



CHAPTER 4

Configuring Security Features on an External AAA Server

The authentication, authorization, and accounting (AAA) feature 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) or Terminal Access Controller Access Control device 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 a AAA server. 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 feature provides a central management capability for AAA servers.

This chapter includes the following sections:

- [Switch Management Security, page 4-2](#)
- [Switch AAA Functionalities, page 4-3](#)
- [Configuring AAA Server Monitoring Parameters Globally, page 4-9](#)
- [Configuring RADIUS Server Monitoring Parameters, page 4-9](#)
- [One Time Password Support, page 4-17](#)
- [Configuring TACACS+ Server Monitoring Parameters, page 4-18](#)
- [.Configuring Server Groups, page 4-25](#)
- [AAA Server Distribution, page 4-27](#)
- [CHAP Authentication, page 4-31](#)
- [MSCHAP Authentication, page 4-31](#)
- [Local AAA Services, page 4-33](#)
- [Configuring Accounting Services, page 4-33](#)
- [Configuring Cisco Access Control Servers, page 4-34](#)
- [Default Settings, page 4-37](#)

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

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).

This section includes the following topics:

- [Fabric Manager Security Options, page 4-2](#)
- [Fabric Manager Security Options, page 4-2](#)
- [SNMP Security Options, page 4-2](#)

Fabric Manager Security Options

You can access Fabric Manager using TCP/UDP SNMP or HTTP traffic. For each management path (console, 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 RADIUS
See the [“Configuring RADIUS Server Monitoring Parameters”](#) section on page 4-9
 - Using TACACS+
See the [“Configuring TACACS+ Server Monitoring Parameters”](#) section on page 4-18
- Local security control.
See the [“Local AAA Services”](#) section on page 4-33.

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

- iSCSI authentication
See the *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide* and the *Cisco Fabric Manager IP Services Configuration Guide*.
- Fibre Channel Security Protocol (FC-SP) authentication
See [Chapter 8, “Configuring FC-SP and DHCHAP.”](#)

SNMP Security Options

The SNMP agent supports security features for SNMPv1, SNMPv2c, and SNMPv3. Normal SNMP security features apply to all applications that use SNMP (for example, Cisco MDS 9000 Fabric Manager).

SNMP security options also apply to the Fabric Manager and Device Manager.

See the *Cisco MDS 9000 NX-OS Family System Management Configuration Guide* for more information on the SNMP security options.

Refer to the *Cisco Fabric Manager Fundamentals Configuration Guide* for information on Fabric Manager and Device Manager.

Send documentation comments to fm-docfeedback@cisco.com

Switch AAA Functionalities

Using the CLI or Fabric Manager, or an SNMP application, you can configure AAA switch functionalities on any switch in the Cisco MDS 9000 Family.

This section includes the following topics:

- [Authentication, page 4-3](#)
- [Authorization, page 4-3](#)
- [Accounting, page 4-4](#)
- [Remote AAA Services, page 4-4](#)
- [Remote Authentication Guidelines, page 4-4](#)
- [Server Groups, page 4-5](#)
- [AAA Service Configuration Options, page 4-5](#)
- [Authentication and Authorization Process, page 4-6](#)

Authentication

Authentication is the process of verifying the identity of the person or device accessing the switch. This identity verification is based on the user ID and password combination provided by the entity trying to access 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 through 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 switch authenticates the SNMPv3 protocol data units (PDUs) with your Telnet or SSH login name as the SNMPv3 user. The management station can temporarily use the Telnet or 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 SNMPv3 operations.



Note

Fabric Manager does not support AAA passwords with trailing white space, for example “passwordA.”

Authorization

The following authorization 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.
- Default-role—Has permission to use the GUI (Fabric Manager and Device Manager). This access is automatically granted to all users for accessing the GUI.

Send documentation comments to fm-docfeedback@cisco.com

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



Note

FMS users can be AAA authenticated only using cisco-av-pair. Use of shell:roles construct will result in user getting assigned to network-operator role within FM.

Accounting

The accounting feature tracks and maintains a log of every management configuration 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 local AAA services:

- User password lists for each switch in the fabric can be managed more easily.
- AAA servers are already deployed widely across enterprises and can be easily adopted.
- The accounting log for all switches in the fabric can be centrally managed.
- User role mapping for each switch in the fabric can be managed more easily.

Remote Authentication Guidelines

If 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 the *Cisco Fabric Manager IP Services Configuration Guide*). We recommend this method.
- SAN networks connected to the switch should have at least one gateway switch connected to the Ethernet LAN reaching the AAA servers.

Send documentation comments to fm-docfeedback@cisco.com

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 failover 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 fail 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 (Fabric Manager and Device Manager login)
- Console login
- iSCSI authentication (See the *Cisco Fabric Manager IP Services Configuration Guide*).
- FC-SP authentication (See [Chapter 8, “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 options fail, local is tried.



Caution

Cisco MDS NX-OS supports user names that are created with alphanumeric characters or specific special characters (+ [plus], = [equal], _ [underscore], - [hyphen], \ [backslash], and . [period]) whether created remotely (using TACACS+ or RADIUS) or locally, provided the user name starts with an alphabetical character. Local user names cannot be created with all numbers or with any special characters (apart from those specified). If a numeric-only user name or a non-supported special character user name exists on an AAA server, and is entered during login, then the user is denied access.



Note

Even if local is not specified as one of the options, it is tried by default if all AAA servers configured for authentication are unreachable.)

When RADIUS times out, local login is attempted depending on the fallback configuration. For this local login to be successful, a local account for the user with the same password should exist, and the RADIUS timeout and retries should take less than 40 seconds. The user is authenticated if the username and password exist in the local authentication configuration.

