



Configuring Switch Security

The authentication, authorization, and accounting (AAA) mechanism verifies the identity of, grants access to, and tracks the actions of users managing a switch. The Cisco MDS 9020 Fabric Switch uses Remote Access Dial-In User Service (RADIUS) 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 servers 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, page 9-1](#)
- [Switch AAA Functionalities, page 9-2](#)
- [Configuring RADIUS, page 9-3](#)
- [Local AAA Services, page 9-4](#)
- [Authentication and Authorization Process, page 9-4](#)
- [Role-Based Authorization, page 9-5](#)
- [Configuring User Accounts, page 9-6](#)
- [Configuring Accounting Services, page 9-8](#)
- [Configuring SSH Services, page 9-9](#)
- [Recovering the Administrator Password, page 9-10](#)
- [Configuring Cisco Access Control Server, page 9-12](#)
- [Default Settings, page 9-14](#)

Switch Management Security

Management security in the Cisco MDS 9020 Fabric Switch provides security to all management access methods including the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

Send documentation comments to mdsfeedback-doc@cisco.com.

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 or remote (RADIUS).

- Remote security control. (See the [“Configuring RADIUS” section on page 9-3.](#))
- Local security control. (See the [“Local AAA Services” section on page 9-4.](#))

SNMP Security Options

The SNMP agent supports security features for SNMP v1 and SNMP v2c. Normal SNMP security mechanisms apply to all applications that use SNMP (for example, Cisco MDS 9000 Family Fabric Manager).

CLI security options also apply to the Cisco MDS Fabric Manager and Device Manager. (See [Chapter 10, “Configuring SNMP”](#).)

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

Switch AAA Functionalities

Using the CLI or an SNMP application, you can configure authentication, authorization, and accounting (AAA) switch functionalities in the Cisco MDS 9020 Fabric Switch.

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. The Cisco MDS 9020 Fabric Switch allows you to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS servers).

Authorization

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.

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 are stored locally.

Send documentation comments to mdsfeedback-doc@cisco.com.

Configuring RADIUS

The Cisco MDS 9020 Fabric Switch can use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers 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 the switch and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

You can add up to five 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, perform this task:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode
Step 2	switch(config)# radius-server host 10.10.0.0 key abcdefgh01234567	Specifies the preshared key for the selected RADIUS server. In this example, the host is 10.10.0.0 and the shared secret is abcdefgh01234567. The shared secret must be exactly 16 characters.
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 10.10.0.0 and the authentication port is 2003. The default authentication port is 1812, and the valid range is 0 to 65,366.
Step 4	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 5	switch(config)# radius-server host 10.10.0.0 timeout 30	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default timeout is one (1) second. The time ranges from 1 to 60 seconds.
Step 6	switch(config)# radius-server host 10.10.0.0 retransmit 3	Configures the number of times (3) the switch tries to connect to the RADIUS server before reverting to local authentication.

Send documentation comments to mdsfeedback-doc@cisco.com.

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 9-6.)

Use the **show accounting log** command to view the local accounting log. (See [Example 9-1](#).)

Example 9-1 *Displays the Accounting Log Information*

```
switch# show accounting log
[1][Thu Jan 20 21:30:20.599 UTC 2005][AU][0000.00FF][None][Zoning Default Zone changed in
Config default to False]
[2][Thu Jan 20 21:30:35.119 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@IB-session1 User Login]
[3][Thu Jan 20 21:30:35.122 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@OB-session2 User Login]
[4][Thu Jan 20 21:30:50.409 UTC 2005][AU][0000.0001][None][IP 10.0.0.254 User
admin@OB-session3 User Login]
[5][Thu Jan 20 21:31:14.514 UTC 2005][AU][0000.0001][None][IP 10.0.0.254 User
maint@OB-session4 User Login]
...
```

