



## Administering the Firewall Services Module

This chapter describes how to administer the Firewall Services Module and contains these sections:

- [Administering the Software Images, page 5-1](#)
- [Changing and Recovering Passwords, page 5-11](#)
- [Resetting the Firewall Services Module, page 5-14](#)
- [Troubleshooting the Firewall Services Module, page 5-16](#)

### Administering the Software Images

Five partitions on the compact Flash contain the following information:

- Maintenance partition (MP) (cf:1) contains the maintenance image. You use the maintenance partition to upgrade or install all application images, reset the application image password, and display the crash dump information.
- Network configuration partition (cf:2) contains the network configuration of the maintenance image.
- Crash dump partition (cf:3) is used to store the crash dump information.
- Application partitions (APs) (cf:4 and cf:5) store the firewall image and configuration.

You can have two application images stored in Flash. One image in partition 4 and one in partition 5. Depending on which partition you want to boot, you can use cf:4 or cf:5 in the **boot device module module\_number partition\_number** command. For example:

```
Router(config)# boot device module 3 cf:5  
Router(config)# boot device module 4 cf:4
```

The configurations related to that image is stored in the same partition as the image.

If the module's application partition gets corrupted, the maintenance partition can be used to recover the application configuration. The network configuration partition stores the network parameters for the maintenance partition.

When the application image fails, a log is created in the crash dump partition, which contains all failure-related information. You can use this log later for debugging using the **show crashdump** CLI command from both the maintenance partition and the application partition, if the application partition recovers without a problem on restart.

You can also upgrade the application from the maintenance partition. You can clear the enable password for the module from the maintenance partition CLI.

This section contains the various administrative tasks you can perform using the software images:

- [Quick Software Upgrade, page 5-2](#)
- [Logging into the Application Software, page 5-3](#)
- [Logging into the Maintenance Software, page 5-3](#)
- [Upgrading Software Images, page 5-5](#)

## Quick Software Upgrade



### Caution

Upgrading the software image is a disaster recovery process. The procedure erases the flash or nvram of the firewall services module. Ensure that your configuration has been backed up so that you can restore it after the software upgrade.

To quickly upgrade the Firewall Services Module software image, follow these steps:

- Step 1** Make the new software image available on a TFTP server, or make the MSFC a TFTP server by using this command:

```
msfc(config)# tftp-server bootflash: image name
```

- Step 2** If the MSFC is the TFTP server, make sure you have a VLAN interface on the MSFC reachable from the module. For example:

- a. On the MSFC, enter these commands:

```
router(config)# interface vlan30
router(config)# description to_fwsm_vlan_30
router(config)# ip address 10.20.30.2 255.255.255.0
router(config)# no ip redirects
```

- b. On the module, enter these commands:

```
nameif vlan30 inside security100
...
ip address inside 10.20.30.5 255.255.255.0
```

- c. From the module make sure that you can ping the MSFC, by entering this command:

```
FWSM# ping 10.20.30.2
10.20.30.2 response received -- 0ms
10.20.30.2 response received -- 0ms
10.20.30.2 response received -- 0ms
```

- Step 3** From the module enter the **copy tftp flash** command:

```
FWSM# copy tftp flash
Address or name of remote host [127.0.0.1]? 10.20.30.2
Source file name [cdisk]? c6svc-fw-m-k9.1-1-0-207.bin
copying tftp://10.20.30.2/c6svc-fw-m-k9.1-1-0-207.bin to flash:image
[yes|no|again]? yes
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The output shows the MSFC as the TFTP server.

- Step 4** Reload the module by entering this command:

```
FWSM# reload
```

```
Proceed with reload? [confirm]
```

---

## Logging into the Application Software

The application software has one user level. Use the **enable** command in the EXEC mode to log into the application partition.

Refer to the “[Changing and Recovering Passwords](#)” section on page 5-11 if you need to change or recover passwords.

To log into the Firewall Services Module, follow these steps:

**Step 1** Log into the Catalyst 6500 series switch using the Telnet connection or the console port connection.

**Step 2** At the CLI prompt, establish a console session with the module using the **session slot slot\_number processor 1** command:

### Cisco IOS:

```
Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote
prompt to end the session Trying 127.0.0.81 ... Open
Cisco Maintenance image
```

### Catalyst Operating System:

