

Cisco Secure Firewall ASA Upgrade Guide

First Published: 2010-01-01

Last Modified: 2026-09-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Planning Your Upgrade** 1

- Important Guidelines Before You Upgrade 1
  - ASA Upgrade Guidelines 1
    - Version-Specific Guidelines and Migrations 1
    - Clustering Guidelines 5
    - Failover Guidelines 5
  - FXOS Upgrade Guidelines 6
- ASA Upgrade Checklist 6
- Compatibility 7
  - ASA and ASDM Compatibility Per Model 7
    - ASA 9.24 7
    - ASA 9.23 and 9.22 8
    - ASA 9.20 and 9.19 9
    - ASA 9.18 to 9.17 10
    - ASA 9.16 11
  - Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense 12
  - Radware DefensePro Compatibility 20
- Upgrade Path 25
  - Upgrade Path: ASA Appliances 25
  - Upgrade Path: ASA on Firepower 2100 in Platform Mode 31
  - Upgrade Path: ASA Logical Devices for the Firepower 4100/9300 34
- Download the Software from Cisco.com 42
  - Download ASA Software 42
  - Download FXOS for the Firepower 4100/9300 49
- Back Up Your Configurations 50

CHAPTER 2

Upgrade the ASA 51

Upgrade the ASA Appliance 51

Upgrade a Standalone Unit 51

Upgrade a Standalone Unit Using the CLI 51

Upgrade a Standalone Unit from Your Local Computer Using ASDM 53

Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard 54

Upgrade an Active/Standby Failover Pair 57

Upgrade an Active/Standby Failover Pair Using the CLI 58

Upgrade an Active/Standby Failover Pair Using ASDM 60

Upgrade an Active/Active Failover Pair 61

Upgrade an Active/Active Failover Pair Using the CLI 62

Upgrade an Active/Active Failover Pair Using ASDM 65

Upgrade an ASA Cluster (Secure Firewall 3100/4200/6100) 66

Upgrade an ASA Cluster Using the CLI (Secure Firewall 3100/4200/6100) 66

Upgrade an ASA Cluster Using ASDM (Secure Firewall 3100/4200/6100) 69

Upgrade the Firepower 4100/9300 71

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster 71

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using Secure Firewall Chassis Manager 71

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using the FXOS CLI 72

Upgrade FXOS and an ASA Active/Standby Failover Pair 76

Upgrade FXOS and an ASA Active/Standby Failover Pair Using Secure Firewall Chassis Manager 76

Upgrade FXOS and an ASA Active/Standby Failover Pair Using the FXOS CLI 78

Upgrade FXOS and an ASA Active/Active Failover Pair 86

Upgrade FXOS and an ASA Active/Active Failover Pair Using Secure Firewall Chassis Manager 86

Upgrade FXOS and an ASA Active/Active Failover Pair Using the FXOS CLI 88

Upgrade FXOS and an ASA Inter-chassis Cluster 97

Upgrade FXOS and an ASA Inter-chassis Cluster Using Secure Firewall Chassis Manager 97

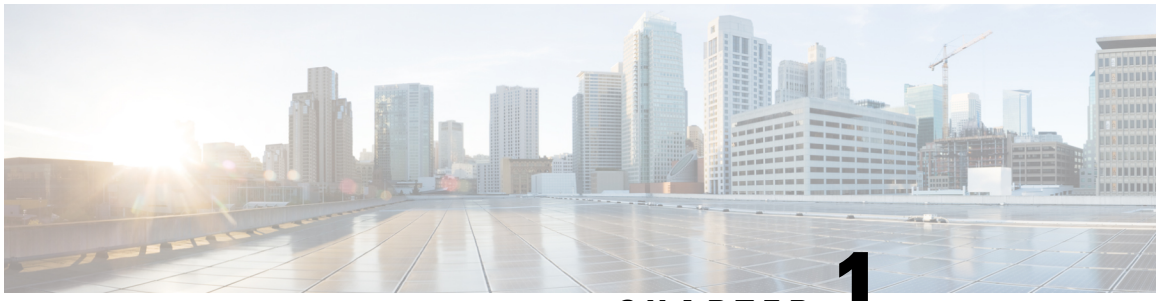
Upgrade FXOS and an ASA Inter-chassis Cluster Using the FXOS CLI 98

Monitor the Upgrade Progress 102

Verify the Installation 103

Upgrade the ASA Virtual, ISA 3000, or ASA 5500-X 104
Upgrade a Standalone Unit 104
Upgrade a Standalone Unit Using the CLI 104
Upgrade a Standalone Unit from Your Local Computer Using ASDM 106
Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard 107
Upgrade an Active/Standby Failover Pair 109
Upgrade an Active/Standby Failover Pair Using the CLI 109
Upgrade an Active/Standby Failover Pair Using ASDM 112
Upgrade an Active/Active Failover Pair 113
Upgrade an Active/Active Failover Pair Using the CLI 113
Upgrade an Active/Active Failover Pair Using ASDM 117
Upgrade an ASA Cluster 118
Upgrade an ASA Cluster Using the CLI 118
Upgrade an ASA Cluster Using ASDM 123
Upgrade the Firepower 2100 in Platform Mode 126
Upgrade a Standalone Unit 126
Upgrade a Standalone Unit Using the Firepower Chassis Manager 126
Upgrade a Standalone Unit Using the FXOS CLI 127
Upgrade an Active/Standby Failover Pair 130
Upgrade an Active/Standby Failover Pair Using the Firepower Chassis Manager 130
Upgrade an Active/Standby Failover Pair Using the FXOS CLI 132
Upgrade an Active/Active Failover Pair 137
Upgrade an Active/Active Failover Pair Using the Firepower Chassis Manager 137
Upgrade an Active/Active Failover Pair Using the FXOS CLI 139

CHAPTER 3 **Downgrade the ASA** 145
Guidelines and Limitations for Downgrading 145
Incompatible Configuration Removed After Downgrading 146
Downgrade the ASA Appliance 147
Downgrade the Firepower 2100 in Platform Mode 148
Downgrade the Firepower 4100/9300 148
Downgrade the ISA 3000 or ASA 5500-X 149



CHAPTER 1

Planning Your Upgrade

Before upgrading the Secure Firewall ASA, you should perform the following preparation:

- Check the upgrade path for the current version to the target version; ensure you plan for any intermediate versions required for each operating system.
- Check for guidelines and limitations that affect your intermediate and target versions, or that affect failover and clustering zero downtime upgrading.
- Download all software packages required from Cisco.com.
- Back up your configurations, especially if there is a configuration migration.

The following topics explain how to upgrade your ASA.

- Important Guidelines Before You Upgrade, on page 1
- ASA Upgrade Checklist, on page 6
- Compatibility, on page 7
- Upgrade Path, on page 25
- Download the Software from Cisco.com, on page 42
- Back Up Your Configurations, on page 50

Important Guidelines Before You Upgrade

Check for upgrade guidelines and limitations, and configuration migrations for each operating system.

ASA Upgrade Guidelines

Before you upgrade, check for migrations and any other guidelines.

Version-Specific Guidelines and Migrations

Depending on your current version, you might experience one or more configuration migrations, and have to consider configuration guidelines for all versions between the starting version and the ending version when you upgrade.

9.24 Guidelines

- **ASDM 7.24(1) requires Java 11**—ASDM 7.24(1) now requires Java 11. For the Oracle version, which is the version bundled with the ASA image, you will need to install Oracle JDK 11: https://www.oracle.com/java/technologies/javase/jdk11-archive-downloads.html. Later versions are not compatible. To minimize risk and ensure better compatibility and stability with Java, we are taking a phased approach to moving off of Java 8, starting with this move to Java 11. If you upgrade to the ASDM Launcher 1.9(10) or later that comes with 7.24(1), you can still launch earlier versions of ASDM.

  For the OpenJRE version, you do not need to install Java; it is built-in.

- **ASA Virtual cannot be downgraded from 9.24(1)**—After upgrading to 9.24(1), which includes a new Grub bootloader, you cannot downgrade to an earlier version. To upgrade to later versions, you will first have to upgrade to 9.24(1).

9.23 Guidelines

- **The ASA SSH stack was deprecated in 9.23**—You can no longer use the ASA SSH stack. The Cisco SSH stack is now the only stack. Because the Cisco SSH stack does not support EDDSA, before you upgrade you must change your configuration for a supported key pair:

  1. Generate the default key pair.

     crypto key generate {**ecdsa elliptic-curve** *size* | **rsa modulus** *size*}

     Do not add the **label** keyword; SSH only uses the default key pair (named Default-*type*-Key).

  2. If you configured the **ssh key-exchange hostkey eddsa** command, you need to remove it with the **no** form. If you use this command, you may get unexpected results.

9.22 Guidelines

- **Smart licensing default transport changed in 9.22**—In 9.22, the smart licensing default transport changed from Smart Call Home to Smart Transport. You can configure the ASA to use Smart Call Home if necessary using the **transport type callhome** command. When you upgrade to 9.22, the transport is automatically changed Smart Transport. If you downgrade, the transport is set back to Smart Call Home, and if you want to use Smart Transport, you need to specify **transport type smart**. Note also that the licensing URL for Smart Transport is https://smartreceiver.cisco.com (compared to tools.cisco.com), so be sure to allow that URL on upstream routers.

  Note Ensure your device can connect to the Smart License Authority. For known connectivity issues and workarounds refer to CSCwp10957 and CSCws62173.

- **For models with built-in-switches, subinterfaces can't use VLAN 1 in 9.22 and later**—For models with built-in switches, you cannot create a subinterface using VLAN 1. VLAN 1 is reserved for the logical VLAN interface for switch ports. If you upgrade a 1010 to 9.22(1) or later, and you have assigned VLAN 1 to a subinterface, you must first change the VLAN ID for your subinterface to a new VLAN. After upgrading, if present, VLAN 1 will be removed from the subinterface.

9.20 Guidelines

- **Smart licensing default transport changed in 9.20(4)**—In 9.20(4), the smart licensing default transport changed from Smart Call Home to Smart Transport. You can configure the ASA to use Smart Call Home if necessary using the **transport type callhome** command. When you upgrade to 9.20(4), the transport is automatically changed to Smart Transport. If you downgrade, the transport is set back to Smart Call Home, and if you want to use Smart Transport, you need to specify **transport type smart**. Note also that the licensing URL for Smart Transport is https://smartreceiver.cisco.com (compared to tools.cisco.com), so be sure to allow that URL on upstream routers.



Note Ensure your device can connect to the Smart License Authority. For known connectivity issues and workarounds refer to CSCwp10957 and CSCws62173.

- **OSPFv3 redistribute commands that specify a route-map that matches a prefix-list will be removed in 9.20(2)**—When you upgrade to 9.20(2), OSPFv3 **redistribute** commands where the specified **route-map** uses a **match ip address prefix-list** will be removed from the configuration. Although prefix lists have never been supported, the parser still accepted the command. Before upgrading, you should reconfigure OSPFv3 to use route maps that specify an ACL in the **match ip address** command.



Remember Redistribution of route maps with IPv4 prefix list on OSPFv2 is supported.

9.19 Guidelines

- **ASDM 7.19(1) requires Oracle Java version 8u261 or later**—Before you upgrade to ASDM 7.19, be sure to update Oracle Java (if used) to version 8u261 or later. This version supports TLSv1.3, which is required to upgrade the ASDM Launcher. OpenJRE is not affected.

9.18 Guidelines

- **ASDM signed-image support in 9.18(2)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. (CSCwb05291, CSCwb05264)
- **9.18(1) upgrade issue if you enabled HTTPS/ASDM (with HTTPS authentication) and SSL on the same interface with the same port**—If you enable both SSL (**webvpn** > **enable** *interface*) and HTTPS/ASDM (**http**) access on the same interface, you can access AnyConnect from **https://***ip_address* and ASDM from **https://***ip_address***/admin**, both on port 443. However, if you also enable HTTPS authentication (**aaa authentication http console**), then you must specify a different port for ASDM access starting in 9.18(1). Make sure you change the port before you upgrade using the **http** command. (CSCvz92016)
- **ASDM Upgrade Wizard**—Due to ASD API migration, you must use ASDM 7.18 or later to upgrade to ASA 9.18 or later. Because ASDM is backwards compatible with earlier ASA versions, you can upgrade ASDM to 7.18 or later for any ASA version.

9.17 Guidelines

- **ASDM signed-image support in 9.17(1.13)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. (CSCwb05291, CSCwb05264)
- **No support for Clientless SSL VPN in 9.17(1) and later**—Clientless SSL VPN is no longer supported.
  - **webvpn**—The following subcommands are removed:
    - **apcf**
    - **java-trustpoint**
    - **onscreen-keyboard**
    - **port-forward**
    - **portal-access-rule**
    - **rewrite**
    - **smart-tunnel**
  - **group-policy webvpn**—The following subcommands are removed:
    - **port-forward**
    - **smart-tunnel**
    - **ssl-clientless**
- **ASDM Upgrade Wizard**—Due to an internal change, starting in March 2022 the upgrade wizard will no longer work with pre-ASDM 7.17(1.152) versions. You must manually upgrade to 7.17(1.152) to use the wizard.

9.16 Guidelines

- **ASDM signed-image support in 9.16(3.19)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. (CSCwb05291, CSCwb05264)
- **SNMPv3 users using MD5 hashing and DES encryption are no longer supported, and the users will be removed when you upgrade to 9.16(1)**—Be sure to change any user configuration to higher security algorithms using the **snmp-server user** command before you upgrade.
- **SSH host key action required in 9.16(1)**—In addition to RSA, we added support for the EDDSA and ECDSA host keys for SSH. The ASA tries to use keys in the following order if they exist: EDDSA, ECDSA, and then RSA. When you upgrade to 9.16(1), the ASA will fall back to using the existing RSA key. However, we recommend that you generate higher-security keys as soon as possible using the **crypto key generate** {**eddsa** | **ecdsa**} command. Moreover, if you explicitly configure the ASA to use the RSA key with the **ssh key-exchange hostkey rsa** command, you must generate a key that is 2048 bits or

higher. For upgrade compatibility, the ASA will use smaller RSA host keys only when the default host key setting is used. RSA support will be removed in a later release.

- **In 9.16 and later, certificates with RSA keys are not compatible with ECDSA ciphers**—When you use the ECDHE_ECDSA cipher group, configure the trustpoint with a certificate that contains an ECDSA-capable key.
- **ssh version command removed in 9.16(1)**—This command has been removed. Only SSH version 2 is supported.
- **When you upgrade to 9.16 or later, you might see a different certificate serial number**—In 9.16, the ASA started using OpenSSL, which causes negative values in certificates to be computed differently, so you may see a different serial number after upgrading. This change does not affect operation. (CSCvv30338)
- **SAMLv1 feature removed in 9.16(1)**—Support for SAMLv1 was removed.
- **No support for DH groups 2, 5, and 24 in 9.16(1)**—Support has been removed for the DH groups 2, 5, and 24 in SSL DH group configuration. The **ssl dh-group** command has been updated to remove the command options **group2**, **group5**, and **group24**.

Clustering Guidelines

There are no special requirements for Zero Downtime Upgrades for ASA clustering.

Note Zero Downtime *Downgrades* are not officially supported with clustering.

During a software upgrade of ASA cluster, the VPN load-balancing cluster does not form if members run different ASA versions. Perform one of these actions:

- Upgrade all members to the same version. The VPN load-balancing cluster re-forms automatically after all members run the same version. VPN load balancing is unavailable during the mixed-version window.
- For a hitless upgrade, temporarily remove the cluster keys from all members. Keep the interval without cluster keys as short as possible. Upgrade all members and then reconfigure the cluster keys on all members. VPN load balancing remains available during the upgrade.

This requirement applies to: ASA version 9.22.3.26, 9.20.4.49, 9.24.1.26, 9.18.4.94, 9.23.1.47, and 9.16.4.103. In these ASA versions, if you choose option 2, syslog 718089 is logged:

%ASA-1-718089: VPN LB cluster is running without authentication. Configure *cluster key* to secure the cluster.

Cluster encryption and cluster keys secure authentication between VPN load-balancing members and help in protecting the group from denial-of-service (DoS) and spoofing attacks.

Failover Guidelines

There are no special requirements for Zero Downtime Upgrades for failover with the following exceptions:

- Upgrade issue with GTP inspection—There could be some downtime during the upgrade, because the GTP data structures are not replicated to the new node.

FXOS Upgrade Guidelines

Before you upgrade, read the release notes for each FXOS version in your chosen upgrade path. Release notes contain important information about each FXOS release, including new features and changed functionality.

Upgrading may require configuration changes that you must address. For example, new hardware supported in an FXOS release might also require that you update the FXOS firmware.

FXOS release notes are available here: https://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html.

ASA Upgrade Checklist

To plan your upgrade, use this checklist.

1. ASA model (Upgrade Path: ASA Appliances, on page 25): _____

   Current ASA version (Upgrade Path: ASA Appliances, on page 25): _____

2. Check the ASA/ASDM compatibility per model (ASA and ASDM Compatibility Per Model, on page 7).

   Target ASA version: _____

   Target ASDM version: _____

3. Check the upgrade path for the Firepower 2100 in Platform mode (Upgrade Path: ASA on Firepower 2100 in Platform Mode, on page 31). Are there intermediate versions required? Yes _____ No _____

   If yes, intermediate ASA version(s): _____

4. Download the target ASA/ASDM versions (Download ASA Software, on page 42).

Note ASDM is included in the image package for all Firepower and Secure Firewall platforms.