Authentication and Authorization Process

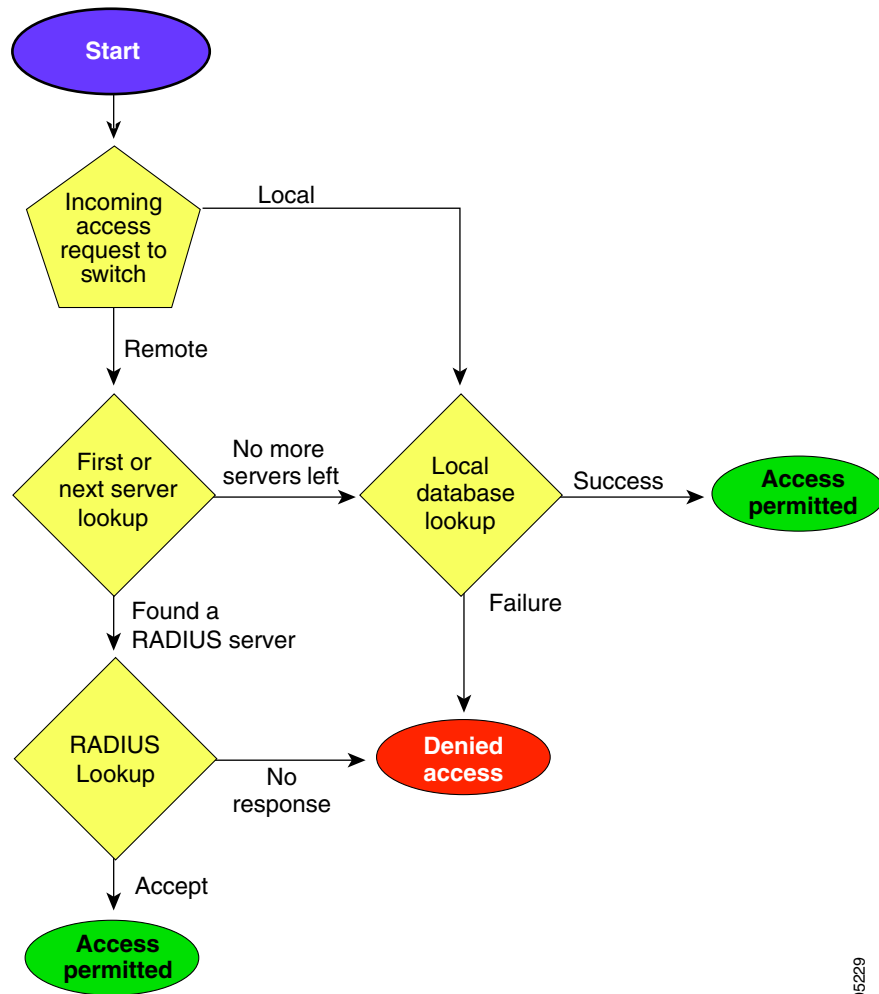
Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. The Cisco MDS 9020 Fabric Switch allows you to perform local authentication (using the lookup database) or remote authentication (using one or more RADIUS servers).

The following steps explain the authorization and authentication process. [Figure 9-1](#) shows a flow chart of the process.

-
- | | |
|---------------|---|
| Step 1 | If you can log in to the required Cisco MDS 9020 Fabric Switch, then you can use the Telnet, SSH, Fabric Manager/Device Manager, or console login options. |
| Step 2 | An authentication request is sent to the first RADIUS server. <ul style="list-style-type: none">• If a RADIUS server fails to respond, then another RADIUS server is tried and so on until a RADIUS server responds to the authentication request.• If all RADIUS servers fail to respond, then the local database is used for authentication. |
| Step 3 | If you are successfully authenticated through a RADIUS server, then user roles are downloaded with an authentication response. If user roles are not successfully retrieved from the RADIUS 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. |
-

Send documentation comments to mdsfeedback-doc@cisco.com.

Figure 9-1 Switch Authorization and Authentication Flow



105229

Role-Based Authorization

The Cisco MDS 9020 Fabric Switch performs authentication based on roles. The Cisco MDS 9020 Fabric Switch supports two roles: network-administrator and network operator. Role-based authorization limits access to switch operations by assigning users to roles. When you execute a command, perform command completion, or obtain context sensitive help, the switch software allows the operation to progress if you have permission to access that command.



Note

Only the admin user name can create or modify user accounts. Users can change their own passwords.

Send documentation comments to mdsfeedback-doc@cisco.com.

Displaying Role-Based Information

Use the **show role** command to display rules configured on the switch. (See [Example 9-2](#).)

Example 9-2 *Displays Information for All Roles*

```
switch# show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands
```

Configuring User Accounts

Every Cisco MDS 9020 Fabric Switch user has the account information stored by the system. Your authentication information, user name, user password, password expiration date, and role membership are stored in your user profile.

The tasks explained in this section enable you to create users and modify the profile of an existing user. These tasks are restricted to privileged users as determined by your administrator.

Creating or Updating Users

By default, the user account does not expire unless you explicitly configure it to expire. The **expire** option determines the date on which the user account is disabled. The date is specified in the YYYY-MM-DD format.



Tip

The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nsd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys.



Note

User passwords are not displayed in the switch configuration file.



Tip

If a password is trivial (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password, as shown in the sample configuration. Passwords are case-sensitive. Admin is not the default password for the Cisco MDS 9020 Fabric Switch. You must explicitly configure a password that meets the above requirements.

Send documentation comments to mdsfeedback-doc@cisco.com.

