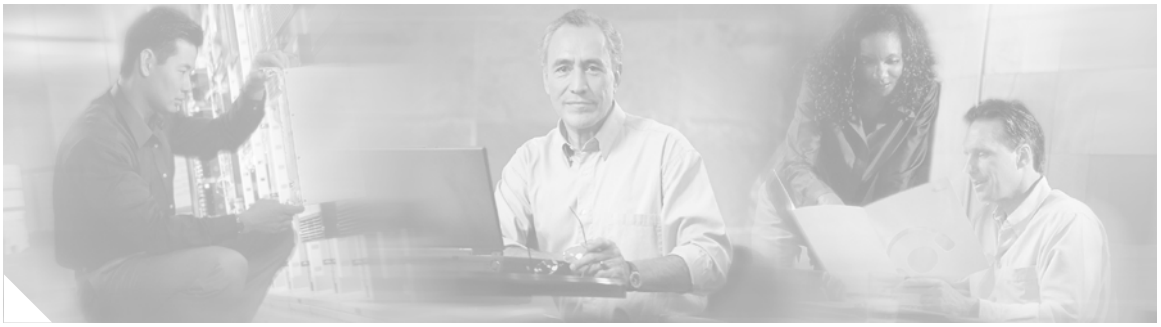

Upgrading the Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module from Release 2.x to Release 3.1

This guide describes how to upgrade from FWSM Release 2.2 or 2.3 to FWSM Release 3.1. This guide describes the features and commands that have changed or been deprecated in FWSM Release 3.1.

This guide is written for FWSM administrators with an understanding of FWSM CLI commands and features and with experience configuring the FWSM. This document includes the following sections:

- New Features, page 1
- Upgrading the FWSM from Release 2.x to 3.1, page 4
- Restoring the FWSM to Release 2.x, page 22
- Changed and Deprecated Commands, page 29
- Obtaining More Information, page 52

New Features

This section includes a brief summary of new features in Release 3.1. For more information on these features and the accompanying CLI commands, see the following documents:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*
- Online Help for ASDM (previously known as PDM for FWSM)

FWSM Release 3.1 introduces the following new functionality and features:

- AAA
  - Support for simultaneous RADIUS accounting servers
  - Accounting for management traffic
  - Configuring an FTP authentication challenge
  - MAC address-based AAA exemption
  - Cut-through proxy authentication using the local database

- Access Lists
  - Time-based ACEs
  - Modular Policy Framework
  - Access list editing with line numbers
  - Using the **interface** keyword as an address in access lists
- NAT
  - Configurable NAT control
  - Overlapping static NAT configuration
- Inspection Engines (Fixups)
  - TCP stream assembly for application inspection
  - Persistent TCP connections and TCP pools for URL filtering
  - Configurable application inspection engines
  - ESMTP application inspection
  - FTP command filtering
  - ActiveX and Java filtering
  - Enhanced PPTP PAT and application inspection
- VoIP Inspection Engines (Fixups)
  - Enhanced H.323 application inspection (for T.38 and GKRCS)
  - MGCP NAT
  - GTP application inspection
  - SIP instant messaging application inspection
  - TAPI/CTIQBE application inspection
  - Skinny video support
- Application Firewall
  - Enhanced HTTP application inspection
  - Detecting and blocking applications and attacks tunneled over HTTP
  - RFC compliance checking
  - HTTP command filtering
  - MIME type filtering
  - Checking for minimum and maximum size of the HTTP message, header length and URI
  - Content validation
  - HTTP message filtering based on keywords
- High Availability
  - Active/Active failover
  - Preempt option for Active/Active failover
- Scalability
  - Support for 250 security contexts
  - Save all context configurations from the system execution space

  - Increasing the number of global statements to 4 K
  - Enhanced access list memory
  - Sessions for non-TCP/UDP packets
  - Support up to ten DHCP relay statements
  - Support for 80 HTTPS sessions to ASDM
- Network Integration
  - Mixed routed and transparent mode support for contexts
  - Multiple pairs of interfaces in transparent mode
  - Private VLAN support
  - Enabling DHCP relay on specific interfaces
- Core IP Enhancements
  - IPv6
  - Asymmetric routing support
  - Multicast support in single mode
  - OSPF neighbor support
- Monitoring and Management
  - SSHv2
  - Ping, logging, and memory management enhancements
  - Syslog server failure policy for TCP transport
  - 4K certificate support
  - SNMPv2c
  - Additional MIBs
  - Enhanced parser and CLI
  - Extra information in the command prompt
  - Debug message timestamp
  - System execution space logging to external syslog server using the admin context
  - ACE information as part of message 106023

Upgrading the FWSM from Release 2.x to 3.1

This section describes how to upgrade the FWSM to 3.1, and includes the following topics:

- Upgrade Requirements, page 4
- Backing up the Configuration, page 4
- Upgrading Maintenance Software to Release 2.1(2), page 6
- Upgrading the Application Software, page 9
- Removing Unused Commands from the System Configuration, page 15
- Upgrading from PDM to ASDM, page 16
- Upgrade Examples, page 16

Upgrade Requirements

- You must install maintenance software Release 2.1(2) before you upgrade to FWSM Release 3.1. See the "Upgrading Maintenance Software to Release 2.1(2)" section on page 6 for more information.
- Client PC operating system and browser requirements for ASDM Version 5.0F are listed in Table 1.

Table 1 Operating System and Browser Requirements for ASDM Version 5.0

	Operating System	Browser	Other Requirements
Windows[1]	Windows 2000 (Service Pack 4) or Windows XP operating systems	Internet Explorer 6.0 with Java Plug-in 1.4.2 or 1.5.0 **Note** **HTTP 1.1**—Settings for Internet Options Advanced HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections. Netscape 7.1/7.2 with Java Plug-in 1.4.2 or 1.5.0	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Java Plug-in 1.4.2 or 1.5.0	
Linux	Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running GNOME or KDE	Mozilla 1.7.3 with Java Plug-in 1.4.2 or 1.5.0	

1. ASDM is not supported on Windows 3.1, 95, 98, ME or Windows NT4.

Backing up the Configuration

This section describes how to back up your configuration before beginning the upgrade procedure. You might need the original configuration if you have to restore Release 2.x. See the "Restoring the FWSM to Release 2.x" section on page 22.

Note If you are running failover, be sure to back up the configuration from both units; be sure to save the synchronized configuration on the secondary unit (use the **write memory** command) so that it can run independently with a full configuration.

To back up your configuration, use the following methods:

- Backing up the Single Mode Configuration or Multiple Mode System Configuration, page 5
- Backing Up a Context Configuration in Flash Memory, page 5
- Backing Up a Context Configuration within a Context, page 6
- Copying the Configuration from the Terminal Display, page 6

Note If you have contexts on an external server, make copies of the contexts on the server.

Backing up the Single Mode Configuration or Multiple Mode System Configuration

In single context mode or from the system configuration in multiple mode, you can copy the startup configuration or running configuration to an external server or to the local Flash memory:

- To copy to a TFTP server, enter the following command:

  ```
  hostname# copy {startup-config | running-config} tftp://server[/path]/filename
  ```

- To copy to a FTP server, enter the following command:

  ```
  hostname# copy {startup-config | running-config}
  ftp://[user[:password]@]server[/path]/filename
  ```

- To copy to local Flash memory, enter the following command:

  ```
  hostname# copy {startup-config | running-config} disk:[path/]filename
  ```

  Be sure the destination directory exists. If it does not exist, first create the directory using the **mkdir** command.

Backing Up a Context Configuration in Flash Memory

In multiple context mode, copy context configurations that are on the local Flash memory by entering one of the following commands in the system execution space:

- To copy to a TFTP server, enter the following command:

  ```
  hostname# copy disk:[path/]filename tftp://server[/path]/filename
  ```

- To copy to a FTP server, enter the following command:

  ```
  hostname# copy disk:[path/]filename ftp://[user[:password]@]server[/path]/filename
  ```

- To copy to local Flash memory, enter the following command:

  ```
  hostname# copy disk:[path/]filename disk:[path/]newfilename
  ```

  Be sure the destination directory exists. If it does not exist, first create the directory using the **mkdir** command.

  For example, copy the admin.cfg file to a 2_3 subdirectory:

```
hostname# mkdir 2_3
Create directory filename [2_3]?

Created dir disk:/2_3
hostname# copy disk:admin.cfg disk:2_3/admin.cfg
```

Backing Up a Context Configuration within a Context

In multiple context mode, from within a context, you can perform the following backups:

- To copy the running configuration to the startup configuration server (connected to the admin context), enter the following command:

  ```
  hostname/contexta# copy running-config startup-config
  ```

- To copy the running configuration to a TFTP server connected to the context network, enter the following command:

  ```
  hostname/contexta# copy running-config tftp:/server[/path]/filename
  ```

Copying the Configuration from the Terminal Display

To print the configuration to the terminal, enter the following command:

```
hostname# show running-config
```

Copy the output from this command, then paste the configuration in to a text file.

Upgrading Maintenance Software to Release 2.1(2)

You must install maintenance software Release 2.1(2) or later before you upgrade to FWSM Release 3.1. The latest maintenance release also works with FWSM Release 2.x, so if you later have to restore the FWSM to Release 2.x, this procedure will not prevent it.

Note If you are running failover, be sure to upgrade the maintenance software on both units.

This section includes the following topics:

- Checking the Maintenance Software Release, page 6
- Upgrading the Maintenance Software, page 7

Checking the Maintenance Software Release

To determine the maintenance software release, boot in to the maintenance partition and view the release by performing the following steps:

Step 1 If necessary, end the FWSM session by entering the following command:

```
hostname# exit

Logoff
```

```
[Connection to 127.0.0.31 closed by foreign host]
Router#
```

You might need to enter the **exit** command multiple times if you are in a configuration mode.

Step 2 To boot the FWSM into the maintenance partition, enter the command for your operating system at the switch prompt:

- For Cisco IOS, enter the following command:

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

- For Catalyst operating system software, enter the following command:

  ```
  Console> (enable) reset mod_num cf:1
  ```

Step 3 To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

  ```
  Router# session slot number processor 1
  ```

- Catalyst operating system software

  ```
  Console> (enable) session module_number
  ```

Step 4 To log in to the FWSM maintenance partition as root, enter the following command:

```
Login: root
```

Step 5 Enter the password at the prompt:

```
Password:
```

By default, the password is **cisco**.

The FWSM shows the version when you first log in, as in the following example:

```
Maintenance image version: 2.1(2)
```

Step 6 To view the maintenance version after you log in, enter the following command:

```
root@localhost# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 : integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-FWM-1
Number of Pentium-class Processors :       2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9
Total available memory: 1004 MB
Size of compact flash: 123 MB
Daughter Card Info: Number of DC Processors: 3
Size of DC Processor Memory (per proc): 32 MB
```

Upgrading the Maintenance Software

To upgrade the maintenance software, perform the following steps. If you have a failover pair, upgrade the standby unit first, and then the active unit. The standby unit will become active while the formerly active unit is upgrading.

Step 1 Download the maintenance software from Cisco.com at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-serv-maint

Put the software on a TFTP, HTTP, or HTTPS server that is accessible from the FWSM admin context (if you are using multiple context mode).

