aaa accounting default**

Error-Enabled Status

When you log in, the login is processed by rolling over to local user database if the remote AAA servers do not respond. In such cases, the following message is displayed on the user's terminal—if you have enabled the error-enabled feature:

```
Remote AAA servers unreachable; local authentication done.
```

To enable this message display, use the **aaa authentication login error-enable** command.

To disable this message display, use the **no aaa authentication login error-enable** command.

To view the current display status, use the **show aaa authentication login error-enable** command (see Example 28-6).

Example 28-1 Displays AAA Authentication Login Information

```
switch# show aaa authentication login error-enable
enabled
```

Configuring RADIUS

Cisco MDS 9000 Family switches can use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers and server groups and set timeout and retry counts.

This section defines the RADIUS operation, identifies its network environments, and describes its configuration possibilities.

RADIUS is a distributed client/server protocol that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS 9000 Family switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Setting the RADIUS Server Address

You can add up to 64 RADIUS servers. RADIUS keys are always stored in encrypted form in persistent storage. The running configuration also displays encrypted keys.

To specify the host RADIUS server address and the options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host 10.10.0.0 key HostKey`	Specifies the preshared key for the selected RADIUS server. This key overrides the key assigned using the **radius-server key** command. In this example, the host is IP address 10.10.0.0 and the key is HostKey.
Step 3	`switch(config)# radius-server host 10.10.0.0 auth-port 2003`	Specifies the destination UDP port number to which the RADIUS authentication messages should be sent. In this example, the host is IP address 10.10.0.0 and the authentication port is 2003. The default authentication port is 1812, and the valid range is 0 to 65366.
Step 4	`switch(config)# radius-server host 10.10.0.0 acct-port 2004`	Specifies the destination UDP port number to which RADIUS accounting messages should be sent. The default accounting port is 1813, and the valid range is 0 to 65366.
Step 5	`switch(config)# radius-server host 10.10.0.0 accounting`	Specifies this server to be used only for accounting purposes. **Note** If neither the **authentication** nor the **accounting** options are specified, the server is used for both accounting and authentication purposes.
Step 6	`switch(config)# radius-server host radius2 key 0 abcd`	Specifies a clear text key for the specified server. The key is restricted to 64 characters.
	`switch(config)# radius-server host radius3 key 4 da3Asda2ioyuoiuH`	Specifies a encrypted key for the specified server. The key is restricted to 64 characters.

Setting the Global Preshared Key

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 64 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch.

You can override this global key assignment by explicitly using the **key** option in the **radius-server host** command.

To set the RADIUS preshared key, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server key AnyWord`	Configures a preshared key (AnyWord) to authenticate communication between the RADIUS client and server. The default is clear text.
	`switch(config)# radius-server key 0 AnyWord`	Configures a preshared key (AnyWord) specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server.
	`switch(config)# radius-server key 7 abe4DFeeweo00o`	Configures a preshared key (specified in encrypted text) specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.

Setting the RADIUS Server Timeout Interval

To specify the time between retransmissions to the RADIUS servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server timeout 30`	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default timeout is one (1) second. The time ranged from 1 to 60 seconds.
	`switch(config)# no radius-server timeout 30`	Reverts the transmission time to its default (1) second.

Setting Iterations of the RADIUS Server

By default, a switch retries a RADIUS server only once. This number can be configured. The maximum is five retries per server.

You can revert the retry number to its default by issuing the **no radius-server retransmit** command.

To specify the number of times that RADIUS servers should try to authenticate a user, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server retransmit 3`	Configures the number of times (3) the switch tries to connect to a RADIUS server(s) before reverting to local authentication.

Defining Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for

general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named `cisco-avpair`. The value is a string with the following format:

```
protocol : attribute sep value *
```

Where `protocol` is a Cisco attribute for a particular type of authorization, and `sep` is `=` for mandatory attributes, and `*` is for optional attributes.

When you use RADIUS servers to authenticate yourself to a Cisco MDS 9000 Family switch, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

The following VSA protocol options are supported by the Cisco SAN-OS software:

- `Shell` protocol—used in access-accept packets to provide user profile information.
- `Accounting` protocol—used in accounting-request packets. If a value contains any white spaces, it should be put within double quotation marks.

The following attributes are supported by the Cisco SAN-OS software:

- `roles`–This attribute lists all the roles to which the user belongs. The value field is a string storing the list of group names delimited by white space. For example, if you belong to roles `vsan-admin` and `storage-admin`, the value field would be "`vsan-admin storage-admin`." This subattribute is sent in the VSA portion of the Access-Accept frames from the RADIUS server, and it can only be used with the shell protocol value. These are two examples using the roles attribute:

  ```
  shell:roles="network-admin vsan-admin"
  shell:roles*"network-admin vsan-admin"
  ```

  When an VSA is specified as `shell:roles*"network-admin vsan-admin"`, this VSA is flagged as an optional attribute, and other Cisco devices ignore this attribute.