5. Is your ASA model a Firepower 4100 or 9300? Yes _____ No _____

   If yes:

   a. Current FXOS version: _____

   b. Check ASA/Firepower 4100 and 9300 compatibility (Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense, on page 12).

      Target FXOS version: _____

   c. Are there intermediate versions required? Yes _____ No _____

      If yes, intermediate FXOS versions: _____

      Make sure you plan to upgrade the ASA in step with the FXOS upgrades to stay compatible.

      Intermediate ASA versions required to stay compatible during the upgrade:

      _____

d. Download the target and intermediate FXOS version (Download FXOS for the Firepower 4100/9300, on page 49).

   Download the intermediate ASA versions (Download ASA Software, on page 42).

e. Do you use the Radware DefensePro decorator application? Yes _____ No _____

   If yes:

   1. Current DefensePro version: _____
   2. Check ASA/FXOS/DefensePro compatibility (Radware DefensePro Compatibility, on page 20).

      Target DefensePro version: _____
   3. Download the target DefensePro version.

6. Check upgrade guidelines for each operating system.
   - ASA Upgrade Guidelines, on page 1.
   - FXOS guidelines: see the FXOS Release Notes for each intermediate and target version.
7. Back up your configurations. See the configuration guide for each operating system for backup methods.

Compatibility

This section includes tables showing the compatibility between platforms, operating systems, and applications.

ASA and ASDM Compatibility Per Model

The following tables list ASA and ASDM compatibility for current versions and models. For older versions and models, see Cisco ASA Compatibility.

ASA 9.24

Releases in **bold** are the recommended versions.

Note

- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.22(1) can manage an ASA 5516-X on ASA 9.10(1).
- New ASA versions require the coordinating ASDM version or a later version; you cannot use an old version of ASDM with a new version of ASA. For example, you cannot use ASDM 7.23 with ASA 9.24. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.24(1.2) with ASDM 7.24(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.

Table 1: ASA and ASDM Compatibility: 9.24

ASA	ASDM	ASA Model										
		ASA Virtual	Secure Firewall 220	Firepower 1010 1010E 1120 1140 1150	Secure Firewall 1210CE 1210CP 1220CX	Secure Firewall 1230 1240 1250	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Secure Firewall 6160 6170	Firepower 9300	ISA 3000
9.24(1)	7.24(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.24(10)	7.24(10)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

ASA 9.23 and 9.22

Releases in **bold** are the recommended versions.

Note

- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.22(1) can manage an ASA 5516-X on ASA 9.10(1).
- New ASA versions require the coordinating ASDM version or a later version; you cannot use an old version of ASDM with a new version of ASA. For example, you cannot use ASDM 7.20 with ASA 9.22. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.22(1.2) with ASDM 7.22(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.

Table 2: ASA and ASDM Compatibility: 9.23 and 9.22

ASA	ASDM	ASA Model								
		ASA Virtual	Firepower 1010 1010E 1120 1140 1150	Secure Firewall 1210CE 1210CP 1220CX	Secure Firewall 1230 1240 1250	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.23(1)	7.23(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.22(3)	7.22(3)	**YES**	**YES**	**YES**	—	**YES**	**YES**	**YES**	**YES**	**YES**
9.22(2)	7.22(1)	**YES**	**YES**	**YES**	—	**YES**	**YES**	**YES**	**YES**	**YES**

ASA	ASDM	ASA Model								
		ASA Virtual	Firepower 1010 1010E 1120 1140 1150	Secure Firewall 1210CE 1210CP 1220CX	Secure Firewall 1230 1240 1250	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.22(1.1)	7.22(1)	YES	YES	YES	—	YES	YES	YES	YES	YES

ASA 9.20 and 9.19

Note

- ASA 9.20(x) was the final version for the Firepower 2100 series.
- ASA 9.18(x) was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.
- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.19(1) can manage an ASA 5516-X on ASA 9.10(1). See the following exceptions:
  - For the Firepower 1010E, ASDM 7.19(1) is not supported. You must use 7.19(1.90)+ or 7.18(2.1).
- New ASA versions require the coordinating ASDM version or a later version; you cannot use an old version of ASDM with a new version of ASA. For example, you cannot use ASDM 7.18 with ASA 9.19. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.20(1.5) with ASDM 7.20(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.

Table 3: ASA and ASDM Compatibility: 9.20 and 9.19

ASA	ASDM	ASA Model								
		ASA Virtual	Firepower 1010 1120 1140 1150	Firepower 1010E	Firepower 2110 2120 2130 2140	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.20(4)	7.20(4)	YES	YES	YES	YES	YES	YES	YES	YES	YES
9.20(3)	7.20(2)	YES	YES	YES	YES	YES	YES	YES	YES	YES

ASA	ASDM	ASA Model								
		ASA Virtual	Firepower 1010 1120 1140 1150	Firepower 1010E	Firepower 2110 2120 2130 2140	Secure Firewall 3105 3110 3120 3130 3140	Firepower 4112 4115 4125 4145	Secure Firewall 4215 4225 4245	Firepower 9300	ISA 3000
9.20(2)	7.20(2)	YES	YES	YES	YES	YES	YES	YES	YES	YES
9.20(1)	7.20(1)	—	—	—	—	—	—	YES	—	—
9.19(1)	7.19(1)	YES	YES	—	YES	YES	YES	—	YES	YES

ASA 9.18 to 9.17

Note

- ASA 9.16(x) was the final version for the ASA 5506-X, 5506H-X, 5506W-X, 5508-X, and 5516-X.
- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.17(1) can manage an ASA 5516-X on ASA 9.10(1). See the following exceptions:
  - For the Firepower 1010E, ASDM 7.19(1) is not supported. You must use 7.19(1.90)+ or 7.18(2.1).
- New ASA versions require the coordinating ASDM version or a later version; you cannot use an old version of ASDM with a new version of ASA. For example, you cannot use ASDM 7.17 with ASA 9.18. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.17(1.2) with ASDM 7.17(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.
- ASA 9.17(1.13) and 9.18(2) and later requires ASDM 7.18(1.152) or later. The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image than 7.18(1.152) with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. (CSCwb05291, CSCwb05264)

Table 4: ASA and ASDM Compatibility: 9.18 to 9.17

ASA	ASDM	ASA Model							
		ASA Virtual	Firepower 1010 1120 1140 1150	Firepower 1010E	Firepower 2110 2120 2130 2140	Secure Firewall 3110 3120 3130 3140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.18(4)	7.19(1)95	YES	YES	YES	YES	YES	YES	YES	YES
9.18(3)	7.18(1.152)	YES	YES	YES	YES	YES	YES	YES	YES
9.18(2.218)	7.18(2.1)	—	—	YES	—	—	—	—	—
9.18(2)	7.18(1.152)	YES	YES	—	YES	YES	YES	YES	YES
9.18(1)	7.18(1)	YES	YES	—	YES	YES	YES	YES	YES
9.17(1.13)	7.18(1.152)	YES	YES	—	YES	YES	YES	YES	YES
9.17(1)	7.17(1.155)	YES	YES	—	YES	YES	YES	YES	YES

ASA 9.16

Note

- ASA 9.16(x) was the final version for the ASA 5506-X, 5506H-X, 5506W-X, 5508-X, and 5516-X.
- ASA 9.14(x) was the final version for the ASA 5525-X, 5545-X, and 5555-X.
- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.15(1) can manage an ASA 5516-X on ASA 9.10(1).
- New ASA versions require the coordinating ASDM version or a later version; you cannot use an old version of ASDM with a new version of ASA. For example, you cannot use ASDM 7.15 with ASA 9.16. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.16(1.15) with ASDM 7.16(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.
- ASA 9.16(3.19) and later requires ASDM 7.18(1.152) or later. The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image than 7.18(1.152) with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. (CSCwb05291, CSCwb05264)

Table 5: ASA and ASDM Compatibility: 9.16

ASA	ASDM	ASA Model						
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASAv	Firepower 1010 1120 1140 1150	Firepower 2110 2120 2130 2140	Firepower 4110 4112 4115 4120 4125 4140 4145 4150	Firepower 9300	ISA 3000
9.16(4)	7.18(1.152)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.16(3.19)	7.18(1.152)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.16(3)	7.16(1.150)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.16(2)	7.16(1.150)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.16(1)	7.16(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense

For the Firepower 4100/9300, you must maintain compatibility between FXOS and all ASA and Firewall Threat Defense logical devices. Upgrade FXOS before you upgrade the software. The **bold** versions in the following table are specially-qualified (enhanced testing) companion releases. Use these combinations whenever possible.

Note In most cases we recommend the latest FXOS build for each version. For Firewall Threat Defense minimum builds, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.

For device models other than the Firepower 4100/9300, the FXOS compatibility work is done for you. In most cases, upgrading the software automatically upgrades FXOS. For the Secure Firewall 3100/4200 in multi-instance mode, the Firewall Management Center guides you through upgrading FXOS and then Firewall Threat Defense.

To upgrade:

- FXOS: From FXOS 2.2.2 and later, you can upgrade directly to any higher version. (FXOS 2.0.1–2.2.1 can upgrade as far as 2.8.1. For versions earlier than 2.0.1, you need to upgrade to each intermediate version.) Note that you cannot upgrade FXOS to a version that does not support your current logical device version. You will need to upgrade in steps: upgrade FXOS to the highest version that supports your current logical device; then upgrade your logical device to the highest version supported with that

FXOS version. For example, if you want to upgrade from FXOS 2.2/ASA 9.8 to FXOS 2.13/ASA 9.19, you would have to perform the following upgrades:

1. FXOS 2.2 → FXOS 2.11 (the highest version that supports 9.8)
2. ASA 9.8 → ASA 9.17 (the highest version supported by 2.11)
3. FXOS 2.11 → FXOS 2.13
4. ASA 9.17 → ASA 9.19

- Firewall Threat Defense: Interim upgrades may be required for Firewall Threat Defense, in addition to the FXOS requirements above. For the exact upgrade path, refer to the Firewall Management Center upgrade guide for your version.
- ASA: ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

Note FXOS 2.8(1.125)+ and later versions do not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases, such as 9.13 or 9.12, are not affected.

Table 6: Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.18.10	Firepower 4112	**9.24.10** (recommended) 9.24.1 9.23 9.22 9.20 9.19	**10.1** (recommended) 10.0 7.7 7.6 7.4 7.3
	Firepower 4145 Firepower 4125 Firepower 4115	**9.24.10** (recommended) 9.24.1 9.23 9.22 9.20 9.19	**10.1** (recommended) 10.0 7.7 7.6 7.4 7.3
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.18.0	Firepower 4112	**9.24.1** (recommended) 9.23 9.22 9.20 9.19	**10.0** (recommended) 7.7 7.6 7.4 7.3
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.24.1** (recommended) 9.23 9.22 9.20 9.19	**10.0** (recommended) 7.7 7.6 7.4 7.3
2.17	Firepower 4112	**9.23** (recommended) 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.23** (recommended) 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.16	Firepower 4112	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.14(1)	Firepower 4112	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.13	Firepower 4112	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.12	Firepower 4112	**9.18** (recommended) 9.17 9.16 9.14	**7.2** (recommended) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.11	Firepower 4112	**9.17** (recommended) 9.16 9.14	**7.1** (recommended) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommended) 9.16 9.14 9.12	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommended) 9.16 9.14 9.12 9.8	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Note** For compatibility with 7.0.2+ and 9.16(3.11)+, you need FXOS 2.10(1.179)+.	Firepower 4112	**9.16** (recommended) 9.14	**7.0** (recommended) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommended) 9.14 9.12	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommended) 9.14 9.12 9.8	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.8	Firepower 4112	**9.14**	**6.6** **Note** 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommended) 9.12 **Note** Firepower 9300 SM-56 requires ASA 9.12(2)+	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommended) 9.12 9.8	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.6(1.157) **Note** You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Note** Firepower 9300 SM-56 requires ASA 9.12.2+	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	**6.4** (recommended) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Not supported
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	**6.2.3** (recommended) **Note** 6.2.3.16+ requires FXOS 2.3.1.157+
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Firewall Threat Defense versions are EoL
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Radware DefensePro Compatibility

The following table lists the supported Radware DefensePro version for each security appliance and associated logical device.

Note Radware DefensePro 8.22.2 is the final version of Radware DefensePro that is supported on the Firepower 4100/9300 platforms. Firepower 4100/9300 platforms do not support any version later than 8.22.2.

Table 7: Radware DefensePro Compatibility

FXOS Version	ASA	Firewall Threat Defense	Radware DefensePro	Security Appliance Models
2.17	923(1)	7.7	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145

FXOS Version	ASA	Firewall Threat Defense	Radware DefensePro	Security Appliance Models
2.16	9.22(1)	7.6	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.14(1)	9.20(1)	7.4(1)	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.13.0	9.19(1)	7.3	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4112 Firepower 4115 Firepower 4125 Firepower 4145
2.12.0	9.18(1)	7.2	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS Version	ASA	Firewall Threat Defense	Radware DefensePro	Security Appliance Models
2.11.1	9.17(1)	7.1	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS Version	ASA	Firewall Threat Defense	Radware DefensePro	Security Appliance Models
2.9.1	9.15(1)	6.7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.8.1	9.14(1)	6.6.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS Version	ASA	Firewall Threat Defense	Radware DefensePro	Security Appliance Models
2.6(1)	9.12(1) 9.10(1)	6.4.0 6.3.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.4(1)	9.9(2) 9.10(1)	6.2.3 6.3	8.13.01.09-2	Firepower 9300 Firepower 4110 Firepower 4120 Firepower 4140 Firepower 4150
2.3(1)	9.9(1) 9.9(2)	6.2.2 6.2.3	8.13.01.09-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense only) Firepower 4120 Firepower 4140 Firepower 4150
2.2(2)	9.8(1) 9.8(2) 9.8(3)	6.2.0 6.2.2	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense only) Firepower 4120 Firepower 4140 Firepower 4150
2.2(1)	9.7(1) 9.8(1)	6.2.0	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense only) Firepower 4120 Firepower 4140 Firepower 4150

FXOS Version	ASA	Firewall Threat Defense	Radware DefensePro	Security Appliance Models
2.1(1)	9.6(2) 9.6(3) 9.6(4) 9.7(1)	not supported	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
2.0(1)	9.6(1) 9.6(2) 9.6(3) 9.6(4)	not supported	8.10.01.16-5	Firepower 9300 Firepower 4120 Firepower 4140 Firepower 4150
1.1(4)	9.6(1)	not supported	1.1(2.32-3)	9300

Upgrade Path

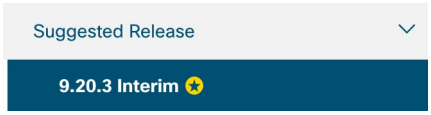
For each operating system that you are upgrading, check the supported upgrade path. In some cases, you may have to install interim upgrades before you can upgrade to your final version.

Upgrade Path: ASA Appliances

What Version Should I Upgrade To?

On the Cisco Support & Download site, the suggested release is marked with a gold star. For example:

Figure 1: Suggested Release



View Your Current Version

To view your current version and model, use one of the following methods:

- ASDM: Choose **Home** > **Device Dashboard** > **Device Information**.
- CLI: Use the **show version** command.

Upgrade Guidelines

Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage. See ASA Upgrade Guidelines, on page 1.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Upgrade Paths

This table provides upgrade paths for ASA.

Note ASA 9.20 was the final version for the Firepower 2100.

ASA 9.18 was the final version for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300.

ASA 9.16 was the final version for the ASA 5506-X, 5508-X, and 5516-X.

ASA 9.14 was the final version for the ASA 5525-X, 5545-X, and 5555-X.

ASA 9.12 was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.

ASA 9.2 was the final version for the ASA 5505.

ASA 9.1 was the final version for the ASA 5510, 5520, 5540, 5550, and 5580.

Table 8: Upgrade Path

Current Version	Interim Upgrade Version	Target Version
9.23	—	Any of the following: → 9.24
9.22	—	Any of the following: → 9.24 → 9.23
9.20	—	Any of the following: → 9.24 → 9.23 → 9.22
9.19	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20

Current Version	Interim Upgrade Version	Target Version
9.18	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19
9.17	—	Any of the following: → 9.24 → 9.22 → 9.20 → 9.19 → 9.18
9.16	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17
9.15	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

Current Version	Interim Upgrade Version	Target Version
9.14	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.13	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.12	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

Current Version	Interim Upgrade Version	Target Version
9.10	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.9	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.8	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

Current Version	Interim Upgrade Version	Target Version
9.7	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.6	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.5	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

Current Version	Interim Upgrade Version	Target Version
9.4	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.3	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16
9.2	—	Any of the following: → 9.24 → 9.23 → 9.22 → 9.20 → 9.19 → 9.18 → 9.17 → 9.16

Upgrade Path: ASA on Firepower 2100 in Platform Mode

To view your current version and model, use one of the following methods:

- ASDM: Choose **Home** > **Device Dashboard** > **Device Information**.
- CLI: Use the **show version** command.

