



# CHAPTER 22

## Managing Software, Licenses, and Configurations

---

This chapter describes how to install new software on the FWSM from an FTP, TFTP, HTTP, or HTTPS server. You can upgrade the application software, the maintenance software, and ASDM management software. You can also enable Auto Update support. This chapter includes the following sections:

- [Managing Licenses, page 22-1](#)
- [Installing Application or ASDM Software, page 22-3](#)
- [Upgrading Failover Pairs, page 22-9](#)
- [Installing Maintenance Software, page 22-12](#)
- [Downloading and Backing Up Configuration Files, page 22-15](#)
- [Configuring Auto Update Support, page 22-18](#)



**Note**

---

Because the FWSM runs its own operating system, upgrading the Cisco IOS or Catalyst operating software does not affect the operation of the FWSM.

---

## Managing Licenses

When you install the software, the existing activation key is extracted from the original image and stored in a file in the FWSM file system. This section includes the following topics:

- [Obtaining an Activation Key, page 22-1](#)
- [Entering a New Activation Key, page 22-2](#)
- [Entering Activation Keys in a Failover Pair, page 22-2](#)

## Obtaining an Activation Key

To obtain an activation key, you will need a Product Authorization Key, which you can purchase from your Cisco account representative. After obtaining the Product Authorization Key, register it on the Web to obtain an activation key by performing the following steps:

---

**Step 1** Obtain the serial number for your FWSM by entering the following command:

```
hostname> show version | include Number
```

Enter the pipe character (|) as part of the command.

**Step 2** Connect a web browser to one of the following websites (the URLs are case-sensitive):

Use the following website if you are a registered user of Cisco.com:

```
http://www.cisco.com/go/license
```

Use the following website if you are not a registered user of Cisco.com:

```
http://www.cisco.com/go/license/public
```

**Step 3** Enter the following information when prompted:

- Your Product Authorization Key
- The serial number of your FWSM.
- Your e-mail address.

The activation key is automatically generated and sent to the e-mail address that you provide.

---

## Entering a New Activation Key

To enter the activation key, enter the following command:

```
hostname(config)# activation-key key
```

The key is a four- or five-element hexadecimal string with one space between each element. For example, a key in the correct form might look like the following key:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal.

If you are already in multiple context mode, enter this command in the system execution space.



### Note

The activation key is not stored in your configuration file. The key is tied to the serial number of the device.

---

This example shows how to change the activation key on the FWSM:

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

## Entering Activation Keys in a Failover Pair

To enter activation keys in a failover configuration, perform the following steps:

**Step 1** Disable failover by entering the **no failover** command on the active FWSM:

```
hostname(config)# no failover
```

The active FWSM remains active, and the standby FWSM moves to a pseudo-standby state.



---

**Note** Disabling failover does not affect transient traffic.

---

**Step 2** Apply different activation keys to the active FWSM and to the standby FWSM. Each device has his own unique key that is tied to the serial number on the FWSM.

**Step 3** Re-enable failover by entering the **failover** command on the active FWSM:

```
hostname(config)# failover
```

Entering the command on the active FWSM re-enables failover between both units and brings up the failover pair.

---

## Installing Application or ASDM Software

This section contains the following topics:

- [Installation Overview, page 22-3](#)
- [Installing Application Software from the FWSM CLI, page 22-4](#)
- [Installing Application Software from the Maintenance Partition, page 22-5](#)
- [Installing ASDM from the FWSM CLI, page 22-9](#)

## Installation Overview

For application software, you can use one of two methods to upgrade:

- Installing to the current application partition from the FWSM CLI

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.

- Installing to any application partition from the maintenance partition

The benefit of this method is you can copy software to both application partitions, and you do not have to have an operational configuration. You just need to configure some routing parameters in the maintenance partition so you can reach the server on VLAN 1.

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

This method supports downloading from an FTP server only.

To upgrade ASDM, you can only install to the current application partition from the FWSM CLI.

See the “[Managing the Firewall Services Module Boot Partitions](#)” section on page 2-10 for more information about application and maintenance partitions.

## Installing 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.

For multiple context mode, you must be in the system execution space.