- `accountinginfo`—This attribute stores additional accounting information besides the attributes covered by a standard RADIUS accounting protocol. This attribute is only sent in the VSA portion of the Account-Request frames from the RADIUS client on the switch, and it can only be used with the accounting protocol-related PDUs.

Specifying SNMPv3 on AAA Servers

The vendor/custom attribute `cisco-av-pair` can be used to specify user's role mapping using the format:

```
shell:roles="roleA roleB …"
```

If the roll option in the `cisco-av-pair` attribute is not set, the default user role is network-operator.

The VSA format optionally specifies your SNMPv3 authentication and privacy protocol attributes also as follows:

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The privacy protocol options are AES-128 and DES. If these options are not specified in the `cisco-av-pair` attribute on the ACS server, MD5 and DES are used by default.

Displaying RADIUS Server Details

Use the **show radius-server** command to display configured RADIUS parameters (see Example 28-2).

Example 28-2 Displays Configured RADIUS Information

```
switch# show radius-server
Global RADIUS shared secret:*******
retransmission count:5
timeout value:10
following RADIUS servers are configured:
        myradius.cisco.users.com:
                available for authentication on port:1812
                available for accounting on port:1813
        172.22.91.37:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
```

Example 28-3 Displays Configured RADIUS Server-Group Order

```
switch# show radius-server groups
total number of groups:4
following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group Group1:
                server: Server3 on auth-port 1812, acct-port 1813
                server: Server5 on auth-port 1812, acct-port 1813
        group Group5:
```

Configuring TACACS+

A Cisco MDS switch uses the Terminal Access Controller Access Control System Plus (TACACS+) protocol to communicate with remote AAA servers. You can configure multiple TACACS+ servers and set timeout values.

About TACACS+

TACACS+ is a client/server protocol that uses TCP (TCP port 49) for transport requirements. All switches in the Cisco MDS 9000 Family provide centralized authentication using the TACACS+ protocol. The addition of TACACS+ support in Cisco SAN-OS 1.3 enables the following advantages over RADIUS authentication:

- Provides independent, modular AAA facilities. Authorization can be done without authentication.
- TCP transport protocol to send data between the AAA client and server, using reliable transfers with a connection-oriented protocol.
- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality. The RADIUS protocol only encrypts passwords.

Enabling TACACS+

By default, the TACACS+ feature is disabled in all switches in the Cisco MDS 9000 Family. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for fabric authentication. When you disable this feature, all related configurations are automatically discarded.

To enable TACACS+ for a Cisco MDS switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ enable`	Enables the TACACS+ in this switch.
	`switch(config)# no tacacs+ enable`	Disables (default) the TACACS+ in this switch.

Setting the TACACS+ Server Address

If a secret key is not configured for a configured server, a warning message is issued if a global key is not configured. If a server key is not configured, the global key (if configured) is used for that server (see the "Setting the Global Secret Key" section on page 28-11).

Note Prior to Cisco MDS SAN-OS Release 2.1(2), you can use the dollar sign ($) in the key but the key must be enclosed in double quotes, for example "k$". The percent sign (%) is not allowed. In Cisco MDS SAN-OS Release 2.1(2) and later, you can use the dollar sign ($) (without double quotes) and the percent sign (%) in global secret keys.

To configure the TACACS+ server option, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host 171.71.58.91` `warning: no key is configured for the host`	Configures the TACACS+ server identified by the specified IPv4 address.
	`switch(config)# no tacacs-server host 10.10.1.0`	Deletes the specified TACACS+ server identified by the IPv4 address. By default, no server is configured.
	`switch(config)# tacacs-server host 2001::db8:800:200c:417a/64` `warning: no key is configured for the host`	Configures the TACACS+ server identified by the specified IPv6 address.
	`switch(config)# no tacacs-server host 2001::db8:800:200c:417a/64`	Deletes the specified TACACS+ server identified by the IPv6 address. By default, no server is configured.
Step 3	`switch(config)# tacacs-server host 171.71.58.91 port 2`	Configures the TCP port for all TACACS+ requests.
	`switch(config)# no tacacs-server host 171.71.58.91 port 2`	Reverts to the factory default of using Port 49 for server access.
Step 4	`switch(config)# tacacs-server host host1.cisco.com key MyKey`	Configures the TACACS+ server identified by the specified domain name and assigns the secret key.
Step 5	`switch(config)# tacacs-server host host100.cisco.com timeout 25`	Configures the timeout period for the switch to wait for a response from the specified server before it declares a timeout failure.

Setting the Global Secret Key

You can configure global values for the secret key for all TACACS+ servers.

Note If secret keys are configured for individual servers, those keys override the globally configured key.

Note Prior to Cisco MDS SAN-OS Release 2.1(2), you can use the dollar sign ($) in the key but the key must be enclosed in double quotes, for example “k$”. The percent sign (%) is not allowed. In Cisco MDS SAN-OS Release 2.1(2) and later, you can use the dollar sign ($) (without double quotes) and the percent sign (%) in global secret keys.