This table provides upgrade paths for the ASA on the Firepower 2100 in Platform mode. Some versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

Be sure to check the upgrade guidelines for each release between your starting version and your ending version. You may need to change your configuration before upgrading in some cases, or else you could experience an outage. See ASA Upgrade Guidelines, on page 1.

For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the ASA Security Advisories.

Note ASA 9.20 was the final version for the Firepower 2100.

Table 9: Upgrade Path

Current Version	Interim Upgrade Version	Target Version
9.19	—	Any of the following: → **9.20**
9.18	—	Any of the following: → **9.20** → **9.19**
9.17	—	Any of the following: → **9.20** → **9.19** → **9.18**
9.16	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17

Current Version	Interim Upgrade Version	Target Version
9.15	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.14	—	Any of the following: → **9.20** → **9.19** → **9.18** → 9.17 → **9.16**
9.13	→ 9.18	Any of the following: → **9.20** → **9.19**
9.13	—	Any of the following: → **9.18** → 9.17 → **9.16**
9.12	→ 9.18	Any of the following: → **9.20** → **9.19**
9.12	—	Any of the following: → **9.18** → 9.17 → **9.16**
9.10	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**

Current Version	Interim Upgrade Version	Target Version
9.10	—	Any of the following: → 9.17 → **9.16**
9.9	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**
9.9	—	Any of the following: → 9.17 → **9.16**
9.8	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**
9.8	—	Any of the following: → 9.17 → **9.16**

Upgrade Path: ASA Logical Devices for the Firepower 4100/9300

To view your current version and model, use one of the following methods:

- Firepower Chassis Manager: Choose **Overview**, and look at the **Model** and **Version** fields at the top.
- CLI: For the version, use the **show version** command, and look at the Package-Vers: field. For the model, enter **scope chassis 1**, and then **show inventory**.
- FXOS: From FXOS 2.2.2 and later, you can upgrade directly to any higher version. (FXOS 2.0.1–2.2.1 can upgrade as far as 2.8.1. For versions earlier than 2.0.1, you need to upgrade to each intermediate version.) Note that you cannot upgrade FXOS to a version that does not support your current logical device version. You will need to upgrade in steps: upgrade FXOS to the highest version that supports your current logical device; then upgrade your logical device to the highest version supported with that FXOS version. For example, if you want to upgrade from FXOS 2.2/ASA 9.8 to FXOS 2.13/ASA 9.19, you would have to perform the following upgrades:

  1. FXOS 2.2 → FXOS 2.11 (the highest version that supports 9.8)
  2. ASA 9.8 → ASA 9.17 (the highest version supported by 2.11)

3. FXOS 2.11 → FXOS 2.13
4. ASA 9.17 → ASA 9.19

- Firewall Threat Defense: Interim upgrades may be required for Firewall Threat Defense, in addition to the FXOS requirements above. For the exact upgrade path, refer to the Firewall Management Center upgrade guide for your version.
- ASA: ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

Table 10: Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.18.10	Firepower 4112	**9.24.10** (recommended) 9.24.1 9.23 9.22 9.20 9.19	**10.1** (recommended) 10.0 7.7 7.6 7.4 7.3
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.24.10** (recommended) 9.24.1 9.23 9.22 9.20 9.19	**10.1** (recommended) 10.0 7.7 7.6 7.4 7.3
2.18.0	Firepower 4112	**9.24.1** (recommended) 9.23 9.22 9.20 9.19	**10.0** (recommended) 7.7 7.6 7.4 7.3
	Firepower 4145 Firepower 4125 Firepower 4115 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.24.1** (recommended) 9.23 9.22 9.20 9.19	**10.0** (recommended) 7.7 7.6 7.4 7.3

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.17	Firepower 4112	**9.23** (recommended) 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
	Firepower 4145 Firepower 4125 Firepower 4115	**9.23** (recommended) 9.22 9.20 9.19 9.18	**7.7** (recommended) 7.6 7.4 7.3 7.2
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.16	Firepower 4112	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 4145 Firepower 4125 Firepower 4115	**9.22** (recommended) 9.20 9.19 9.18 9.17	**7.6** (recommended) 7.4 7.3 7.2 7.1
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.14(1)	Firepower 4112	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.20** (recommended) 9.19 9.18 9.17 9.16 9.14	**7.4** (recommended) 7.3 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
2.13	Firepower 4112	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.12	Firepower 4112	**9.18** (recommended) 9.17 9.16 9.14	**7.2** (recommended) 7.1 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.18** (recommended) 9.17 9.16 9.14 9.12	**7.2** (recommended) 7.1 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.11	Firepower 4112	**9.17** (recommended) 9.16 9.14	**7.1** (recommended) 7.0 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.17** (recommended) 9.16 9.14 9.12	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.17** (recommended) 9.16 9.14 9.12 9.8	**7.1** (recommended) 7.0 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.10 **Note** For compatibility with 7.0.2+ and 9.16(3.11)+, you need FXOS 2.10(1.179)+.	Firepower 4112	**9.16** (recommended) 9.14	**7.0** (recommended) 6.6
	Firepower 4145 Firepower 4125 Firepower 4115	**9.16** (recommended) 9.14 9.12	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.16** (recommended) 9.14 9.12 9.8	**7.0** (recommended) 6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.9	Firepower 4112	9.14	6.6
	Firepower 4145 Firepower 4125 Firepower 4115	9.14 9.12	6.6 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14 9.12 9.8	6.6 6.4
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.8	Firepower 4112	**9.14**	**6.6** **Note** 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4145 Firepower 4125 Firepower 4115	**9.14** (recommended) 9.12 **Note** Firepower 9300 SM-56 requires ASA 9.12(2)+	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.14** (recommended) 9.12 9.8	**6.6** (recommended) **Note** 6.6.1+ requires FXOS 2.8(1.125)+. 6.4 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.6(1.157) **Note** You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis	Firepower 4145 Firepower 4125 Firepower 4115	**9.12** **Note** Firepower 9300 SM-56 requires ASA 9.12.2+	**6.4**
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40		
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	**6.4** (recommended) 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.6(1.131)	Firepower 9300 SM-48 Firepower 9300 SM-40	**9.12**	Not supported
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.12** (recommended) 9.8	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.3(1.73)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	**6.2.3** (recommended) **Note** 6.2.3.16+ requires FXOS 2.3.1.157+
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

FXOS Version	Model	ASA Version	Firewall Threat Defense Version
2.3(1.66) 2.3(1.58)	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.8 **Note** 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	**9.8**	Firewall Threat Defense versions are EoL
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

Download the Software from Cisco.com

Download all software packages from Cisco.com before you start your upgrade. Depending on the operating system and whether you are using CLI or GUI, you should place the images on a server or on your management computer. See each installation procedure for details on supported file locations.

Note A Cisco.com login and Cisco service contract are required.

Download ASA Software

ASA software can be downloaded from Cisco.com. These tables include naming conventions and information about ASA packages.

- If you are using the ASDM Upgrade Wizard, you do not have to pre-download the software. If you are manually upgrading, for example for a failover upgrade, download the images to your local computer.

- For a CLI upgrade, you can put the software on many server types, including TFTP, HTTP, and FTP. See the **copy** command in the ASA command reference.
- For either CLI or ASDM, if your device has a USB port, you can download images onto a USB type A storage device that is formatted for FAT-32. You can then copy or select the file from the drive. When you insert the drive, it is referred to as **disk1**.



Note When you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA because they have the same name (**asdm.bin**). But if you manually chose a different ASDM image that you uploaded (for example, **asdm-7131.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should either upgrade ASDM before you upgrade the bundle, or you should reconfigure the ASA to use the bundled ASDM image (**asdm.bin**) just before upgrading the ASA bundle.

Table 11: Current Platforms

ASA Model	Download Location	Packages
ASA virtual	http://www.cisco.com/go/asav-software	
	ASA Software (Upgrade) Choose **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA virtual upgrade file has a filename like asa962-**smp-k8.bin**; use this upgrade file for all hypervisors. **Note:** The .zip (VMware), .vhdx (Hyper-V), and .qcow2 (KVM) files are only for initial deployment. **Note** To upgrade the ASA virtual for public cloud services such as Amazon Web Services, you can download the above image from Cisco.com (which requires a Cisco.com login and Cisco service contract) and perform the upgrade as described in this guide. There is no way to obtain an *upgrade* image from the public cloud service.
	ASDM Software (Upgrade) Choose **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide.
	ASA Device Package for Cisco Application Policy Infrastructure Controller (APIC) Choose **ASA for Application Centric Infrastructure (ACI) Device Packages** > *version*.	For APIC 1.2(7) and later, choose either the Policy Orchestration with Fabric Insertion, or the Fabric Insertion-only package. The device package software file has a filename like asa-device-pkg-1.2.7.10**.zip**. To install the ASA device package, see the "Importing a Device Package" chapter of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.
Secure Firewall 200	See: https://www.cisco.com/go/asa-firepower-sw	
	ASA package Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The package has a filename like cisco-asa-csf200.9.24.1.**SPA**. This package includes ASA and ASDM.
	ASDM software (upgrade) To upgrade to a later version of ASDM using your current ASDM or the ASA CLI, choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-7241.**bin** for Oracle Java and asdm-openjre-7241.**bin** for OpenJRE.

ASA Model	Download Location	Packages
Firepower 1000	http://www.cisco.com/go/asa-firepower-sw	
	ASA, ASDM, and FXOS Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes ASA, ASDM, and FXOS software. The ASA package has a filename like cisco-asa-fp1k.9.13.1**.SPA**.
	ASDM Software (Upgrade) Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-7131**.bin**.
Secure Firewall 1200	http://www.cisco.com/go/asa-firepower-sw	
	ASA, ASDM, and FXOS Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes ASA, ASDM, and FXOS software. The ASA package has a filename like cisco-asa-csf1200.9.22.1.3**.SPA**.
	ASDM Software (Upgrade) Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-7221**.bin**.
Secure Firewall 3100	https://cisco.com/go/asa-secure-firewall-sw	
	ASA, ASDM, and FXOS Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes ASA, ASDM, and FXOS software. The ASA package has a filename like cisco-asa-fp3k.9.17.1**.SPA**.
	ASDM Software (Upgrade) Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-7171**.bin**.
Firepower 4100	http://www.cisco.com/go/firepower4100-software	
	ASA and ASDM Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes both ASA and ASDM. The ASA package has a filename like cisco-asa.9.6.2**.SPA.csp**.
	ASDM Software (Upgrade) Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide.

ASA Model	Download Location	Packages
Secure Firewall 4200	https://cisco.com/go/asa-secure-firewall-sw	
	ASA, ASDM, and FXOS Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes ASA, ASDM, and FXOS software. The ASA package has a filename like cisco-asa-fp4200.9.20.1**.SPA**.
	ASDM Software (Upgrade) Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-7201**.bin**.
Secure Firewall 6100	See: https://cisco.com/go/asa-secure-firewall-sw	
	ASA package Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The package has a filename like cisco-asa-fp6100.9.24.1.**SPA**. This package includes ASA and ASDM.
	ASDM software (upgrade) To upgrade to a later version of ASDM using your current ASDM or the ASA CLI, choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-7241.**bin** for Oracle Java and asdm-openjre-7241.**bin** for OpenJRE.
Firepower 9300	http://www.cisco.com/go/firepower9300-software	
	ASA and ASDM Software Choose **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes both ASA and ASDM. The ASA package has a filename like cisco-asa.9.6.2**.SPA.csp**.
	ASDM Software (Upgrade) Choose **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide.

ASA Model	Download Location	Packages
ISA 3000	http://www.cisco.com/go/isa3000-software	
	ASA Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**lfbff-k8.SPA**.
	ASDM Software Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide.

Table 12: Legacy Platforms

ASA Model	Download Location	Packages
ASA 5506-X, ASA 5508-X, and ASA 5516-X	http://www.cisco.com/go/asa-firepower-sw	
	ASA Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**lfbff-k8.SPA**.
	ASDM Software Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide
	ROMMON Software Choose your *model* > **ASA Rommon Software** > *version*.	The ROMMON software file has a filename like asa5500-firmware-1108**.SPA**.

ASA Model	Download Location	Packages
ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X	http://www.cisco.com/go/asa-software	
	ASA Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**smp-k8.bin**.
	ASDM Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide
	ASA Device Package for Cisco Application Policy Infrastructure Controller (APIC) Choose your *model* > **Software on Chassis** > **ASA for Application Centric Infrastructure (ACI) Device Packages** > *version*.	For APIC 1.2(7) and later, choose either the Policy Orchestration with Fabric Insertion, or the Fabric Insertion-only package. The device package software file has a filename like asa-device-pkg-1.2.7.10**.zip**. To install the ASA device package, see the "Importing a Device Package" chapter of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.

ASA Model	Download Location	Packages
ASA 5585-X	http://www.cisco.com/go/asa-software	
	ASA Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA software file has a filename like asa962-**smp-k8.bin**.
	ASDM Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.
	REST API Software Choose your *model* > **Software on Chassis** > **Adaptive Security Appliance REST API Plugin** > *version*.	The API software file has a filename like asa-restapi-132-**lfbff-k8.SPA**. To install the REST API, see the API quick start guide.
	ASA Device Package for Cisco Application Policy Infrastructure Controller (APIC) Choose your *model* > **Software on Chassis** > **ASA for Application Centric Infrastructure (ACI) Device Packages** > *version*.	For APIC 1.2(7) and later, choose either the Policy Orchestration with Fabric Insertion, or the Fabric Insertion-only package. The device package software file has a filename like asa-device-pkg-1.2.7.10**.zip**. To install the ASA device package, see the "Importing a Device Package" chapter of the Cisco APIC Layer 4 to Layer 7 Services Deployment Guide.
Firepower 2100	http://www.cisco.com/go/asa-firepower-sw	
	ASA, ASDM, and FXOS Software Choose your *model* > **Adaptive Security Appliance (ASA) Software** > *version*.	The ASA package includes ASA, ASDM, and FXOS software. The ASA package has a filename like cisco-asa-fp2k.9.8.2**.SPA**.
	ASDM Software (Upgrade) Choose your *model* > **Adaptive Security Appliance (ASA) Device Manager** > *version*.	Use this image to upgrade to a later version of ASDM using your current ASDM or the ASA CLI. The ASDM software file has a filename like asdm-782**.bin**.

Download FXOS for the Firepower 4100/9300

FXOS packages for the Firepower 4100/9300 are available on the Cisco Support & Download site.

- Firepower 4100 series: http://www.cisco.com/go/firepower4100-software
- Firepower 9300: http://www.cisco.com/go/firepower9300-software

To find FXOS packages, select or search for your Firepower appliance model, then browse to the Firepower Extensible Operating System download page for the target version.

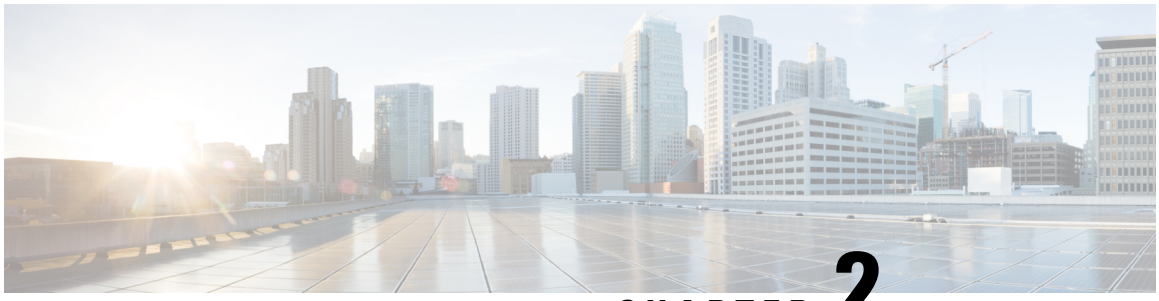
Note If you plan to use the CLI to upgrade FXOS, copy the upgrade package to a server that the Firepower 4100/9300 can access using SCP, SFTP, TFTP, or FTP.

Table 13: FXOS Packages for the Firepower 4100/9300

Package Type	Package
FXOS image	fxos-k9.*version*.**SPA**
Recovery (kickstart)	fxos-k9-**kickstart**.*version*.**SPA**
Recovery (manager)	fxos-k9-**manager**.*version*.**SPA**
Recovery (system)	fxos-k9-**system**.*version*.**SPA**
MIBs	fxos-**mibs**-fp9k-fp4k.*version*.**zip**
Firmware: Firepower 4100 series	fxos-k9-fpr4k-**firmware**.*version*.**SPA**
Firmware: Firepower 9300	fxos-k9-fpr9k-**firmware**.*version*.**SPA**

Back Up Your Configurations

We recommend that you back up your configurations and other critical files before you upgrade, especially if there is a configuration migration. Each operating system has a different method to perform backups. Check the ASA, ASDM, and FXOS configuration guides for more information.



CHAPTER 2

Upgrade the ASA

Upgrade the ASA according to the procedures in this document.