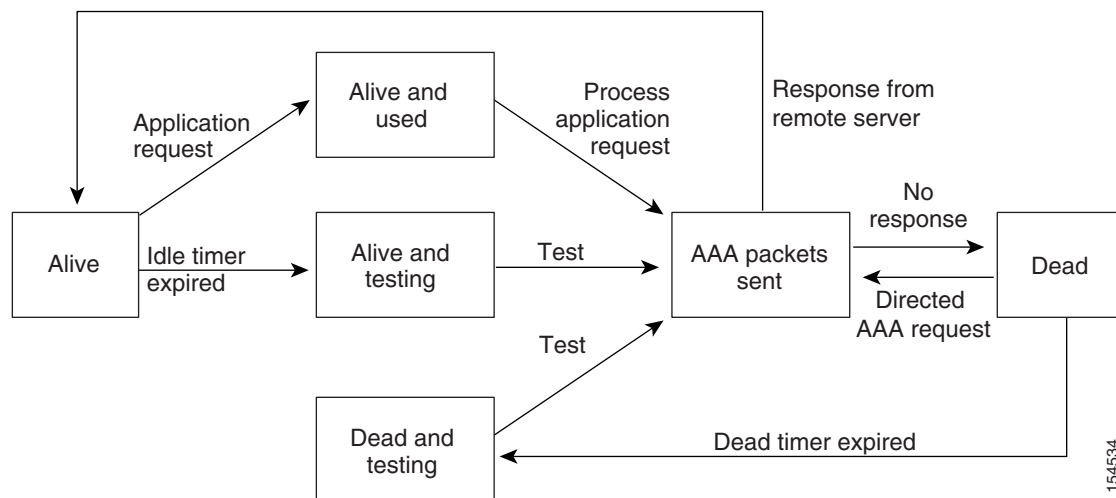
AAA Server Monitoring

An unresponsive AAA server introduces a delay in the processing of AAA requests. An MDS switch can periodically monitor an AAA server to check whether it is responding (or alive) to save time in processing AAA requests. The MDS switch marks unresponsive AAA servers as dead and does not send AAA requests to any dead AAA servers. An MDS switch periodically monitors dead AAA servers and brings them to the alive state once they are responding. This monitoring process verifies that an AAA

Send documentation comments to fm-docfeedback@cisco.com

server is in a working state before real AAA requests are sent its way. Whenever an AAA server changes to the dead or alive state, an SNMP trap is generated and the MDS switch warns the administrator that a failure is taking place before it can impact performance. See [Figure 4-1](#) for AAA server states.

Figure 4-1 AAA Server States



Note

The monitoring interval for alive servers and dead servers is different and can be configured by the user. The AAA server monitoring is performed by sending a test authentication request to the AAA server.

The user name and password to be used in the test packet can be configured.

See the [“Configuring RADIUS Server Monitoring Parameters”](#) section on page 4-9.

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 managing 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).

Authorization provides access control. It is the process of assembling a set of attributes that describe what the user is authorized to perform. Based on the user ID and password combination, the user is authenticated and authorized to access the network as per the assigned role. You can configure parameters that can prevent unauthorized access by an user, provided the switches use the TACACS+ protocol.

AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in the Cisco NX-OS software is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

The following steps explain the authorization and authentication process:

- Step 1** Log in to the required switch in the Cisco MDS 9000 Family, using the Telnet, SSH, Fabric Manager or Device Manager, or console login options.

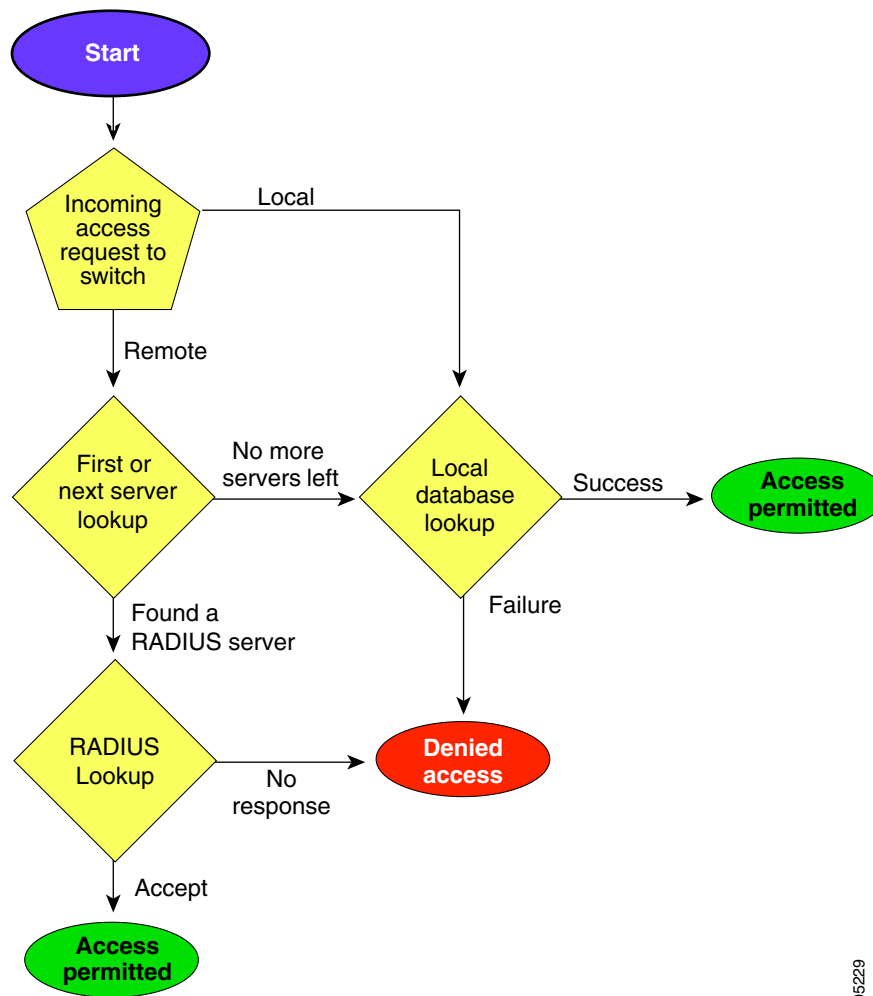
Send documentation comments to fm-docfeedback@cisco.com

- 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 contacted 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 contacted.
 - If all configured methods fail, then by default local database is used for authentication. The next section will describe the way to disable this fallback.
- Step 3** When you are successfully authenticated through a remote AAA server, then the following possible actions are taken:
- If the AAA server protocol is RADIUS, then user roles specified in the **cisco-av-pair** attribute are downloaded with an authentication response.
 - If the 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 if the **show aaa user default-role** command is enabled. You are denied access if this command is disabled.
- Step 4** When 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 4-2 shows a flow chart of the authorization and authentication process.

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-2 Switch Authorization and Authentication Flow



105529



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.



Note

Authorization configuration is provided only for authentication done using TACACS+ server.



Note

The “none” option from AAA authorization methods has been deprecated. If you did an upgrade from the 4.x image and “none” was configured as one of the authorization methods, replace it with local. The functionality remains the same.

Send documentation comments to fm-docfeedback@cisco.com

Configuring Fallback Mechanism for Authentication

You can enable and disable fallback to the local database in case the remote authentication is set and all AAA servers are unreachable (authentication error). The fallback is set to local by default in case of an authentication error. You can disable this fallback for both console and SSH or Telnet login. Disabling this fallback will tighten the security of authentication.

The following occurs in the fallback authentication method:

- By default fallback is enabled for both the default and console login. The “**sh run aaa all**” command is used to verify this.
- A warning message is displayed when fallback is disabled.