To set the secret key for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

	Command	Purpose
Step 2	`switch(config)# tacacs-server key 7 3sdaA3daKUngd`	Assigns the global secret key (in encrypted format) to access the TACACS+ server. This example specifies **7** to indicate the encrypted format being used. If this global key and the individual server keys are not configured, clear text messages are sent to the TACACS+ server(s).
	`switch(config)# no tacacs-server key oldPword`	Deletes the configured global secret key to access the TACACS+ server and reverts to the factory default of allowing access to all configured servers.

Setting the Timeout Value

You can configure global timeout values for all TACACS+ servers.

Note If timeout values are configured for individual servers, those values override the globally configured values.

To set the global timeout value for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server timeout 30`	Configures the global timeout period for the switch to wait for a response from all servers before it declares a timeout failure.
	`switch(config)# no tacacs-server timeout 30`	Deletes the configured timeout period and reverts to the factory default of 5 seconds.

Defining Custom Attributes for Roles

Cisco MDS 9000 Family switches use the TACACS+ custom attribute for service shells to configure roles to which a user belongs. TACACS+ attributes are specified in `name=value` format. The attribute name for this custom attribute is `cisco-av-pair`. The following example illustrates how to specify roles using this attribute:

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

You can also configure optional custom attributes to avoid conflicts with non-MDS Cisco switches using the same AAA servers.

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

Additional custom attribute shell:roles are also supported:

```
shell:roles="network-admin vsan-admin"
```

or

```
shell:roles*"network-admin vsan-admin"
```

Note TACACS+ custom attributes can be defined on an Access Control Server (ACS) for various services (for example, shell). Cisco MDS 9000 Family switches require the TACACS+ custom attribute for the service shell to be used for defining roles.

Supported TACACS+ Servers

The Cisco SAN-OS software currently supports the following parameters for the listed TACACS+ servers:

- TACACS+

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

- Cisco ACS TACACS+

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

- Open TACACS+

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

Displaying TACACS+ Server Details

Use the **show tacacs+** commands to display configurations for the TACACS+ protocol configuration in all switches in the Cisco MDS 9000 Family (see Examples 28-4 to 28-8).

Example 28-4 Displays Configured TACACS+ Server Information

```
switch# show tacacs-server
Global TACACS+ shared secret:***********
timeout value:30
total number of servers:3

following TACACS+ servers are configured:
        171.71.58.91:
                available on port:2
        cisco.com:
                available on port:49
        171.71.22.95:
                available on port:49
                TACACS+ shared secret:*****
```

Example 28-5 Displays AAA Authentication Information

```
switch# show aaa authentication
         default: group TacServer local none
         console: local
         iscsi: local
         dhchap: local
```

Example 28-6 Displays AAA Authentication Login Information

```
switch# show aaa authentication login error-enable
enabled
```

Example 28-7 Displays Configured TACACS+ Server Groups

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
        group TacacsServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

Example 28-8 Displays All AAA Server Groups

```
switch# show aaa groups
radius
TacServer
```

Configuring Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the same protocol, either RADIUS or TACACS+. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to a AAA service. You configure AAA policies for CLI users or Fabric Manager or Device Manager users.

To specify the TACACS+ server order within a group, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa group server tacacs+ TacacsServer1` `switch(config-tacacs+)#`	Creates a server group named TacacsServer1 and enters the submode for that group.
	`switch(config)# no aaa group server tacacs+ TacacsServer19`	Deletes the server group called TacacsServer19 from the authentication list.
Step 3	`switch(config-tacacs+)# server ServerA`	Configures ServerA to be tried first within the server group called the TacacsServer1. **Tip** If the specified TACACS+ server is not found, configure it using the **tacacs-server host** command and retry this command.
Step 4	`switch(config-tacacs+)# server ServerB`	Configures ServerB to be tried second within TacacsServer1.
	`switch(config-tacacs+)# no server ServerZ`	Deletes ServerZ within the TacacsServer1 list of servers.

To verify the configured server group order, use the **show tacacs-server groups** command:

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
        group TacacsServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

Distributing AAA Server Configuration

Configuration for RADIUS and TACACS+ AAA on a MDS switch can be distributed using the Cisco Fabric Services (CFS). The distribution is disabled by default (see Chapter 5, "Using the CFS Infrastructure").

After enabling the distribution, the first server or global configuration starts an implicit session. All server configuration commands entered thereafter are stored in a temporary database and applied to all switches in the fabric (including the originating one) when you explicitly commit the database. The various server and global parameters are distributed, except the server and global keys. These keys are unique secrets to a switch and should not be shared with other switches.

Note Server group configurations are not distributed.

Enabling the RADIUS Server Distribution

Only switches where distribution is enabled can participate in the distribution activity.

To enable RADIUS server distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius distribute`	Enables RADIUS configuration distribution in this switch.
	`switch(config)# no radius distribute`	Disables RADIUS configuration distribution in this switch (default).