- Upgrade the ASA Appliance, on page 51
- Upgrade the Firepower 4100/9300, on page 71
- Upgrade the ASA Virtual, ISA 3000, or ASA 5500-X, on page 104
- Upgrade the Firepower 2100 in Platform Mode, on page 126

Upgrade the ASA Appliance

This document describes how to plan and implement an ASA, FXOS, and ASDM upgrade for standalone, failover, or clustering deployments on the following models:

- Secure Firewall 200
- Firepower 1000
- Secure Firewall 1200
- Firepower 2100 Appliance mode
- Secure Firewall 3100
- Secure Firewall 4200
- Secure Firewall 6100

For the Firepower 2100 in 9.12 and earlier, only Platform mode is available. In 9.13 and later, Appliance mode is the default. Check the mode by using the **show fxos mode** command at the ASA CLI.

Upgrade a Standalone Unit

Use the CLI or ASDM to upgrade the standalone unit.

Upgrade a Standalone Unit Using the CLI

This section describes how to install the ASDM and ASA images on the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100.

Before you begin

This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Alternatively, if your device includes a USB port, you can download the software image to a USB type A storage device formatted for FAT-32, and insert it into the port. You can then copy from the disk using **copy disk1:***/path_and_filename* **disk0:***/path_and_filename*.

Procedure

Step 1 In global configuration mode, if you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

asdm image disk0:/asdm.bin

write memory

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

Step 2 In privileged EXEC mode (minimum), copy the ASA software to flash memory.

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
ciscoasa# copy https://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Step 3 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Step 4 Show the current boot image configured, if present.

show running-config boot system

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the image from ROMMON, have a new device, or you removed the command manually.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Step 5 If you have a **boot system** command configured, remove it so that you can enter the new boot image.

no boot system disk*n*:/[*path*/]*asa_image_name*

If you did not have a **boot system** command configured, skip this step.

Example:

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Step 6 Set the ASA image to boot (the one you just uploaded).

boot system disk*n*:/[*path*/]*asa_image_name*

You can only enter a single **boot system** command. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA. If you change your mind prior to reloading, you can enter the **no boot system** command to delete the new image from the boot location, so the current image continues to run.

Example:

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

Step 7 Save the new settings to the startup configuration:

write memory

Step 8 Reload the ASA:

reload

Upgrade a Standalone Unit from Your Local Computer Using ASDM

The **Upgrade Software from Local Computer** tool lets you upload an image file from your computer to the flash file system to upgrade the ASA for the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100.

Procedure

Step 1 If you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) In the main ASDM application window, choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
b) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.
c) Click **Apply**.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

Step 3 From the **Image to Upload** drop-down list, choose **ASA**.

Step 4 In the **Local File Path** field, click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**.

The uploading process might take a few minutes.

Step 7 You are prompted to set this image as the ASA image. Click **Yes**.

Step 8 You are reminded to reload the ASA to use the new image. Click **OK**.

You exit the **Upgrade** tool.

Step 9 Choose **Tools** > **System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload.

a) Click the **Save the running configuration at the time of reload** radio button (the default).
b) Choose a time to reload (for example, **Now**, the default).
c) Click **Schedule Reload**.

Once the reload is in progress, a **Reload Status** window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard

The **Upgrade Software from Cisco.com Wizard** lets you automatically upgrade the ASDM and ASA to more current versions for the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.

Note ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 9.9(1), the download might be 9.9(1.2). This behavior is expected, so you can proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, reload the ASA to save the configuration and complete the upgrade.

Before you begin

For a successful certificate validation during an upgrade, ensure that you download all certificates:

1. Choose **Configuration** > **Device Management** > **System Image/Configuration** > **Certificate Settings**.
2. From the **Select the URLs** drop-down list, select each URL, and click **Retrieve Certificates**.
3. Accept each certificate when prompted.
4. Repeat the process until all certificates listed in the drop-down list are downloaded and displayed in the **Certificates** table.

Procedure

Step 1 Choose **Tools** > **Check for ASA/ASDM Updates**.

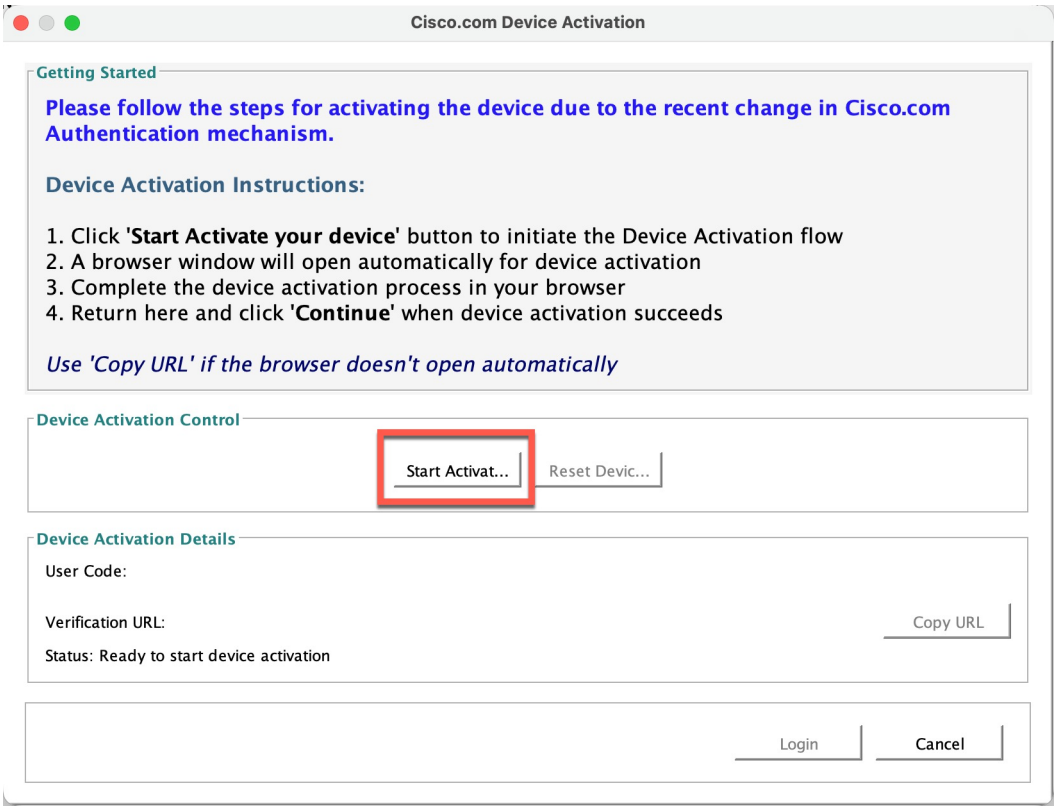
In multiple context mode, access this menu from the System.

The **Cisco.com Device Activation** dialog box appears.

Note
In ASDM 7.23 and earlier, the Cisco.com login is slightly different.

Step 2 Click **Start Activate your device** to open a browser window where you can activate the ASA on your Cisco.com account. Return to ASDM and click **Continue**.

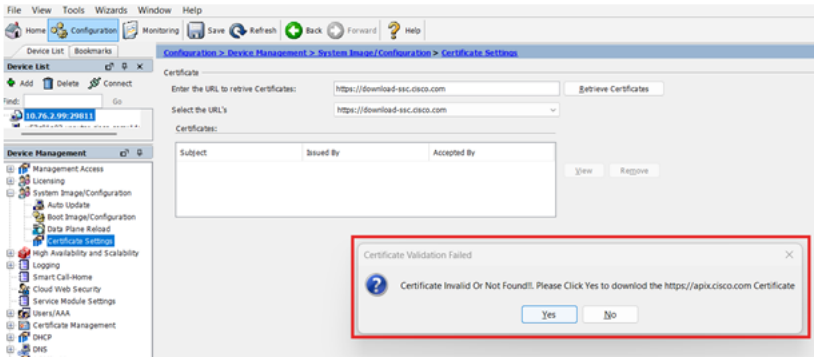
Figure 2: Device Activation



If the browser window did not open, you can manually copy the activation URL using the **Copy URL** button. You can then open a browser and paste in the URL to activate the ASA.

After you activate the ASA, the **Cisco.com Upgrade Wizard** appears.

The **Certificate Validation Failed** error message may appear as follows:



In such cases, go to **Configuration** > **Device Management** > **System Image/Configuration** > **Certificate Settings** and download all the certificates.

Note
If there is no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

Step 3 Click **Next** to display the **Select Software** screen.

The current ASA version and ASDM version appear.

Step 4 To upgrade the ASA version and ASDM version, perform the following steps:

a) In the **ASA** area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.

b) In the **ASDM** area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.

Step 5 Click **Next** to display the **Review Changes** screen.

Step 6 Verify the following items:

- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
- The ASA image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASA boot image has been selected.

Step 7 Click **Next** to start the upgrade installation.

You can then view the status of the upgrade installation as it progresses.

The **Results** screen appears, which provides additional details, such as the upgrade installation status (success or failure).

Step 8 If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.

Step 9 Click **Finish** to exit the wizard and save the configuration changes that you have made.

Note
To upgrade to the next higher version, if any, you must restart the wizard.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Upgrade an Active/Standby Failover Pair

Use the CLI or ASDM to upgrade the Active/Standby failover pair for a zero downtime upgrade.



Note A zero downtime upgrade is guaranteed only for active data traffic forwarding through the failover pair, and does not assure uninterrupted management-plane (SSH/ASDM) access.

When the inside interface is configured as a data interface and also as the management interface (shared management/data interface), it can result in SSH packet loss and a brief ARP resolution delays on adjacent switches during the reload/failover phase.

Upgrade an Active/Standby Failover Pair Using the CLI

To upgrade the Active/Standby failover pair for the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100, perform the following steps.

Before you begin

- Perform these steps on the active unit. For SSH access, connect to the active IP address; the active unit always owns this IP address. When you connect to the CLI, determine the failover status by looking at the ASA prompt; you can configure the ASA prompt to show the failover status and priority (primary or secondary), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show failover** command to view this unit's status and priority (primary or secondary).
- This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.
- Alternatively, if your device includes a USB port, you can download the software image to a USB type A storage device formatted for FAT-32, and insert it into the port. You can then copy from the disk using **copy disk1:***/path_and_filename* **disk0:***/path_and_filename*.

Procedure

Step 1 On the primary unit in global configuration mode, if you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

asdm image disk0:/asdm.bin

write memory

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

Step 2 On the active unit in privileged EXEC mode (minimum), copy the ASA software to the active unit flash memory:

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act# copy https://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Step 3 Copy the software to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Step 4 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 5 Show the current boot image configured, if present.

show running-config boot system

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the image from ROMMON, have a new device, or you removed the command manually.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Step 6 If you have a **boot system** command configured, remove it so that you can enter the new boot image.

no boot system disk*n***:/**[*path*/]*asa_image_name*

If you did not have a **boot system** command configured, skip this step.

Example:

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Step 7 Set the ASA image to boot (the one you just uploaded).

boot system disk*n***:/**[*path*/]*asa_image_name*

You can only enter a single **boot system** command. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA. If you change your mind prior to reloading, you can enter the **no boot system** command to delete the new image from the boot location, so the current image continues to run.

Example:

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
```

```
Install_status: update-software-pack-completed
ciscoasa(config)#
```

Step 8 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the standby unit.

Step 9 Reload the standby unit to boot the new image:

failover reload-standby

Wait for the standby unit to finish loading. Use the **show failover** command to verify that the standby unit is in the Standby Ready state.

Note
If you are connected to the standby unit's console port, you may see a prompt on the standby unit after it reloads; however, it can take several minutes to get to the Standby Ready state, during which the standby unit will have failover disabled. Be patient and wait for the Standby Ready state.

Step 10 Force the active unit to fail over to the standby unit.

no failover active

If you are disconnected from your SSH session, reconnect to the main IP address, now on the new active/former standby unit.

Step 11 From the new active unit, reload the former active unit (now the new standby unit).

failover reload-standby

Example:

```
asa/act# failover reload-standby
```

Note
If you are connected to the former active unit console port, you should instead enter the **reload** command to reload the former active unit.

Upgrade an Active/Standby Failover Pair Using ASDM

The **Upgrade Software from Local Computer** tool lets you upload an image file from your computer to the flash file system to upgrade the Active/Standby failover pair for the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100.

Procedure

Step 1 Launch ASDM on the *standby* unit by connecting to the standby IP address.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASA**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 7 Connect ASDM to the *active* unit by connecting to the main IP address.

Step 8 If you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) Choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
b) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.
c) Click **Apply**.

Step 9 Upload the ASA software, using the same file location you used on the standby unit.

Step 10 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 11 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the standby unit.

Step 12 Reload the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the standby unit reloads.

Step 13 After the standby unit reloads, force the active unit to fail over to the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Standby**.

ASDM will automatically reconnect to the new active unit.

Step 14 Reload the (new) standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Upgrade an Active/Active Failover Pair

Use the CLI or ASDM to upgrade the Active/Active failover pair for a zero downtime upgrade.

Upgrade an Active/Active Failover Pair Using the CLI

To upgrade two units in an Active/Active failover configuration, perform the following steps on the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100.

Before you begin

- Perform these steps on the primary unit.
- Perform these steps in the system execution space.
- This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.
- Alternatively, if your device includes a USB port, you can download the software image to a USB type A storage device formatted for FAT-32, and insert it into the port. You can then copy from the disk using **copy disk1:***/path_and_filename* **disk0:***/path_and_filename*.

Procedure

Step 1 On the primary unit in global configuration mode, if you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

asdm image disk0:/asdm.bin

write memory

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

Step 2 On the primary unit in privileged EXEC mode (minimum), copy the ASA software to flash memory:

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Note
ASDM is included in the ASA image.

Example:

```
asa/act/pri# copy https://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Step 3 Copy the software to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm
```

```
https://jcrichton:aeryn@10.1.1.1/cisco-asa-fp1k.9.14.1.SPA
disk0:/cisco-asa-fp1k.9.14.1.SPA
```

Step 4 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 5 Show the current boot image configured, if present.

show running-config boot system

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the image from ROMMON, have a new device, or you removed the command manually.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Step 6 If you have a **boot system** command configured, remove it so that you can enter the new boot image.

no boot system disk*n***:/**[*path*/]*asa_image_name*

If you did not have a **boot system** command configured, skip this step.

Example:

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.13.1.SPA
```

Step 7 Set the ASA image to boot (the one you just uploaded).

boot system disk*n***:/**[*path*/]*asa_image_name*

You can only enter a single **boot system** command. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA. If you change your mind prior to reloading, you can enter the **no boot system** command to delete the new image from the boot location, so the current image continues to run.

Example:

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.14.1.SPA

The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.14.1 will do the following:
   - upgrade to the new platform version 2.8.1
   - upgrade to the CSP ASA version 9.14.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
```

```
ciscoasa(config)#
```

Step 8 Save the new settings to the startup configuration.

write memory

These configuration changes are automatically saved on the secondary unit.

Step 9 Make both failover groups active on the primary unit.

failover active group 1

failover active group 2

Example:

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Step 10 Reload the secondary unit to boot the new image:

failover reload-standby

Wait for the secondary unit to finish loading. Use the **show failover** command to verify that both failover groups are in the Standby Ready state.

Step 11 Force both failover groups to become active on the secondary unit:

no failover active group 1

no failover active group 2

Example:

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

If you are disconnected from your SSH session, reconnect to the failover group 1 IP address, now on the secondary unit.

Step 12 Reload the primary unit:

failover reload-standby

Example:

```
asa/act/sec# failover reload-standby
```

Note
If you are connected to the primary unit console port, you should instead enter the **reload** command to reload the primary unit.

You may be disconnected from your SSH session.

Step 13 If the failover groups are configured with the **preempt** command, they automatically become active on their designated unit after the preempt delay has passed.

Upgrade an Active/Active Failover Pair Using ASDM

The **Upgrade Software from Local Computer** tool lets you upload an image file from your computer to the flash file system to upgrade the Active/Active failover pair for the Secure Firewall 200, Firepower 1000, Secure Firewall 1200, Firepower 2100 in Appliance mode, Secure Firewall 3100/4200, Secure Firewall 6100.

Before you begin

- Perform these steps in the system execution space.
- Place the ASA image on your local management computer.

Procedure

Step 1 Launch ASDM on the *secondary* unit by connecting to the management address in failover group 2.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASA**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 7 Connect ASDM to the *primary* unit by connecting to the management IP address in failover group 1.

Step 8 If you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) Choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
b) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.
c) Click **Apply**.

Step 9 Upload the ASA software, using the same file location you used on the secondary unit.

Step 10 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 11 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the secondary unit.

Step 12 Make both failover groups active on the primary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 13 Reload the secondary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the secondary unit reloads.

Step 14 After the secondary unit comes up, make both failover groups active on the secondary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the secondary unit, and clicking **Make Standby**.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

Step 15 Reload the primary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Step 16 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. ASDM will automatically reconnect to the failover group 1 IP address on the primary unit.

Upgrade an ASA Cluster (Secure Firewall 3100/4200/6100)

Use the CLI or ASDM to upgrade devices in a cluster.

Upgrade an ASA Cluster Using the CLI (Secure Firewall 3100/4200/6100)

To upgrade all nodes in an ASA cluster, perform the following steps. This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Alternatively, if your device includes a USB port, you can download the software image to a USB type A storage device formatted for FAT-32, and insert it into the port. You can then copy from the disk using **copy disk1:***/path_and_filename* **disk0:***/path_and_filename*.

Before you begin

- Perform these steps on the control node. You can configure the ASA prompt to show the cluster node and state (control or data), which is useful to determine which node you are connected to. See the prompt command. Alternatively, enter the **show cluster info** command to view each node's role.
- You must use the console port; you cannot enable or disable clustering from a remote CLI connection.
- Perform these steps in the system execution space for multiple context mode.

Procedure

Step 1 On the control node in global configuration mode, if you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

asdm image disk0:/asdm.bin

write memory

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

Step 2 On the control node in privileged EXEC mode (minimum), copy the ASA software to all nodes in the cluster.

cluster exec copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/unit1/control# cluster exec copy /noconfirm
https://dwinchester:sam@10.1.1.1/cisco-asa-fp3k.9.19.1.SPA
disk0:/cisco-asa-fp3k.9.19.1.SPA
```