Step 2 If required, log out of the maintenance partition and reload the application partition by performing the following steps:

a. Log out of the maintenance partition by entering the following command:

```
root@localhost# logout
```

b. If required, reboot the module into the application partition by entering the command for your operating system:

- For Cisco IOS, enter the following command:

```
Router# hw-module module mod_num reset
```

- For Catalyst operating system software, enter the following command:

```
Console> (enable) reset mod_num
```

c. To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

```
Router# session slot number processor 1
```

- Catalyst operating system software

```
Console> (enable) session module_number
```

The default password is **cisco** (see the **password** command). In single mode, you can configure Telnet authentication, so the username and password depends on your configuration.

Step 3 To upgrade the maintenance partition software, enter one of the following commands, directed to the appropriate download server. For multiple context mode, you must be in the system execution space.

- To download the maintenance software from a TFTP server, enter the following command:

```
hostname# upgrade-mp tftp[://server[:port][/path]/filename]
```

You are prompted to confirm the server information. If you do not supply it in the command, you can enter it in response to the prompt.

- To download the maintenance software from an HTTP or HTTPS server, enter the following command:

```
hostname# upgrade-mp http[s]://[user[:password]@]server[:port][/path]/filename
```

Passwords for the root and guest accounts of the maintenance partition are retained after the upgrade.

The following example shows the prompts for the TFTP server information:

```
hostname# upgrade-mp tftp
Address or name of remote host [127.0.0.1]? 10.1.1.5
Source file name [cdisk]? mp.2-1-0-3.bin.gz
copying tftp://10.1.1.5/mp.2-1-0-3.bin.gz to flash
[yes|no|again]? yes
!!!!!!!!!!!!!!!!!!!!!!
Received 1695744 bytes.
Maintenance partition upgraded.
```

Step 4 Reload the FWSM to load the new maintenance software by entering the following command:

```
hostname# reload
```

Alternatively, you can log out of the FWSM in preparation for booting in to the maintenance partition; from the maintenance partition, you can install application software to both application partitions. To end the FWSM session, enter the following command:

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

You might need to enter the **exit** command multiple times if you are in a configuration mode.

See the "Downloading Application Software Using the Maintenance Partition" section on page 12 to reload the FWSM into the maintenance partition.

Upgrading the Application Software

To upgrade the FWSM application software, use one of the following methods:

- Upgrading Application Software from the FWSM CLI, page 10

  The benefit of this method is you do not have to boot in to the maintenance partition; instead you log in as usual and copy the new software.

  This method supports downloading from a TFTP, FTP, HTTP, or HTTPS server.

  You cannot copy software to the other application partition. You might want to copy to the other partition if you want to keep the old version of software as a backup in the current partition.

  You must have an operational configuration with network access. For multiple context mode, you need to have network connectivity through the admin context.

- Upgrading Application Software Using the Maintenance Partition, page 12

  The benefit of this method is you can copy software to both application partitions, and you do not have to have an operational network on the application configuration. You just need to configure some routing parameters in the maintenance partition so you can reach the server on VLAN 1. For example, you can leave Release 2.x on one partition and install 3.1 on the other partition, in case you need to restore the FWSM to 2.x.

  The disadvantage is that you need to boot in to the maintenance partition, which might not be convenient if you have active connections.

  This method supports downloading from an FTP server only.

Note If you do not have an activation key entered (0x000) before upgrading, then when you enter the **show version** command after upgrading, you see the following message:

```
The running activation key is not valid
```

This cosmetic issue can be ignoredl; the FWSM is not affected.

Upgrading Application Software from the FWSM CLI

When you log in to the FWSM during normal operation, you can copy the application software to the current application partition from a TFTP, FTP, HTTP, or HTTPS server.

Note If you are running failover, be sure to upgrade the application software on both units.

To upgrade software to the current application partition from an FTP, TFTP, or HTTP(S) server, perform the following steps:

Step 1 Enter the following command to confirm access to the selected FTP, TFTP, or HTTP(S) server:

```
hostname# ping ip_address
```

Step 2 To copy the application software, enter one of the following commands, directed to the appropriate download server.

- To copy from a TFTP server, enter the following command:

  ```
  hostname# copy tftp://server[/path]/filename flash:
  ```

  The **flash** keyword refers to the application partition on the FWSM. You can only copy an image and ASDM software to the **flash** partition. Configuration files are copied to the **disk** partition.

- To copy from an FTP server, enter the following command:

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename flash:
  ```

- To copy from an HTTP or HTTPS server, enter the following command:

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename flash:
  ```

For example, to copy the application software from an FTP server, enter the following command:

```
hostname# copy ftp://10.94.146.80/tftpboot/bnair/cdisk flash:

copying ftp://10.94.146.80/tftpboot/bnair/cdisk to flash:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Received 6128128 bytes.
Erasing current image.This may take some time..
Writing 6127616 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image installed.
```

Step 3 To run the new software, you need to reload the system.

- If you do not have a failover pair, enter the following command:

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

At the 'Proceed with reload?' prompt, press **Enter** to confirm the command.

```
Rebooting...
```

- If you have a failover pair, perform the following steps:

a. Ensure that the secondary unit has a configuration saved to memory by entering the following command:

```
secondary(config)# write memory
```

The saved configuration will load when you restart the secondary unit. This step is useful if the primary unit fails to start up correctly.

For multiple context mode, if the primary unit has context configurations in Flash memory, be sure to enter the **write memory** command in each primary unit context; the context will automiticallly be copied to the secondary unit Flash memory.

b. To load the new software, reload the primary unit and then reload the secondary unit before the primary unit comes online. Enter the following command separately on each unit:

```
primary(config)# reload
Proceed with reload? [confirm]
```

At the 'Proceed with reload?' prompt, press **Enter** to confirm the command.

```
Rebooting...

secondary(config)# reload
Proceed with reload? [confirm]
```

While the units reload, all active connections are terminated. We recommend reloading both units at the same time because if both units are running, and the major version number does not match (2.x vs. 3.1), then both units become active. Two active units can cause networking problems.

After the upgrade to FWSM Release 3.1 is completed, the startup configuration will still be a Release 2.x configuration, but the running configuration will be the newly migrated 3.1 configuration. Once the FWSM is running the 3.1 image, you can no longer enter the Release 2.x commands.

Until you save the new configuration to Flash memory, the software will convert the old startup configuration automatically every time the FWSM reboots.

Step 4 To save the converted Release 3.1 configuration to Flash memory, enter the following command:

```
hostname# write memory
```

In multiple context mode, enter the new **write memory all** command from the system execution space. This command saves all context configurations to which the FWSM has write access.

If the context configurations are on an HTTP/HTTPS server, or you otherwise do not have write access, use the **show running-config** command for each context and copy the new configuration so you can later update the context configuration on the server.

Upgrading Application Software Using the Maintenance Partition

You must install maintenance software Release 2.1(2) before you upgrade to FWSM Release 3.1.

If you log in to the maintenance partition, you can install application software to either application partition (cf:4 or cf:5).

Note The FWSM maintenance partition can only use VLAN 1 on the switch. The FWSM does not support 802.1Q tagging on VLAN 1.

To install application software from an FTP server while logged in to the maintenance partition, perform the following steps.

Note If you have a failover pair, upgrade the primary unit first, but then be sure to start the upgrade on the secondary unit before the primary unit comes online with the new version. If both units are running, and the major version number does not match (2.x vs. 3.1), then both units become active. Two active units can cause networking problems.

Step 1 Each application partition has its own startup configuration, so you need to make the 2.x configuration available to copy to the 3.1 application partition. You can either copy it to an available TFTP, FTP, or HTTP(S) server, or you can enter the **show running-config** command and cut and paste the configuration from the terminal. See the "Backing up the Single Mode Configuration or Multiple Mode System Configuration" section on page 5.

Step 2 If necessary, end the FWSM session by entering the following command:

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

You might need to enter the **exit** command multiple times if you are in a configuration mode.

Step 3 To view the current (2.x) boot partition, enter the command for your operating system. Note the current boot partition so you can set a new default boot partition.

- Cisco IOS software

  ```
  Router# show boot device [mod_num]
  ```

  For example:

  ```
  Router# show boot device
  [mod:1 ]:
  [mod:2 ]:
  [mod:3 ]:
  ```

```
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

- Catalyst operating system software

```
Console> (enable) show boot device mod_num
```

For example:

```
Console> (enable) show boot device 4
Device BOOT variable = cf:4
```

Step 4 To change the default boot partition to the backup, enter the command for your operating system:

- Cisco IOS software

```
Router(config)# boot device module mod_num cf:{4 | 5}
```

- Catalyst operating system software

```
Console> (enable) set boot device cf:{4 | 5} mod_num
```

Step 5 To boot the FWSM into the maintenance partition, enter the command for your operating system at the switch prompt:

- For Cisco IOS, enter the following command:

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

- For Catalyst operating system software, enter the following command:

```
Console> (enable) reset mod_num cf:1
```

Step 6 To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

```
Router# session slot number processor 1
```

- Catalyst operating system software

```
Console> (enable) session module_number
```

Step 7 To log in to the FWSM maintenance partition as root, enter the following command:

```
Login: root
Password:
```

By default, the password is **cisco**.

Step 8 To set network parameters, perform the following steps:

a. To assign an IP address to the maintenance partition, enter the following command:

```
root@localhost# ip address ip _address netmask
```

This address is the address for VLAN 1, which is the only VLAN used by the maintenance partition.

b. To assign a default gateway to the maintenance partition, enter the following command:

```
root@localhost# ip gateway ip_address
```

c. (Optional) To ping the FTP server to verify connectivity, enter the following command:

```
root@localhost# ping ftp_address
```

Step 9 To download the application software from the FTP server, enter the following command:

```
root@localhost# upgrade ftp://[user[:password]@]server[/path]/filename cf:{4 | 5}
```

cf:4 and **cf:5** are the application partitions on the FWSM. Install the new software to the backup partition.

Follow the screen prompts during the upgrade.

Step 10 To log out of the maintenance partition, enter the following command:

```
root@localhost# logout
```

Step 11 To reboot the FWSM into the 3.1 application partition (that you set as the default in Step 4), enter the command for your operating system:

- For Cisco IOS, enter the following command:

  ```
  Router# hw-module module mod_num reset
  ```

- For Catalyst operating system software, enter the following command:

  ```
  Console> (enable) reset mod_num
  ```

Step 12 To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

  ```
  Router# session slot number processor 1
  ```

- Catalyst operating system software

  ```
  Console> (enable) session module_number
  ```

By default, the password to log in to the FWSM is **cisco** (set by the **password** command). If this partition does not have a startup configuration, the default password is used.

Step 13 Enter privileged EXEC mode using the following command:

```
hostname> enable
```

The default password is blank (set by the **enable password** command). If this partition does not have a startup configuration, the default password is used.

Step 14 Each application partition has its own startup configuration, so you need to copy the current 2.x configuration to the 3.1 application partition using one of the following methods:

- If you paste the 2.x configuration at the command line, enter the following command to save it:

  ```
  hostname# write memory
  ```

- To copy from a TFTP server, enter the following command:

  ```
  hostname# copy tftp://server[/path]/filename startup-config
  ```

- To copy from an FTP server, enter the following command:

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename startup-config
  ```

- To copy from an HTTP or HTTPS server, enter the following command:

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename
  startup-config
  ```

Step 15 The default context mode is single mode, so if you are running in multiple context mode, set the mode to multiple in the 3.1 application partition using the following command:

```
hostname# configuration terminal
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
```

Confirm to reload the FWSM.

Note Be sure to back up your configurations because the switch to mutiple mode can overwrite the default configurations.

Step 16 If you did not change the mode and reload in Step 15, then reload the FWSM using the following command:

```
hostname# reload
```

After you reload, the startup configuration will still be a Release 2.x configuration, but the running configuration will be the newly migrated 3.1 configuration. Once the FWSM is running the 3.1 image, you can no longer enter the Release 2.x commands.

Until you save the new configuration to Flash memory, the software will convert the old startup configuration automatically every time the FWSM reboots.

Step 17 To save the converted Release 3.1 configuration to Flash memory, enter the following command:

```
hostname# write memory
```

In multiple context mode, enter the **write memory all** command from the system execution space. This command saves all context configurations to which the FWSM has write access.

If the context configurations are on an HTTP/HTTPS server, or you otherwise do not have write access, use the **show running-config** command for each context and copy the new configuration so you can later update the context configuration on the server.

Removing Unused Commands from the System Configuration

Most commands are converted automatically when you load Release 3.1. Some deprecated commands are left in your configuration so you can decide how to manage the changes. For example, you can no longer configure any **logging** commands in the system execution space. Instead, system messages (including failover messages) are output to the admin context. However, **logging** commands are *not* automatically removed from the system configuration.

When the FWSM loads deprecated commands, you see error messages; however, they do not affect the running of your configuration. To clean up your configuration, perform the following steps:

Step 1 To view deprecated commands, enter the following command:

```
hostname# show startup-config errors
```

Step 2 To remove the commands, enter the **no** form of the command.

Upgrading from PDM to ASDM

To upgrade from PDM 4.x to ASDM 5.0F, which runs with application software Release 3.1, see the *Cisco ASDM Release Notes*.

Upgrade Examples

This section includes sample Release 2.3 configurations and converted Release 3.1 configurations. This section contains the following topics:

- Single Mode Sample Configurations, page 16
- Multiple Mode Sample Configurations, page 19

Single Mode Sample Configurations

The following is sample output from the **show version** command for a system running FWSM Release 2.3 before upgrading to FWSM Release 3.1:

```
hostname(config)# show version

FWSM Firewall Version 2.3(2)9

Compiled on Thu 14-Jul-05 01:30 by dalecki

FWSM up 28 mins 48 secs

Hardware:   WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash  V1.01   SMART ATA FLASH DISK @ 0xc321, 20MB

0: gb-ethernet0: irq 5
1: gb-ethernet1: irq 7
2: ethernet0: irq 11

Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 256
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Throughput:         Unlimited
ISAKMP peers:       Unlimited
Security Contexts:  2

This machine has an Unrestricted (UR) license.

Serial Number: SAD062302U5
Running Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000
Configuration last modified by enable_15 at 06:36:55 Aug 24 2005
```

Table 2 shows the unmodified startup configuration and the converted running configuration after upgrading to Release 3.1.

Table 2 2.3 Startup Configuration and 3.1 Running Configuration

2.3 Startup Configuration	3.1 Running Configuration
FWSM(config)# **show startup-config** : Saved : Written by enable_15 at 06:37:02 Aug 24 2005 FWSM Version 2.3(2)9 nameif Vlan10 outside security100 nameif Vlan30 inside security0 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname FWSM ftp mode passive fixup protocol dns maximum-length 512 fixup protocol ftp 21 fixup protocol h323 H225 1720 fixup protocol h323 ras 1718-1719 fixup protocol rsh 514 fixup protocol sip 5060 no fixup protocol sip udp 5060 fixup protocol skinny 2000 fixup protocol smtp 25 fixup protocol sqlnet 1521 names access-list deny-flow-max 4096 access-list alert-interval 300 pager lines 24 logging buffer-size 4096 mtu outside 1500 mtu inside 1500 ip address outside 10.6.8.20 255.0.0.0 ip address inside 11.1.1.1 255.0.0.0 no failover failover lan unit secondary failover polltime unit 1 holdtime 15 failover polltime interface 15 failover interface-policy 50% icmp permit any outside no pdm history enable arp timeout 14400 ! interface outside ! interface inside ! timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server TACACS+ max-failed-attempts 3 aaa-server TACACS+ deadtime 10 aaa-server RADIUS protocol radius aaa-server RADIUS max-failed-attempts 3 aaa-server RADIUS deadtime 10 aaa-server LOCAL protocol local (continued...)	FWSM(config)# **show running-config** : Saved : FWSM Version 3.1(0)78 ! hostname FWSM enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Vlan10 nameif outside security-level 100 ip address 10.6.8.20 255.0.0.0 ! interface Vlan30 nameif inside security-level 0 ip address 11.1.1.1 255.0.0.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive pager lines 24 mtu outside 1500 mtu inside 1500 no failover failover lan unit secondary icmp permit any outside no asdm history enable arp timeout 14400 nat-control timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 non_TCP_UDP 0:10:00 timeout uauth 0:05:00 absolute aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS protocol radius no snmp-server location no snmp-server contact snmp-server community public snmp-server enable traps snmp authentication linkup linkdown coldstart telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map class_sip_tcp match port tcp eq sip class-map inspection_default match default-inspection-traffic ! ! (continued...)

Table 2 2.3 Startup Configuration and 3.1 Running Configuration (continued)

2.3 Startup Configuration	3.1 Running Configuration

(...continued)
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
floodguard enable
fragment size 200 outside
fragment chain 24 outside
fragment size 200 inside
fragment chain 24 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:c0c7b48ccf97530e2c57a90aeb5f9621
	(...continued)
	policy-map global_policy
	 class inspection_default
	  inspect dns maximum-length 512
	  inspect ftp
	  inspect h323 h225
	  inspect h323 ras
	  inspect netbios
	  inspect rsh
	  inspect skinny
	  inspect smtp
	inspect sqlnet
	  inspect sunrpc
	  inspect tftp
	  inspect xdmcp
	 class class_sip_tcp
	  inspect sip
	!
	service-policy global_policy global
	prompt hostname context
	Cryptochecksum:c0c7b48ccf97530e2c57a90aeb5f9621
	: end

The following is sample output from the **show version** command for a system after upgrading to FWSM Release 3.1:

```
hostname(config)# show version

FWSM Firewall Version 3.1(0)78

Compiled on Tue 23-Aug-05 23:54 by bnair

FWSM up 20 mins 17 secs

Hardware:   WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash SMART ATA FLASH DISK @ 0xc321, 20MB
Disk Partition: ATA Compact Flash, 57MB

 0: Int: Not licensed        : irq 5
 1: Int: Not licensed        : irq 7
 2: Int: Not licensed        : irq 11
The Running Activation Key is not valid, using default settings:

Licensed features for this platform:
Maximum Interfaces          : 256
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 2
GTP/GPRS                    : Disabled
VPN Peers                   : Unlimited

Serial Number: SAD062302U5
Running Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000
Configuration has not been modified since last system restart.
```

Multiple Mode Sample Configurations

The following is sample output from the **show version** command for a system running FWSM Release 2.3 before upgrading to FWSM Release 3.1:

```
hostname/admin(config)# show version

FWSM Firewall Version 2.3(2)20 <context>

Compiled on Tue 20-Sep-05 02:29 by bnair

FWSM up 4 mins 4 secs

Hardware:   WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash  V1.01   SMART ATA FLASH DISK @ 0xc321, 20MB

0: gb-ethernet0: irq 5
1: gb-ethernet1: irq 7
2: ethernet0: irq 11

Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 256 (per security context)
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Throughput:         Unlimited
ISAKMP peers:       Unlimited
Security Contexts:  2

This machine has an Unrestricted (UR) license.

Serial Number: SAD062302U5
Running Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000
Configuration last modified by enable_15 at 04:46:56 Sep 20 2005
```

Table 3 shows the unmodified system startup configuration and the converted system running configuration after upgrading to Release 3.1.

Table 4 shows the unmodified context startup configuration and the converted context running configuration after upgrading to Release 3.1.

Table 3 System Configurations: 2.3 Startup Configuration and 3.1 Running Configuration

System Configuration: 2.3 Startup Configuration	System Configuration: 3.1 Running Configuration

FWSM(config)# **show startup-config**
: Saved
: Written by enable_15 at 06:37:02 Aug 24 2005
 	
FWSM Version 2.3(2)20 <system>
resource acl-partition 12
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname FWSM
ftp mode passive
pager lines 24
logging buffer-size 4096
class default
  limit-resource IPSec 5
  limit-resource Mac-addresses 65535
  limit-resource PDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!
no failover
failover lan unit secondary
failover polltime unit 1 holdtime 15
failover polltime interface 15
failover interface-policy 50%
arp timeout 14400
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 rpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
terminal width 80
admin-context admin
context admin
  allocate-interface vlan10
  config-url disk:/admin.cfg
!
Cryptochecksum:00000000000000000000000000000000
: end
	FWSM(config)# **show running-config**
	: Saved
	:
	FWSM Version 3.1(0)93 <system>
	!
	resource acl-partition 12
	hostname FWSM
	enable password 8Ry2YjIyt7RRXU24 encrypted
	!
	interface Vlan10
	!
	passwd 2KFQnbNIdI.2KYOU encrypted
	class default
	  limit-resource IPSec 5
	  limit-resource Mac-addresses 65535
	  limit-resource ASDM 5
	  limit-resource SSH 5
	  limit-resource Telnet 5
	  limit-resource All 0
	!
	
	ftp mode passive
	pager lines 24
	no failover
	no asdm history enable
	arp timeout 14400
	console timeout 0
	
	admin-context admin
	context admin
	  allocate-interface Vlan10
	  config-url disk:/admin.cfg
	!
	
	prompt hostname context
	Cryptochecksum:1ee5609cafee6e7c8ce9c0541c56f05a
	: end

Table 4 Context Configurations: 2.3 Startup Configuration and 3.1 Running Configuration

Context Configuration: 2.3 Startup Configuration

```
FWSM(config)# show startup-config
: Saved
: Written by enable_15 at 06:37:02 Aug 24 2005

FWSM Version 2.3(2)20 <context>
nameif vlan10 outside security0
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname FWSM
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol rsh 514
fixup protocol sip 5060
no fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list deny-flow-max 4096
access-list alert-interval 300
pager lines 24
logging buffer-size 4096
mtu outside 1500
ip address outside 10.6.8.20 255.0.0.0
icmp permit any outside
no pdm history enable
arp timeout 14400
!
interface outside
!
!
route outside 0.0.0.0 0.0.0.0 10.6.8.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02 rpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp
floodguard enable
fragment size 200 outside
fragment chain 24 outside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:4119f9fbe77dd6c853e17f1c0626f06d
: end
```

Context Configuration: 3.1 Running Configuration

```
FWSM(config)# show running-config
: Saved
:
FWSM Version 3.1(0)93 <context>
!
hostname FWSM
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 10.6.8.20 255.0.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
pager lines 24
mtu outside 1500
icmp permit any outside
no asdm history enable
arp timeout 14400
nat-control
route outside 0.0.0.0 0.0.0.0 10.6.8.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media
0:02:00 non_TCP_UDP 0:10:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
snmp-server enable traps snmp authentication linkup
linkdown coldstart
telnet timeout 5
ssh timeout 5
!
class-map class_sip_tcp
 match port tcp eq sip
class-map inspection_default
 match default-inspection-traffic
!
!