To enable TACACS+ server distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ distribute`	Enables TACACS+ configuration distribution in this switch.
	`switch(config)# no tacacs+ distribute`	Disables TACACS+ configuration distribution in this switch. (default)

Starting a Distribution Session on a Switch

A distribution session starts the moment you begin a RADIUS/TACACS+ server or global configuration. For example, the following tasks start an implicit session:

- Specifying the global timeout for RADIUS servers.
- Specifying the global timeout for TACACS+ servers.

Note After you issue the first configuration command related to AAA servers, all server and global configurations made (including the configuration that caused the distribution session start) are stored in a temporary buffer—not in the running configuration.

To specify the global timeout and start an implicit session for RADIUS servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server timeout 30`	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default timeout is one (1) second. The time range in seconds is 1 to 60.

To specify the global timeout and start an implicit session for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server timeout 30`	Configures the global timeout period for the switch to wait for a response from all servers before it declares a timeout failure.
	`switch(config)# no tacacs-server timeout 30`	Deletes the configured timeout period and reverts to the factory default of 5 seconds.

Displaying the Session Status

Once the implicit distribution session has started, you can check the session status using the **show radius distribution status** command.

```
switch# show radius distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

Once the implicit distribution session has started, you can check the session status using the **show tacacs+ distribution status** command.

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

Displaying the Configuration to Be Distributed

To display the RADIUS global and/or server configuration stored in the temporary buffer, use the **show radius pending** command.

```
switch(config)# show radius pending-diff
   +radius-server host testhost1 authentication accounting
   +radius-server host testhost2 authentication accounting
```

To display the TACACS+ global and/or server configuration stored in the temporary buffer, use the **show tacacs+ pending** command.

```
switch(config)# show tacacs+ pending-diff
   +tacacs-server host testhost3
   +tacacs-server host testhost4
```

Committing the Distribution

The RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer can be applied to the running configuration across all switches in the fabric (including the originating switch).

To commit RADIUS configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius commit`	Commits the RADIUS configuration changes to the running configuration.

To commit TACACS+ configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ commit`	Commits the TACACS+ configuration changes to the running configuration.

Discarding the Distribution Session

Discarding the distribution of a session-in-progress causes the configuration in the temporary buffer to be dropped. The distribution is no applied.

To discard the RADIUS session-in-progress distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius abort`	Discard the RADIUS configuration changes to the running configuration.

To discard the TACACS+ session-in-progress distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ abort`	Discard the TACACS+ configuration changes to the running configuration.

Clearing Sessions

To clear the ongoing CFS distribution session (if any) and to unlock the fabric for the RADIUS feature, issue the **clear radius session** command from any switch in the fabric.

```
switch# clear radius session
```

To clear the ongoing CFS distribution session (if any) and to unlock the fabric for the TACACS+ feature, issue the **clear tacacs+ session** command from any switch in the fabric.

```
switch# clear tacacs+ session
```

Merge Guidelines for RADIUS and TACACS+ Configurations

The RADIUS and TACACS+ server and global configuration are merged when two fabrics merge. The merged configuration is applied to CFS distribution-enabled switches.

When merging the fabric, be aware of the following conditions:

- The server groups are not merged
- The server and global keys are not changed during merge
- The merged configuration contains all servers found on all CFS enabled switches
- The timeout and retransmit parameters of the merged configuration are the largest values found per server and global.

Caution If there is a conflict between two switches in the server ports configured, the merge fails.

Use the **show radius distribution status** command to view the status of the RADIUS fabric merge (see Example 28-9).

Example 28-9 Displays the RADIUS Fabric Merge Status

```
switch# show radius distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge response received
merge error: conflict: server dmtest2 has auth-port 1812 on this switch and 1999
on remote

last operation: enable
last operation status: success
```

Use the **show tacacs+ distribution status** command to view the status of the TACACS+ fabric merge (see Example 28-10).

Example 28-10 Displays the TACACS+ Fabric Merge Status

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done

last operation: enable
last operation status: success
```

Local AAA Services

The system maintains the user name and password locally and stores the password information in encrypted form. You are authenticated based on the locally stored user information.

Use the **username** command to configure local users and their roles (see the "Creating or Updating Users" section on page 26-11).

Use the **show accounting log** command to view the local accounting log (see Example 28-11).

Example 28-11 Displays the Accounting Log Information

```
switch# show accounting log

Sat Jan 24 03:22:06 1981:stop:snmp_349154526_171.71.58.69:admin:
Sat Jan 24 03:22:06 1981:start:snmp_349154526_171.71.58.69:admin:
Sat Jan 24 03:22:06 1981:update:snmp_349154526_171.71.58.69:admin:Added member [
 WWN: 21:00:00:20:37:a6:be:00 ID: 2] to zone test-27 on VSAN 1
...
Sat Jan 24 23:59:56 1981:stop:/dev/pts/0_349228792:root:shell terminated
Sun Jan 25 00:00:06 1981:start:/dev/pts/1_349228806:admin:
```

Disabling AAA Authentication

You can turn off password verification using the **none** option. If you configure this option, users can login without giving a valid password. But the user should at least exist locally on the Cisco MDS 9000 Family switch.