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:
```

- To use secure copy, first enable SSH, then enter the following command:

```
hostname# ssh scopy enable
```

Then from a Linux client, enter the following command:

```
scp filename username@fwsm_address:disk:
```

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

```
hostname# copy ftp://10.94.146.80/tftpboot/user1/cdisk flash:
```

```
copying ftp://10.94.146.80/tftpboot/user1/cdisk to flash:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Received 6128128 bytes.
Erasing current image.This may take some time.
Writing 6127616 bytes of image.
```



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 (3.1 vs. 3.2), then both units become active. Two active units can cause networking problems.

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

**Step 1** Each application partition has its own startup configuration, so you need to make the current configuration available to copy to the backup application partition, if desired. 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.

**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 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 software, 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:

- 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. Using an address in the 10.3.1.0/24 subnet for the maintenance partition IP address can cause communication problems with other hosts on that subnet; the FWSM uses 10.3.1.1 for internal diagnostics.

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

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

- (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 backup application partition (that you set as the default in [Step 4](#)), enter the command for your operating system:

- For Cisco IOS software, 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 might need to copy a current 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 configuration to the running configuration, use one of the following methods:

- Paste the 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 new 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.

---

## Installing ASDM from the FWSM CLI

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

For multiple context mode, you must be in the system execution space.

To check connectivity, use the **ping** command.

To copy ASDM software, enter one of the following commands for the appropriate download server:

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

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

The **flash** keyword represents to 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:asdm
```

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

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

- To use secure copy, first enable SSH, then enter the following command:

```
hostname# ssh scopy enable
```

Then from a Linux client enter the following command:

```
scp filename username@fwsn_address:disk:
```

For example, to copy ASDM from a TFTP server, enter:

```
hostname# copy tftp://209.165.200.226/cisco/asdm.bin flash:asdm
```

To copy to the ASDM from an HTTPS server, enter:

```
hostname# copy http://admin:letmein@209.165.200.228/adsm/asdm.bin flash:asdm
```

## Upgrading Failover Pairs

The two units in a failover configuration should have the same major (first number), minor (second number), and maintenance (third number) software version.

However, you can have different *maintenance* versions of the software running on each unit and still maintain failover support. You can upgrade from any maintenance release to any other maintenance release within a minor release. For example, you can upgrade from 3.1(1) to 3.1(3) without first installing the maintenance release in between.

To ensure long-term compatibility and stability, we recommend upgrading both units to the same version as soon as possible.

The FWSM does not support upgrading from between major or minor releases, for example, from 2.3 to 3.1, without downtime.



### Note

To upgrade failover pairs from the maintenance partition, see the [“Installing Application Software from the Maintenance Partition”](#) section on page 22-5.

This section includes the following topics:

- [Upgrading Failover Pairs to a New Maintenance Release, page 22-10](#)
- [Upgrading Failover Pairs to a New Minor or Major Release, page 22-11](#)

## Upgrading Failover Pairs to a New Maintenance Release

You can upgrade from any maintenance release to any other maintenance release within a minor release without downtime.

For example, you can upgrade from 3.1(1) to 3.1(3) without first installing the maintenance releases in between.

This section includes the following topics:

- [Upgrading an Active/Standby Failover Pair to a New Maintenance Release, page 22-10](#)
- [Upgrading an Active/Active Failover Pair to a New Maintenance Release, page 22-11](#)

### Upgrading an Active/Standby Failover Pair to a New Maintenance Release

To upgrade two units in an Active/Standby failover configuration to a new maintenance release, perform the following steps.

- 
- Step 1** Download the new software to both units. See the “[Installing Application Software from the FWSM CLI](#)” section on page 22-4.
- Step 2** 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.

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.

- Step 3** Reload the standby unit to boot the new image by entering the following command on the active unit:
- ```
primary# failover reload-standby
```
- Step 4** When the standby unit has finished reloading, and is in the Standby Ready state, force the active unit to fail over to the standby unit by entering the following command on the active unit.




---

**Note** Use the **show failover** command to verify that the standby unit is in the Standby Ready state.

---


```
primary# no failover active
```

- Step 5** Reload the former active unit (now the new standby unit) by entering the following command:
- ```
primary# reload
```
- Step 6** (Optional) When the new standby unit has finished reloading, and is in the Standby Ready state, return the original active unit to active status by entering the following command:
- ```
primary# failover active
```

---

## Upgrading an Active/Active Failover Pair to a New Maintenance Release

To upgrade two units in an Active/Active failover configuration to a new maintenance release, perform the following steps.