Step 3 If you are not already in global configuration mode, access it now.

configure terminal

Example:

```
asa/unit1/control# configure terminal
asa/unit1/control(config)#
```

Step 4 Show the current boot image configured, if present.

show running-config boot system

Note that you may not have a **boot system** command present in your configuration; for example, if you installed the image from ROMMON, have a new device, or you removed the command manually.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cisco-asa-fp1k.9.17.1.SPA
```

Step 5 If you have a **boot system** command configured, remove it so that you can enter the new boot image.

no boot system disk*n***:/**[*path/*]*asa_image_name*

If you did not have a **boot system** command configured, skip this step.

Example:

```
ciscoasa(config)# no boot system disk0:/cisco-asa-fp1k.9.17.1.SPA
```

Step 6 Set the ASA image to boot (the one you just uploaded).

boot system disk*n***:/**[*path/*]*asa_image_name*

You can only enter a single **boot system** command. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA. If you change your mind prior

to reloading, you can enter the **no boot system** command to delete the new image from the boot location, so the current image continues to run.

Example:

```
ciscoasa(config)# boot system disk0:/cisco-asa-fp1k.9.19.1.SPA

The system is currently installed with security software package 9.17.1, which has:
   - The platform version:  2.11.1
   - The CSP (asa) version: 9.17.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.19.1 will do the following:
   - upgrade to the new platform version 2.13.1
   - upgrade to the CSP ASA version 9.19.1
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
ciscoasa(config)#
```

Step 7 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the data nodes.

Step 8 Upgrade the data nodes by reloading.

Note
During the upgrade process, never use the **cluster control-node unit** command to force a data node to become control; you can cause network connectivity and cluster stability-related problems. You must upgrade and reload all data nodes first, and then continue with this procedure to ensure a smooth transition from the current control node to a new control node.

a) On the control node, to view member names, enter **cluster exec unit ?**, or enter the **show cluster info** command.

b) Reload a data node.

cluster exec unit *data-node* **reload noconfirm**

Example:

```
asa/unit1/control# cluster exec unit node2 reload noconfirm
```

c) Repeat for each data node.

To avoid connection loss and allow traffic to stabilize, wait for each node to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next node. To view when a node rejoins the cluster, enter **show cluster info**.

Step 9 Upgrade the control node by reloading.

a) Disable clustering. We recommend manually disabling clustering on the control node if possible so that a new control node can be elected as quickly and cleanly as possible.

cluster group *name*

no enable

Wait for 5 minutes for a new control node to be selected and traffic to stabilize.

Do not save this configuration; you want clustering to be enabled when you reload.

Example:

```
asa/unit1/control(config)# cluster group cluster1
asa/unit1/control(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit node1 transitioned from CONTROL to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Reload this node.

reload noconfirm

When the former control node rejoins the cluster, it will be a data node.

Upgrade an ASA Cluster Using ASDM (Secure Firewall 3100/4200/6100)

To upgrade all nodes in an ASA cluster, perform the following steps.

Before you begin

- Perform these steps on the control node.
- Perform these steps in the system execution space for multiple context mode.
- Place the ASA image on your local management computer.

Procedure

Step 1 Launch ASDM on the *control* node by connecting to the main cluster IP address.

This IP address always stays with the control node.

Step 2 If you previously set a non-default ASDM image, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) In the main ASDM application window, choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
b) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.

c) Click **Apply**.

Step 3 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software from Local Computer** dialog box appears.

Step 4 Click the **All devices in the cluster** radio button.

The **Upgrade Software** dialog box appears.

Step 5 From the **Image to Upload** drop-down list, choose **ASA**.

Step 6 In the **Local File Path** field, click **Browse Local Files** to find the file on your computer.

Step 7 (Optional) In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

By default, this field is prepopulated with the following path: **disk0:**/*filename*.

Step 8 Click **Upload Image**. The uploading process might take a few minutes.

Step 9 You are prompted to set this image as the ASA image. Click **Yes**.

Step 10 You are reminded to reload the ASA to use the new image. Click **OK**.

You exit the Upgrade tool.

Step 11 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the data nodes.

Step 12 Take note of the individual management IP addresses for each node on **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members** so that you can connect ASDM directly to data nodes later.

Step 13 Upgrade the data nodes by reloading.

Note
During the upgrade process, never change the control node using the **Monitoring** > **ASA Cluster** > **Cluster Summary** page to force a data node to become control; you can cause network connectivity and cluster stability-related problems. You must reload all data nodes first, and then continue with this procedure to ensure a smooth transition from the current control node to a new control node.

a) On the control node, choose **Tools** > **System Reload**.
b) Choose a data node name from the **Device** drop-down list.
c) Click **Schedule Reload**.
d) Click **Yes** to continue the reload.
e) Repeat for each data node.

To avoid connection loss and allow traffic to stabilize, wait for each node to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next node. To view when a node rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

Step 14 Upgrade the control node by reloading.

a) In ASDM on the control node, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** pane.
b) Uncheck the **Participate in ASA cluster** check box, and click **Apply**.

You are prompted to exit ASDM.

c) Wait for up to 5 minutes for a new control node to be selected and traffic to stabilize.

When the former control node rejoins the cluster, it will be a data node.

d) Re-connect ASDM to the former control node by connecting to its *individual* management IP address that you noted earlier.

The main cluster IP address now belongs to the new control node; this former control node is still accessible on its individual management IP address.

e) Choose **Tools** > **System Reload**.
f) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this node reloads, you want clustering to be enabled on it.

g) Click **Schedule Reload**.
h) Click **Yes** to continue the reload.

You are prompted to exit ASDM. Restart ASDM on the main cluster IP address; you will reconnect to the new control node.

Upgrade the Firepower 4100/9300

This document describes how to upgrade the ASA on the Firepower 4100/9300.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and a standalone ASA device or an ASA intra-chassis cluster on a Firepower 9300.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using Secure Firewall Chassis Manager

The upgrade process can take up to 45 minutes. Traffic will not traverse through the device while it is upgrading. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 In Secure Firewall Chassis Manager, choose **System** > **Updates**.

The **Available Updates** area shows a list of the packages available on the chassis.

Step 2 Upload the new FXOS platform bundle image and ASA software image::

a) Click **Upload Image**.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the chassis.

Step 3 After the new FXOS platform bundle image has successfully uploaded, click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Step 4 Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 102).

Step 6 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 7 Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.

Step 8 For each ASA logical device that you want to upgrade:

a) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
b) For the **New Version**, choose the software version to which you want to upgrade.
c) Click **OK**.

Step 9 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using the FXOS CLI

The upgrade process can take up to 45 minutes. Traffic will not traverse through the device while it is upgrading. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the images.

- Fully qualified names of the image files.

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Download the new FXOS platform bundle image to the chassis:

a) Enter firmware mode:

scope firmware

b) Download the FXOS platform bundle software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

c) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 102.

Step 4 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 5 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 6 For each ASA logical device that you want to upgrade:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

scope app-instance asa *instance_name*

d) Set the Startup version to the new ASA software version:

set startup-version *version_number*

Step 7 Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 8 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 103.

Upgrade FXOS and an ASA Active/Standby Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and an ASA Active/Standby failover pair.

Upgrade FXOS and an ASA Active/Standby Failover Pair Using Secure Firewall Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is active and which is standby: connect ASDM to the active ASA IP address. The active unit always owns the active IP address. Then choose **Monitoring** > **Properties** > **Failover** > **Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 On the chassis that contains the *standby* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

a) In Secure Firewall Chassis Manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
b) Click **Upload Image**.
c) Click **Choose File** to navigate to and select the image that you want to upload.
d) Click **Upload**.
The selected image is uploaded to the chassis.

Step 2 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the chassis that contains the *standby* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 3 Secure Firewall Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 102).

Step 4 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 5 Upgrade the ASA logical device image:

a) Choose **Logical Devices** to open the Logical Devices page.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
c) For the **New Version**, choose the software version to which you want to update.
d) Click **OK**.

Step 6 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Step 7 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.
b) Force the standby unit to become active by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Active**.

Step 8 On the chassis that contains the *new standby* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

a) In Secure Firewall Chassis Manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
b) Click **Upload Image**.
c) Click **Choose File** to navigate to and select the image that you want to upload.
d) Click **Upload**.
The selected image is uploaded to the chassis.

Step 9 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the chassis that contains the *new standby* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 10 Secure Firewall Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 102).

Step 11 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 12 Upgrade the ASA logical device image:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.
b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
c) For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 13 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.

b) Verify the application version and operational status.

Step 14 (Optional) Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.

b) Force the standby unit to become active by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Active**.

Upgrade FXOS and an ASA Active/Standby Failover Pair Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is active and which is standby: connect to the ASA console on the chassis and enter the **show failover** command to view the Active/Standby status of the unit.
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 On the chassis that contains the *standby* ASA logical device, download the new FXOS platform bundle image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 2 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 102.

Step 3 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 4 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 5 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

scope app-instance asa *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 6 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 103.

Step 7 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) On the chassis that contains the standby ASA logical device, connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
```

```
asa>
```

c) Make this unit active:

failover active

d) Save the configuration:

write memory

e) Verify that the unit is active:

show failover

Step 8 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 9 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 10 On the chassis that contains the *new standby* ASA logical device, download the new FXOS platform bundle image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 11 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 102.

Step 12 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 13 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ---------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 14 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

scope app-instance asa *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 15 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 103.

Step 16 (Optional) Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) On the chassis that contains the standby ASA logical device, connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make this unit active:

failover active

d) Save the configuration:

write memory

e) Verify that the unit is active:

show failover

Upgrade FXOS and an ASA Active/Active Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and an ASA Active/Active failover pair.

Upgrade FXOS and an ASA Active/Active Failover Pair Using Secure Firewall Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is the primary unit: connect ASDM and then choose **Monitoring** > **Properties** > **Failover** > **Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 Make both failover groups active on the *primary* unit.

a) Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.
b) Choose **Monitoring** > **Failover** > **Failover Group 2**, and click **Make Active**.
c) Stay connected to ASDM on this unit for later steps.

Step 2 On the chassis that contains the *secondary* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

a) Connect to the Secure Firewall Chassis Manager on the *secondary* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image**.
d) Click **Choose File** to navigate to and select the image that you want to upload.
e) Click **Upload**.
The selected image is uploaded to the chassis.

Step 3 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the chassis that contains the *secondary* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 4 Secure Firewall Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 102).

Step 5 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 6 Upgrade the ASA logical device image:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
c) For the **New Version**, choose the software version to which you want to update.
d) Click **OK**.

Step 7 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Step 8 Make both failover groups active on the *secondary* unit.

a) Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.
b) Choose **Monitoring** > **Failover** > **Failover Group 1**, and click **Make Standby**.
c) Choose **Monitoring** > **Failover** > **Failover Group 2**, and click **Make Standby**.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

Step 9 On the chassis that contains the *primary* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

a) Connect to the Secure Firewall Chassis Manager on the *primary* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image** to open the Upload Image dialog box.
d) Click **Choose File** to navigate to and select the image that you want to upload.
e) Click **Upload**.
The selected package is uploaded to the chassis.
f) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 10 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the chassis that contains the *primary* ASA logical device:

a) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package.

It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 11 Secure Firewall Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 102).

Step 12 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 13 Upgrade the ASA logical device image:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
c) For the **New Version**, choose the software version to which you want to update.
d) Click **OK**.

Step 14 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Step 15 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring > Failover > Failover Group #** pane.

Upgrade FXOS and an ASA Active/Active Failover Pair Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- You need to determine which unit is primary: connect to the ASA console on the chassis and enter the **show failover** command to view the unit's status and priority (primary or secondary).
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 Connect to the FXOS CLI on the *secondary* unit, either the console port (preferred) or using SSH.

Step 2 Make both failover groups active on the primary unit.

a) Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make both failover groups active on the primary unit.

enable

The enable password is blank by default.

no failover active group 1

no failover active group 2

Example:

```
asa> enable
Password: <blank>
asa# no failover active group 1
asa# no failover active group 2
```

Step 3 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 5 On the chassis that contains the *secondary* ASA logical device, download the new FXOS platform bundle image and ASA software image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 6 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

top

scope firmware

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 102.

Step 7 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 8 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- tftp://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 9 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

scope app-instance asa *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 10 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 103.

Step 11 Make both failover groups active on the *secondary* unit.

a) Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

c) Make both failover groups active on the *secondary* unit.

enable

The enable password is blank by default.

failover active group 1

failover active group 2

Example:

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

Step 12 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 13 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

Step 14 On the chassis that contains the *primary* ASA logical device, download the new FXOS platform bundle image and ASA software image:

a) Connect to the FXOS CLI.

b) Enter firmware mode:

scope firmware

c) Download the FXOS platform bundle software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- tftp://*server***:***port-num*/*path*/*image_name*

d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 15 After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

up

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 102.

Step 16 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 17 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*
- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server                Userid          State
    ----------------------------- ---------- --------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1           user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 18 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

scope app-instance asa *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 19 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 103.

Step 20 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring > Failover > Failover Group #** pane.

Upgrade FXOS and an ASA Inter-chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and ASA on all chassis in an inter-chassis cluster.

Upgrade FXOS and an ASA Inter-chassis Cluster Using Secure Firewall Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

Step 1 Determine which chassis has the control node. You will upgrade this chassis last.

a) Connect to Secure Firewall Chassis Manager.
b) Choose **Logical Devices**.
c) Click the plus sign (+) to see the attributes for the security modules included in the cluster.
d) Verify that the control node is on this chassis. There should be an ASA instance with **CLUSTER-ROLE** set to "Control".

Step 2 Connect to Secure Firewall Chassis Manager on a chassis in the cluster that **does not have the control node**.

Step 3 Upload the new FXOS platform bundle image and ASA software image:

a) In Secure Firewall Chassis Manager, choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
b) Click **Upload Image**.
c) Click **Choose File** to navigate to and select the image that you want to upload.
d) Click **Upload**.
The selected image is uploaded to the chassis.
e) Wait for the images to successfully upload before continuing.

Step 4 Upgrade the FXOS bundle:

a) Choose **System** > **Updates**.
b) Click the **Upgrade** icon for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be

rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

c) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 5 Secure Firewall Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see Monitor the Upgrade Progress, on page 102).

Step 6 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 7 Upgrade the ASA logical device image on each security module:

a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
c) For the **New Version**, choose the software version to which you want to update.
d) Click **OK**.

Step 8 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

a) Choose **Logical Devices**.
b) Verify the application version and operational status.

Step 9 Repeat steps Step 2, on page 97-Step 8, on page 98 for all remaining chassis in the cluster that do not have the control node.

Step 10 After all chassis in the cluster that do not have the control node have been upgraded, repeat steps Step 2, on page 97-Step 8, on page 98 on the chassis **with the control node**.
A new control node will be chosen from one of the previously upgraded chassis.

Step 11 For distributed VPN clustering mode, after the cluster has stabilized you can redistribute active sessions among all modules in the cluster using the ASA console on the control node.

cluster redistribute vpn-sessiondb

What to do next

Set the chassis Site ID. For more information about how to set the chassis Site ID, see the Inter-Site Clustering topic in Deploying a Cluster for ASA on the Firepower 4100/9300 for Scalability and High Availability on Cisco.com.

Upgrade FXOS and an ASA Inter-chassis Cluster Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:

- IP address and authentication credentials for the server from which you are copying the image.
- Fully qualified name of the image file.

Procedure

Step 1 Determine which chassis has the control node. You will upgrade this chassis last.

a) Connect to the FXOS CLI.

b) Verify that the control node is on this chassis. There should be an ASA instance with Cluster Role set to "Control":

scope ssa

show app-instance

Step 2 Connect to the FXOS CLI on a chassis in the cluster that **does not have the control node**.

Step 3 Download the new FXOS platform bundle image to the chassis:

a) Enter firmware mode:

scope firmware

b) Download the FXOS platform bundle software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*/*image_name*
- **scp**://*username@server*/*path*/*image_name*
- **sftp**://*username@server*/*path*/*image_name*
- **tftp**://*server***:***port-num*/*path*/*image_name*

c) To monitor the download process:

scope download-task *image_name*

**show detail*

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
```

```
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 4 Upgrade the FXOS bundle:

a) If necessary, return to firmware mode:

top

scope firmware

b) Make note of the version number for the FXOS platform bundle you are installing:

show package

c) Enter auto-install mode:

scope auto-install

d) Install the FXOS platform bundle:

install platform platform-vers *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

e) The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently-installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.

f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

g) To monitor the upgrade process, see Monitor the Upgrade Progress, on page 102.

Step 5 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see Verify the Installation, on page 103).

Step 6 Download the new ASA software image to the chassis:

a) Enter Security Services mode:

top

scope ssa

b) Enter Application Software mode:

scope app-software

c) Download the logical device software image:

download image *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@server*/*path*

- **scp**://*username@server*/*path*
- **sftp**://*username@server*/*path*
- **tftp**://*server*:*port-num*/*path*

d) To monitor the download process:

show download-task

e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes
```

Step 7 Upgrade the ASA logical device image:

a) Enter Security Services mode:

top

scope ssa

b) Set the scope to the security module you are updating:

scope slot*slot_number*

c) Set the scope to the ASA application:

scope app-instance asa *instance_name*

d) Set the Startup version to the version you want to update:

set startup-version *version_number*

e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 8 To verify the status of the security modules/security engine and any installed applications, see Verify the Installation, on page 103.