Caution Use this option cautiously. If configured, any user will be able to access the switch at any time.

Use the **none** option in the **aaa authentication login** command to disable password verification.

A user created using the **username** command will exist locally on the Cisco MDS 9000 Family switch.

Displaying AAA Authentication

The **show aaa authentication** command displays the configured authentication methods (see Example 28-12).

Example 28-12 Example 16-8 Displays Authentication Information

```
switch# show aaa authentication

    No AAA Authentication
    default: group TacServer local none
    console: local none
    iscsi: local
    dhchap: local
```

Authentication and Authorization Process

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. The Cisco MDS 9000 Family switches allow you to perform local authentication (using the lookup database) or remote authentication (using one or more RADIUS servers or TACACS+ servers).

Figure 28-1 shows a flow chart of the process. The following steps explain the authorization and authentication process.

Step 1 When you can log in to the required switch in the Cisco MDS 9000 Family, you can use the Telnet, SSH, Fabric Manager/Device Manager, or console login options.

Step 2 When you have configured server groups using the server group authentication method, an authentication request is sent to the first AAA server in the group.

- If the AAA server fails to respond, then the next AAA server is tried and so on until the remote server responds to the authentication request.
- If all AAA servers in the server group fail to respond, then the servers in the next server group are tried.
- If all configured methods fail, then the local database is used for authentication.

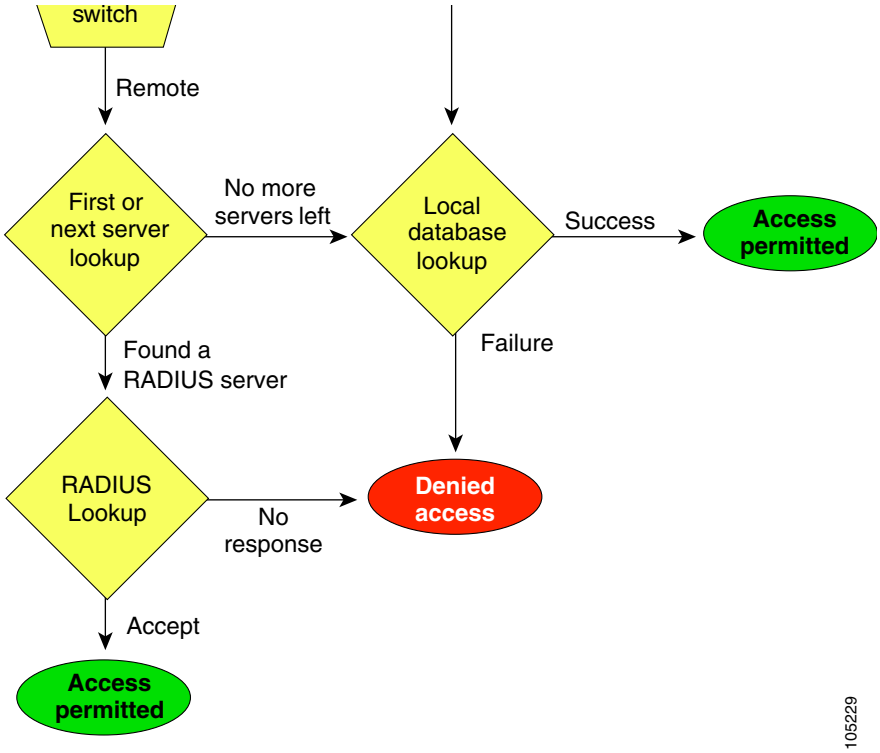
Step 3 If you are successfully authenticated through a remote AAA server, then the following possibilities apply.

- If AAA server protocol is RADIUS, then user roles specified in the `cisco-av-pair` attribute are downloaded with an authentication response.
- If AAA server protocol is TACACS+, then another request is sent to the same server to get the user roles specified as custom attributes for the shell.

- If user roles are not successfully retrieved from the remote AAA server, then the user is assigned the network-operator role.

Step 4 If your user name and password are successfully authenticated locally, you are allowed to log in, and you are assigned the roles configured in the local database.

Figure 28-1 Switch Authorization and Authentication Flow



Note No more server groups left = no response from any server in all server groups.
No more servers left = no response from any server within this server group.

Tip In Step 1, use the **aaa authentication login default** command to configure policies for using Telnet, SSH, or Fabric Manager/Device Manager and the **aaa authentication login console** command to configure AAA policies using the console. If the **aaa authentication login console** command is not configured for console login, the software automatically uses policies used by the **aaa authentication login default** command.

Configuring Accounting Services

Accounting refers to the log information that is kept for each management session in a switch. This information may be used to generate reports for troubleshooting and auditing purposes. Accounting can be implemented locally or remotely (using RADIUS). The default maximum size of the accounting log is 250,000 bytes and cannot be changed.