To configure a new user or to modify the profile of an existing user, perform this task:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# username usam password abcd123AAA expire 2005-05-31	Creates or updates the user account (usam), along with a password (abcd123AAA) that is set to expire on 2003-05-31. The password is limited to 20 characters.
	switch(config)# username msam password abcd12AAA role network-operator	Creates or updates the user account (msam), along with a password (abcd12AAA) specified in clear text. The password can be from 8 to 20 characters.
Step 3	switch(config)# username usam role network-admin	Adds the specified user (usam) to the network-admin role.

Displaying User Account Information

Use the **show user-account** command to display configured information about user accounts. (See Examples 9-3 to 9-4.)

Example 9-3 Displays Information for a Specified User

```
switch# show user-account user1
user:user1
    this user account has no expiry date
    roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

Example 9-4 Displays Information for All Users

```
switch# show user-account
show user-account
user:admin
    this user account has no expiry date
    roles:network-admin
user:usam
    expires on Sat May 28 00:00:00 2005
    roles:network-admin network-operator
user:msam
    this user account has no expiry date
    roles:network-operator
user:user1
    this user account has no expiry date
    roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

Send documentation comments to mdsfeedback-doc@cisco.com.

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).



Tip

The Cisco MDS 9020 Fabric 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 the Accounting Log

The **show accounting log** command displays the contents of the accounting log. (See Example 9-5.) To display the size of the local accounting log, use the **show accounting logsize** command.

Example 9-5 Displays the Entire Log File

```
switch# show accounting log
[1][Mon Apr 25 11:01:59.888 UTC 2005][AU][0000.00FF][None][Zoning Default Zone changed in
Config default to False]
[2][Mon Apr 25 11:02:03.228 UTC 2005][AU][0000.0001][None][IP Unknown User
admin@OB-session1 User Login]
[3][Mon Apr 25 11:02:07.376 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@IB-session2 User Login]
[4][Mon Apr 25 11:02:07.379 UTC 2005][AU][0000.0001][None][IP Unknown User
snmp@OB-session3 User Login]
[5][Mon Apr 25 15:58:40.548 UTC 2005][AU][0000.0001][None][IP 10.20.33.160 User
admin@OB-session4 User Login]
[6][Mon Apr 25 16:08:38.188 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session5 User Login]
[7][Mon Apr 25 16:38:23.054 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session6 User Login]
[8][Mon Apr 25 20:02:43.211 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session7 User Login]
[9][Tue Apr 26 13:49:28.317 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session8 User Login]
[10][Tue Apr 26 18:47:00.064 UTC 2005][AU][0000.0001][None][IP 10.20.32.70 User
admin@OB-session9 User Login]
...
```


Send documentation comments to mdsfeedback-doc@cisco.com.

Configuring SSH Services

The Telnet service is enabled by default on the Cisco MDS 9020 Fabric Switch. Before enabling the SSH service, generate a server key pair. (See the “Generating the SSH Server Key Pair” section on page 9-9.)

Use the **ssh key** command to generate a server key.

Generating the SSH Server Key Pair

Be sure to have an SSH server key pair with the appropriate version before enabling the SSH service. Generate the SSH server key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 2048. The **rsa** option generates the RSA key pair for the SSH version 2 protocol.



Caution If you delete all of the SSH keys, you cannot start a new SSH session.

To generate the SSH server key pair, perform this task:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# ssh key rsa generating rsa key..... generated rsa key	Generates the RSA server key pair.
	switch(config)# no ssh key rsa cleared RSA keys	Clears the RSA server key pair configuration.

Enabling SSH Service

By default, the SSH service is disabled.

To enable or disable the SSH service, perform this task:

	Command	Purpose
Step 1	switch# config t	Enters configuration mode.
Step 2	switch(config)# ssh server enable updated	Enables the use of the SSH service.
	switch(config)# no ssh server enable updated	Disables (default) the use of the SSH service and resets the switch to its factory defaults.



Caution

If you are logging in to a switch through SSH and you have entered the **aaa authentication login default none** command, you must enter one or more keystrokes to log in. If you press the **Enter** key without entering at least one keystroke, your log in will be rejected.

Send documentation comments to mdsfeedback-doc@cisco.com.

Displaying SSH Protocol Status

Use the **show ssh server** command to display the status of the SSH protocol (enabled or disabled). (See [Example 9-6](#).)