Caution

If fallback is disabled for both default and console, remote authentication is enabled and the servers are unreachable. If this occurs the switch will be locked.

Configuring AAA Server Monitoring Parameters Globally

The AAA server monitoring parameters can be configured globally for all servers or individually for a specific server. This section explains how the global configuration can be set. The global configurations will apply to all servers that do not have individual monitoring parameters defined. For any server, the individual test parameter defined for that particular server will always get precedence over the global settings.



Note

Replace “radius” with “tacacs” in the previous procedure to get equivalent commands for TACACS server global test parameter configurations.

The global AAA server monitoring parameters function as follows:

- When a new AAA server is configured, it is monitored using the global test parameters, if defined.
- When global test parameters are added or modified, all the AAA servers, which do not have any test parameters configured, start being monitored using the new global test parameters.
- When the server test parameters are removed for a server or when the idle-time is set to zero (default value), it starts being monitored using the global test parameters, if defined.
- If global test parameters are removed or global idle-time is set to zero, servers for which the server test parameters are present will not be affected. However, monitoring will stop for all other servers that were previously being monitored using global parameters.
- If the server monitoring fails with the user-specified server test parameters, the server monitoring does not fall back to global test parameters.

Configuring RADIUS Server Monitoring Parameters

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.

Send documentation comments to fm-docfeedback@cisco.com

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.

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

This section includes the following topics:

- [About RADIUS Server Default Configuration, page 4-10](#)
- [About the Default RADIUS Server Encryption Type and Preshared Key, page 4-10](#)
- [Configuring the Default RADIUS Server Encryption Type and Preshared Key, page 4-11](#)
- [About RADIUS Servers, page 4-13](#)
- [Configuring a RADIUS Server, page 4-13](#)
- [About Validating a RADIUS Server, page 4-15](#)
- [Periodically Validating a RADIUS Server, page 4-15](#)
- [Displaying RADIUS Server Statistics, page 4-16](#)
- [Allowing Users to Specify a RADIUS Server at Login, page 4-16](#)
- [About Vendor-Specific Attributes, page 4-16](#)

About RADIUS Server Default Configuration

Fabric Manager allows you to set up a default configuration that can be used for any RADIUS server that you configure the switch to communicate with. The default configuration includes:

- Encryption type
- Timeout value
- Number of retransmission attempts
- Allowing the user to specify a RADIUS server at login

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.

About the Default RADIUS Server Encryption Type and 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 when configuring an individual RADIUS server.

Send documentation comments to fm-docfeedback@cisco.com

Configuring the Default RADIUS Server Encryption Type and Preshared Key

To configure the default RADIUS server encryption type and preshared key using Fabric Manager, follow these steps:

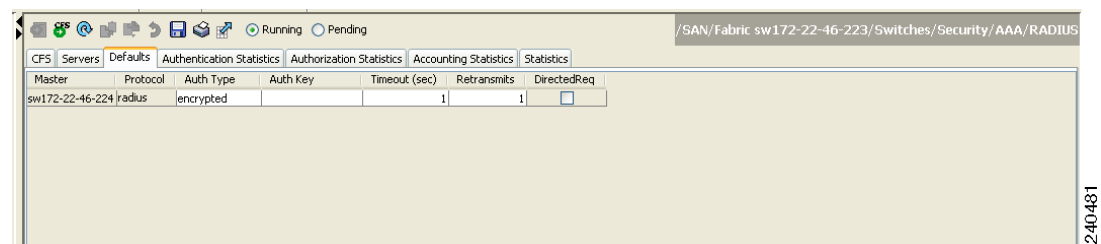
Step 1 Expand **Switches > Security > AAA**, and then select **RADIUS**.

You see the RADIUS configuration in the Information pane.

Step 2 Click the **Defaults** tab.

You see the RADIUS default settings as shown in [Figure 4-3](#).

Figure 4-3 RADIUS Default Settings



Step 3 Select **plain** or **encrypted** from the AuthType drop-down menu.

Step 4 Set the key in the Auth Key field.

Step 5 Click the **Apply Changes** icon to save the changes.

Setting the RADIUS Server Timeout Interval

You can configure a global timeout value between transmissions for all RADIUS servers.



Note

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

Setting the Default RADIUS Server Timeout Interval and Retransmits

By default, a switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also configure the timeout value for the RADIUS server.

To configure the number of retransmissions and the time between retransmissions to the RADIUS servers using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA** and then select **RADIUS**.

You see the RADIUS configuration in the Information pane.

Step 2 Choose the **Defaults** tab.

Send documentation comments to fm-docfeedback@cisco.com

You see the RADIUS default settings.

Step 3 Fill in the Timeout and Retransmits fields for authentication attempts.

Step 4 Click the **Apply Changes** icon to save the changes.

Configuring RADIUS Server Monitoring Parameters

You can configure parameters for monitoring RADIUS servers. You can configure this option to test the server periodically, or you can run a one-time only test.

This section includes the following topics:

- [Configuring the Test Idle Timer, page 4-12](#)
- [Configuring Test User Name, page 4-12](#)
- [Configuring the Dead Timer, page 4-12](#)

Configuring the Test Idle Timer

The test idle timer specifies the interval during which a RADIUS server receives no requests before the MDS switch sends out a test packet.

**Note**

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Configuring Test User Name

You can configure a username and password for periodic RADIUS server status testing. You do not need to configure the test username and password to issue test messages to monitor RADIUS servers. You can use the default test username (test) and default password (test).

**Note**

We recommend that the test username not be the same as an existing username in the RADIUS database for security reasons.

Configuring the Dead Timer

The dead timer specifies the interval that the MDS switch waits, after declaring that a RADIUS server is dead, before sending out a test packet to determine if the server is now alive.

**Note**

The default dead timer value is 0 minutes. When the dead timer interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead-time interval for the group is greater than 0 minutes. (See the [“Server Groups” section on page 4-5](#)).

Send documentation comments to fm-docfeedback@cisco.com

**Note**

If the dead timer of a dead RADIUS server expires before it is sent a RADIUS test message, that server is marked as alive again even if it is still not responding. To avoid this scenario, configure a test user with a shorter idle time than the dead timer time.

About RADIUS Servers

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. When you configure a new RADIUS server, you can use the default configuration or modify any of the parameters to override the default RADIUS configuration.

Configuring a RADIUS Server

To configure a RADIUS server and all its options using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **RADIUS**.
You see the RADIUS configuration in the Information pane.
- Step 2** Click the **Servers** tab.
You see any existing RADIUS servers.
- Step 3** Click **Create Row** to add a new RADIUS server.
You see the Create RADIUS Server dialog box shown in [Figure 4-4](#).