(continued...)
```

Table 4 Context Configurations: 2.3 Startup Configuration and 3.1 Running Configuration (continued)

Context Configuration: 2.3 Startup Configuration	Context Configuration: 3.1 Running Configuration
	(...continued) policy-map global_policy class inspection_default inspect dns maximum-length 512 inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect skinny inspect smtp inspect sqlnet inspect sunrpc inspect tftp inspect xdmcp class class_sip_tcp inspect sip ! service-policy global_policy global Cryptochecksum:4119f9fbe77dd6c853e17f1c0626f06d : end

Restoring the FWSM to Release 2.x

You can restore the FWSM to the 2.x release using the following methods:

- Downloading Release 2.x to the Current Application Partition, page 22
- Booting Release 2.x from the Backup Application Partition, page 24
- Installing Release 2.x and Booting in to the Backup Application Partition, page 26

Downloading Release 2.x to the Current Application Partition

If you want to replace Release 3.1 with Release 2.x, you can download the 2.x software over the 3.1 software in the current application partition. To restore 2.x, perform the following steps:

Step 1 Copy the 2.x configuration to the startup configuration. In multiple context mode, copy the system configuration. If you have a failover pair, download the 2.x configuration to both units.

- If you paste the 2.x configuration at the command line, enter the following command to save it:

  hostname# **write memory**

- To copy from a TFTP server, enter the following command:

  hostname# **copy tftp://***server*[**/***path*]**/***filename* **startup-config**

- To copy from an FTP server, enter the following command:

  hostname# **copy ftp://**[*user*[**:***password*]**@**]*server*[**/***path*]**/***filename* **startup-config**

- To copy from an HTTP or HTTPS server, enter the following command:

  hostname# **copy http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][**/***path*]**/***filename*
  startup-config

- To copy from the local Flash memory, enter the following command:

  ```
  hostname# copy disk:[path/]filename startup-config
  ```

Step 2 For multiple mode, if you store the context configurations on an external server, copy the 2.x configurations onto the server. If you store the context configurations on Flash memory, copy the 2.x context configurations using one of the following methods from the system execution space:

- To copy from a TFTP server, enter the following command:

  ```
  hostname# copy tftp://server[/path]/filename disk:[path/]filename
  ```

- To copy from a FTP server, enter the following command:

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename disk:[path/]filename
  ```

- To copy from an HTTP or HTTPS server, enter the following command:

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename
  disk:[path/]filename
  ```

Step 3 To copy the 2.x software, enter one of the following commands, directed to the appropriate download server. For a failover pair, copy the software to both units.

- To copy from a TFTP server, enter the following command:

  ```
  hostname# copy tftp://server[/path]/filename flash:
  ```

- To copy from an FTP server, enter the following command:

  ```
  hostname# copy ftp://[user[:password]@]server[/path]/filename flash:
  ```

- To copy from an HTTP or HTTPS server, enter the following command:

  ```
  hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename flash:
  ```

Step 4 To run the new software, you need to reload the system.

- If you do not have a failover pair, enter the following command:

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

  At the 'Proceed with reload?' prompt, press **Enter** to confirm the command.

  ```
  Rebooting...
  ```

- If you have a failover pair, perform the following steps:

  a. Restart the standby unit to load the new software by entering the following command:

  ```
  standby(config)# reload
  ```

  After the standby unit restarts, the version mismatch causes failover to be disabled; because the standby unit sensed the version mismatch with an active unit, it continues to be in a standby state.

  b. After the standby unit restarts, restart the active unit by entering the following command:

  ```
  active(config)# reload
  ```

  Current connections to the active unit will be disconnected. New connections will be handled by the standby unit after you reenable failover.

  c. Immediately reenable failover on the standby unit by entering the following command:

  ```
  standby(config)# failover
  ```

The standby unit senses that the failover link is down, and becomes active.

d. (Optional) Restore the former active unit to be active by entering the following command:

```
formeractive(config)# failover active
```

Before performing this step, ensure that the configuration and stateful connections are synchronized between the two units to minimize traffic loss.

Booting Release 2.x from the Backup Application Partition

If you already have Release 2.x and a current 2.x startup configuration on the backup application partition, perform the following steps.

Note If you have a failover pair, perform this procedure on the standby unit first. After you complete the procedure for the standby unit, start the procedure for the active unit. To minimize downtime, immediately reenable failover on the standby unit using the **failover** command as soon as you reboot the active unit. Failover was disabled on the standby unit because it sensed a version mismatch. When you reenable failover on the standby unit while the active unit is down, then the standby unit becomes active.

Step 1 Each partition has its own startup configuration. However, for multiple mode, if you store the context configurations on an external server, copy the 2.x configurations onto the server. If you store the context configurations on Flash memory, copy the 2.x context configurations using one of the following methods from the system execution space:

- To copy from a TFTP server, enter the following command:

```
hostname# copy tftp://server[/path]/filename disk:[path/]filename
```

- To copy from a FTP server, enter the following command:

```
hostname# copy ftp://[user[:password]@]server[/path]/filename disk:[path/]filename
```

- To copy from an HTTP or HTTPS server, enter the following command:

```
hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename
disk:[path/]filename
```

- To copy from the local Flash memory, enter the following command:

```
hostname# copy disk:[path/]filename disk:[path/]newfilename
```

Step 2 End the FWSM session by entering the following command:

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

You might need to enter the **exit** command multiple times if you are in a configuration mode.

Step 3 To view the current (3.1) boot partition, enter the command for your operating system. Note the current boot partition so you can change the default partition in the next step.

- Cisco IOS software

```
Router# show boot device [mod_num]
```

For example:

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

- Catalyst operating system software

```
Console> (enable) show boot device mod_num
```

For example:

```
Console> (enable) show boot device 4
Device BOOT variable = cf:4
```

Step 4 To change the default boot partition to the backup (2.x) partition, enter the command for your operating system:

- Cisco IOS software

```
Router(config)# boot device module mod_num cf:{4 | 5}
```

- Catalyst operating system software

```
Console> (enable) set boot device cf:{4 | 5} mod_num
```

Step 5 To reboot the FWSM into the backup application partition (that you set as the new default boot partition in the previous step), enter the command for your operating system:

- For Cisco IOS, enter the following command:

```
Router# hw-module module mod_num reset
```

- For Catalyst operating system software, enter the following command:

```
Console> (enable) reset mod_num
```

Step 6 To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

```
Router# session slot number processor 1
```

- Catalyst operating system software

```
Console> (enable) session module_number
```

By default, the password to log in to the FWSM is **cisco** (set by the **password** command).

Installing Release 2.x and Booting in to the Backup Application Partition

To preserve the 3.1 software image in the current application partition, you can install Release 2.x in the backup partition and then boot into the backup partition. To install software in the non-current application partition, you must boot in to the maintenance partition, where you can download software to either partition from an FTP server only.

The FWSM maintenance partition can only use VLAN 1 on the switch. The FWSM does not support 802.1Q tagging on VLAN 1.

To install 2.x software from an FTP server while logged into the maintenance partition then boot in to the backup partition, perform the following steps.

Note If you have a failover pair, perform this procedure on the standby unit first. After you complete the procedure for the standby unit, start the procedure for the active unit. To minimize downtime, immediately reenable failover on the standby unit using the **failover** command as soon as you reboot the active unit. Failover was disabled on the standby unit because it sensed a version mismatch. When you reenable failover on the standby unit while the active unit is down, then the standby unit becomes active.

Step 1 If necessary, end the FWSM session by entering the following command:

```
hostname# exit

Logoff

[Connection to 127.0.0.31 closed by foreign host]
Router#
```

You might need to enter the **exit** command multiple times if you are in a configuration mode.

Step 2 To view the current (3.1) boot partition, enter the command for your operating system. Note the current boot partition so you can set a new default boot partition.

- Cisco IOS software

  ```
  Router# show boot device [mod_num]
  ```

  For example:

  ```
  Router# show boot device
  [mod:1 ]:
  [mod:2 ]:
  [mod:3 ]:
  [mod:4 ]: cf:4
  [mod:5 ]: cf:4
  [mod:6 ]:
  [mod:7 ]: cf:4
  [mod:8 ]:
  [mod:9 ]:
  ```

- Catalyst operating system software

  ```
  Console> (enable) show boot device mod_num
  ```

  For example:

  ```
  Console> (enable) show boot device 4
  Device BOOT variable = cf:4
  ```

Step 3 To change the default boot partition to the backup, enter the command for your operating system:

- Cisco IOS software

  ```
  Router(config)# boot device module mod_num cf:{4 | 5}
  ```

- Catalyst operating system software

  ```
  Console> (enable) set boot device cf:{4 | 5} mod_num
  ```

Step 4 To boot the FWSM into the maintenance partition, enter the command for your operating system at the switch prompt:

- For Cisco IOS, enter the following command:

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

- For Catalyst operating system software, enter the following command:

  ```
  Console> (enable) reset mod_num cf:1
  ```

Step 5 To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

  ```
  Router# session slot number processor 1
  ```

- Catalyst operating system software

  ```
  Console> (enable) session module_number
  ```

Step 6 To log in to the FWSM maintenance partition as root, enter the following command:

```
Login: root
Password:
```

By default, the password is **cisco**.

Step 7 To set network parameters, perform the following steps:

a. To assign an IP address to the maintenance partition, enter the following command:

```
root@localhost# ip address ip _address netmask
```

This address is the address for VLAN 1, which is the only VLAN used by the maintenance partition.

b. To assign a default gateway to the maintenance partition, enter the following command:

```
root@localhost# ip gateway ip_address
```

c. (Optional) To ping the FTP server to verify connectivity, enter the following command:

```
root@localhost# ping ftp_address
```

Step 8 To download the application software from the FTP server, enter the following command:

```
root@localhost# upgrade ftp://[user[:password]@]server[/path]/filename cf:{4 | 5}
```

Install the new software to the backup partition.

Follow the screen prompts during the upgrade.

Step 9 To log out of the maintenance partition, enter the following command:

```
root@localhost# logout
```

Step 10 To reboot the FWSM into the 2.x application partition (that you set as the new default boot partition in Step 3), enter the command for your operating system:

- For Cisco IOS, enter the following command:

  ```
  Router# hw-module module mod_num reset
  ```

- For Catalyst operating system software, enter the following command:

```
Console> (enable) reset mod_num
```

Step 11 To session in to the FWSM, enter the command for your operating system:

- Cisco IOS software

```
Router# session slot number processor 1
```

- Catalyst operating system software