```
Console> session 8
The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote
prompt to end the session Trying 127.0.0.81 ... Open
Cisco Maintenance image
```

**Step 3** If the module does not boot into the application partition, reset the module with the following command:

### Cisco IOS:

```
Router# hw-module module slot_number reset cf:4
```

### Catalyst Operating System:

```
Console(enable)> reset module-number [boot device:partition]
Console(enable)> reboot
```

---

## Logging into the Maintenance Software

The maintenance software has two user levels with different access privileges:

- **root**—Allows you to configure the network partition parameters, upgrade the software images on the application partitions, change the guest account password, and enable or disable the guest account.

The default password is **cisco**.

- **guest**— Allows you to configure the network partition parameters and show crash dump information.

The default password is **cisco**.

Refer to the [“Changing and Recovering Passwords”](#) section on page 5-11 if you need to change or recover passwords.

To log into the Firewall Services Module maintenance partition, follow these steps:

**Step 1** Log into the Catalyst 6500 series switch using the Telnet connection or the console port connection.

**Step 2** At the CLI prompt, establish a console session with the module using the Cisco IOS **session slot slot\_number processor 1** command or the Catalyst operating system **session mod** command.

**Cisco IOS:**

```
Router# session slot 8 processor 1
The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote
prompt to end the session Trying 127.0.0.81 ... Open
Cisco Maintenance image
```

**Catalyst Operating System:**

```
Console> session 8
The default escape character is Ctrl-^, then x. You can also type 'exit' at the remote
prompt to end the session Trying 127.0.0.81 ... Open
Cisco Maintenance image
```

**Step 3** At the Maintenance software login prompt, enter **root** to log in as the root user or **guest** to log in as a guest user.

```
login: root
```

**Step 4** At the password prompt, enter the password for the account. The default password for both accounts is **cisco**.

```
Password:
```

After a successful login, the command line prompt appears as follows:

```
Maintenance image version: 1.1(0.3)
root@localhost#
```

**Step 5** If the module does not boot into the maintenance partition, reset the module with the following commands:

**Cisco IOS:**

```
Router# hw-module module slot_number reset cf:1
```

**Catalyst Operating System:**

```
Console(enable)> reset module-number [boot device:partition]
Console(enable)> reboot
```

## Upgrading Software Images

You can upgrade both the application software and the maintenance software. To upgrade the application software, see the [“Upgrading the Application Software” section on page 5-6](#). To upgrade the maintenance software, see the [“Upgrading the Maintenance Software” section on page 5-9](#).

The entire application and maintenance partitions are stored on the FTP or TFTP server. The images are downloaded and extracted to the application or maintenance partition depending on which image is being upgraded.

To upgrade the application partition, change the boot sequence to boot the module from the maintenance partition. The maintenance partition downloads and installs the application image. The supervisor engine must be executing the run-time image to provide network access to the maintenance partition.

Set the boot sequence for the module using the supervisor engine CLI commands. As the maintenance partition boots, it determines the application type. If the network parameters are already configured, you can directly download the new image. If network parameters are not set, you need to manually configure them.

When you specify the target device and partition number for upgrading the application partition, software recognition checks are made to ensure that you do not upgrade the maintenance partition.

Before starting the upgrade process, you will need these software images:

- The application image for the module.
- The maintenance partition image for the module.

A TFTP and FTP server are required to copy the images. The TFTP server should be connected to the switch and the port connecting to the TFTP server should be included in VLAN 1 on the switch.

Another TFTP server is required in the network. This TFTP server must be reachable from the module when the module image is booted up.

## Upgrading the Application Software

To upgrade the application software image you must first copy the firewall software image to a directory accessible to FTP, and then log in to the switch through the console port or through a Telnet session.

To upgrade the application partition software, perform these tasks:

	Command	Purpose
Step 1	Cisco IOS: <pre>Router# hw-module module slot_number reset cf:1</pre> Catalyst Operating System: <pre>Console&gt;(enable) reset module-number boot cf:1</pre>	Reboots the module into the maintenance partition.
Step 2	Cisco IOS: <pre>Router# session slot slot_number processor 1</pre> Catalyst Operating System: <pre>Console&gt;(enable) session module</pre>	Establishes a console session with the module.
Step 3	<pre>login:root</pre>	At the login prompt, logs into the root account of the module.
Step 4	<pre>root@localhost# ip address ip _address netmask</pre> <pre>root@localhost# ip gateway ip_address</pre>	Assigns an IP address and a default gateway to the maintenance partition.  Because the module maintenance partition can only use VLAN 1 on the switch, use the IP addresses and gateway for VLAN 1. The FTP server is reachable after the IP parameters are specified.

	Command	Purpose
Step 5	root@localhost# <b>show ip</b>	Displays the current settings. If the parameters are not correct, use the commands described in <a href="#">Step 4</a> . The module image should be available on the FTP server reachable through VLAN 1.
Step 6	root@localhost# <b>ping ip_address</b>	Pings the FTP server to verify if the configuration is correct.
Step 7	root@localhost# <b>upgrade ftp_url cf:x</b>	<p>Upgrades the application image from the appropriate directory on the FTP server that is reachable from the module.</p> <p>The <i>ftp_url</i> values contain the following options:</p> <ul style="list-style-type: none"> <li>The username to log in to the FTP server. The command prompts for the password. Enter the password for the username you are using to log in to the FTP server.</li> <li><i>ftp_url</i> is the IP address of the FTP server and the complete path of the file on the FTP server.</li> </ul> <p><b>Note</b> If the FTP server does not allow anonymous users, use the following syntax for the <i>ftp-url</i> value: <b>ftp://user@host/absolute-path/filename.</b></p> <p>Enter your password when prompted.</p> <ul style="list-style-type: none"> <li><i>cf:x</i> is the partition where the image must be copied on the compact Flash. Use partitions cf:4 or cf:5 for this step.</li> </ul>
Step 8		<p>Follow the screen prompts during the upgrade.</p> <p>The image is copied from the FTP server to the compact Flash. The upgrade command also ensures that the configuration on the corresponding application partition is backed up and restored at the end of the upgrade operation.</p>
Step 9	Router# <b>logout</b>	Logs out of the maintenance software.
Step 10	<p>Cisco IOS:</p> <pre>Router# <b>hw-module module slot_number reset cf:4</b></pre> <p>Catalyst Operating System:</p> <pre>Console&gt;(enable) <b>reset module-number boot cf:4</b></pre>	Resets the module into the application partition.

This example shows how to upgrade the Firewall Services Module application software:

```
Router# hw-module module 9 reset cf:1

Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:16:06:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:16:06:SP:The PC in slot 9 is shutting down. Please wait ...
00:16:21:SP:PC shutdown completed for module 9
```

```
00:16:21:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:16:24:SP:Resetting module 9 ...
00:16:24:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:18:21:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:18:21:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:18:21:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
```

```
Router# session slot 9 proc 1
```

```
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open
```

```
Cisco Maintenance image
```

```
login:root
```

```
Password:
```

```
Maintenance image version: 1.1(0.3)
```

```
root@localhost.cisco.com# upgrade
```

```
ftp://user:password@address/tftpboot/user/c6svc-fwk9.1-1-0-170.bin cf:4
```

```
Downloading the image. This may take several minutes...
```

```
ftp://user:password@address/tftpboot/c6svc-fwk9.1-1-0-170.bin (5919K)
/tmp/upgrade.gz [#####] 5919K | 821.24K/s
6061947 bytes transferred in 7.38 sec (821.23k/sec)
```

```
Upgrade file ftp://ftp://user:password@address/tftpboot/user/c6svc-fwk9.1-1-0-170.bin
.gz is downloaded.
```

```
Upgrading will wipe out the contents on the hard disk.
```

```
Do you want to proceed installing it [y|N]:y
```

```
Proceeding with upgrade. Please do not interrupt.
```

```
If the upgrade is interrupted or fails, boot into
```

```
Maintenance image again and restart upgrade.
```

```
Proceeding with image upgrade.
```

```
Backing up FWSM configuration.
```

```
Restoring FWSM configuration.
```

```
Application image upgrade complete. You can boot the image now.
```

```
Partition upgraded successfully.
```

```
root@hostname.cisco.com# logout
```

```
[Connection to 127.0.0.91 closed by foreign host]
```

```
Router# hw-module module 9 reset
```

```
Device BOOT variable for reset =
```

```
Warning:Device list is not verified.
```

```
Proceed with reload of module? [confirm] y
```

```
% reset issued for module 9
```

```
Router#
```

```
00:24:04:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
```

```

00:24:04:SP:The PC in slot 9 is shutting down. Please wait ...
00:24:18:SP:PC shutdown completed for module 9
00:24:18:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:24:21:SP:Resetting module 9 ...
00:24:21:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:26:19:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:26:19:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:26:19:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online

```

The module is now upgraded and ready for further firewall configuration. You can do further application partition upgrades from the module console, by entering the command:

```
copy tftp://tftp_ip/file_name flash:
```

## Upgrading the Maintenance Software

To upgrade the maintenance software image, you must first copy the module maintenance software image to a directory accessible to TFTP, and then log into the switch through the console port or through a Telnet session.



### Note

If you have changed the passwords for the root and guest accounts of the maintenance partition, they will be retained across upgrades.

To upgrade the maintenance partition software, perform these tasks:

	Command	Purpose
<b>Step 1</b>	Cisco IOS: <pre>Router# <b>hw-module module</b> <i>slot_number</i> <b>reset cf:4</b></pre> Catalyst Operating System: <pre>Console&gt; (enable) <b>reset</b> <i>module-number</i> <b>cf:4</b></pre>	Reboots the module into the application partition.
<b>Step 2</b>	Cisco IOS: <pre>Router# <b>session slot</b> <i>slot_number</i> <b>processor 1</b></pre> Catalyst Operating System: <pre>Console&gt; (enable) <b>session</b> <i>module</i></pre>	Establishes a console session with the module. Enter <b>cisco</b> at the password prompt.

	Command	Purpose
Step 3	<pre>FWSM# upgrade-mp ftp_url tftp-path</pre>	<p>Upgrades the maintenance partition from the appropriate directory on the TFTP server that is reachable from the module.</p> <p>The <i>tftp_url</i> values contain the following:</p> <ul style="list-style-type: none"> <li>• Username is the username to log in to the TFTP server.</li> <li>• The command prompts for the password. Enter the password for the username you are using to log in to the TFTP server.</li> <li>• <i>tftp_url</i> is the IP address of the TFTP server and the complete path of the file on the TFTP server.</li> </ul> <p><b>Note</b> If the TFTP server does not allow anonymous users, use the following syntax for <i>ftp_url</i> value: <b>tftp://absolute-path/filename.</b></p> <p>Enter your password when prompted.</p> <p>Follow the screen prompts during the upgrade.</p> <p>The image is copied from the TFTP server to the compact Flash. The upgrade command also ensures that the configuration on the corresponding maintenance partition is backed up and restored at the end of the upgrade operation.</p>
Step 4	<pre>Router# logout</pre>	Logs out of the application software.
Step 5	<p>Cisco IOS:</p> <pre>Router# hw-module module slot_number reset cf:1</pre> <p>Catalyst Operating System:</p> <pre>Console&gt;(enable) reset module-number boot cf:1</pre>	Resets the module in the maintenance partition.
Step 6	<pre>root@localhost# show ip</pre>	(Optional) Verifies the initial configuration after the maintenance software comes back online after the module is reset and you log into the maintenance software's root account.
Step 7	<p>Cisco IOS:</p> <pre>Router# hw-module module slot_number reset cf:x</pre> <p>Catalyst Operating System:</p> <pre>Console&gt;(enable) reset module-number boot cf:x</pre>	(Optional) Resets the module in the application partition. You can reset the module in either cf:4 or cf:5.

This example shows how to upgrade the module maintenance software:

```
Router# hw-module module 9 reset cf:4

Device BOOT variable for reset = cf:4
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9
```

```

Router#
00:31:11:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:31:11:SP:The PC in slot 9 is shutting down. Please wait ...
00:31:25:SP:PC shutdown completed for module 9
00:31:25:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
00:31:28:SP:Resetting module 9 ...
00:31:28:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
00:33:26:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
00:33:26:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
00:33:26:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online

Router# session slot 9 proc 1

The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

fws# upgrade-mp
Address or name of remote host [160.251.101.128]? 192.168.253.79
Source file name []? mp-1.0.1-bin.gz
copying upgrade-mp tftp://10.1.1.1/tftpboot/mp.1-1-0-3.bin.gz to flash
[yes|no|again]? y
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 7700916 bytes.
Maintenance partition upgraded.

Router# hw-module module 9 reset cf:1

Device BOOT variable for reset = cf:1
Warning:Device list is not verified.