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-4 Create RADIUS Server

- Step 4** Select the switches that you want to assign as RADIUS servers.
- Step 5** Assign an index number to identify the RADIUS server.
- Step 6** Select the IP address type for the RADIUS server.
- Step 7** Fill in the IP address or name for the RADIUS server.
- Step 8** (Optional) Modify the authentication and accounting ports used by this RADIUS server.
- Step 9** Select the appropriate key type for the RADIUS server.
- Step 10** Select the TimeOut value in seconds. The valid range is 0 to 60 seconds.
- Step 11** Select the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication.
- Step 12** Enter the test idle time interval value in minutes. The valid range is 1 to 1440 minutes.
- Step 13** Enter the test user with the default password. The default username is test.
- Step 14** Click **Create** to save these changes.

Configuring the Test Idle Timer

The test idle timer specifies the interval during which a RADIUS server receives no requests before the MDS switch sends out a test packet.



Note

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

Send documentation comments to fm-docfeedback@cisco.com

To configure the test idle timer, see [“Configuring a RADIUS Server” section on page 4-13](#).

Configuring Test User Name

You can configure a username and password for periodic RADIUS server status testing. You do not need to configure the test username and password to issue test messages to monitor RADIUS servers. You can use the default test username (test) and default password (test).

**Note**

We recommend that the test username not be the same as an existing username in the RADIUS database for security reasons.

To configure the optional username and password for periodic RADIUS server status testing, see [“Configuring a RADIUS Server” section on page 4-13](#).

About Validating a RADIUS Server

As of Cisco SAN-OS Release 3.0(1), you can periodically validate a RADIUS server. The switch sends a test authentication to the server using the username and password that you configure. If the server does not respond to the test authentication, then the server is considered non responding.

**Note**

For security reasons we recommend that you do not use a username that is configured on your RADIUS server as a test username.

You can configure this option to test the server periodically, or you can run a one-time only test.

Periodically Validating a RADIUS Server

To configure the switch to periodically test a RADIUS server using Fabric Manager, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Expand Switches > Security > AAA , and then select RADIUS .
You see the RADIUS configuration in the Information pane. |
| Step 2 | Click the Servers tab.
You see any existing RADIUS servers. |
| Step 3 | Click Create Row to add a new RADIUS server.
You see the Create RADIUS Server dialog box (see Figure 4-4). |
| Step 4 | Fill in the IP address. |
| Step 5 | Modify the authentication and accounting ports used by this RADIUS server. |
| Step 6 | Fill in the TestUser field and, optionally, the TestPassword field. The default password for the test is Cisco . |
| Step 7 | Set the IdleTime field for the time that the server is idle before you send a test authentication. |
| Step 8 | Click Create to save these changes. |
-

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

Displaying RADIUS Server Statistics

To display RADIUS server statistics using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **RADIUS**.
You see the RADIUS configuration in the Information pane.
- Step 2** Click the **Statistics** tab.
You see the RADIUS server statistics.
-

Sending RADIUS Test Messages for Monitoring

You can manually send test messages to monitor a RADIUS server.

Allowing Users to Specify a RADIUS Server at Login

By default, an MDS switch forwards an authentication request to the first server in the RADIUS server group. You can configure the switch to allow the user to specify which RADIUS server to send the authenticate request by enabling the directed request option. If you enable this option, the user can log in as *username@hostname*, where the *hostname* is the name of a configured RADIUS server.

To allow users logging into an MDS switch to select a RADIUS server for authentication using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **RADIUS**.
You see the RADIUS configuration in the Information pane.
- Step 2** Click the **Defaults** tab.
You see the RADIUS default settings.
- Step 3** Check the **DirectedReq** check box for the RADIUS server.
- Step 4** Click the **Apply Changes** icon to save the changes.
-