Tip The Cisco MDS 9000 Family switch uses interim-update RADIUS accounting-request packets to communicate accounting log information to the RADIUS server. The RADIUS server must be appropriately configured to log the information communicated in these packets. Several servers typically have log update/watchdog packets flags in the AAA client configuration. Turn on this flag to ensure proper RADIUS accounting.

Note Configuration operations are automatically recorded in the accounting log if they are performed in configuration mode. Additionally, important system events (for example, configuration save and system switchover) are also recorded in the accounting log.

Displaying Accounting Configuration

The **show accounting** command displays configured accounting information. See Examples 28-13 to 28-15. To specify the size of the local accounting log to be displayed, use the **show accounting log** command. By default about 250KB of accounting log is displayed.

Example 28-13 Displays Two Samples of Configured Accounting Parameters

```
switch# show accounting config
show aaa accounting
                default: local

switch# show aaa accounting
                default: group rad1
```

Example 28-14 Displays 60,000 Bytes of the Accounting Log

```
switch# show accounting log 60000
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
...
```

Example 28-15 Displays the Entire Log File.

```
switch# show accounting log
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:17 1981:stop:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:start:snmp_348530298_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:stop:snmp_348530298_171.71.150.105:admin:
...
Fri Jan 16 23:37:02 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 23:37:26 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Fri Jan 16 23:53:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server3
Fri Jan 16 23:54:00 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server5
Fri Jan 16 23:54:22 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerA
Fri Jan 16 23:54:25 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerB
Fri Jan 16 23:55:03 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Sat Jan 17 00:01:41 1981:start:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:41 1981:stop:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:start:snmp_348537702_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:stop:snmp_348537702_171.71.58.100:admin:
...
```

Clearing Accounting Logs

To clear out the contents of the current log, use the **clear accounting log** command.

```
switch# clear accounting log
```

Configuring Cisco ACS Servers

The Cisco Access Control Server (ACS) uses TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment.When using the AAA server, user management is normally done using Cisco ACS. Figure 28-2, Figure 28-3, Figure 28-4, and Figure 28-5 display ACS server user setup configurations for network-admin roles and multiple roles using either TACACS+ or RADIUS.

Caution Cisco MDS SAN-OS does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric username exists on an AAA server and is entered during login, the user is not logged in.