Proceed with reload of module? [confirm] y
% reset issued for module 9
Router#
02:27:19:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
02:27:19:SP:The PC in slot 9 is shutting down. Please wait ...
02:27:36:SP:PC shutdown completed for module 9
02:27:36:%C6KPWR-SP-4-DISABLED:power to module in slot 9 set off (admin
request)
02:27:39:SP:Resetting module 9 ...
02:27:39:%C6KPWR-SP-4-ENABLED:power to module in slot 9 set on
02:29:37:%SNMP-5-MODULETRAP:Module 9 [Up] Trap
02:29:37:%DIAG-SP-6-BYPASS:Module 9:Online Diagnostics is Bypassed
02:29:37:%OIR-SP-6-INSCARD:Card inserted in slot 9, interfaces are now
online
Router#

```

## Changing and Recovering Passwords

You can change and recover passwords using a Telnet connection to the module and CLI.

To change the password, use a Telnet connection to the module, and then use the **passwd** or **passwd-guest** commands to change the password.

**Note**


---

New passwords must be at least six characters in length, and may include uppercase and lowercase letters, numbers, and punctuation marks.

---

**Note**


---

If the Firewall Services Module application image password is lost, you can clear the password by booting into the maintenance image. If the module maintenance image passwords are lost for the root or guest account, you can clear both passwords by booting into the application image.

---

This section describes how to change passwords on the module:

- [Changing the Application Partition Passwords, page 5-12](#)
- [Changing the Maintenance Partition Passwords, page 5-12](#)
- [Recovering the Application Partition Passwords, page 5-13](#)
- [Recovering the Maintenance Partition Passwords, page 5-14](#)

## Changing the Application Partition Passwords

To change the application partition password, follow these steps while you are logged in to the account application account. Enter the **passwd** command with a password, for example:

```
FWSM# passwd freedom
```

If you do not enter a password, you receive the following result:

```
FWSM# passwd
Not enough arguments.
Usage: passwd <password> encrypted
```

## Changing the Maintenance Partition Passwords

To change the password, follow these steps while you are logged in to the root account on the maintenance software partition. The **passwd** command is available for the maintenance partition's root and guest account.

---

**Step 1** Enter this command:

```
root@localhost# passwd
```

**Step 2** Enter the new password:

```
Changing password for user root
New password:
```

**Step 3** Enter the new password again:

```
Retype new password:
passwd: all authentication tokens updated successfully
```

---

This example shows how to set the password for the root account:

```
root@localhost# passwd
Changing password for user root
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

To change the password for the guest account, enter the **passwd-guest** command. This command is available from the maintenance partition root account only.

---

**Step 1** Enter this command:

```
root@localhost# passwd-guest
```

**Step 2** Enter the new password:

```
Changing password for user guest
New password:
```

**Step 3** Enter the new password again:

```
Retype new password:
passwd: all authentication tokens updated successfully
```

---

This example shows how to set the password for the guest account:

```
root@localhost# passwd-guest
Changing password for user guest
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

## Recovering the Application Partition Passwords

If you have forgotten or lost the passwords for either the module application or maintenance software, they can be reset to the default values. Clearing the password resets the Telnet password to **cisco** and clears the enable password. To reset an application image password, follow these steps:

---

**Step 1** Enter this command:

```
root@localhost# clear passwd cf:partition_number
```

*partition\_number* refers to the number of the application or maintenance partition where you are resetting the password.



**Note**

If you are resetting the application password, you must be logged into the maintenance partition. If you are changing the maintenance partition password, you must be logged into the application partition.

---

**Step 2** Follow the screen prompts during the operation.

```
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
    enable password 8Ry2YjIyt7RRXU24 encrypted
    passwd 2KFQnbNIdI.2KYOU encrypted
Do you want to remove the commands listed above from the configuration?
```

```
[yn] y
Passwords and aaa commands have been erased.
```

This example shows how to clear the password for the module application software on partition 4 of the compact flash:

```
root@localhost# clear passwd cf:4
Do you wish to erase the passwords? [yn] y
The following lines will be removed from the configuration:
    enable password 8Ry2YjIyt7RRXU24 encrypted
    passwd 2KFQnbNIdI.2KYOU encrypted
Do you want to remove the commands listed above from the configuration?
[yn] y
Passwords and aaa commands have been erased.
```

## Recovering the Maintenance Partition Passwords

If you have forgotten or lost the passwords for either the module application or maintenance software, they can be reset to the default values. Clearing the password resets the Telnet password to **cisco** and clears the enable password.



### Note

If you are resetting the maintenance partition password, you must be logged into the application partition.

To reset a maintenance image password, enter this command:

```
fwsm# clear mp-passwd
```

This example shows how to clear the password for the module maintenance software on partition cf:1 of the compact Flash:

```
root@localhost# clear mp-passwd
Passwords for 'root' and 'guest' accounts cleared successfully.
```

## Resetting the Firewall Services Module

If you cannot reach the module through the CLI or an external Telnet session, enter the **reset** command to reset and reboot the module. The reset process requires several minutes.

When the module initially boots, by default it runs a partial memory test. To perform a full memory test, use the **mem-test-full** keyword in the **hw-module module *module\_number* reset device:partition mem-test-full** command.



### Note

This command is specific to Cisco IOS software and is not available in Catalyst operating system software.

A full memory test takes more time to complete than a partial memory test depending on the memory size. [Table 2-2 on page 2-12](#) lists the memory and approximate boot time for a long memory test.

This section describes how to reset the module:

[Resetting the Module with Cisco IOS Software, page 5-15](#)

[Resetting the Module with Catalyst Operating System Software, page 5-15](#)

## Resetting the Module with Cisco IOS Software

To reset the module from the CLI, perform this task in privileged mode:

Command	Purpose
<code>hw-module module <i>mod_num</i> reset</code> <code>[<i>device:partition</i>] [<i>mem-test-full</i>]</code>	Resets the module. The <i>device:partition</i> variable is the string for the boot device, for example, cf: designates the compact Flash and x is the number for the partition on each device.



### Note

For the boot device, you can specify cf:4 or cf:5 for the application image or cf:1 for the maintenance image.

This example shows how to reset the module, installed in slot 9, from the CLI:

```
Router# hw-mod mod 9 reset
```

```
Proceed with reload of module? [confirm] y
% reset issued for module 9
```

```
Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

To reboot the module from the application software, perform this task while you are sessioned into the root account on the module in the privileged mode:

Command	Purpose
<code>reboot</code> or <code>reload</code>	Reboots the module.

This example shows how to reboot the module:

```
Router# reload
```

## Resetting the Module with Catalyst Operating System Software

To reset the module from the CLI, perform this task in privileged mode:

Command	Purpose
<code>reset <i>module_number</i> [<i>boot device:partition</i>]</code>	Resets the module. The <i>device:partition</i> variable is the string for the boot device, for example, cf: designates the compact Flash and x is the number for the partition on each device.

**Note**

For the boot device, you can specify cf:4 or cf:5 for the application image or cf:1 for the maintenance image. The default boot partition for the module is cf:4.

This example shows how to reset the module, installed in slot 9, from the application partition:

```
Router# reset mod 9

Proceed with reload of module? [confirm] y
% reset issued for module 9

Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```

To reboot the module from the application software, perform this task while you are sessioned into the root account on the module in the privileged mode:

Command	Purpose
reboot	Reboots the module.

This example shows how to reboot the module:

```
FWSM# reboot
```

## Troubleshooting the Firewall Services Module

This section provides troubleshooting information for the Firewall Services Module.

**Symptom** You cannot connect to the module.

**Possible Cause** The initial configuration is incorrect or not configured.

**Recommended Action** Perform a **show module** command and check that the status is OK.

**Symptom** When a **reset** command is entered from the supervisor engine CLI, the system always boots into the maintenance image.

**Possible Cause** If the boot device is configured in the supervisor engine as cf:1, when you enter a **reset module** command the system always boots to the maintenance image.

**Recommended Action** Override the configured boot device in the supervisor engine by entering the boot string during reset. In Cisco IOS software, to boot to the application image, enter the **hw-module mod 9 reset cf:4** (or **cf:5**) command.

**Symptom** You are unable to log into the maintenance image with the same password for the module application image.

**Possible Cause** The module application image and the maintenance image have different password databases. Any password change performed in the module application image does not change the maintenance image passwords and vice versa.

**Recommended Action** Use the maintenance image password.

**Symptom** You lost your password for the maintenance image and want to recover it.

**Possible Cause** The maintenance image does not support resetting passwords from the switch. Upgrading the maintenance image retains the password for root and guest across the upgrades.

**Recommended Action** Refer to [“Changing and Recovering Passwords” section on page 5-11](#).