Step 9 Repeat steps Step 2, on page 99-Step 8, on page 102 for all remaining chassis in the cluster that do not have the control node.

Step 10 After all chassis in the cluster that do not have the control node have been upgraded, repeat steps Step 2, on page 99-Step 8, on page 102 on the chassis **with the control node**.
A new control node will be chosen from one of the previously upgraded chassis.

Step 11 For distributed VPN clustering mode, after the cluster has stabilized you can redistribute active sessions among all modules in the cluster using the ASA console on the control node.

cluster redistribute vpn-sessiondb

What to do next

Set the chassis Site ID. For more information about how to set the chassis Site ID, see the Inter-Site Clustering topic in Deploying a Cluster for ASA on the Firepower 4100/9300 for Scalability and High Availability on Cisco.com.

Monitor the Upgrade Progress

You can monitor the upgrade process using the FXOS CLI:

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Enter **scope system**.

Step 3 Enter **show firmware monitor**.

Step 4 Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example

```
Firepower-chassis# scope system
Firepower-chassis /system # show firmware monitor
FPRM:
```

```
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Verify the Installation

Enter the following commands to verify the status of the security modules/security engine and any installed applications:

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Enter **top**.

Step 3 Enter **scope ssa**.

Step 4 Enter **show slot**.

Step 5 Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

Example:

Step 6 Enter **show app-instance**.

Step 7 Verify that the Oper State is `Online` for any logical devices installed on the chassis and that the correct version is listed.

If this chassis is part of a cluster, verify that the cluster operational state is "In-Cluster" for all security modules installed in the chassis. Also, verify that the control unit is not on the chassis for which you are upgrading—there should not be any instance with Cluster Role set to "Master".

Example

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
```

```
Firepower-chassis /ssa #
Firepower-chassis /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- -------------- ---------------
 --------------- ------------
asa        asa1       1          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
asa        asa2       2          Enabled     Online           9.10.0.85       9.10.0.85
    Not Applicable  None
Firepower-chassis /ssa #
```

Upgrade the ASA Virtual, ISA 3000, or ASA 5500-X

This document describes how to plan and implement an ASA and ASDM upgrade for the following models for standalone, failover, or clustering deployments:

- ASA Virtual
- ISA 3000
- ASA 5500-X

Upgrade a Standalone Unit

Use the CLI or ASDM to upgrade the standalone unit.

Upgrade a Standalone Unit Using the CLI

This section describes how to install the ASDM and ASA images, and also when to upgrade the ASA FirePOWER module.

Before you begin

This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Procedure

Step 1 In privileged EXEC mode, copy the ASA software to flash memory.

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
ciscoasa# copy https://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin
disk0:/asa-9-12-1-smp-k8.bin
```

Step 2 Copy the ASDM image to flash memory.

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
ciscoasa# copy https://jcrichton:aeryn@10.1.1.1/asdm-7121.bin
disk0:/asdm-7121.bin
```

Step 3 Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Step 4 Show the current boot images configured (up to 4):

show running-config boot system

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Example:

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

Step 5 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Example:

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

Step 7 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Example:

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

Step 8 Save the new settings to the startup configuration:

write memory

Step 9 Reload the ASA:

reload

Step 10 If you are upgrading the ASA FirePOWER module, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

You can reenable it after the upgrade:

rest-api agent

Note
The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 11 Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit from Your Local Computer Using ASDM

The **Upgrade Software from Local Computer** tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

Procedure

Step 1 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 2 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 3 In the **Local File Path** field, click **Browse Local Files** to find the file on your PC.

Step 4 In the **Flash File System Path** field, click **Browse Flash** to find the directory or file in the flash file system.

Step 5 Click **Upload Image**.

The uploading process might take a few minutes.

Step 6 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 7 You are reminded to exit ASDM and save the configuration. Click **OK**.

You exit the **Upgrade** tool. **Note:** You will save the configuration and exit and reconnect to ASDM *after* you upgrade the ASA software.

Step 8 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list. You can also use this procedure to upload other file types.

Step 9 Choose **Tools** > **System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload.

a) Click the **Save the running configuration at the time of reload** radio button (the default).
b) Choose a time to reload (for example, **Now**, the default).
c) Click **Schedule Reload**.

Once the reload is in progress, a **Reload Status** window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Step 11 If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

rest-api agent

Note
The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard

The **Upgrade Software from Cisco.com Wizard** lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.



Note ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 9.9(1), the download might be 9.9(1.2). This behavior is expected, so you can proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, reload the ASA to save the configuration and complete the upgrade.

Before you begin

Due to an internal change, the wizard is only supported using ASDM 7.10(1) and later; also, due to an image naming change, you must use ASDM 7.12(1) or later to upgrade to ASA 9.10(1) and later. Because ASDM is backwards compatible with earlier ASA releases, you can upgrade ASDM no matter which ASA version you are running.

Procedure

Step 1 Choose **Tools** > **Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The **Cisco.com Device Activation** dialog box appears.

Note
In ASDM 7.23 and earlier, the Cisco.com login is slightly different.

Step 2 Click **Start Activate your device** to open a browser window where you can activate the ASA on your Cisco.com account. Return to ASDM and click **Continue**.

If the browser window did not open, you can manually copy the activation URL using the **Copy URL** button. You can then open a browser and paste in the URL to activate the ASA.

After you activate the ASA, the **Cisco.com Upgrade Wizard** appears.

Note
If there is no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

Step 3 Click **Next** to display the **Select Software** screen.

The current ASA version and ASDM version appear.

Step 4 To upgrade the ASA version and ASDM version, perform the following steps:

a) In the **ASA** area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.
b) In the **ASDM** area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.

Step 5 Click **Next** to display the **Review Changes** screen.

Step 6 Verify the following items:

- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
- The ASA image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASA boot image has been selected.

Step 7 Click **Next** to start the upgrade installation.

You can then view the status of the upgrade installation as it progresses.

The **Results** screen appears, which provides additional details, such as the upgrade installation status (success or failure).

Step 8 If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.

Step 9 Click **Finish** to exit the wizard and save the configuration changes that you have made.

Note
To upgrade to the next higher version, if any, you must restart the wizard.

Step 10 After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

Step 11 If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

rest-api agent

Note
The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade an Active/Standby Failover Pair

Use the CLI or ASDM to upgrade the Active/Standby failover pair for a zero downtime upgrade.

Note A zero downtime upgrade is guaranteed only for active data traffic forwarding through the failover pair, and does not assure uninterrupted management-plane (SSH/ASDM) access.

When the inside interface is configured as a data interface and also as the management interface (shared management/data interface), it can result in SSH packet loss and a brief ARP resolution delays on adjacent switches during the reload/failover phase.

Upgrade an Active/Standby Failover Pair Using the CLI

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

- Perform these steps on the active unit. For SSH access, connect to the active IP address; the active unit always owns this IP address. When you connect to the CLI, determine the failover status by looking at the ASA prompt; you can configure the ASA prompt to show the failover status and priority (primary or secondary), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show failover** command to view this unit's status and priority (primary or secondary).

- This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Procedure

Step 1 On the active unit in privileged EXEC mode, copy the ASA software to the active unit flash memory:

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act# copy https://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

Step 2 Copy the software to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

Step 3 Copy the ASDM image to the active unit flash memory:

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/act# copy https://jcrichton:aeryn@10.1.1.1/asdm-7151.bin
disk0:/asdm-7151.bin
```

Step 4 Copy the ASDM image to the standby unit; be sure to specify the same path as for the active unit:

failover exec mate copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/act# failover exec mate copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/asdm-7151.bin
disk0:/asdm-7151.bin
```

Step 5 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 6 Show the current boot images configured (up to 4):

show running-config boot system

Example:

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/act(config)# asdm image disk0:/asdm-7151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the standby unit.

Step 11 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

Step 12 Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete.

Step 13 Reload the standby unit to boot the new image:

failover reload-standby

Wait for the standby unit to finish loading. Use the **show failover** command to verify that the standby unit is in the Standby Ready state.

Step 14 Force the active unit to fail over to the standby unit.

no failover active

If you are disconnected from your SSH session, reconnect to the main IP address, now on the new active/former standby unit.

Step 15 Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete.

Step 16 From the new active unit, reload the former active unit (now the new standby unit).

failover reload-standby

Example:

```
asa/act# failover reload-standby
```

Note
If you are connected to the former active unit console port, you should instead enter the **reload** command to reload the former active unit.

Upgrade an Active/Standby Failover Pair Using ASDM

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

Place the ASA and ASDM images on your local management computer.

Procedure

Step 1 Launch ASDM on the *standby* unit by connecting to the standby IP address.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click **No**. You exit the Upgrade tool.

Step 7 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 8 Connect ASDM to the *active* unit by connecting to the main IP address, and upload the ASDM software, using the same file location you used on the standby unit.

Step 9 When you are prompted to set the image as the ASDM image, click **Yes**.

You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Upload the ASA software, using the same file location you used for the standby unit.

Step 11 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the standby unit.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 15 Reload the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the standby unit reloads.

Step 16 After the standby unit reloads, force the active unit to fail over to the standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Standby**.

ASDM will automatically reconnect to the new active unit.

Step 17 Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 18 Reload the (new) standby unit by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Reload Standby**.

Upgrade an Active/Active Failover Pair

Use the CLI or ASDM to upgrade the Active/Active failover pair for a zero downtime upgrade.

Upgrade an Active/Active Failover Pair Using the CLI

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps on the primary unit.
- Perform these steps in the system execution space.
- This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Procedure

Step 1 On the primary unit in privileged EXEC mode, copy the ASA software to flash memory:

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act/pri# copy https://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

Step 2 Copy the software to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name* **disk***n***:/**[*path/*]*asa_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

Step 3 Copy the ASDM image to the primary unit flash memory:

copy https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/act/pri# copy https://jcrichton:aeryn@10.1.1.1/asdm-7151.bin
disk0:/asdm-7151.bin
```

Step 4 Copy the ASDM image to the secondary unit; be sure to specify the same path as for the primary unit:

failover exec mate copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name* **disk***n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/act/pri# failover exec mate copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/asdm-7151.bin
disk0:/asdm-7151.bin
```

Step 5 If you are not already in global configuration mode, access global configuration mode:

configure terminal

Step 6 Show the current boot images configured (up to 4):

show running-config boot system

Example:

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/act/pri(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/act/pri(config)# asdm image disk0:/asdm-7151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the secondary unit.

Step 11 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

no rest-api agent

Step 12 Make both failover groups active on the primary unit:

failover active group 1

failover active group 2

Example:

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Step 13 Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete.

Step 14 Reload the secondary unit to boot the new image:

failover reload-standby

Wait for the secondary unit to finish loading. Use the **show failover** command to verify that both failover groups are in the Standby Ready state.

Step 15 Force both failover groups to become active on the secondary unit:

no failover active group 1

no failover active group 2

Example:

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

If you are disconnected from your SSH session, reconnect to the failover group 1 IP address, now on the secondary unit.

Step 16 Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete.

Step 17 Reload the primary unit:

failover reload-standby

Example:

```
asa/act/sec# failover reload-standby
```

Note
If you are connected to the primary unit console port, you should instead enter the **reload** command to reload the primary unit.

You may be disconnected from your SSH session.

Step 18 If the failover groups are configured with the **preempt** command, they automatically become active on their designated unit after the preempt delay has passed.

Upgrade an Active/Active Failover Pair Using ASDM

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps in the system execution space.
- Place the ASA and ASDM images on your local management computer.

Procedure

Step 1 Launch ASDM on the *secondary* unit by connecting to the management address in failover group 2.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software** dialog box appears.

Step 3 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 4 In the **Local File Path** field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

Step 6 Click **Upload Image**. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click **No**. You exit the Upgrade tool.

Step 7 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

When you are prompted to set this image as the ASA image, click **No**. You exit the Upgrade tool.

Step 8 Connect ASDM to the *primary* unit by connecting to the management IP address in failover group 1, and upload the ASDM software, using the same file location you used on the secondary unit.

Step 9 When you are prompted to set the image as the ASDM image, click **Yes**.

You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Upload the ASA software, using the same file location you used for the secondary unit.

Step 11 When you are prompted to set the image as the ASA image, click **Yes**.

You are reminded to reload the ASA to use the new image. Click **OK**. You exit the Upgrade tool.

Step 12 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the secondary unit.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Make both failover groups active on the primary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 15 Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the primary unit.

Step 16 Reload the secondary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Stay on the **System** pane to monitor when the secondary unit reloads.

Step 17 After the secondary unit comes up, make both failover groups active on the secondary unit by choosing **Monitoring** > **Failover** > **Failover Group #**, where **#** is the number of the failover group you want to move to the secondary unit, and clicking **Make Standby**.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

Step 18 Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 *standby* management IP address. Wait for the upgrade to complete, and then connect ASDM back to the secondary unit.

Step 19 Reload the primary unit by choosing **Monitoring** > **Failover** > **System**, and clicking **Reload Standby**.

Step 20 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. ASDM will automatically reconnect to the failover group 1 IP address on the primary unit.

Upgrade an ASA Cluster

Use the CLI or ASDM to upgrade the ASA Cluster for a zero downtime upgrade.

Upgrade an ASA Cluster Using the CLI

To upgrade all units in an ASA cluster, perform the following steps. This procedure uses HTTPS. For SCP, FTP, TFTP, HTTP, or other server types, see the **copy** command in the ASA command reference.

Before you begin

- Perform these steps on the control unit. If you are also upgrading the ASA FirePOWER module, then you need console or ASDM access on each data unit. You can configure the ASA prompt to show the cluster unit and state (control or data), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the **show cluster info** command to view each unit's role.
- You must use the console port; you cannot enable or disable clustering from a remote CLI connection.
- Perform these steps in the system execution space for multiple context mode.

Procedure

Step 1 On the control unit in privileged EXEC mode, copy the ASA software to all units in the cluster.

cluster exec copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asa_image_name*
disk*n***:/**[*path/*]*asa_image_name*

Example:

```
asa/unit1/master# cluster exec copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/asa9-15-1-smp-k8.bin
disk0:/asa9-15-1-smp-k8.bin
```

Step 2 Copy the ASDM image to all units in the cluster:

cluster exec copy /noconfirm https://[[*user*[**:***password*]**@**]*server*[*/path*]*/asdm_image_name*
disk*n***:/**[*path/*]*asdm_image_name*

Example:

```
asa/unit1/master# cluster exec copy /noconfirm
https://jcrichton:aeryn@10.1.1.1/asdm-7151.bin
disk0:/asdm-7151.bin
```

Step 3 If you are not already in global configuration mode, access it now.

configure terminal

Example:

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

Step 4 Show the current boot images configured (up to 4).

show running-config boot system

Example:

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 5 Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

no boot system disk*n***:/**[*path/*]*asa_image_name*

Example:

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
```

```
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6 Set the ASA image to boot (the one you just uploaded):

boot system disk*n***:/**[*path*/]*asa_image_name*

Example:

```
asa/unit1/master(config)# boot system disk0://asa9-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 7 Set the ASDM image to use (the one you just uploaded):

asdm image disk*n***:/**[*path*/]*asdm_image_name*

Example:

```
asa/unit1/master(config)# asdm image disk0:/asdm-7151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 8 Save the new settings to the startup configuration:

write memory

These configuration changes are automatically saved on the data units.

Step 9 If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the ASA FirePOWER module upgrade will fail.

no rest-api agent

Step 10 If you are upgrading ASA FirePOWER modules that are managed by ASDM, you will need to connect ASDM to the *individual* management IP addresses, so you need to note the IP addresses for each unit.

show running-config interface *management_interface_id*

Note the **cluster-pool** poolname used.

show ip[**v6**] **local pool** *poolname*

Note the cluster unit IP addresses.