Figure 28-2 Configuring the network-admin Role When Using RADIUS

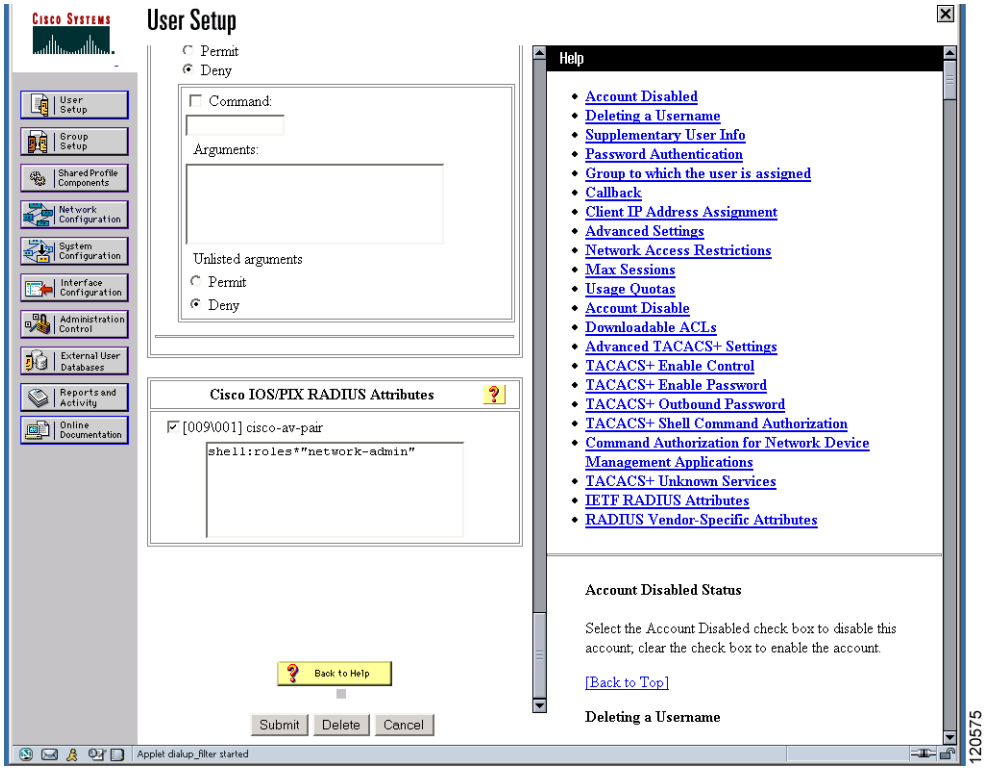


Figure 28-3 Configuring Multiple Roles with SNMPv3 Attributes When Using RADIUS

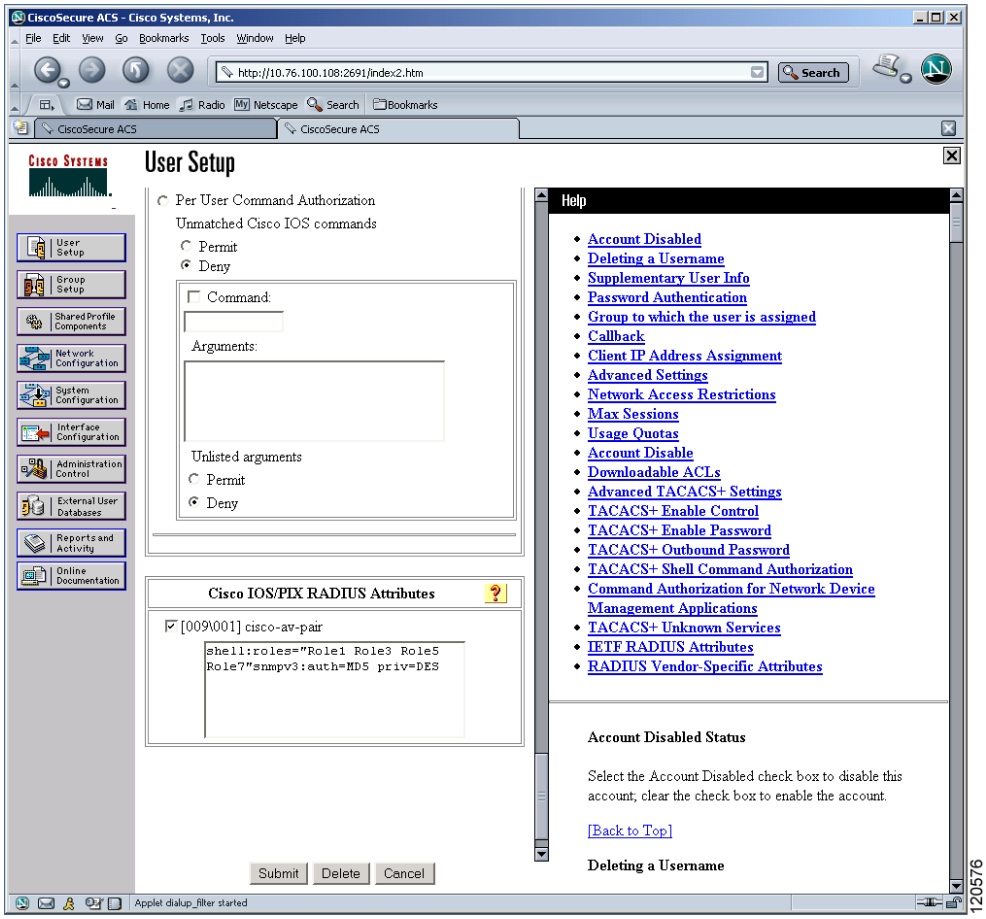


Figure 28-4 Configuring the network-admin Role with SNMPv3 Attributes When Using TACACS+