About 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 separator value *
```

Where **protocol** is a Cisco attribute for a particular type of authorization, **separator** is = (equal sign) for mandatory attributes, and * (asterisk) is for optional attributes.

Send documentation comments to fm-docfeedback@cisco.com

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 NX-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 NX-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 role 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.

One Time Password Support

A one-time password (OTP) is a password that is valid for a single login session or transaction. OTPs avoid a number of disadvantages that are associated with usual (static) passwords. The most vital disadvantage that is addressed by OTPs is that, they are not at risk to replay attacks. If an intruder manages to record an OTP that was already used to log into a service or to conduct an operation, it will not be misused as it will no longer be valid.

Send documentation comments to fm-docfeedback@cisco.com

One Time Password is applicable only to RADIUS and TACACS protocol daemons. With a RADIUS protocol daemon, there is no configuration required from the switch side. With a TACACS protocol, ascii authentication mode needs to be enabled. .

Configuring TACACS+ Server Monitoring Parameters

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.

This section includes the following topics:

- [About TACACS+, page 4-18](#)
- [About TACACS+ Server Default Configuration, page 4-18](#)
- [About the Default TACACS+ Server Encryption Type and Preshared Key, page 4-19](#)
- [Setting the Default TACACS+ Server Encryption Type and Preshared Key, page 4-19](#)
- [Setting the Default TACACS+ Server Timeout Interval and Retransmits, page 4-20](#)
- [About TACACS+ Servers, page 4-20](#)
- [Configuring a TACACS+ Server, page 4-21](#)
- [About Validating a TACACS+ Server, page 4-24](#)
- [Displaying TACACS+ Server Statistics, page 4-25](#)
- [About Users Specifying a TACACS+ Server at Login, page 4-25](#)
- [Allowing Users to Specify a TACACS+ Server at Login, page 4-25](#)

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 TACACS+ has the following advantages over RADIUS authentication:

- Provides independent, modular AAA facilities. Authorization can be done without authentication.
- Uses the TCP transport protocol to send data between the AAA client and server, making 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.

About TACACS+ Server Default Configuration

Fabric Manager allows you to set up a default configuration that can be used for any TACACS+ server that you configure the switch to communicate with. The default configuration includes:

- Encryption type
- Preshared key
- Timeout value
- Number of retransmission attempts

Send documentation comments to fm-docfeedback@cisco.com

- Allowing the user to specify a TACACS+ server at login

About the Default TACACS+ Server Encryption Type and Preshared Key

You need to configure the TACACS+ preshared key to authenticate the switch to the TACACS+ 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 TACACS+ server configurations on the switch.

You can override this global key assignment by explicitly using the **key** option when configuring and individual TACACS+ server.

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.

Setting the Default TACACS+ Server Encryption Type and Preshared Key

To configure the default TACACS+ server encryption type and preshared key using Fabric Manager, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Expand Switches > Security > AAA , and then select TACACS+ .
You see the TACACS+ configuration in the Information pane. |
| Step 2 | If the Defaults tab is dimmed, click the CFS tab. |
| Step 3 | Click the Defaults tab.
You see the TACACS+ default settings. |
| Step 4 | Select plain or encrypted from the AuthType drop-down menu and set the key in the Auth Key field. |
| Step 5 | Click the Apply Changes icon to save the changes. |
-

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 Default TACACS+ Server Timeout Interval and Retransmits”](#) section on page 4-20).



Note

You can use the dollar sign (\$) and the percent sign (%) in global secret keys.

Send documentation comments to fm-docfeedback@cisco.com

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

You can use the dollar sign (\$) and the percent sign (%) in global secret keys.

Setting the Default TACACS+ Server Timeout Interval and Retransmits

By default, a switch retries a TACACS+ server only once. This number can be configured. The maximum is five retries per server. You can also configure the timeout value for the TACACS+ server.

To configure the number of retransmissions and the time between retransmissions to the TACACS+ servers using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **TACACS+**.
You see the TACACS+ configuration in the Information pane.
 - Step 2** Click the **Defaults** tab. (If the **Defaults** tab is disabled, click the **CFS** tab first).
You see the TACACS+ default settings.
 - Step 3** Supply values for the Timeout and Retransmits fields for authentication attempts.
 - Step 4** Click the **Apply Changes** icon to save the changes.
-

Setting the Timeout Value

You can configure a global timeout value between transmissions for all TACACS+ servers.



Note

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

About TACACS+ Servers

By default, the TACACS+ feature is disabled in all switches in the Cisco MDS 9000 Family. Fabric Manager or Device Manager enables the TACACS+ feature automatically when you configure a TACACS+ server.

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.

Send documentation comments to fm-docfeedback@cisco.com

**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.

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.

Configuring a TACACS+ Server

To configure a TACACS+ server and all its options using Fabric Manager, follow these steps:

- Step 1** Expand **Switches > Security > AAA**, and then select **TACACS+**.
You see the TACACS+ configuration in the Information pane.
- Step 2** Click the **Servers** tab.
You see any existing TACACS+ servers.
- Step 3** Click **Create Row** to add a new TACACS+ server.
You see the Create TACACS+ Server dialog box as shown in [Figure 4-5](#).

Figure 4-5 Create TACACS+ Server Dialog Box

- Step 4** Select the switches that you want to assign as TACACS servers.

Send documentation comments to fm-docfeedback@cisco.com

- Step 5** Assign an index number to identify the TACACS server.
 - Step 6** Select the IP address type for the TACACS server.
 - Step 7** Fill in the IP address or name for the TACACS server.
 - Step 8** Modify the authentication and accounting ports used by this TACACS server.
 - Step 9** Select the appropriate key type for the TACACS server.
 - Step 10** Select the TimeOut value in seconds. The valid range is 0 to 60 seconds.
 - Step 11** Select the number of times the switch tries to connect to a TACACS server(s) before reverting to local authentication.
 - Step 12** Enter the test idle time interval value in minutes. The valid range is 1 to 1440 minutes.