Example:

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
```

```
unit1                           10.86.118.17
asa1/unit2/slave#
```

Step 11 Upgrade the data units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedures minimize the number of ASA reloads when also upgrading the ASA FirePOWER module. You can choose to use the data Console or ASDM for these procedures. You may want to use ASDM instead of the Console if you do not have ready access to all of the console ports but can reach ASDM over the network.

Note
During the upgrade process, never use the **cluster master unit** command to force a data unit to become control; you can cause network connectivity and cluster stability-related problems. You must upgrade and reload all data units first, and then continue with this procedure to ensure a smooth transition from the current control unit to a new control unit.

If you do not have ASA FirePOWER module upgrades:

a) On the control unit, to view member names, enter **cluster exec unit ?**, or enter the **show cluster info** command.
b) Reload a data unit.

cluster exec unit *data-unit* **reload noconfirm**

Example:

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter **show cluster info**.

If you also have ASA FirePOWER module upgrades (using the data Console):

a) Connect to the console port of a data unit, and enter global configuration mode.

enable

configure terminal

Example:

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) Disable clustering.

cluster group *name*

no enable

Do not save this configuration; you want clustering to be enabled when you reload. You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

Example:

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) Upgrade the ASA FirePOWER module on this data unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *individual* management IP address that you noted earlier. Wait for the upgrade to complete.

d) Reload the data unit.

reload noconfirm

e) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter **show cluster info**.

If you also have ASA FirePOWER module upgrades (using ASDM):

a) Connect ASDM to the *individual* management IP address of this data unit that you noted earlier.
b) Choose **Configuration** > **Device ManagementHigh Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** > **.**
c) Uncheck the **Participate in ASA cluster** check box.

You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

Do not uncheck the **Configure ASA cluster settings** check box; this action clears all cluster configuration, and also shuts down all interfaces including the management interface to which ASDM is connected. To restore connectivity in this case, you need to access the CLI at the console port.

Note
Some older versions of ASDM do not support disabling the cluster on this screen; in this case, use the **Tools** > **Command Line Interface** tool, click the **Multiple Line** radio button, and enter **cluster group** *name* and **no enable**. You can view the cluster group name in the **Home** > **Device Dashboard** > **Device Information** > **ASA Cluster** area.

d) Click **Apply**.
e) You are prompted to exit ASDM. Reconnect ASDM to the same IP address.
f) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

g) In ASDM, choose **Tools** > **System Reload**.

h) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

i) Click **Schedule Reload**.
j) Click **Yes** to continue the reload.
k) Repeat for each data unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane on the control unit.

Step 12 Upgrade the control unit.

a) Disable clustering.

cluster group *name*

no enable

Wait for 5 minutes for a new control unit to be selected and traffic to stabilize.

Do not save this configuration; you want clustering to be enabled when you reload.

We recommend manually disabling cluster on the control unit if possible so that a new control unit can be elected as quickly and cleanly as possible.

Example:

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover
either enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Upgrade the ASA FirePOWER module on this unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the *individual* management IP address that you noted earlier. The main cluster IP address now belongs to the new control unit; this former control unit is still accessible on its individual management IP address.

Wait for the upgrade to complete.

c) Reload this unit.

reload noconfirm

When the former control unit rejoins the cluster, it will be a data unit.

Upgrade an ASA Cluster Using ASDM

To upgrade all units in an ASA cluster, perform the following steps.

Before you begin

- Perform these steps on the control unit. If you are also upgrading the ASA FirePOWER module, then you need ASDM access to each data unit.
- Perform these steps in the system execution space for multiple context mode.
- Place the ASA and ASDM images on your local management computer.

Procedure

Step 1 Launch ASDM on the *control* unit by connecting to the main cluster IP address.

This IP address always stays with the control unit.

Step 2 In the main ASDM application window, choose **Tools** > **Upgrade Software from Local Computer**.

The **Upgrade Software from Local Computer** dialog box appears.

Step 3 Click the **All devices in the cluster** radio button.

The **Upgrade Software** dialog box appears.

Step 4 From the **Image to Upload** drop-down list, choose **ASDM**.

Step 5 In the **Local File Path** field, click **Browse Local Files** to find the file on your computer.

Step 6 (Optional) In the **Flash File System Path** field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

By default, this field is prepopulated with the following path: **disk0:**/*filename*.

Step 7 Click **Upload Image**. The uploading process might take a few minutes.

Step 8 You are prompted to set this image as the ASDM image. Click **Yes**.

Step 9 You are reminded to exit ASDM and save the configuration. Click **OK**.

You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 10 Repeat these steps, choosing **ASA** from the **Image to Upload** drop-down list.

Step 11 Click the **Save** icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the data units.

Step 12 Take note of the individual management IP addresses for each unit on **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members** so that you can connect ASDM directly to data units later.

Step 13 If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing **Tools** > **Command Line Interface**, and entering **no rest-api enable**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14 Upgrade the data units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedure minimizes the number of ASA reloads when also upgrading the ASA FirePOWER module.

Note
During the upgrade process, never change the control unit using the **Monitoring** > **ASA Cluster** > **Cluster Summary** page to force a data unit to become control; you can cause network connectivity and cluster stability-related problems. You must reload all data units first, and then continue with this procedure to ensure a smooth transition from the current control unit to a new control unit.

If you do not have ASA FirePOWER module upgrades:

a) On the control unit, choose **Tools** > **System Reload**.
b) Choose a data unit name from the **Device** drop-down list.
c) Click **Schedule Reload**.
d) Click **Yes** to continue the reload.
e) Repeat for each data unit.

   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

If you also have ASA FirePOWER module upgrades:

a) On the control unit, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Members**.
b) Select the data unit that you want to upgrade, and click **Delete**.
c) Click **Apply**.
d) Exit ASDM, and connect ASDM to the data unit by connecting to its *individual* management IP address that you noted earlier.
e) Upgrade the ASA FirePOWER module.

   Wait for the upgrade to complete.

f) In ASDM, choose **Tools** > **System Reload**.
g) Click the **Reload without saving the running configuration** radio button.

   You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

h) Click **Schedule Reload**.
i) Click **Yes** to continue the reload.
j) Repeat for each data unit.

   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring** > **ASA Cluster** > **Cluster Summary** pane.

Step 15 Upgrade the control unit.

a) In ASDM on the control unit, choose **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration** pane.
b) Uncheck the **Participate in ASA cluster** check box, and click **Apply**.

   You are prompted to exit ASDM.

c) Wait for up to 5 minutes for a new control unit to be selected and traffic to stabilize.

When the former control unit rejoins the cluster, it will be a data unit.

d) Re-connect ASDM to the former control unit by connecting to its *individual* management IP address that you noted earlier.

The main cluster IP address now belongs to the new control unit; this former control unit is still accessible on its individual management IP address.

e) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.

f) Choose **Tools** > **System Reload**.

g) Click the **Reload without saving the running configuration** radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

h) Click **Schedule Reload**.

i) Click **Yes** to continue the reload.

You are prompted to exit ASDM. Restart ASDM on the main cluster IP address; you will reconnect to the new control unit.

Upgrade the Firepower 2100 in Platform Mode

This document describes how to plan and implement an ASA, FXOS, and ASDM upgrade for standalone or failover deployments for the Firepower 2100 in Platform mode. Prior to version 9.13, the Firepower 2100 only supported Platform mode. In 9.14 and later, Appliance mode is the default. In 9.14 and later, use the **show fxos mode** command on the ASA to determine your current mode. For appliance mode procedures, see Upgrade the ASA Appliance, on page 51.

Upgrade a Standalone Unit

Use the FXOS CLI or Firepower Chassis Manager to upgrade the standalone unit.

Upgrade a Standalone Unit Using the Firepower Chassis Manager

This section describes how to upgrade the ASA bundle, which includes both ASA and ASDM, for a standalone unit. You will upload the package from your management computer.

Procedure

Step 1 If you previously set a non-default ASDM image in the ASA configuration, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same

name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) In the main ASDM application window, choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
b) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.
c) Click **Apply**
d) Click the **Save** icon on the toolbar to save your configuration changes.
e) Quit ASDM.

Step 2 Connect to the Firepower Chassis Manager.

Step 3 Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.

Step 4 Click **Upload Image** to upload the new package from your management computer.

Step 5 Click **Choose File** to navigate to and select the package that you want to upload.

Step 6 Click **Upload**.

The selected package is uploaded to the chassis. The **Upload Image** dialog box shows the upload status. Wait for the **Success** dialog box, and click **OK**. After completing the upload, the integrity of the image is automatically verified.

Step 7 Click the **Upgrade** icon to the right of the new package.

Step 8 Click **Yes** to confirm that you want to proceed with installation.

There is no indicator that the new package is being loaded. You will still see the Firepower Chassis Manager at the beginning of the upgrade process. When the system reboots, you will be logged out. You must wait for the system to come back up before you can log in to the Firepower Chassis Manager. The reboot process takes approximately 20 minutes. After the reboot, you will see the login screen.

Upgrade a Standalone Unit Using the FXOS CLI

This section describes how to upgrade the ASA bundle, which includes both ASA and ASDM, for a standalone unit. You can use FTP, SCP, SFTP, or TFTP to copy the package to the Firepower 2100 chassis.

Procedure

Step 1 Connect to the FXOS CLI, either the console port (preferred) or using SSH.

Step 2 If you previously set a non-default ASDM image in the ASA configuration, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) Connect to ASA.

connect asa

Example:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

b) Access privileged EXEC mode, and then global configuration mode.

enable

configure terminal

c) Set the ASDM image.

asdm image disk0:/asdm.bin

d) Save the configuration.

write memory

e) Return to the FXOS console by entering **Ctrl+a**, **d**.

Step 3 In FXOS, download the package to the chassis.

a) Enter firmware mode.

scope firmware

Example:

```
firepower-2110# scope firmware
firepower-2110 /firmware#
```

b) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

Example:

```
firepower-2110 /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Monitor the download process.

show download-task

Example:

```
firepower-2110 /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181            0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181            0                 Downloading
firepower-2110 /firmware #
```

Step 4 When the new package finishes downloading (**Downloaded** state), boot the package.

a) View the version number of the new package.

show package

Example:

```
firepower-2110 /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
firepower-2110 /firmware #
```

b) Install the package.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the ASA image and reboots.

Example:

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
firepower-2110 /firmware/auto-install #
```

Step 5 Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the ASA to come up (5 minutes). Wait until you see the following messages:

```
firepower-2110#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Upgrade an Active/Standby Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade the Active/Standby failover pair for a zero downtime upgrade.

Upgrade an Active/Standby Failover Pair Using the Firepower Chassis Manager

This section describes how to upgrade the ASA bundle, which includes both ASA and ASDM, for an Active/Standby failover pair. You will upload the package from your management computer.

Before you begin

You need to determine which unit is active and which is standby: connect ASDM to the active ASA IP address. The active unit always owns the active IP address. Then choose **Monitoring** > **Properties** > **Failover** > **Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.

Procedure

Step 1 If you previously set a non-default ASDM image in the ASA configuration, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) Connect to ASDM on the *active* unit.
b) In the main ASDM application window, choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
c) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.
d) Click **Apply**
e) Click the **Save** icon on the toolbar to save your configuration changes.

f) Quit ASDM.

Step 2 Upgrade the *standby* unit.

a) Connect to the Firepower Chassis Manager on the *standby* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image** to upload the new package from your management computer.
d) Click **Choose File** to navigate to and select the package that you want to upload.
e) Click **Upload**.

The selected package is uploaded to the chassis. The **Upload Image** dialog box shows the upload status. Wait for the **Success** dialog box, and click **OK**. After completing the upload, the integrity of the image is automatically verified.

f) Click the **Upgrade** icon to the right of the new package.
g) Click **Yes** to confirm that you want to proceed with installation.

There is no indicator that the new package is being loaded. You will still see the Firepower Chassis Manager at the beginning of the upgrade process. When the system reboots, you will be logged out. You must wait for the system to come back up before you can log in to the Firepower Chassis Manager. The reboot process takes approximately 20 minutes. After the reboot, you will see the login screen.

Step 3 Make the unit that you just upgraded the active unit so that traffic flows to the upgraded unit.

a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.
b) Force the standby unit to become active by choosing **Monitoring** > **Properties** > **Failover** > **Status**, and clicking **Make Active**.

Step 4 Upgrade the former *active* unit.

a) Connect to the Firepower Chassis Manager on the former *active* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image** to upload the new package from your management computer.
d) Click **Choose File** to navigate to and select the package that you want to upload.
e) Click **Upload**.

The selected package is uploaded to the chassis. The **Upload Image** dialog box shows the upload status. Wait for the **Success** dialog box, and click **OK**. After completing the upload, the integrity of the image is automatically verified.

f) Click the **Upgrade** icon to the right of the new package.
g) Click **Yes** to confirm that you want to proceed with installation.

There is no indicator that the new package is being loaded. You will still see the Firepower Chassis Manager at the beginning of the upgrade process. When the system reboots, you will be logged out. You must wait for the system to come back up before you can log in to the Firepower Chassis Manager. The reboot process takes approximately 20 minutes. After the reboot, you will see the login screen.

Upgrade an Active/Standby Failover Pair Using the FXOS CLI

This section describes how to upgrade the ASA bundle, which includes both ASA and ASDM, for an Active/Standby failover pair. You can use FTP, SCP, SFTP, or TFTP to copy the package to the Firepower 2100 chassis.

Before you begin

You need to determine which unit is active and which is standby. To determine the failover status, look at the ASA prompt; you can configure the ASA prompt to show the failover status and priority (primary or secondary), which is useful to determine which unit you are connected to. See the prompt command. However, the FXOS prompt is not aware of ASA failover. Alternatively, enter the ASA **show failover** command to view this unit's status and priority (primary or secondary).

Procedure

Step 1 If you previously set a non-default ASDM image in the ASA configuration, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) Connect to the FXOS CLI on the *active* unit, either the console port (preferred) or using SSH.

b) Connect to ASA.

connect asa

Example:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

c) Access privileged EXEC mode, and then global configuration mode.

enable

configure terminal

d) Set the ASDM image.

asdm image disk0:/asdm.bin

e) Save the configuration.

write memory

f) Return to the FXOS console by entering **Ctrl+a**, **d**.

Step 2 Upgrade the *standby* unit.

a) Connect to the FXOS CLI on the *standby* unit, either the console port (preferred) or using SSH.

b) Enter firmware mode.

scope firmware

Example:

```
2110-sec# scope firmware
2110-sec /firmware#
```

c) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

Example:

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) Monitor the download process.

show download-task

Example:

```
2110-sec /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

e) When the new package finishes downloading (**Downloaded** state), boot the package. View the version number of the new package.

show package

Example:

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

f) Install the package.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the ASA image and reboots.

Example:

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

g) Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the ASA to come up (5 minutes). Wait until you see the following messages:

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Step 3 Make the unit that you just upgraded the active unit so that traffic flows to the upgraded unit.

a) Connect to the standby ASA CLI from FXOS.

connect asa

enable

Example:

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: *****
asa/stby/sec#
```

b) Force to the standby unit to become active.

failover active

Example:

```
asa/stby/sec> failover active
asa/act/sec#
```

c) To return to the FXOS console, enter **Ctrl+a**, **d**.

Step 4 Upgrade the former *active* unit.

a) Connect to the FXOS CLI on the former *active* unit, either the console port (preferred) or using SSH.

b) Enter firmware mode.

scope firmware

Example:

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

Example:

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) Monitor the download process.

show download-task

Example:

```
2110-pri /firmware # show download
```

```
Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) When the new package finishes downloading (**Downloaded** state), boot the package. View the version number of the new package.

show package

Example:

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) Install the package.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the ASA image and reboots.

Example:

```
2110-pri /firmware # scope auto-install
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

g) Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the ASA to come up (5 minutes). Wait until you see the following messages:

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Upgrade an Active/Active Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade the Active/Active failover pair for a zero downtime upgrade.

Upgrade an Active/Active Failover Pair Using the Firepower Chassis Manager

This section describes how to upgrade the ASA bundle, which includes both ASA and ASDM, for an Active/Active failover pair. You will upload the package from your management computer.

Procedure

Step 1 Make both failover groups active on the *primary* unit.

a) Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.
b) Choose **Monitoring** > **Failover** > **Failover Group 2**, and click **Make Active**.
c) Stay connected to ASDM on this unit for later steps.

Step 2 If you previously set a non-default ASDM image in the ASA configuration, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) In the main ASDM application window on the primary unit, choose **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration**.
b) For the **ASDM Image File Path**, enter **disk0:/asdm.bin**.
c) Click **Apply**
d) Click the **Save** icon on the toolbar to save your configuration changes.

Step 3 Upgrade the *secondary* unit.

a) Connect to the Firepower Chassis Manager on the *secondary* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image** to upload the new package from your management computer.
d) Click **Choose File** to navigate to and select the package that you want to upload.
e) Click **Upload**.

The selected package is uploaded to the chassis. The **Upload Image** dialog box shows the upload status. Wait for the **Success** dialog box, and click **OK**. After completing the upload, the integrity of the image is automatically verified.

f) Click the **Upgrade** icon to the right of the new package.
g) Click **Yes** to confirm that you want to proceed with installation.

There is no indicator that the new package is being loaded. You will still see the Firepower Chassis Manager at the beginning of the upgrade process. When the system reboots, you will be logged out. You must wait for the system to come back up before you can log in to the Firepower Chassis Manager. The reboot process takes approximately 20 minutes. After the reboot, you will see the login screen.