- 
- Step 1** Download the new software to both units. See the [“Installing Application Software from the FWSM CLI” section on page 22-4](#).
- Step 2** 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.
- 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.
- Step 3** Make both failover groups active on the primary unit by entering the following command in the system execution space of the primary unit:
- ```
primary# failover active
```
- Step 4** Reload the secondary unit to boot the new image by entering the following command in the system execution space of the primary unit:
- ```
primary# failover reload-standby
```
- Step 5** When the secondary unit has finished reloading, and both failover groups are in the Standby Ready state on that unit, make both failover groups active on the secondary unit using the following command in the system execution space of the primary unit:
- ```
primary# no failover active
```
-  **Note** Use the **show failover** command to verify that both failover groups are in the Standby Ready state on the secondary unit.
- 
- Step 6** Make sure both failover groups are in the Standby Ready state on the primary unit, and then reload the primary unit using the following command:
- ```
primary# reload
```
- If the failover groups are configured with the **preempt** command, they will automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with the **preempt** command, you can return them to active status on their designated units using the **failover active group** command.
- 

## Upgrading Failover Pairs to a New Minor or Major Release

To upgrade two units in an Active/Active or Active/Standby failover configuration to a new minor or major release, perform the following steps.

- 
- Step 1** Download the new software to both units. See the “[Installing Application Software from the FWSM CLI](#)” section on page 22-4.
- Step 2** 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.
- 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.
- Step 3** 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 or minor version number does not match (3.1 vs. 3.2), then both units become active. Two active units can cause networking problems.
- 

## Installing Maintenance Software

You must install maintenance software Release 2.1(2) or later before you upgrade to FWSM Release 3.1. This section includes the following topics:

- [Checking the Maintenance Software Release, page 22-12](#)
- [Upgrading the Maintenance Software, page 22-13](#)

### Checking the Maintenance Software Release

To determine the maintenance software release, you must 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 software, 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
```

```
Password:
```

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

The FWSM shows the version when you first log in:

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

**Step 5** 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

If you need to upgrade the maintenance software, perform the following steps:

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

<http://www.cisco.com/cisco/software/navigator.html>

Put the software on a TFTP, HTTP, or HTTPS server that is accessible from the FWSM admin context.

**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 FWSM into the application partition by entering the command for your operating system:

- For Cisco IOS software, 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
```

- Step 3** To upgrade the maintenance partition software, enter one of the following commands for 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, or if you do not supply it in the command, you can enter it at the prompts.

- 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.

- 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 “[Installing Application Software from the Maintenance Partition](#)” section on page 22-5 to reload the FWSM into the maintenance partition.

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.

```

## Downloading and Backing Up Configuration Files

This section describes how to download and back up configuration files, and includes the following sections:

- [Viewing Files in Flash Memory, page 22-15](#)
- [Downloading a Text Configuration to the Startup or Running Configuration, page 22-15](#)
- [Downloading a Context Configuration to Disk, page 22-16](#)
- [Backing Up the Configuration, page 22-17](#)

## Viewing Files in Flash Memory

You can view files in Flash memory and see information about the files.

- To view the files in Flash memory, enter the following command:

```
hostname# dir disk:
```

For example:

```
hostname# dir
```

```
Directory of disk:/
```

```

9      -rw-  1411      08:53:42 Oct 06 2005  old_running.cfg
10     -rw-   959      09:21:50 Oct 06 2005  admin.cfg
11     -rw-  1929      08:23:44 May 07 2005  admin_backup.cfg

```

- To view extended information about a specific file, enter the following command:

```
hostname# show file information [path:/]filename
```

The default path is the root directory of the internal Flash memory (disk:/).

For example:

```
hostname# show file info admin.cfg
```

```

disk:/admin.cfg:
  type is ascii text
  file size is 959 bytes

```

## Downloading a Text Configuration to the Startup or Running Configuration

You can download a text file from the following server types to the single mode configuration or the multiple mode system configuration:

- TFTP

- FTP
- HTTP
- HTTPS

For a multiple mode context, see the [“Downloading a Context Configuration to Disk”](#) section on page 22-16.



#### Note

When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.

To copy the startup configuration or running configuration from the server to the FWSM, enter one of the following commands for the appropriate download server:

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

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

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

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

The **type** can be one of the following keywords:

- **ap**—ASCII passive mode
- **an**—ASCII normal mode
- **ip**—(Default) Binary passive mode
- **in**—Binary normal mode

You can use ASCII or binary for configuration files.

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

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

For example, to copy the configuration from a TFTP server, enter the following command:

```
hostname# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

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

```
hostname# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg;type=an
startup-config
```

To copy the configuration from an HTTP server, enter the following command:

```
hostname# copy http://209.165.200.228/configs/startup.cfg startup-config
```