 - Step 13** Enter the test user with the default password. The default username is test.
 - Step 14** Click **Create** to save these changes.
-

Configuring TACACS+ Server Monitoring Parameters

You can configure parameters for monitoring TACACS+ servers.

This section includes the following topics:

- [Configuring the TACACS+ Test Idle Timer, page 4-22](#)
- [Configuring Test Username, page 4-22](#)
- [Configuring the Dead Timer, page 4-22](#)

Configuring the TACACS+ Test Idle Timer

The test idle timer specifies the interval during which a TACACS+ server receives no requests before the MDS switch sends out a test packet.



Note

The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic TACACS+ server monitoring is not performed.

Configuring Test Username

You can configure a username and password for periodic TACACS+ server status testing. You do not need to configure the user name and password to monitor TACACS+ servers. You can use the default test username (test) and default password (test).

Configuring the Dead Timer

The dead timer specifies the interval that the MDS switch waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

Send documentation comments to fm-docfeedback@cisco.com

**Note**

The default dead timer value is 0 minutes. TACACS+ server monitoring is not performed if the dead timer interval is 0 minutes, unless the TACACS+ server is a part of a bigger group with the dead-time interval greater than 0 minutes. (See [“Configuring RADIUS Server Monitoring Parameters”](#) section on page 4-9).

**Note**

If the dead timer of a dead TACACS+ server expires before it is sent a TACACS+ test message, that server is marked as alive again even if it is still not responding. To avoid this scenario, configure a test user with a shorter idle time than the dead timer time.

Send documentation comments to fm-docfeedback@cisco.com

Sending TACACS+ Test Messages for Monitoring

You can manually send test messages to monitor a TACACS+ server.

Password Aging Notification through TACACS+ Server

Password aging notification is initiated when the user authenticates to a Cisco MDS 9000 switch via a TACACS+ account. The user is notified when a password is about to expire or has expired. If the password has expired, user is prompted to change the password.



Note

As of Cisco MDS SAN-OS Release 3.2(1), only TACACS+ supports password aging notification. If you try to use RADIUS servers by enabling this feature, RADIUSs will generate a SYSLOG message and authentication will fall back to the local database.

Password aging notification facilitates the following:

- Password change—You can change your password by entering a blank password.
- Password aging notification—Notifies password aging. Notification happens only if the AAA server is configured and MSCHAP and MSCHAPv2 is disabled.
- Password change after expiration—Initiates password change after the old password expires. Initiation happens from the AAA server.



Note

Password aging notification fails if you do not disable MSCHAP and MSCHAPv2 authentication.

About Validating a TACACS+ Server

As of Cisco SAN-OS Release 3.0(1), you can periodically validate a TACACS+ server. The switch sends a test authentication to the server using the test username and test password that you configure. If the server does not respond to the test authentication, then the server is considered nonresponding.



Note

We recommend that you do not configure the test user on your TACACS+ server for security reasons.

You can configure this option to test the server periodically, or you can run a one-time only test.

Periodically Validating a TACACS+ Server

To configure the switch to periodically test a TACACS+ server using Fabric Manager, see the “[Configuring TACACS+ Server Monitoring Parameters](#)” section on page 4-18.

[Send documentation comments to fm-docfeedback@cisco.com](mailto:fm-docfeedback@cisco.com)

Displaying TACACS+ Server Statistics

To display TACACS+ server statistics using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **TACACS+**.
You see the TACACS+ configuration in the Information pane.
- Step 2** Choose the **Statistics** tab.
You see the TACACS+ server statistics.
-

About Users Specifying a TACACS+ Server at Login

By default, an MDS switch forwards an authentication request to the first server in the TACACS+ server group. You can configure the switch to allow the user to specify which TACACS+ server to send the authenticate request. If you enable this feature, the user can log in as *username@hostname*, where the *hostname* is the name of a configured TACACS+ server.

Allowing Users to Specify a TACACS+ Server at Login

To configure the switch to allow users to specify a TACACS+ server at login using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **TACACS+**.
You see the TACACS+ configuration in the Information pane.
- Step 2** Click the **Defaults** tab.
You see the TACACS+ default settings.
- Step 3** Check the **DirectedReq** check box.
- Step 4** Click the **Apply Changes** icon to save the changes.
-

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.

The AAA server monitoring feature can mark an AAA server as dead. You can configure a period of time in minutes to elapse before the switch sends requests to a dead AAA server. (See the [“AAA Server Monitoring”](#) section on page 4-5).

This section includes the following topics:

- [About Configuring Server Groups, page 4-26](#)
- [Configuring Server Groups, page 4-26](#)

Send documentation comments to fm-docfeedback@cisco.com

About Configuring Server Groups

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

Configuring Server Groups

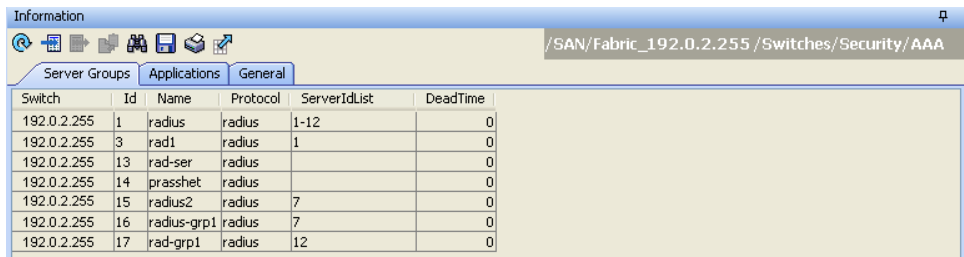
To configure a RADIUS or TACACS+ server group using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security**, and then select **AAA**.

You see the AAA configuration in the Information pane shown in [Figure 4-6](#). If you do not see the screen in [Figure 4-6](#), click the **Server Groups** tab.

You see the RADIUS or TACACS+ server groups configured.

Figure 4-6 AAA Server Groups



Switch	Id	Name	Protocol	ServerIdList	DeadTime
192.0.2.255	1	radius	radius	1-12	0
192.0.2.255	3	rad1	radius	1	0
192.0.2.255	13	rad-ser	radius		0
192.0.2.255	14	prasshet	radius		0
192.0.2.255	15	radius2	radius	7	0
192.0.2.255	16	radius-grp1	radius	7	0
192.0.2.255	17	rad-grp1	radius	12	0

Step 2 Click **Create Row** to create a server group.

You see the Create Server dialog box.

Step 3 Click the **radius** radio button to add a RADIUS server group or the **tacacs+** radio button to add a TACACS+ server group.

Step 4 Supply server names for the ServerIdList field.

Step 5 Set the DeadTime field for the number of minutes that a server can be nonresponsive before it is marked as bypassed. See the [“About Bypassing a Nonresponsive Server”](#) section on page 4-27.

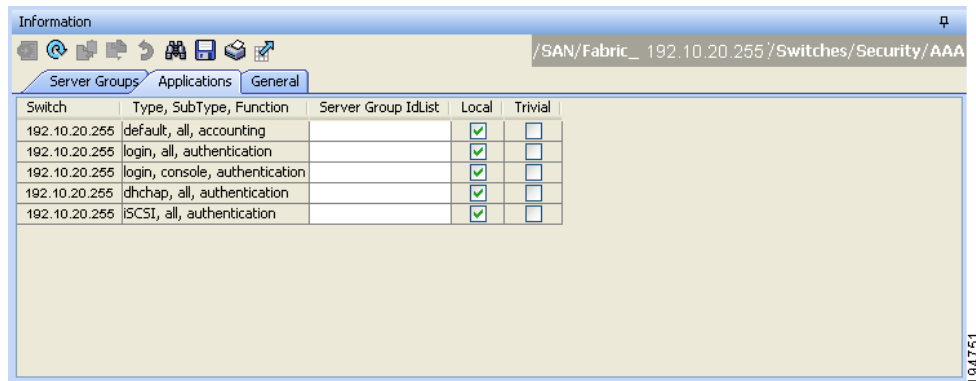
Step 6 Click **Create** to create this server group.

Step 7 Click the **Applications** tab to assign this server group to an application (see [Figure 4-7](#)).

You can associate a server group with all applications or you can specify certain applications.

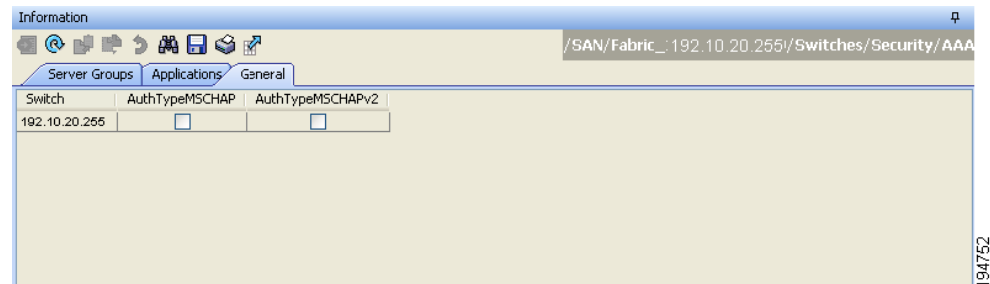