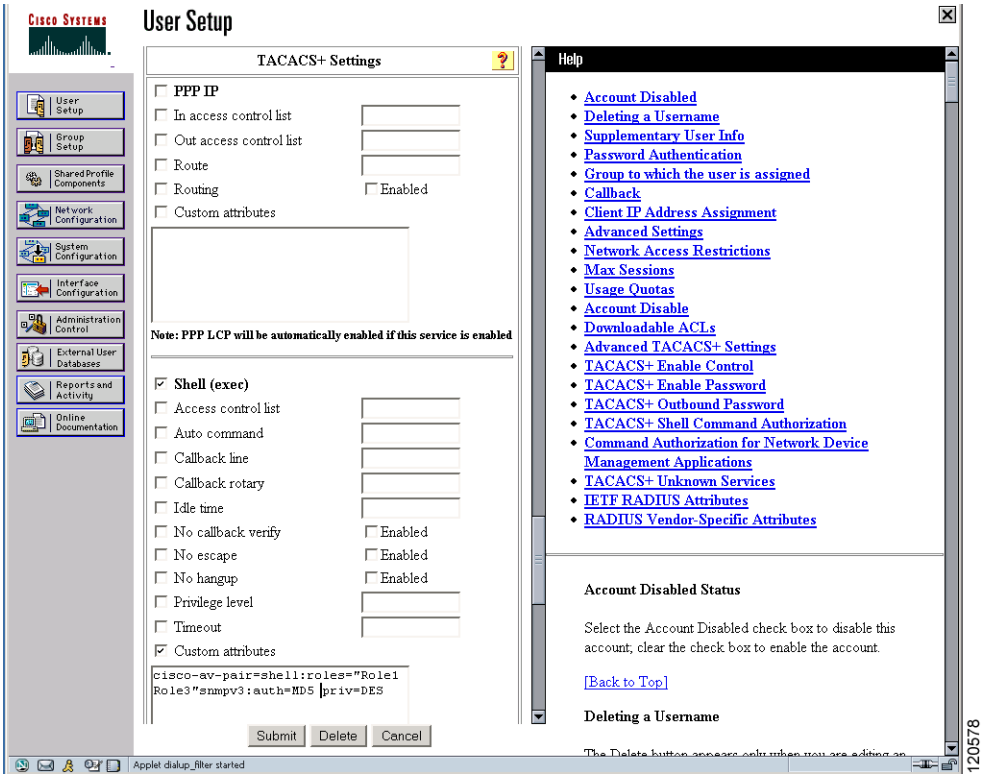
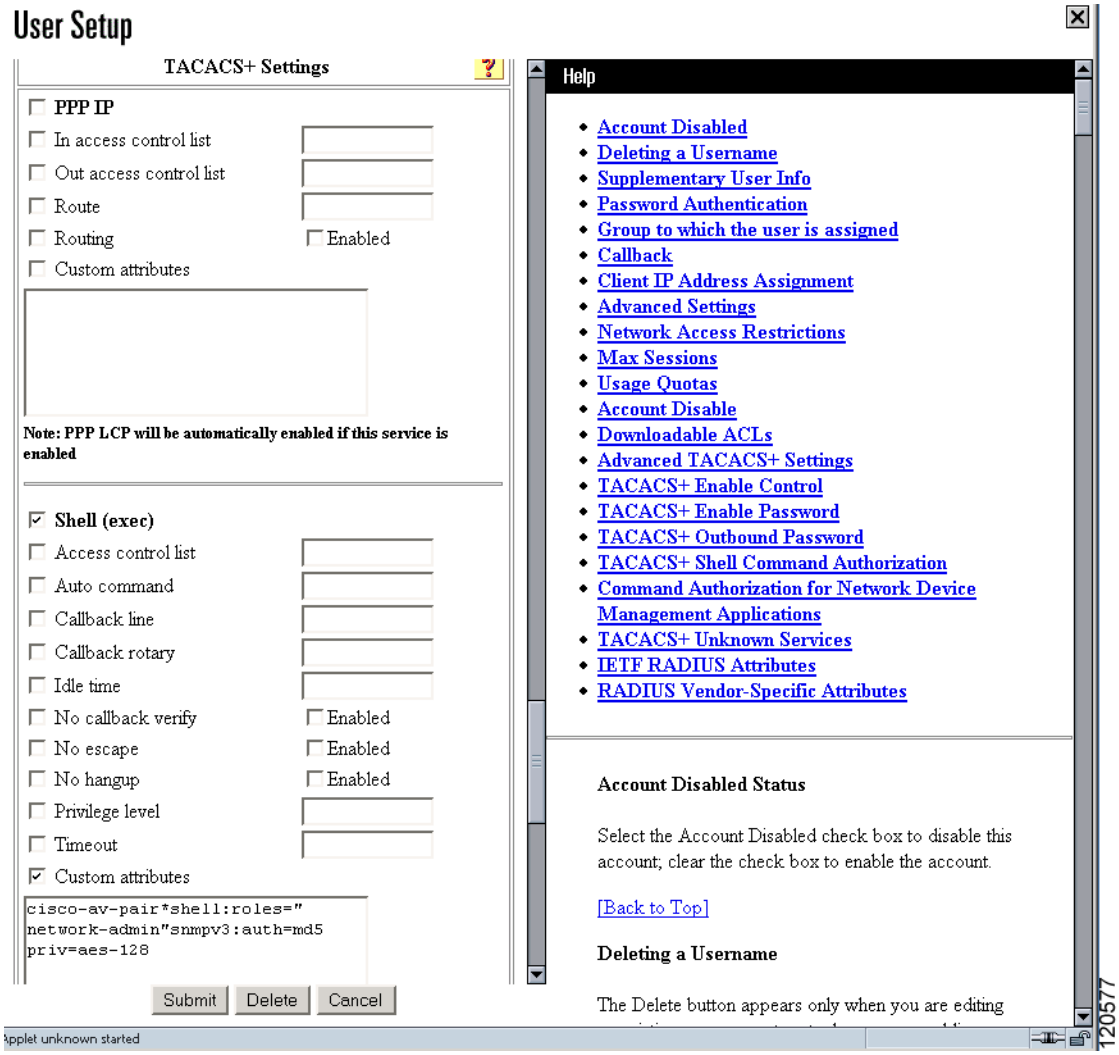


Figure 28-5 Configuring Multiple Roles with SNMPv3 Attributes When Using TACACS+



Default Settings

Table 28-2 lists the default settings for all switch security features in any switch.

Table 28-2 Default Switch Security Settings

Parameters	Default
Roles in Cisco MDS Switches	Network operator (network-operator).
AAA configuration services	Local.
Authentication port	1821.
Accounting port	1813.
Preshared key communication	Clear text.
RADIUS server time out	1 (one) second.
RADIUS server retries	Once.
TACACS+	Disabled.
TACACS+ servers	None configured.
TACACS+ server timeout	5 seconds.
AAA server distribution	Disabled.
Accounting log size	250 KB.