Example 9-6 Displays SSH Protocol Status

```
switch# show ssh server
ssh service is enabled
```

Recovering the Administrator Password

To recover the administrator password, you must restore the factory account name password using maintenance mode. This restores the password for the Admin account name to the default (admin123) and removes all other user accounts from the switch. To reset the switch password, follow these steps:

-
- Step 1** Isolate the switch from the fabric.
- Step 2** Establish a serial connection from the PC console to the switch console port.
- Configure the baud rate and character format of the PC terminal emulation program to match the following management port default characteristics:
 - 9600 baud
 - 8 data bits
 - 1 stop bit
 - No parity
 - Flow control: none
 - Connect a null-modem F/F DB9 cable from the switch console port to the PC serial port.
- Step 3** Place the switch in maintenance mode. Press and hold the **Maintenance** button with a pointed tool. The Maintenance button is located under the Ethernet port. When the Heartbeat LED alone turns on, release the button. The switch will reboot and display the Switch Login: prompt.
- Step 4** Enter the maintenance mode account name and password (prom, prom), and press **Enter**.
- ```
Switch login: prom
Password:xxxx
```
- Step 5** Enter 3 for **Reset User Accounts to Default**.
- ```
0) Exit
1) Image Unpack
2) Reset Network Config
3) Reset User Accounts to Default
4) Copy Log Files
5) Remove Switch Config
6) Remake Filesystem
7) Reset Switch
8) Update Boot Loader
Option: 3
```
- Step 6** Enter 7 for **Reset Switch**.

Send documentation comments to mdsfeedback-doc@cisco.com.

```
0) Exit
1) Image Unpack
2) Reset Network Config
3) Reset User Accounts to Default
4) Copy Log Files
5) Remove Switch Config
6) Remake Filesystem
7) Reset Switch
8) Update Boot Loader
Option: 7
```

Step 7 Enter **yes** when prompted to reset the switch.

Send documentation comments to mdsfeedback-doc@cisco.com.

Configuring Cisco Access Control Server

The Cisco Access Control Server (ACS) uses 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 9-2](#) and [Figure 9-3](#) display ACS server user setup configurations for network-administrator roles and multiple roles using RADIUS.

Figure 9-2 Configuring the network-admin Role When Using RADIUS

The screenshot shows the Cisco Systems User Setup web interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "User Setup" and includes a "Permit/Deny" section with radio buttons (Permit is selected). Below this is a "Command:" field and an "Arguments:" text area. A section titled "Cisco IOS/PIX RADIUS Attributes" contains a checked checkbox for "[009/001] cisco-av-pair" and a text field containing "shell:roles*"network-admin". At the bottom are "Submit", "Delete", and "Cancel" buttons. On the right is a "Help" sidebar with a list of links: Account Disabled, Deleting a Username, Supplementary User Info, Password Authentication, Group to which the user is assigned, Callback, Client IP Address Assignment, Advanced Settings, Network Access Restrictions, Max Sessions, Usage Quotas, Account Disable, Downloadable ACLs, Advanced TACACS+ Settings, TACACS+ Enable Control, TACACS+ Enable Password, TACACS+ Outbound Password, TACACS+ Shell Command Authorization, Command Authorization for Network Device Management Applications, TACACS+ Unknown Services, IETF RADIUS Attributes, and RADIUS Vendor-Specific Attributes. Below the links is the "Account Disabled Status" section with instructions and a "[Back to Top]" link. At the very bottom of the sidebar is the "Deleting a Username" section. The status bar at the bottom of the browser window shows "Applet dialup_filter started" and the page number "120575".

Send documentation comments to mdsfeedback-doc@cisco.com.

Figure 9-3 Configuring Multiple Roles with SNMPv3 Attributes When Using RADIUS

User Setup

☐ Per User Command Authorization
Unmatched Cisco IOS commands

☐ Permit
☒ Deny

☐ Command:
Arguments:

Unlisted arguments
☐ Permit
☒ Deny

Cisco IOS/PIX RADIUS Attributes

☒ [009/001] cisco-av-pair

```
shell:roles="Role1 Role3 Role5
Role7"snmpv3:auth=MD5 priv=DES
```

Help

- [Account Disabled](#)
- [Deleting a Username](#)
- [Supplementary User Info](#)
- [Password Authentication](#)
- [Group to which the user is assigned](#)
- [Callback](#)
- [Client IP Address Assignment](#)
- [Advanced Settings](#)
- [Network Access Restrictions](#)
- [Max Sessions](#)
- [Usage Quotas](#)
- [Account Disable](#)
- [Downloadable ACLs](#)
- [Advanced TACACS+ Settings](#)
- [TACACS+ Enable Control](#)
- [TACACS+ Enable Password](#)
- [TACACS+ Outbound Password](#)
- [TACACS+ Shell Command Authorization](#)
- [Command Authorization for Network Device Management Applications](#)
- [TACACS+ Unknown Services](#)
- [IETF RADIUS Attributes](#)
- [RADIUS Vendor-Specific Attributes](#)

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

Deleting a Username

Submit Delete Cancel

Send documentation comments to mdsfeedback-doc@cisco.com.

Default Settings

Table 9-1 lists the default settings for all switch security features in any switch.

Table 9-1 **Default Switch Security Settings**

Parameters	Default
Roles in a Cisco MDS 9020 Fabric Switch	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.
User account	No expiry (unless configured).
Password	None.
Accounting log size	250 KB.
SSH service	Disabled.
Telnet service	Enabled.