Send documentation comments to fm-docfeedback@cisco.com

Figure 4-7 Applications Tab



- Step 8** Click the **General** tab to assign the type of authentication to this server group (see Figure 3-8). Check either the MSCHAP or MSCHAPv2 check box based on the type of server group.

Figure 4-8 General Tab



- Step 9** Click the **Apply Changes** icon to save the changes.



Note Configuration of a TACACS+ group fails if MSCHAPv2 authentication is not disabled.

About Bypassing a Nonresponsive Server

As of Cisco SAN-OS Release 3.0(1), you can bypass a nonresponsive AAA server within a server group. If the switch detects a nonresponsive server, it will bypass that server when authenticating users. Use this feature to minimize login delays caused by a faulty server. Instead of sending a request to a nonresponsive server and waiting for the authentication request to timeout, the switch sends the authentication request to the next server in the server group. If there are no other responding servers in the server group, the switch continues to attempt authentications against the nonresponsive server.

AAA Server Distribution

Configuration for RADIUS and TACACS+ AAA on an MDS switch can be distributed using the Cisco Fabric Services (CFS). The distribution is disabled by default (see the *Cisco Fabric Manager System Management Configuration Guide*).

Send documentation comments to fm-docfeedback@cisco.com

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.

This section includes the following topics:

- [Enabling AAA Server Distribution, page 4-28](#)
- [Starting a Distribution Session on a Switch, page 4-29](#)
- [Displaying the Session Status, page 4-29](#)
- [Displaying the Pending Configuration to be Distributed, page 4-29](#)
- [Committing the Distribution, page 4-29](#)
- [Discarding the Distribution Session, page 4-30](#)
- [Clearing Sessions, page 4-30](#)
- [Merge Guidelines for RADIUS and TACACS+ Configurations, page 4-30](#)

**Note**

For an MDS switch to participate in AAA server configuration distribution, it must be running Cisco MDS SAN-OS Release 2.0(1b) or later, or Cisco NX-OS Release 4.1(1).

Enabling AAA Server Distribution

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

To enable RADIUS server distribution using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **RADIUS**.
You see the RADIUS configuration in the Information pane.
- Step 2** Click the **CFS** tab. You see the RADIUS CFS configuration.
- Step 3** Choose **enable** from the Admin drop-down list for all switches that you want to enable CFS for RADIUS.
- Step 4** Click **Apply Changes** to distribute these changes through the fabric.
-

To enable TACACS+ server distribution using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select **TACACS+**.
You see the TACACS+ configuration in the Information pane.
- Step 2** Click the **CFS** tab.
You see the TACACS+ CFS configuration.

Send documentation comments to fm-docfeedback@cisco.com

- Step 3** Choose **enable** from the Admin drop-down list for all switches that you want to enable CFS on for TACACS+.
- Step 4** Click **Apply Changes** to distribute these changes through the fabric.
-

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 that are created (including the configuration that caused the distribution session start) are stored in a temporary buffer, not in the running configuration.

Displaying the Session Status

Once the implicit distribution session has started, you can check the session status from Fabric Manager by expanding **Switches > Security > AAA**, and selecting **RADIUS** or **TACACS+**.

Displaying the Pending Configuration to be Distributed

To display the RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer using Fabric Manager, follow these steps:

- Step 1** Expand **Switches > Security > AAA**, and then select **RADIUS** or select **TACACS+**.
- Step 2** Click the **CFS** tab.
- You see the distribution status on the CFS tab.
- Step 3** Click the **pending** or **running** radio button.
- Step 4** Click **Apply Changes** to save the changes.
- Step 5** Click the **Servers** tab to view the pending or running configuration.
-

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).

Send documentation comments to fm-docfeedback@cisco.com

To distribute a RADIUS or TACACS+ configuration using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select either **RADIUS** or **TACACS+**. You see the RADIUS or TACACS+ configuration in the Information pane.
 - Step 2** Click the **CFS** tab. You see the RADIUS or TACACS+ CFS configuration.
 - Step 3** Choose **commitChanges** in the Config Action drop-down list for all switches that you want to enable CFS for RADIUS or TACACS+.
 - Step 4** Click **Apply Changes** to distribute the changes through the fabric.
-

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 not applied.

To discard RADIUS or TACACS+ distribution using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA**, and then select either **RADIUS** or **TACACS+**. You see either the RADIUS or TACACS+ configuration in the Information pane.
 - Step 2** Click the **CFS** tab. You see either the RADIUS or TACACS+ CFS configuration.
 - Step 3** Choose **abort** from the Config Action drop-down list for each switch that should discard the pending RADIUS or TACACS+ distribution.
 - Step 4** Click **Apply Changes**.
-

Clearing Sessions

To clear a RADIUS or TACACS+ distribution using Fabric Manager, follow these steps:

-
- Step 1** Expand **Switches > Security > AAA** and then select either **RADIUS** or **TACACS+**. You see either the RADIUS or TACACS+ configuration in the Information pane.
 - Step 2** Choose the **CFS** tab. You see either the RADIUS or TACACS+ CFS configuration.
 - Step 3** Choose **clear** from the Config Action drop-down list for each switch that should clear the pending RADIUS or TACACS+ distribution.
 - Step 4** Click **Apply Changes**.
-

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.

Send documentation comments to fm-docfeedback@cisco.com

When merging the fabric, consider the following conditions:

- The server groups are not merged.
- The server and global keys are not changed during the 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 configuration.

**Note**

The test parameter is distributed through CFS for the TACACS+ Daemon only. If the fabric contains NX-OS 5.0(1) release machines, then the test parameters will be distributed. If the fabric contains machines running NX-OS 5.0(1) release and some running NX-OS release 4.x version, the test parameters will be not distributed.

**Caution**

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

CHAP Authentication

CHAP (Challenge Handshake Authentication Protocol) is a challenge-response authentication protocol that uses the industry-standard Message Digest 5 (MD5) hashing scheme to encrypt the response. CHAP is used by various vendors of network access servers and clients. A server running routing and Remote Access supports CHAP so that remote access clients that require CHAP are authenticated. CHAP is supported as an authentication method in this release.

MSCHAP Authentication