```
Console> (enable) session module_number
```

By default, the password to log in to the FWSM is **cisco** (set by the **password** command). If this partition does not have a startup configuration, the default password is used.

Step 12 Enter privileged EXEC mode using the following command:

```
hostname> enable
```

The default password is blank (set by the **enable password** command). If this partition does not have a startup configuration, the default password is used.

Step 13 For multiple mode, if you store the context configurations on an external server, copy the 2.x configurations onto the server. If you store the context configurations on Flash memory, copy the 2.x context configurations using one of the following methods from the system execution space:

- To copy from a TFTP server, enter the following command:

```
hostname# copy tftp://server[/path]/filename disk:[path/]filename
```

- To copy from a FTP server, enter the following command:

```
hostname# copy ftp://[user[:password]@]server[/path]/filename disk:[path/]filename
```

- To copy from an HTTP or HTTPS server, enter the following command:

```
hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename
disk:[path/]filename
```

- To copy from the local Flash memory, enter the following command:

```
hostname# copy disk:[path/]filename disk:[path/]newfilename
```

Step 14 Each application partition has its own startup configuration, so you need to copy the 2.x configuration to the application partition. If you have an old configuration running on this partition, you might want to clear it before copying to the running configuration. To clear the running configuration, enter the **clear configure all** command. To copy the 2.x configuration to the running configuration, use one of the following methods:

- Paste the 2.x configuration at the command line.
- To copy from a TFTP server, enter the following command:

```
hostname# copy tftp://server[/path]/filename running-config
```

- To copy from an FTP server, enter the following command:

```
hostname# copy ftp://[user[:password]@]server[/path]/filename running-config
```

- To copy from an HTTP or HTTPS server, enter the following command:

```
hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename
running-config
```

- To copy from the local Flash memory, enter the following command:

  ```
  hostname# copy disk:[path/]filename running-config
  ```

Step 15 Save the running configuration to startup using the following command:

```
hostname# write memory
```

Step 16 The default context mode is single mode, so if you are running in multiple context mode, set the mode to multiple in the 2.x application partition using the following command:

```
hostname# configuration terminal
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
```

Confirm to reload the FWSM.

Changed and Deprecated Commands

This section describes the changed and deprecated commands in FWSM Release 3.1 and includes the following topics:

- Command Overview, page 29
- Summary of Changes, page 30
- CLI Processor, page 32
- Application Inspection (fixup Command), page 35
- Mixed Routed and Transparent Firewall Mode, page 37
- Transparent Mode Bridge Groups, page 38
- Interfaces, page 38
- AAA, page 39
- MGCP, page 40
- NAT, page 41
- Miscellaneous Commands, page 41
- Logging Commands, page 43
- Device Management Commands, page 43
- VPN Commands, page 44

Command Overview

Many existing FWSM commands have been extended with new keywords and other command-line options, as a result of the functionality introduced in FWSM Release 3.1 (see Table 5). FWSM Release 3.1 includes over 50 new features, listed in the "New Features" section on page 1 and described in greater detail in the FWSM Release 3.1 documentation.

When you upgrade to FWSM 3.1, deprecated commands are automatically converted to the new syntax. After conversion, FWSM Release 3.1 accepts only the new commands. If you enter the old commands, a syntax error is displayed.

The automatic conversion of commands results in a change in your configuration. You should review the configuration changes after booting to verify that the automatic changes made by the software are acceptable. You should then save the configuration to Flash memory. Saving the new configuration to Flash memory prevents the system from converting your configuration again the next time FWSM Release 3.1 is booted.

Summary of Changes

Highlights of the changes in FWSM Release 3.1 include the following:

- The new Modular Policy Framework provides a consistent and flexible way to configure FWSM features in a manner similar to QoS in the Cisco IOS software CLI. For example, you can use Modular Policy Framework to create a timeout configuration that is specific to a particular TCP application, rather than applying it to all TCP applications.

  Modular Policy Framework is supported with the following features:

  - TCP connection limits and timeouts
  - Application inspection (fixups)

  Configuring Modular Policy Framework consists of three tasks:

  a. Identify the traffic to which you want to apply actions (a class map).
  b. Apply actions to the traffic (a policy map).
  c. Activate the actions on an interface (a service policy).

  By default, the 3.1 configuration includes a policy that matches all default application inspection traffic and applies inspection to the traffic on all interfaces (a global policy). You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one.
- The **fixup** command has been deprecated and is replaced by the **inspect** command. The **inspect** command works within the Modular Policy Framework. (see the "Application Inspection (fixup Command)" section on page 35).
- The **mgcp** command was moved under the **mgcp-map** command (see the "MGCP" section on page 40).
- The **aaa-server** command now provides access to the **aaa-server-group** configuration mode, which lets you configure settings for a specific AAA server group. Certain commands, such as the **aaa** commands, now allow configuration of more specific parameters (see the "AAA" section on page 39).
- The **interface** command now provides access to the interface configuration mode. This mode lets you configure the IP address, name, and security level for a specific interface (see the "Interfaces" section on page 38).
- The **no**, **clear**, and **show** commands changed to be more consistent in operation (see the "CLI Processor" section on page 32).
- The FWSM adds a new command, the **nat-control** command, to your configuration. This command maintains NAT requirements as they were in Release 2.x. A new feature for Release 3.1 lets you disable NAT control, so that inside hosts do not need to be translated when communicating with outside hosts. To disable NAT control, enter the **no nat-control** command. (see the "NAT" section on page 41).

- Command completion and mode navigation have changed.
- Many enhancements and improvements were made to management features and to VPN functionality, which can be used for secure management access (see the "Device Management Commands" section on page 43).

Most changed and deprecated features and commands will be converted automatically when FWSM Release 3.1 boots on your system.

Table 5 lists the commands that were changed or deprecated.

Table 5 Changed and Deprecated Commands

Command/Description	Brief Description	For More Information
aaa-server	Changed	AAA, page 39
aaa-server radius-authport	Changed	AAA, page 39
aaa-server radius-acctport	Changed	AAA, page 39
auth-prompt	Changed	AAA, page 39
ca	Changed	Public Key Infrastructure (PKI) Commands, page 46
ca generate/ca zeroize	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca identity/ca configure	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca authenticate	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca enroll	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca crl	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca subject-name	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca save all	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
ca verifycertdn	Deprecated	Public Key Infrastructure (PKI) Commands, page 46
copy capture	Changed	Device Management Commands, page 43
crypto dynamic-map	Changed	VPN Commands, page 44
crypto ipsec	Changed	VPN Commands, page 44
crypto-map	Changed	VPN Commands, page 44
fixup	Deprecated. Replaced by the **inspect** command.	Application Inspection (fixup Command), page 35
floodguard	Deprecated	AAA, page 39
interface	Changed	Interfaces, page 38
ip address	Converted to **interface** configuration mode command	Interfaces, page 38

Table 5 Changed and Deprecated Commands (continued)

Command/Description	Brief Description	For More Information
isakmp	Changed	Public Key Infrastructure (PKI) Commands, page 46
mgcp	Changed	MGCP, page 40
nameif	Converted to **interface** configuration mode command	Interfaces, page 38
pager	Changed	Device Management Commands, page 43
pdm location	Changed	Device Management Commands, page 43
pdm group	Changed	Device Management Commands, page 43
pdm logging	Changed	Device Management Commands, page 43
security-level	This command is now entered from **interface** configuration mode.	Interfaces, page 38
show snmp-server	Changed	CLI Processor, page 32
url-server	Changed	Miscellaneous Commands, page 41
vpngroup	Changed	VPN Commands, page 44

CLI Processor

The CLI parser capabilities have been enhanced in FWSM Release 3.1 to include Cisco IOS software-like parser services, such as context-sensitive Help and command completion, resulting in some minor behavior changes compared to FWSM Release 2.x. FWSM Release 3.1 also introduces minor changes in mode navigation and terminology so that it is closer to the Cisco IOS software CLI.

This section describes the impact that the changes will have on the CLI commands in FWSM Release 3.1. It includes the following topics:

- Show, Clear, and No Commands, page 32
- Context-Sensitive Help Changes, page 34
- Command Syntax Checking, page 34
- Mode Navigation Changes, page 34
- Documentation Terminology Changes, page 35

Show, Clear, and No Commands

The **show** and **clear** commands in FWSM Release 2.x were applied inconsistently. In some cases, these commands were used to show and clear configuration objects. In other cases they were used to show and clear operational data or statistics. To make the behavior consistent and distinguish between operations on configuration versus statistics, the **show** and **clear** commands have been modified to require additional keywords to show or clear configurations.

The **no** variant no longer removes multiple lines of configuration simultaneously. In FWSM Release 3.1, the **no** variant removes a single configuration line only. For clearing a configuration, FWSM Release 3.1 supports only the use of the **clear configure** *cmd* command in configuration mode.

For example, in FWSM Release 2.x, a single **no access-list** *access-list name* command removes the following commands:

```
access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.209 eq
37000
access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.68 eq 37000
access-list myaccesslist extended permit tcp host 10.175.28.98 host 10.180.210.68 eq 37000
```

But in FWSM Release 3.1, the preceding commands are removed by using either the **clear configure access-list** *access-list name* command or by entering a **no** command for each line:

```
no access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.209 eq
37000
no access-list myaccesslist extended permit tcp host 10.175.28.97 host 10.180.210.68 eq
37000
no access-list myaccesslist extended permit tcp host 10.175.28.98 host 10.180.210.68 eq
37000
```

The following examples illustrate the use of the **clear configure** command:

FWSM Release 2.x syntax:

```
clear access-list name
clear ssh
```

FWSM Release 3.1 syntax:

```
clear configure access-list name
clear configure ssh
```

In this example, if you use the **no access-list** *name* command, you will receive an error message.

The **show** *cmd* command shows statistics, buffer, counters, and others. The **show running-config** *cmd* command shows the configuration.

For example, in FWSM Release 2.x, the **show snmp-server** command displayed the running configuration. In FWSM Release 3.1, the **show running-config snmp-server** command displays the running configuration and the **show snmp-server statistics** command displays run-time information about SNMP.

Context-Sensitive Help Changes

Table 6 lists the context-sensitive Help changes in FWSM Release 3.1:

Table 6 Context-Sensitive Help Changes

Feature	FWSM Release 2.x	FWSM Release 3.1
Command Completion	When TAB is entered, it is ignored. When **?** is entered, the following message is displayed: `Type help or ? for a list of available commands.`	You can type a partial command, then enter TAB to complete the command, or type a partial command, then enter **?** to show all commands that begin with the partial command.
Command **?**	The usage text for the command is displayed.	You can enter a command, followed by a space, and then type **?** to show relevant input choices.
Command *keyword* **?**	The usage text for the command is displayed.	Lists arguments that are available for the keyword.

Command Syntax Checking

Table 7 lists changes that occur as a result of the upgrade to FWSM Release 3.1:

Table 7 Command Syntax Checking

Feature	FWSM Release 2.x	FWSM Release 3.1
Syntax error	An error message might be displayed followed by the usage text for the command.	The FWSM displays a ^ symbol to indicate the location of a command syntax error.
Incomplete command	An error message “Not enough arguments” might be displayed, followed by the usage text for the command.	The FWSM displays an ‘Incomplete command’ message to indicate additional arguments are required.

Mode Navigation Changes

FWSM Release 3.1 introduces minor changes in mode navigation so that its behavior is more similar to Cisco IOS software CLI.

In Release 2.x, **Ctrl+Z** logs you out from the console. However, in Release 3.1, **Ctrl+Z** is not supported as an exit method. However, you can still use **exit**, **quit**, or **logout** commands as in FWSM Release 2.x. In FWSM Release 3.1, if you enter **Ctrl+Z**, the following error message is displayed:

```
ERROR:% Invalid input detected at '^' marker.
```

Documentation Terminology Changes

FWSM Release 3.1 introduces minor changes in documentation terminology so that it is more similar to Cisco IOS documentation.

Table 8 describes the terminology changes between FWSM Release 2.x and FWSM Release 3.1.

Table 8 Mode Terminology Changes

FWSM Release 2.x Terminology	FWSM Release 3.1 Terminology
Unprivileged mode	User EXEC mode
Privileged mode	Privileged EXEC mode
Configuration mode	Global configuration mode
Subcommand mode	Command-specific configuration mode

Application Inspection (fixup Command)

The FWSM uses stateful application inspection, often called fixups, to ensure secure use of applications and services. In FWSM Release 3.1, the **fixup** command has been deprecated and replaced by the **inspect** command in the Modular Policy Framework.

Note The **inspect** command introduced in FWSM Release 3.1 is not the same as the Cisco IOS software command **ip inspect**.

Modular Policy Framework is a CLI framework that lets you define traffic classes and apply feature-specific actions (policies) to them. This improves granularity and flexibility when configuring network policies.

When you upgrade to FWSM Release 3.1, each **fixup** command is automatically converted to the corresponding **inspect** command within the Modular Policy Framework. No manual intervention is required. All **fixups** that were previously non-configurable (such as NetBIOS) are also made configurable and converted to Modular Policy Framework commands.

In FWSM Release 3.1, **fixup** commands are still accepted at the CLI, but an informational message similar to the following appears:

```
hostname(config)# fixup protocol http 8080
INFO: converting 'fixup protocol http 8080' to MPF commands
```

The application inspection engines introduced in FWSM Release 3.1, such as CTIQBE, must be used with the **inspect** command in Modular Policy Framework.

Table 9 lists the **inspect** commands corresponding to each **fixup** command. Note that instead of applying application inspection to all traffic on all interfaces, you now configure a class map to determine the traffic, a policy map to apply the inspections to the traffic, and a service policy to apply the policy to one or more interfaces. In the case of the default policy that follows, the FWSM applies inspections to all traffic on the default port numbers on all interfaces, so that the default functionality is the same as in Release 2.x.

Table 9 Changes in the fixup Command

FWSM Release 2.x	FWSM Release 3.1

`fixup protocol dns maximum-length 512`
`fixup protocol h323 h225 1720`
`fixup protocol http 80`
`fixup protocol rsh 514`
`fixup protocol sip 5060`
`fixup protocol smtp 25`
`fixup protocol ftp 21`
`fixup protocol h323 ras 1718-1719`
`fixup protocol ils 389`
`fixup protocol rtsp 554`
`fixup protocol skinny 2000`
`fixup protocol sqlnet 1521`
	`class-map inspection_default`
	`  match default-inspection-traffic`
	`policy-map global_policy`
	`  class inspection_default`
	`  inspect ftp`
	`  inspect h323 h225`
	`  inspect h323 ras`
	`  inspect ils`
	`  inspect rsh`
	`  inspect rtsp`
	`  inspect smtp`
	`  inspect sqlnet`
	`  inspect sip`
	`  inspect skinny`
	`  inspect netbios`
	`  inspect ctiqbe`
	`  inspect icmp`
	`  inspect http`
	`  inspect dns`
	`service-policy global_policy global`

In the FWSM Release 3.1 column of Table 9, note that the **inspect** commands do not have port numbers, unlike the corresponding **fixup** commands in FWSM Release 2.x. The port numbers in this example are implicitly included in the default class map. Table 10 lists the default ports for each application inspection engine shown in Table 9.

Table 10 Default Ports for Table 9 Commands

Inspected Protocol Name	Protocol	Source Port	Destination Port
ctiqbe	tcp	N/A	2748
dns	udp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp, udp	N/A	5060
skinny	tcp	N/A	2000
smtp	tcp	N/A	25
sqlnet	tcp	N/A	1521
tftp	udp	N/A	69
xdmcp	udp	177	177

Mixed Routed and Transparent Firewall Mode

FWSM Release 3.1 supports mixed firewall modes in different contexts. You can set the firewall mode independently for each context, so some contexts can be in routed mode and others in transparent mode. Therefore, the firewall mode is no longer set in the system configuration (the **firewall transparent** command) but is instead set in each context. The **firewall transparent** command (or the **no** form) is automatically added to each running context configuration.

To view the mode of all the contexts, enter the **show firewall** command in the system execution space. The following is sample output from the **show firewall** command.

```
hostname(config)# show firewall
Context      Mode
------------------------
contexta     Transparent
contextb     Routed
```

Transparent Mode Bridge Groups

In FWSM Release 3.1, each pair of interfaces in transparent mode now belongs to a bridge group. You can configure up to eight bridge groups containing two interfaces each. Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups. Traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM.

You might want to use more than one bridge group if you do not want the overhead of security contexts, or if you want to maximize your use of security contexts. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use separate security contexts with one bridge group in each context.

The new **bridge-group** command in interface configuration mode assigns the interface to a bridge group. The new **interface bvi** command sets the management IP address for the bridge group.

By default, when you upgrade, the interfaces in a transparent firewall are assigned to bridge group 1. The following CLI is added (in multimode, this is added to each transparent context):

```
interface vlan y
   bridge-group 1
interface vlan z
   bridge-group 1
interface bvi 1
   ip address n.n.n.n
```


Note The **nameif** and **security-level** commands are also present under the **interface vlan** command.

Interfaces

In FWSM Release 3.1, you use the **interface vlan** command instead of the **interface name** command. Also, in FWSM Release 3.1, the **nameif**, **ip address**, and **security-level** commands are now available in the interface configuration mode. The interface configuration mode facilitates other feature enhancements such as support for IPv6. The hierarchical output also improves the readability of a configuration file compared with the flat structure used in FWSM Release 2.x.

After upgrading to FWSM Release 3.1, for every VLAN that is allocated to a context with the **allocate-interface** command, **interface** commands are added to the system configuration as well as to each context. In the system configuration, you can shut down or enable an interface for all contexts.

The following example shows the syntax in FWSM Release 2.x and the corresponding configuration in FWSM Release 3.1:

FWSM Release 2.x

```
nameif vlan10 outside security0
nameif vlan15 inside security100
ip address outside 10.6.37.124 255.255.255.0
ip address inside 192.16.1.1 255.255.255.0
interface inside
   no shutdown
interface outside
   shutdown
```

FWSM Release 3.1

```
interface vlan 10
   nameif outside
   security-level 0
   ip address 10.6.37.124 255.255.255.0
   no shutdown
interface vlan 15
    nameif inside
    security-level 100
    ip address 192.16.1.1 255.255.255.0
    no shutdown
```

In multiple context mode, the system configuration also includes the following:

```
interface vlan 10
    no shutdown
interface vlan 15
    no shutdown
```

Table 11 summarizes the changes in the **interface** command syntax.

Table 11 Interface and Interface Configuration Mode Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
interface *interface-name*	**interface** {**vlan** *number* | *mapped_name*}	The name, security level, and IP address are configured by the **nameif**, **security-level**, and **ip address** commands in interface configuration mode. Use the mapped name in multiple context mode if you created a mapped name in the **allocate-interface** command.
ip address *interface-name ip_address* [*netmask*] [**standby** *stdby_address*]	**ip address** *ip_address* [*netmask*] [**standby** *stdby_address*]	Converted to **interface** configuration mode command.
nameif *vlan_id interface-name security_level*	**nameif** *interface-name* **security-level** *level*	Converted to **interface** configuration mode command. *security_level* is configured by the separate **security-level** command.

AAA

In FWSM Release 2.x, server parameters were configured per server group. In FWSM Release 3.1, server parameters can be configured per AAA server with some parameters being configurable only for the entire AAA server group. There is also a change in the way that AAA server groups are mapped to VPN tunnels.

In FWSM Release 3.1, the **aaa-server** command enables a configuration mode that lets you define the parameters for an AAA server group. To use an AAA server for authentication, authorization, or accounting, you must first create at least one AAA server group and add one or more servers to the group. You identify AAA server groups by name. Each server group is specific to one type of protocol: Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

FWSM Release 3.1 allows most AAA server configuration parameters to be configured per server. The **aaa-server** command now has the following two configuration modes:

- Host configuration mode for configuring AAA server specific parameters

- Group configuration mode for configuring parameters that can only be applied to the entire AAA server group

The following is an example:

```
aaa-server svrgrp1 protocol radius
aaa-server svrgrp1 host 10.10.10.1
    timeout 30
    retry 3
    exit
aaa-server svrgrp1 host 10.10.10.2
    timeout 60
    retry 3
    exit
```

Note In FWSM Release 3.1, the FTP connection is reset immediately when authorization is denied. FWSM Release 2.x provided an FTP login before denying authorization.

Table 12 lists changes in the **aaa-server**, **auth-prompt**, and **floodguard** commands.

Table 12 Changes in the AAA, auth-prompt, and floodguard Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
aaa-server radius-acctport [*acct_port*]	**aaa-server** *server-tag* [(*interface-name*)] **host** server-ip **accounting-port** *port*	The **radius-acctport** and **radius-authport** values are now configured as part of the **aaa-server** host-specific configuration mode commands. These settings are now host-based; they were previously server-group based.
aaa-server radius-authport [*auth_port*]	**aaa-server** *server-tag* [(*interface-name*)] **host** *server-ip* **authentication-port** *port*	
aaa-server *server_tag* [*interface_name*] **host** *server_ip* [*key*] [**timeout** *seconds*]	**aaa-server** *server-tag* [(interface-name)] **host** *server-ip* **key** *key* **timeout** seconds	—
auth-prompt [**prompt** | **accept** | **reject**] *prompt text*	**auth-prompt** {**prompt** | **accept** | **reject**} *text*	One of the following keywords is now mandatory: **{prompt | accept | reject}**
floodguard [**enable**|**disable**]	Not supported	The following message will be displayed: "This command is no longer needed. The **floodguard** feature is always enabled."
show floodguard		
clear floodguard		

MGCP

With the introduction of Modular Policy Framework, all **fixup** commands including **fixup mgcp** have been converted to **inspect** commands (see the "Application Inspection (fixup Command)" section on page 35). Also, the existing Media Gateway Control Protocol (MGCP) commands have been moved under the **mgcp-map** command to work within the Modular Policy Framework.

The **fixup mgcp** and **mgcp** commands have been deprecated, and are replaced with the **inspect mgcp** and **mgcp-map** commands, along with commands within the MGCP-map configuration mode. When upgrading to FWSM Release 3.1, MGCP commands are converted automatically and manual intervention is not required. Table 13 summarizes the changes that have occured to the MGCP commands in FWSM Release 3.1.

Table 13 Changes in the MGCP Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
mgcp call-agent *ip-address group-id* **mgcp gateway** *ip-address group-id* **mgcp command-queue** *limit*	**mgcp-map** *map_name* **call-agent** *ip-address group-id* **gateway** *ip-address group-id* **command-queue** *limit*	The **mgcp-map** command is only required to identify call agents and gateways, or to modify the maximum number of commands in the command-queue. To apply the MGCP map and its associated configuration to the application inspection engine, enter the **inspect mgcp** *map_name* command.

NAT

In FWSM Release 3.1, a new command, **nat-control**, has been introduced to maintain FWSM Release 2.x NAT functionality. When you upgrade to FWSM Release 3.1, the new **nat-control** command is automatically incorporated into the configuration.

In FWSM Release 2.x, whenever hosts on a higher security interface communicate with hosts on a lower security interface, you must configure NAT on the higher security interface. In FWSM Release 3.1, this NAT control can be disabled. You can still configure NAT, but NAT is not required for communication. For example, if you disable NAT control, you do not need to configure a static NAT statement for outside hosts to connect to an inside host. When you upgrade from FWSM Release 2.x to Release 3.1, NAT control is enabled.

To disable NAT control, enter the **no nat-control** command.

Miscellaneous Commands

Table 14 Changes in Miscellaneous Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
copy capture:buffer name tftp URL [**pcap**] **copy capture:**[*context-name/*]*capture-name* **tftp://***location/pathname* [**pcap**]	**copy** [/**pcap**] **capture:***bufferSpe URL*	In single mode, *bufferSpec*:= *buffername*. In multimode, [*context name/*] *buffername.*
sysopt connection permit-ipsec	—	Deprecated. This command did not affect traffic because IPSec traffic is always exempt from the interface access list.

Table 14 Changes in Miscellaneous Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
terminal pager lines *lines*	**terminal pager** [**lines**] *lines*	The **lines** keyword is now optional.
pager lines *lines*	**pager** [**lines**] *lines*	

Failover

File system commands (**rename**, **mkdir**, **rmdir**, **delete**, **copy running-config startup-config**) are replicated to the standby unit in FWSM Release 3.1

When a file system command fails on the standby device, no configuration sync occurs between the active and standby devices because the file system commands are not part of the configuration. When a file system command fails on the standby device, an informational message is displayed, noting that the file system may be out of sync.

Both the **write memory** and the **copy running-config startup-config** commands are replicated. The **format** command is not replicated.

Logging Commands

You can no longer configure any **logging** commands in the system execution space. Instead, system messages (including failover messages) are output in the admin context. To differentiate system and admin messages, enter the following command in the admin context:

```
hostname/admin(config)# logging device-id context-name
```

Note The **logging** commands are *not* automatically removed from the system configuration. Errors are displayed until you move the commands from the system configuration to the admin context configuration.

Device Management Commands

In FWSM Release 3.1, the device manager is called ASDM, and not PDM. All **pdm** commands are now **asdm** commands. These commands convert automatically when upgrading to FWSM Release 3.1. Manual intervention is not required.

Table 15 lists changes in these commands.

Table 15 Changes in Device Management Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
pdm disconnect *session_id*	**asdm disconnect** *session* **asdm disconnect log_session** *session*	—
pdm group *ref_group_name ref_intf_name* reference *real_group_name*	**asdm group** *real_grp_name real_if_name*	Do not manually configure this command. ASDM adds **asdm group** commands to the running configuration and uses them for internal purposes.
pdm history [**view** {**all** | **12h** | **5d** | **60m** | **10m**}] [**snapshot**] [**feature** {**all** | **blocks** | **cpu** | **failover** | **ids** | **interface** *interface_name* | **memory** | **perfmon** | **xlates**}] [**pdmclient**]	**asdm history enable**	—

Table 15 Changes in Device Management Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
pdm location *ip_address netmask interface_name*	**asdm location** *ip_addr netmask if_name*	Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication.
pdm logging [*level* [*messages*]]	**logging asdm**	—
show pdm history [**view** {**all** | **12h** | **5d** | **60m** | **10m**}] [**snapshot**] [**feature** {**all** | **blocks** | **cpu** | **failover** | **ids** | **interface** *interface_name* | **memory** | **perfmon** | **xlates**}] [**pdmclient**]	**show asdm history** [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]	—
show pdm logging	**show logging asdm**	—
show pdm sessions	**show asdm log_sessions** **show asdm sessions**	The **show asdm log_sessions** command displays a list of active ASDM logging sessions and their associated session IDs.

VPN Commands

This section describes the VPN commands that have changed in FWSM Release 3.1. It includes the following topics:

- Group Management, page 44
- Remote Peers, page 45
- Public Key Infrastructure (PKI) Commands, page 46
- Summary of Changes in the VPN Commands, page 47

Group Management

The **vpngroup** command has been replaced by the **tunnel-group** and **group-policy** commands. Dividing configuration data between the **tunnel-group** and the **group-policy** commands is intended to facilitate the sharing of group policies.

The tunnel group is generally tied to a VPN peer or group of peers. The group policy is then applied to either a single tunnel group or to several tunnel groups. An additional benefit is that the group policy can be stored or maintained on an external policy server.

All uses of the **vpngroup** command are automatically converted to the **tunnel-group** and **group-policy** commands. The following is an example of some **vpngroup** commands converted to the new syntax:

FWSM Release 2.x syntax:

```
vpngroup group1 address-pool pool1
vpngroup group1 password mypassword
```

FWSM Release 3.1 syntax:

```
tunnel-group group1 type ipsec-ra
tunnel-group group1 general-attributes
    address-pool pool1
```

```
tunnel-group group1 ipsec-attributes
    pre-shared-key mypassword
```

FWSM Release 2.x syntax:

```
crypto map map_name client authenticate aaa_server_group_name
```

FWSM Release 3.1 syntax:

```
tunnel-group group1 type ipsec-ra
tunnel-group group1 general-attributes
    authentication-server-group myservergroup
```

Remote Peers

After upgrading from FWSM Release 2.x to FWSM Release 3.1, connections fail on an FWSM that terminates the remote connections from Cisco IOS peers when using a dynamic crypto map with certificates. The solution is to change the configuration to force the connecting Cisco IOS peers into the ipsec-l2l group.

The following is sample output from the **debug crypto isakmp 50** command, after you perform an upgrade to FWSM Release 3.1:

```
debug crypto isakmp 50
...
[IKEv1], IP = x.x.x.x , Connection landed on tunnel_group DefaultRAGroup
[IKEv1], Group = DefaultRAGroup, IP = x.x.x.x Xauth
required but selected Proposal does not support xauth,  Check
priorities of ike xauth proposals in ike proposal list,
...
```

Xauth

In FWSM Release 2.x, Xauth was disabled by default for dynamic or remote access (client) tunnels. If you did not use Xauth, there will be no indication of this in your configuration.

When you upgrade to FWSM Release 3.1, the default remote access tunnel group has Xauth enabled by default, and it attempts to authenticate tunnels from the local database.

In FWSM Release 2.x, if you terminate dynamic VPN tunnels without Xauth, you must add the following information to your configuration after upgrading to disable Xauth:

For the default group:

```
tunnel-group DefaultRAGroup general-attributes
   authentication-server-group none
```

If any additional tunnel groups were converted, you should add the following command to each tunnel group:

```
tunnel-group group_name general-attributes
   authentication-server-group none
```

In FWSM Release 3.1, the ISAKMP default policy is no longer hidden. The ISAKMP default policy is now visible in the running configuration, and you can retain, modify, or remove it.

FWSM Release 2.x syntax:

```
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
```

```
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
```

FWSM Release 3.1 syntax:

```
isakmp policy 65535 authentication rsa-sig
isakmp policy 65535 encryption des
isakmp policy 65535 hash sha
isakmp policy 65535 group 1

isakmp policy 65535 lifetime 86400
```

Public Key Infrastructure (PKI) Commands

This section describes the PKI commands that are affected when upgrading to FWSM Release 3.1.

The certification authority (**ca**) commands were modified to incorporate more PKI features and to make them look more like Cisco IOS software commands.

The concept of a trustpoint is new for FWSM Release 3.1. A trustpoint is the representation of a certification authority (CA) certificate/identity certificate pair and includes the following information:

- The identity of the CA
- CA specific configuration parameters
- An association with one enrolled identity certificate

In FWSM Release 2.x, the functionality of trustpoints was provided through CA identities, configured with the **ca identity** command.

A trustpoint allows the configuration and use of multiple CA certificates and consequently multiple identity certificates in FWSM Release 3.1. FWSM Release 2.x only supported the configuration and use of a single identity certificate. The following is an example of how the CLI has changed:

FWSM Release 2.x syntax:

```
ca identity myca 10.10.10.100 10.10.10.110
ca configure myca ca 3 3
```

FWSM Release 3.1 syntax:

```
crypto ca trustpoint myca
    enroll url 10.10.10.100
    enrollment mode ca
    enrollment retry period 3
    enrollment retry count 3
    crl required
    crl
        ldap_defaults 10.10.10.110
```

In FWSM Release 3.1, there are two key changes:

- In FWSM Release 3.1, the commands are now based on the **crypto** keyword. In FWSM Release 2.x, the PKI commands were based on the **ca** keyword.
- In FWSM Release 3.1, certificates are stored in the configuration file and are based on the **crypto** command tree. In FWSM Release 2.x, the certificates were stored in a private hidden data file.

In FWSM Release 3.1, the **clear configure crypto** command removes all crypto configurations, including CA configurations.The behavior of any **clear config** *keyword* command is to remove all lines from the running configuration that are based on the *keyword*. To display CA information, enter the **show crypto** command.

In FWSM Release 2.x, the **clear crypto** command removed all crypto configurations other than certification authority (CA) configurations, such as trustpoints, certificates, and certificate maps.

The deprecated **ca** commands are converted automatically when upgrading to FWSM Release 3.1. There are also additional new **ca** commands. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for more information on the new **ca** commands.

The **ca save all** command has been removed and as with Cisco IOS software, keys and certificate data are saved at the same time that the configuration is written to memory.

Summary of Changes in the VPN Commands

Table 16 summarizes the changes that have occurred in the VPN commands between FWSM Release 2.x and FWSM Release 3.1.

Table 16 Changes in the VPN Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
ca generate rsa {**key** | **specialkey**} *key_modulus_size*	**crypto key generate rsa** [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]	The **ca generate** command is deprecated in FWSM Release 3.1.
ca zeroize rsa [*keypair_name*]	**crypto key zeroize rsa**	The **ca zeroize** command is deprecated in FWSM Release 3.1

ca identity *ca_nickname* [*ca_ipaddress* | *hostname* [:*ca_script_location*] [*ldap_ip address* | *hostname*]]	**crypto ca trustpoint** *trustpoint-name*
	  enroll url *ip_address*|*hostname*[:*ca_script_location*]
	  crl
	  ldap_defaults *ldap_ip*|*hostname*
	  exit
	exit
		The **ca identity** command is deprecated in FWSM Release 3.1

Table 16 Changes in the VPN Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
ca configure *ca_nickname* {**ca** | **ra**} *retry_period retry_count* [**crloptional**]	**crypto ca trustpoint** *name* **crl** {**required** | **optional** | **nocheck**} **enrollment retry period** *retry_period* **enrollment retry count** *retry_count*	The **ca configure** command is deprecated in FWSM Release 3.1. The retry period and count are now configured using the trustpoint configuration mode. CRL configuration mode is accessible from the trustpoint configuration mode.
ca authenticate name [**fingerprint**]	**crypto ca authenticate** name [**fingerprint** | **nointeractive**]	The **ca authenticate** command is deprecated in FWSM Release 3.1.
ca enroll *ca_nickname challenge_password* [**serial**] [**ipaddress**]	**crypto ca trustpoint** *name* **ip-address** *address serial-number* **password** *password* **exit** **crypto ca enroll** *name*	The **ca enroll** command is deprecated in FWSM Release 3.1.
ca crl request *id_name*	**crypto ca crl request** *trustpoint*	The **ca crl request** command is deprecated in FWSM Release 3.1.
ca subject-name *ca_nickname X.500_string*	**crypto ca trustpoint** *name* **subject-name** X.500 string	The **ca subject-name** command is deprecated in FWSM Release 3.1.
ca verifycertdn *X.500_string*	**crypto ca verifycertdn** x.500 string	The **ca verifycertdn** command is deprecated in FWSM Release 3.1.
crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *access list_name*	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **match address** *access list_name*	More Diffie-Hellman group types added.
crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *hostname* | *ip_address*	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set peer** {*ip_address* | *hostname*}	—
crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2**]	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set pfs** [**group1** | **group2** | **group5** | **group7**]	—
crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*	—
crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*transform-set-name9*]	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* […*transform-set-name6*]	—

Table 16 Changes in the VPN Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
crypto ipsec security-association lifetime seconds *seconds* | **kilobytes** *kilobytes*	[**crypto**] **ipsec security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*	Authentication Header (AH) support has been removed. **Note** The standalone version of this **ipsec** command works the same as the **crypto** version. Added the following commands: • [**crypto**] **ipsec df-bit** [**clear-df** | **copy-df** | **set-df**] *interface-name* • [**crypto**] **ipsec fragmentation** [**after-encryption** | **before-encryption**] *interface-name* • **clear configure** [*crypto*] **ipsec transform-set** *transform-set-name* • **show** [**crypto**] **ipsec stats** • **show** [**crypto**] **ipsec df-bit** *interface-name* • **show** [**crypto**] **ipsec fragmentation** *interface-name*
crypto ipsec transform-set *transform-set-name transform1* [*transform2* [*transform3*]]	[**crypto**] **ipsec transform-set** *transform-set-name* **transform1** [**transform3**]	
crypto ipsec transform-set *trans-name* [**ah-md5-hmac** | **ah-sha-hmac**] [**esp-aes** | **esp-aes-192** | **esp-aes-256**| **esp-des** | **esp-3des**| **esp-null**] [**esp-md5-hmac** | **esp-sha-hmac** | **esp-none**]	[**crypto**] **ipsec transform-set** *transform-set-name* [**esp-aes** |**esp-aes-192** | **esp-aes-256**| **esp-des** | **esp-3des**| **esp-null**] [**esp-md5-hmac** | **esp-sha-hmac** | **esp-null**]	
crypto ipsec transform-set *transform-set-name* **mode transport**	[**crypto**] **ipsec transform-set** *transform-set-name* **mode transport** [**crypto**] **ipsec df-bit** [**clear-df** | **copy-df** | **set-df**] *interface-name*	
crypto map *map-name* **interface** *interface-name*	**crypto map** *map-name* **interface** *interface-name*	Removed support for the following commands: **crypto map** *map-name seq-num* **set session-key inbound** | **outbound ah** *spi hex-key-string* **crypto map** *map-name seq-num* **set session-key inbound** | **outbound esp** *spi cipher hex-key-string* [**authenticator** *hex-key-string*] Added new group numbers to the Diffie-Hellman (DH) group specification. Added limit of 10 to the number of peers specified. The 9 additional peers are used as fallback peers when the device is used in "originate only" mode via the connection-type parameter. **Note** The standalone version of the **map** command works the same as its **crypto** version.
crypto map *map-name* **client** [**token**] **authentication** *aaa-server-name*	Deprecated	
crypto map *map-name seq-num* **ipsec-isakmp** | **ipsec-manual** [**dynamic** *dynamic-map-name*]	**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*	
crypto map *map-name seq-num* **set pfs** [**group1** | **group2**]	**crypto map** *map-name seq-num* **set pfs** [**group1** | **group2** | **group5** |**group7**]	
crypto map *map-name seq-num* **match address** *access list_name*	**crypto map** *map-name seq-num* **match address** *access list_name*	
crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}	**crypto map** *map-name seq-num* **set peer** {**ip_address1** | **hostname1**} [**..ip_address10** | **hostname10**]	
crypto map *map-name seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*	**crypto map** *map-name seq-num* **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*	
crypto map map-name seq-num set transform-set *transform-set-name1* [*transform-set-name6*]	**crypto map** *map-name seq-num* **set transform-set** *transform-set-name1* [*.. transform-set-name6*]	
crypto map *map-name* **client configuration address initiate** | **respond**	Not supported	

Table 16 Changes in the VPN Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
isakmp keepalive *seconds* [*retry-seconds*]	**tunnel-group** *group name* **type ipsec-ra**|**ipsec-l2l** **tunnel-group** *group name* **ipsec-attributes** **isakmp keepalive** [***threshold*** *seconds*][***retry*** *seconds*]	—
isakmp key *keystring* **address** *peer-address* [**netmask** *mask*] [**no-xauth**] [**no-config-mode**]	**tunnel-group** *group name* **type ipsec-l2l** **tunnel-group** *group name* **ipsec-attributes** **pre-shared-key** *preshared key*	The **isakmp** command was used to set a preshared key for LAN-to-LAN tunnels. This is now done generically for both LAN-to-LAN and remote access tunnels via the **tunnel-group** command.
isakmp client configuration address-pool local *pool-name* [*interface-name*]	**tunnel-group** *group name* **type ipsec-l2l** **tunnel-group** *group name* **general-attributes** **address-pool** [**(***interface***)**] *address_pool1* [*...address-pool6*]	—
isakmp peer fqdn | **ip fqdn** | **ip-address** {**no-xauth** |**no-config-mode**}	**tunnel-group** *group name* **type ipsec-l2l**|**ipsec-ra**	The exclusion of Xauth and modecfg is implicit in the definition of the tunnel group. If a tunnel group is defined as ipsec-l2l, it automatically excludes Xauth and modecfg.
vpngroup *group_name* **address-pool** *pool_name*	**tunnel-group** *group name* **type ipsec-l2l** **tunnel-group** *group name* **general-attributes** **address-pool** [**(***interface***)**] *address_pool1* [*...address-pool6*]	Converted to **tunnel-group** syntax.
vpngroup *group_name* **authentication-server** *servers*	Not supported	Used on FWSM Release 2.x to pass a AAA server address for Individual User Authentication (IUA), a feature used on the hardware client; FWSM 3.1 proxies the AAA request for the hardware client, and therefore always sends its own address.
vpngroup *group_name* **backup-server** {{**ip1** [*ip2 ... ip10*]} | **clear-client-cfg**}	In the group-policy attribute configuration mode: **backup-servers** *peer1 peer2 …..peer10* | **clear-client-config** | **keep-client-config**	Converted to **group-policy** syntax.
vpngroup *group_name* **default-domain** *domain_name*	In the group-policy attribute configuration mode: **default-domain value** *domain-name*	Converted to **group-policy** syntax.
vpngroup *group_name* **device-pass-through**	In the group-policy attribute configuration mode: **ip-phone-bypass** enable|disable **leap-bypass** enable|disable	Converted to **group-policy** syntax. The IUA exemption is no longer MAC address based. The administrator can choose to exempt Cisco IP Phones and/or any LEAP data from Individual User Authentication.

Table 16 Changes in the VPN Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
vpngroup *group_name* **dns-server** *dns_ip_prim* [*dns_ip_sec*]	In the group-policy attribute configuration mode: **dns-server value** *ip_address* [*ip_address*]	Converted to **group-policy** syntax.
vpngroup *group_name* **idle-time** *idle_seconds*	In the group-policy attribute configuration mode: **vpn-idle-timeout** *minutes* | **none**	Converted to **group-policy** syntax.
vpngroup *group_name* **max-time** *max_seconds*	In the group-policy attribute configuration mode: **vpn-session-timeout** *minutes* | **none**	Converted to **group-policy** syntax.
vpngroup *group_name* **password** *preshared_key*	**tunnel-group** *group name* **type ipsec-ra** **tunnel-group** *group name* **ipsec-attributes** **pre-shared-key** *preshared key*	Converted to **tunnel-group** syntax.
vpngroup *group_name* **pfs**	In the group-policy attribute configuration mode: **pfs enable**|**disable**	Converted to **group-policy** syntax.
vpngroup *group_name* **secure-unit-authentication**	In the group-policy attribute configuration mode: **secure-unit-authentication enable**|**disable**	Converted to **group-policy** syntax.
vpngroup *group_name* **split-dns** *domain_name1* [*domain_name2 ... domain_name8*]	In the group-policy attribute configuration mode: **split-dns value** *domain_name1 domain_name2 ... domain_nameN*	Converted to **group-policy** syntax.
vpngroup *group_name* **split-tunnel** *access_list*	In the group-policy attribute configuration mode: **split-tunnel-network-list value** *access-list name*	Converted to **group-policy** syntax.

Table 16 Changes in the VPN Commands

FWSM Release 2.x	FWSM Release 3.1	Notes
vpngroup *group_name* **user-authentication**	In the group-policy attribute configuration mode: **user-authentication enable**|**disable**	Converted to **group-policy** syntax.
vpngroup *group_name* **user-idle-timeout** *user_idle_seconds*	In the group-policy attribute configuration mode: **user-authentication-idle-timeout** *minutes* | **none**	Converted to **group-policy** syntax.
vpngroup *group_name* **wins-server** *wins_ip_prim* [*wins_ip_sec*]	In the group-policy attribute configuration mode: **wins-server value ip_address** [*ip_address*]	Converted to **group-policy** syntax.
show vpngroup [*group_name*]	**show running-config** [**default**] **tunnel-group** [*name* [**general-attributes** | **ipsec-attributes** | **ppp-attributes**]] **show running-config** [**default**] **group-policy** [*name* [**attributes**]]	Converted to **tunnel-group** and **group-policy** syntax; both commands are used to replace the **vpngroup** command.

Obtaining More Information

This section describes where to obtain more information and includes the following topics:

- Obtaining Documentation, page 52
- Documentation Feedback, page 53
- Cisco Product Security Overview, page 54
- Reporting Security Problems in Cisco Products, page 54
- Obtaining Technical Assistance, page 54
- Obtaining Additional Publications and Information, page 56

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html