Step 4 Make both failover groups active on the secondary unit. In ASDM on the *primary* unit, choose **Monitoring** > **Failover** > **Failover Group 1**, and click **Make Standby**.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

Step 5 Upgrade the *primary* unit.

a) Connect to the Firepower Chassis Manager on the *primary* unit.
b) Choose **System** > **Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
c) Click **Upload Image** to upload the new package from your management computer.
d) Click **Choose File** to navigate to and select the package that you want to upload.
e) Click **Upload**.

The selected package is uploaded to the chassis. The **Upload Image** dialog box shows the upload status. Wait for the **Success** dialog box, and click **OK**. After completing the upload, the integrity of the image is automatically verified.

f) Click the **Upgrade** icon to the right of the new package.
g) Click **Yes** to confirm that you want to proceed with installation.

There is no indicator that the new package is being loaded. You will still see the Firepower Chassis Manager at the beginning of the upgrade process. When the system reboots, you will be logged out. You must wait for the system to come back up before you can log in to the Firepower Chassis Manager. The reboot process takes approximately 20 minutes. After the reboot, you will see the login screen.

Step 6 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring > Failover > Failover Group #** pane.

Upgrade an Active/Active Failover Pair Using the FXOS CLI

This section describes how to upgrade the ASA bundle, which includes both ASA and ASDM, for an Active/Active failover pair. You can use FTP, SCP, SFTP, or TFTP to copy the package to the Firepower 2100 chassis.

Procedure

Step 1 If you previously set a non-default ASDM image in the ASA configuration, then reset it to the image that came with your image bundle.

The image bundle includes the ASDM image, and when you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA after reloading because they have the same name (**asdm.bin**). If you manually chose a different ASDM image that you uploaded (for example, **asdm-7191.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should reconfigure the ASA to use the bundled ASDM image.

a) Connect to the FXOS CLI on the *primary* unit, either the console port (preferred) or using SSH.

b) Connect to ASA.

connect asa

Example:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

c) Access privileged EXEC mode, and then global configuration mode.

enable

configure terminal

d) Set the ASDM image.

asdm image disk0:/asdm.bin

e) Save the configuration.

write memory

f) Return to the FXOS console by entering **Ctrl+a**, **d**.

Step 2 Connect to the FXOS CLI on the *secondary* unit, either the console port (preferred) or using SSH.

Step 3 Make both failover groups active on the primary unit.

a) Connect to the ASA CLI from FXOS.

connect asa

enable

The enable password is blank by default.

Example:

```
2110-sec# connect asa
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/act/sec> enable
Password: <blank>
asa/act/sec#
```

b) Make both failover groups active on the primary unit.

no failover active group 1

no failover active group 2

Example:

```
asa/act/sec# no failover active group 1
asa/act/sec# no failover active group 2
```

c) Enter **Ctrl+a**, **d** to return to the FXOS console.

Step 4 Upgrade the *secondary* unit.

a) In FXOS, enter firmware mode.

scope firmware

Example:

```
2110-sec# scope firmware
2110-sec /firmware#
```

b) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp:**//*username@server*/[*path*/]*image_name*
- **scp:**//*username@server*/[*path*/]*image_name*
- **sftp:**//*username@server*/[*path*/]*image_name*
- **tftp:**//*server*[**:***port*]/[*path*/]*image_name*

Example:

```
2110-sec /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

c) Monitor the download process.

show download-task

Example:

```
2110-sec /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
```

```
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-sec /firmware #
```

d) When the new package finishes downloading (**Downloaded** state), boot the package. View the version number of the new package.

show package

Example:

```
2110-sec /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-sec /firmware #
```

e) Install the package.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the ASA image and reboots.

Example:

```
2110-sec /firmware # scope auto-install
2110-sec /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-sec /firmware/auto-install #
```

f) Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the ASA to come up (5 minutes). Wait until you see the following messages:

```
2110-sec#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Step 5 Make both failover groups active on the secondary unit.

a) Connect to the ASA CLI from FXOS.

connect asa

enable

The enable password is blank by default.

Example:

```
2110-sec# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
asa/stby/sec> enable
Password: <blank>
asa/stby/sec#
```

b) Make both failover groups active on the secondary unit.

failover active group 1

failover active group 2

Example:

```
asa/stby/sec# failover active group 1
asa/act/sec# failover active group 2
```

c) Enter **Ctrl+a**, **d** to return to the FXOS console.

Step 6 Upgrade the *primary* unit.

a) Connect to the FXOS CLI on the *primary* unit, either the console port (preferred) or using SSH.

b) Enter firmware mode.

scope firmware

Example:

```
2110-pri# scope firmware
2110-pri /firmware#
```

c) Download the package.

download image *url*

Specify the URL for the file being imported using one of the following:

- **ftp://***username@server*/[*path*/]*image_name*
- **scp://***username@server*/[*path*/]*image_name*
- **sftp://***username@server*/[*path*/]*image_name*
- **tftp://***server*[**:***port*]/[*path*/]*image_name*

Example:

```
2110-pri /firmware# download image tftp://10.88.29.181/cisco-asa-fp2k.9.8.2.2.SPA
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

d) Monitor the download process.

show download-task

Example:

```
2110-pri /firmware # show download

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-asa-fp2k.9.8.2.SPA
              Tftp     10.88.29.181             0                 Downloaded
    cisco-asa-fp2k.9.8.2.2.SPA
              Tftp     10.88.29.181             0                 Downloading
2110-pri /firmware #
```

e) When the new package finishes downloading (**Downloaded** state), boot the package. View the version number of the new package.

show package

Example:

```
2110-pri /firmware # show package
Name                                       Package-Vers
------------------------------------------ ------------
cisco-asa-fp2k.9.8.2.SPA                   9.8.2
cisco-asa-fp2k.9.8.2.2.SPA                 9.8.2.2
2110-pri /firmware #
```

f) Install the package.

scope auto-install

install security-pack version *version*

In the **show package** output, copy the **Package-Vers** value for the **security-pack version** number. The chassis installs the ASA image and reboots.

Example:

```
2110-pri /firmware # scope auto-install
```

```
2110-pri /firmware/auto-install # install security-pack version 9.8.3

The system is currently installed with security software package 9.8.2, which has:
   - The platform version: 2.2.2.52
   - The CSP (asa) version: 9.8.2
If you proceed with the upgrade 9.8.3, it will do the following:
   - upgrade to the new platform version 2.2.2.97
   - upgrade to the CSP asa version 9.8.3
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 9.8.3
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
2110-pri /firmware/auto-install #
```

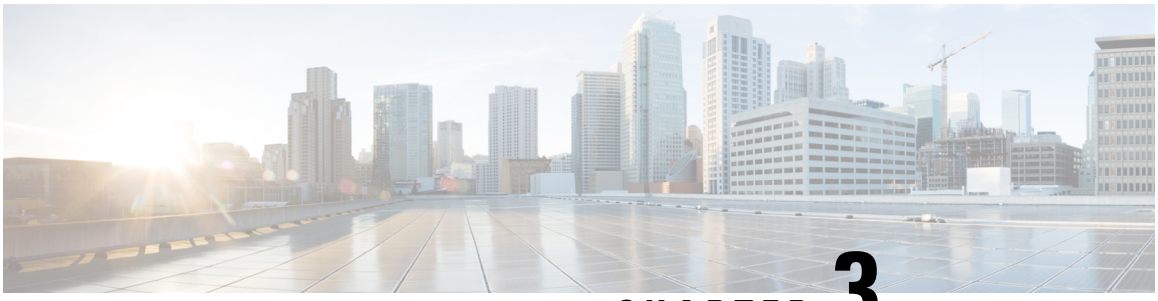
g) Wait for the chassis to finish rebooting (5-10 minutes).

Although FXOS is up, you still need to wait for the ASA to come up (5 minutes). Wait until you see the following messages:

```
2110-pri#
Cisco ASA: CMD=-install, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Verifying signature for cisco-asa.9.8.2.2 ...
Verifying signature for cisco-asa.9.8.2.2 ... success

Cisco ASA: CMD=-start, CSP-ID=cisco-asa.9.8.2.2__asa_001_JAD20280BW90MEZR11, FLAG=''
Cisco ASA starting ...
Registering to process manager ...
Cisco ASA started successfully.
[…]
```

Step 7 If the failover groups are configured with the ASA **preempt** command, they 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 by connecting to the ASA CLI and using the **failover active group** command.



CHAPTER 3

Downgrade the ASA

In many cases, you can downgrade your ASA software and restore a backup configuration from the previous software version. The method of downgrading depends on your ASA platform.

- Guidelines and Limitations for Downgrading, on page 145
- Incompatible Configuration Removed After Downgrading, on page 146
- Downgrade the ASA Appliance, on page 147
- Downgrade the Firepower 2100 in Platform Mode, on page 148
- Downgrade the Firepower 4100/9300, on page 148
- Downgrade the ISA 3000 or ASA 5500-X , on page 149

Guidelines and Limitations for Downgrading

See the following guidelines before downgrading:

- **There is no official Zero Downtime Downgrade support for clustering**—However, in some cases, Zero Downtime Downgrading will work. If you encounter issues, you need to reload your cluster units, which results in downtime.
- **For the ASA Virtual, you cannot downgrade from 9.24+ to a pre-9.24 version**—After you upgrade to 9.24 or later, you cannot downgrade to a version earlier than 9.24.
- **Downgrade issue from 9.22 or later**—If you disable the USB port using the usb-port disable command, but then downgrade to an earlier release, the port will remain disabled, and you cannot re-enable it without erasing the NVRAM (the FXOS local-mgmt **erase secure all** command).
- **Downgrade issue from 9.18 or later**—There is a behavior change in 9.18 where the **access-group** command will be listed before its **access-list** commands. If you downgrade, the **access-group** command will be rejected because it has not yet loaded the **access-list** commands. This outcome occurs even if you had previously enabled the **forward-reference enable** command, because that command is now removed. Before you downgrade, be sure to copy all **access-group** commands manually, and then after downgrading, re-enter them.
- **VPN tunnels are replicated to the standby unit even if the standby unit is running a version of software that does not support the Ciphersuite that the original tunnel negotiated**—This scenario occurs when downgrading. In this case, disconnect your VPN connection and reconnect.

- **Downgrade ASA Virtual with permanent license reservation from Version 9.20(4) to earlier versions** —We recommend that you perform these steps to prevent the permanent license reservation from being unregistered:

  1. Unregister the permanent license reservation.
  2. Downgrade the ASA Virtual.
  3. Register the permanent license reservation again.

  You need to perform these steps as Smart Transport is the default from Version 9.20.4 and later, while Smart Call Home is default in Version 9.20.3 and earlier.

- **Downgrade ASA Virtual with flexible permanent license reservation from Version 9.23(1) to earlier versions** —We recommend that you do not downgrade an ASA Virtual with Version 9.23(1) and flexible permanent license reservation. The license registration status will become **Unregistered**.

Incompatible Configuration Removed After Downgrading

When you downgrade to an old version, commands that were introduced in later versions will be removed from the configuration. There is no automated way to check the configuration against the target version before you downgrade. You can view when new commands were added in ASA new features by release.

You can view rejected commands *after* you downgrade using the **show startup-config errors** command. If you can perform a downgrade on a lab device, you can preview the effects using this command before you perform the downgrade on a production device.

In some cases, the ASA migrates commands to new forms automatically when you upgrade, so depending on your version, even if you did not manually configure new commands, the downgrade could be affected by configuration migrations. We recommend that you have a backup of your old configuration that you can use when you downgrade. In the case of upgrading to 8.3, a backup is automatically created (<old_version>_startup_cfg.sav). Other migrations do not create back-ups. See Version-Specific Guidelines and Migrations, on page 1 for more information about automatic command migrations that could affect downgrading.

See also known downgrade issues in Guidelines and Limitations for Downgrading, on page 145.

For example, an ASA running version 9.8(2) includes the following commands:

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

When you downgrade to 9.0(4), you will see the following errors on startup:

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                  ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                               ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

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

In this example, support for **sctp** in the **access-list extended** command was added in version 9.5(2), support for **pbkdf2** in the **username** command was added in version 9.6(1), and support for **engineID** in the **snmp-server user** command was added in version 9.5(3).

Downgrade the ASA Appliance

You can downgrade the ASA software version by setting the ASA version to the old version, restoring the backup configuration to the startup configuration, and then reloading. This procedure applies to the following models:

- Firewall 200
- Firepower 1000
- Secure Firewall 1200
- Firepower 2100
- Secure Firewall 3100
- Secure Firewall 4200
- Firewall 6100

Before you begin

This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration. If you do not restore the old configuration, you may have incompatible commands representing new or changed features. Any new commands will be rejected when you load the old software version.

Procedure

Step 1 Load the old ASA software version using the upgrade procedure in Upgrade the ASA Appliance, on page 51 for standalone, failover, or clustering deployments. In this case, specify the old ASA version instead of a new version. **Important:** Do *not* reload the ASA yet.

Step 2 At the ASA CLI, copy the backup ASA configuration to the startup configuration. For failover, perform this step on the active unit. This step replicates the command to the standby unit.

copy *old_config_url* **startup-config**

It's important that you do not save the running configuration to the startup configuration using **write memory**; this command will overwrite your backup configuration.

Example:

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

Step 3 Reload the ASA.

ASA CLI

reload

ASDM

Choose **Tools** > **System Reload**.

Downgrade the Firepower 2100 in Platform Mode

You can downgrade the ASA software version by restoring the backup configuration to the startup configuration, setting the ASA version to the old version, and then reloading.

Before you begin

This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration. If you do not restore the old configuration, you may have incompatible commands representing new or changed features. Any new commands will be rejected when you load the old software version.

Procedure

Step 1 At the ASA CLI, copy the backup ASA configuration to the startup configuration. For failover, perform this step on the active unit. This step replicates the command to the standby unit.

copy *old_config_url* **startup-config**

It's important that you do not save the running configuration to the startup configuration using **write memory**; this command will overwrite your backup configuration.

Example:

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

Step 2 In FXOS, use the Firewall Chassis Manager or FXOS CLI to use the old ASA software version using the upgrade procedure in Upgrade the Firepower 2100 in Platform Mode, on page 126 for standalone, failover, or clustering deployments. In this case, specify the old ASA version instead of a new version.

Downgrade the Firepower 4100/9300

You can downgrade the ASA software version by restoring the backup configuration to the startup configuration, setting the ASA version to the old version, and then reloading.

Before you begin

- This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration. If you do not restore the old configuration, you may have incompatible commands representing new or changed features. Any new commands will be rejected when you load the old software version.

- Make sure the old ASA version is compatibile with the current FXOS version. If not, downgrade FXOS as the first step before you restore the old ASA configuration. Just make sure the downgraded FXOS is also compatible with the current ASA version (before you downgrade it). If you cannot achieve compatibility, we suggest you do not perform a downgrade.

Procedure

Step 1 At the ASA CLI, copy the backup ASA configuration to the startup configuration. For failover or clustering, perform this step on the active/control unit. This step replicates the command to the standby/data units.

copy *old_config_url* **startup-config**

It's important that you do not save the running configuration to the startup configuration using **write memory**; this command will overwrite your backup configuration.

Example:

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

Step 2 In FXOS, use the Firewall Chassis Manager or FXOS CLI to use the old ASA software version using the upgrade procedure in Upgrade the Firepower 4100/9300, on page 71 for standalone, failover, or clustering deployments. In this case, specify the old ASA version instead of a new version.

Step 3 If you are also downgrading FXOS, use the Firewall Chassis Manager or FXOS CLI to set the old FXOS software version to be the current version using the upgrade procedure in Upgrade the Firepower 4100/9300, on page 71 for standalone, failover, or clustering deployments.

Downgrade the ISA 3000 or ASA 5500-X

The downgrade feature provides a shortcut for completing the following functions on ISA 3000 models:

- Clearing the boot image configuration (**clear configure boot**).
- Setting the boot image to be the old image (**boot system**).
- (Optional) Entering a new activation key (**activation-key**).
- Saving the running configuration to startup (**write memory**). This sets the BOOT environment variable to the old image, so when you reload, the old image is loaded.
- Copying the old configuration backup to the startup configuration (**copy** *old_config_url* **startup-config**).
- Reloading (**reload**).

Before you begin

- This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration.

Procedure

Step 1 **ASA CLI:** Downgrade the software and restore the old configuration.

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

Example:

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

The **/noconfirm** option downgrades without prompting. The *image_url* is the path to the old image on disk0, disk1, tftp, ftp, or smb. The *old_config_url* is the path to the saved, pre-migration configuration. If you need to revert to a pre-8.3 activation key, then you can enter the old activation key.

Step 2 **ASDM:** Choose **Tools** > **Downgrade Software** .

The Downgrade Software dialog box appears.

Step 3 For the **ASA Image**, click **Select Image File**.

The **Browse File Locations** dialog box appears.

Step 4 Click one of the following radio buttons:

- **Remote Server**—Choose ftp, smb, or http from the drop-down list, and type the path to the old image file.
- **Flash File System**—Click **Browse Flash** to choose the old image file on the local flash file system.

Step 5 For the **Configuration**, click **Browse Flash** to choose the pre-migration configuration file.

Step 6 (Optional) In the **Activation Key** field, enter the old activation key if you need to revert to a pre-8.3 activation key.

Step 7 Click **Downgrade**.