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP.

Cisco MDS 9000 Family switches allow user logins to perform remote authentication using different versions of MSCHAP. MSCHAP is used for authentication on a RADIUS or TACACS+ server, while MSCHAPv2 is used for authentication on a RADIUS server.

About Enabling MSCHAP

By default, the switch uses Password Authentication Protocol (PAP) authentication between the switch and the remote server. If you enable MSCHAP, you need to configure your RADIUS server to recognize the MSCHAP vendor-specific attributes. See the [“About Vendor-Specific Attributes” section on page 4-16](#). [Table 4-1](#) shows the RADIUS vendor-specific attributes required for MSCHAP.

Send documentation comments to fm-docfeedback@cisco.com

Table 4-1 *MSCHAP RADIUS Vendor-Specific Attributes*

Vendor-ID Number	Vendor-Type Number	Vendor-Specific Attribute	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by an AAA server to an MSCHAP user. It can be used in both Access-Request and Access-Challenge packets.
211	11	MSCHAP-Response	Contains the response value provided by an MS-CHAP user in response to the challenge. It is only used in Access-Request packets.

Enabling MSCHAP Authentication



Note

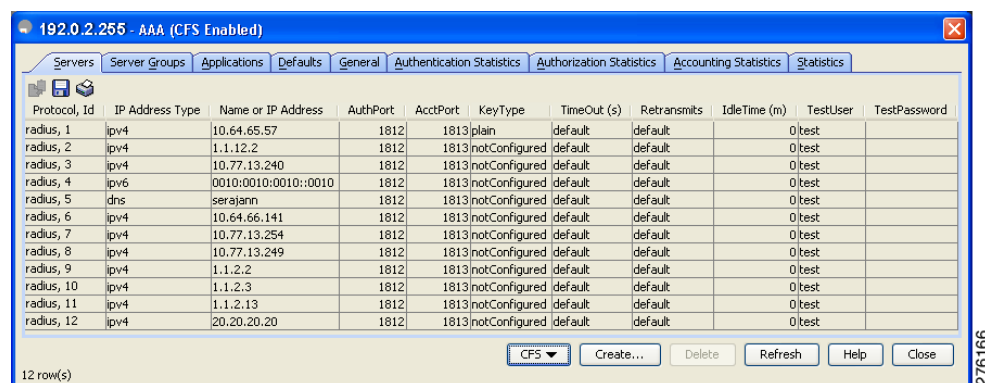
Password aging, MSCHAPv2 and MSCHAP authentication can fail if one of these authentication is not disabled.

To enable MSCHAP authentication using Device Manager, follow these steps:

Step 1 Click **Security > AAA**.

You see the AAA configuration in the Information pane (see [Figure 4-9](#)).

Figure 4-9 *AAA Configuration in Device Manager*

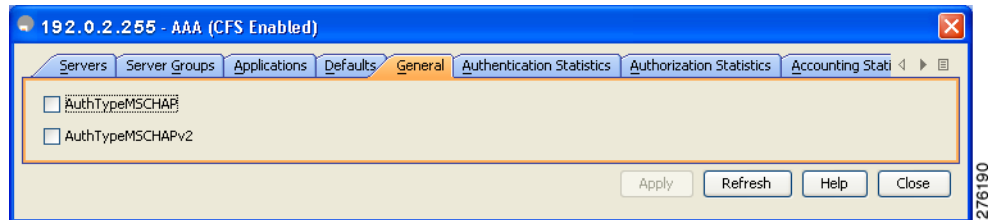


Step 2 Click the **General** tab.

You see the MSCHAP configuration (see [Figure 4-10](#)).

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-10 MSCHAP Configuration



- Step 3** Check the **AuthTypeMSCHAP** or **AuthTypeMSCHAPv2** check box to use MSCHAP or MSCHAPv2 to authenticate users on the switch.
- Step 4** Click **Apply Changes** to save the changes.

Local AAA Services

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

Disabling AAA Authentication

You can turn off password verification using the **none** option. If you configure this option, users can log in 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 can access the switch at any time.

Refer to the *Cisco MDS 9000 Family NX-OS Security Configuration Guide* to configure this option.

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.

Send documentation comments to fm-docfeedback@cisco.com



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.

Configuring Cisco Access Control 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 4-11](#), [Figure 4-12](#), [Figure 4-13](#), and [Figure 4-14](#) display ACS server user setup configurations for network-admin roles and multiple roles using either RADIUS or TACACS+.

Figure 4-11 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 "Command:" field, an "Arguments:" text area, and "Unlisted arguments" radio buttons (Permit, Deny). Below this is the "Cisco IOS/PIX RADIUS Attributes" section, which contains a checked checkbox for "[009/001] cisco-av-pair" and a text area with the value "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 are sections for "Account Disabled Status" and "Deleting a Username".

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-12 Configuring Multiple Roles with SNMPv3 Attributes When Using RADIUS

The screenshot shows the CiscoSecure ACS web interface in a Netscape browser window. The main content area is titled "User Setup" and contains the following sections:

- Per User Command Authorization:**
 - Unmatched Cisco IOS commands:
 - ☐ Permit
 - ☒ Deny
 - Command:
 - Arguments:
 - Unlisted arguments:
 - ☐ Permit
 - ☒ Deny
- Cisco IOS/PIX RADIUS Attributes:**
 - ☒ [009V001] cisco-av-pair
 - Attributes: `shell:roles="Role1 Role3 Role5 Role7"snmpv3:auth=MD5 priv=DES`

At the bottom of the main area are buttons for "Submit", "Delete", and "Cancel".

On the right side, there is a "Help" panel 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](#)
- [RADIUS Vendor-Specific Attributes](#)

Below the links, there is a section titled "Account Disabled Status" with the text: "Select the Account Disabled check box to disable this account; clear the check box to enable the account." and a link [\[Back to Top\]](#).

At the bottom of the help panel, there is a section titled "Deleting a Username".

The status bar at the bottom of the browser window shows "Applet dialup_filter started" and the page number "120576".

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-13 Configuring the network-admin Role with SNMPv3 Attributes When Using TACACS+

The screenshot shows the Cisco 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 contains a 'TACACS+ Settings' section. This section has checkboxes for 'PPP IP', 'In access control list', 'Out access control list', 'Route', 'Routing', and 'Custom attributes'. Below these is a note: 'Note: PPP LCP will be automatically enabled if this service is enabled'. The 'Shell (exec)' section is checked and includes checkboxes for 'Access control list', 'Auto command', 'Callback line', 'Callback rotary', 'Idle time', 'No callback verify', 'No escape', 'No hangup', 'Privilege level', and 'Timeout'. The 'Custom attributes' section contains the text: 'cisco-av-pair=shell:roles="Role1 Role3" snmpv3:auth=MD5 priv=DES'. At the bottom are 'Submit', 'Delete', and 'Cancel' buttons. On the right is a 'Help' panel 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 are sections for 'Account Disabled Status' and 'Deleting a Username'.

Send documentation comments to fm-docfeedback@cisco.com

Figure 4-14 Configuring Multiple Roles with SNMPv3 Attributes When Using TACACS+

User Setup

TACACS+ Settings

☐ PPP IP

☐ In access control list

☐ Out access control list

☐ Route

☐ Routing

☐ Custom attributes

☐ Enabled

Note: PPP LCP will be automatically enabled if this service is enabled

☒ Shell (exec)

☐ Access control list

☐ Auto command

☐ Callback line

☐ Callback rotary

☐ Idle time

☐ No callback verify

☐ No escape

☐ No hangup

☐ Privilege level

☐ Timeout

☒ Custom attributes

cisco-av-pair*shell:roles="network-admin"snmpv3:auth=md5priv=aes-128

Submit Delete Cancel

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

The Delete button appears only when you are editing

Default Settings

Table 4-2 lists the default settings for all switch security features in any switch.

Table 4-2 Default Switch Security Settings

Parameters	Default
Roles in Cisco MDS switches	Network operator (network-operator)
AAA configuration services	Local
Authentication port	1812
Accounting port	1813
Preshared key communication	Clear text

Send documentation comments to fm-docfeedback@cisco.com

Table 4-2 **Default Switch Security Settings (continued)**

Parameters	Default
RADIUS server timeout	1 (one) second
RADIUS server retries	Once
Authorization	Disabled
aaa user default role	enabled
RADIUS server directed requests	Disabled
TACACS+	Disabled
TACACS+ servers	None configured
TACACS+ server timeout	5 seconds
TACACS+ server directed requests	Disabled
AAA server distribution	Disabled
Accounting log size	250 KB