## Downloading a Context Configuration to Disk

To copy context configurations to disk, including the admin configuration, enter one of the following commands for the appropriate download server 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
```

## Backing Up the Configuration

To back up your configuration, use one of the following methods:

- [Backing up the Single Mode Configuration or Multiple Mode System Configuration, page 22-17](#)
- [Backing Up a Context Configuration in Flash Memory, page 22-17](#)
- [Backing Up a Context Configuration within a Context, page 22-18](#)
- [Copying the Configuration from the Terminal Display, page 22-18](#)

### 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.

## 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.

# Configuring Auto Update Support

Auto Update is a protocol specification that allows an Auto Update Server to download configurations and software images to a many FWSMs, and can provide basic monitoring of the FWSMs from a central location. The FWSM periodically polls the Auto Update Server for updates to software images and configuration files.



### Note

---

Auto Update is supported in single context mode only.

---

This section includes the following topics:

- [Configuring Communication with an Auto Update Server, page 22-18](#)
- [Viewing Auto Update Status, page 22-20](#)

## Configuring Communication with an Auto Update Server

To configure Auto Update, perform the following steps:

- 
- Step 1** To specify the URL of the AUS, use the following command:

```
hostname(config)# auto-update server url [source interface] [verify-certificate]
```

Where *url* has the following syntax:

```
http[s]://[user:password@]server_ip[:port]/pathname
```

You can configure only one server. SSL is used when **https** is specified. The *user* and *password* arguments of the URL are used for Basic Authentication when logging in to the server. If you use the **write terminal**, **show configuration** or **show tech-support** commands to view the configuration, the user and password are replaced with '\*\*\*\*\*'.

The default port is 80 for HTTP and 443 for HTTPS.

The **source interface** argument specifies which interface to use when sending requests to the AUS. If you specify the same interface specified by the **management-access** command, the Auto Update requests travel over the same IPsec VPN tunnel used for management access.

The **verify-certificate** keyword verifies the certificate returned by the AUS.

**Step 2** (Optional) To identify the device ID to send when communicating with the AUS, enter the following command:

```
hostname(config)# auto-update device-id {hardware-serial | hostname | ipaddress [if-name]
| mac-address [if-name] | string text}
```

The identifier used is determined by using one of the following parameters:

- **hardware-serial**—Use the FWSM serial number.
- **hostname**—Use the FWSM hostname.
- **ipaddress**—Use the IP address of the specified interface. If the interface name is not specified, it uses the IP address of the interface used to communicate with the AUS.
- **mac-address**—Use the MAC address of the specified interface. If the interface name is not specified, it uses the MAC address of the interface used to communicate with the AUS.
- **string**—Use the specified text identifier, which cannot contain white space or the characters ‘, ‘, , >, & and ?.

**Step 3** (Optional) To specify how often to poll the AUS for configuration or image updates, enter the following command:

```
hostname(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

The *poll-period* argument specifies how often (in minutes) to check for an update. The default is 720 minutes (12 hours).

The *retry-count* argument specifies how many times to try reconnecting to the server if the first attempt fails. The default is 0.

The *retry-period* argument specifies how long to wait (in minutes) between retries. The default is 5.

**Step 4** (Optional) If the Auto Update Server has not been contacted for a certain period of time, the following command will cause it to cease passing traffic:

```
hostname(config)# auto-update timeout period
```

Where *period* specifies the timeout period in minutes between 1 and 35791. The default is to never time out (0). To restore the default, enter the **no** form of this command.

Use this command to ensure that the FWSM has the most recent image and configuration. This condition is reported with system log message 201008.

In the following example, a FWSM is configured to poll an AUS with IP address 209.165.200.224, at port number 1742, from the outside interface, with certificate verification.

It is also configured to use the hostname of the FWSM as the device ID, and the polling period has been decreased from the default of 720 minutes to 600 minutes. On a failed polling attempt, it will try to reconnect to the AUS 10 times, and wait 3 minutes between attempts at reconnecting.

```
hostname(config)# auto-update server
https://jcrichon:farscape@209.165.200.224:1742/management source outside
verify-certificate
hostname(config)# auto-update device-id hostname
hostname(config)# auto-update poll-period 600 10 3
```

## Viewing Auto Update Status

To view the Auto Update status, enter the following command:

```
hostname(config)# show auto-update
```

The following is sample output from the **show auto-update** command:

```
hostname(config)# show auto-update
Server: https://*****@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```