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

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.

9.22 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**.

9.20 Guidelines

- **OSPF 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), OSPF **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 OSPF to use route maps that specify an ACL in the **match ip address** command.

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**.

9.15 Guidelines

- **No support in ASA 9.15(1) and later for the ASA 5525-X, ASA 5545-X, and ASA 5555-X**—ASA 9.14(x) is the last supported version. For the ASA FirePOWER module, the last supported version is 6.6.
- **Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1)**—Limited support will continue on releases prior to 9.17(1).
- **For the Firepower 1010, invalid VLAN IDs can cause problems**—Before you upgrade to 9.15(1), make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See CSCvw33057 for more information.
- **SAMLv1 feature deprecation**—Support for SAMLv1 is deprecated.
- **Low-Security Cipher Removal in ASA 9.15(1)**—Support for the following less secure ciphers used by IKE and IPsec have been removed:
  - Diffie-Hellman groups: 2 and 24
  - Encryption algorithms: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256, NULL, ESP-3DES, ESP-DES, ESP-MD5-HMAC
  - Hash algorithms: MD5

Note Low-security SSH and SSL ciphers have not yet been removed.

Before you upgrade from an earlier version of ASA to Version 9.15(1), you must update your VPN configuration to use the ciphers supported in 9.15(1), or else the old configuration will be rejected. When the configuration is rejected, one of the following actions will occur, depending on the command:

- The command will use the default cipher.
- The command will be removed.

Fixing your configuration before upgrading is especially important for clustering or failover deployments. For example, if the secondary unit is upgraded to 9.15(1), and the removed ciphers are synced to this unit from the primary, then the secondary unit will reject the configuration. This rejection might cause unexpected behavior, like failure to join the cluster.

IKEv1: The following subcommands are removed:

- **crypto ikev1 policy** *priority*:
  - **hash md5**

- **encryption 3des**
- **encryption des**
- **group 2**

IKEv2: The following subcommands are removed:

- **crypto ikev2 policy** *priority*:
  - **prf md5**
  - **integrity md5**
  - **group 2**
  - **group 24**
  - **encryption 3des**
  - **encryption des**
  - **encryption null**

IPsec: The following subcommands are removed:

- **crypto ipsec ikev1 transform-set** *name* **esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal** *name*
  - **protocol esp integrity md5**
  - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile** *name*
  - **set pfs group2 group24**

Crypto Map: The following subcommands are removed:

- **crypto map** *name sequence* **set pfs group2**
- **crypto map** *name sequence* **set pfs group24**
- **crypto map** *name sequence* **set ikev1 phase1-mode aggressive group2**

- **Re-introduction of CRL Distribution Point configuration**—The static CDP URL configuration option, that was removed in 9.13(1), was re-introduced in the **match-certificate** command.
- **Restoration of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was restored.

  The following subcommands were restored:

  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**

- **revocation-check ocsp crl none**

9.14 Guidelines

- **ASDM signed-image support in 9.14(4.14)/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)
- **ASDM Cisco.com Upgrade Wizard failure on Firepower 1000 and 2100 in Appliance mode**—The ASDM Cisco.com Upgrade Wizard does not work for upgrading to 9.14 (**Tools > Check for ASA/ASDM Updates**). The wizard can upgrade ASDM from 7.13 to 7.14, but the ASA image upgrade is grayed out. (CSCvt72183) As a workaround, use one of the following methods:
  - Use **Tools > Upgrade Software from Local Computer** for both ASA and ASDM. Note that the ASDM image (7.14(1)) in the 9.14(1) bundle also has the bug CSCvt72183; you should download the newer 7.14(1.46) image to enable correct functioning of the wizard.
  - Use **Tools > Check for ASA/ASDM Updates** to upgrade to ASDM 7.14 (the version will be 7.14(1.46); then use the new ASDM to upgrade the ASA image. Note that you may see a **Fatal Installation Error**; in this case, click **OK**. You must then set the boot image manually on the **Configuration** > **Device Management** > **System Image/Configuration** > **Boot Image/Configuration** screen. Save the configuration and reload the ASA.
- **For Failover pairs in 9.14(1)+, the ASA no longer shares SNMP client engine data with its peer.**
- **No support in ASA 9.14(1)+ for cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs (**CSCvy22526**)**.
- **Upgrade issue for 9.14(4)24 and RADIUS challenges for AnyConnect mobile users**—To restore RADIUS functionality, upgrade to 9.18(4)22 or later.
- **Upgrading the Firepower 2100 in Platform mode**—When you upgrade to 9.14 or later, if your EtherChannel (port-channel) was disabled at the time of upgrade, then you will need to manually enable both the EtherChannel and its member interfaces after upgrade.
- **Downgrade issue for the Firepower 2100 in Platform mode from 9.13/9.14 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 or 9.14 that you converted to Platform mode: If you downgrade to 9.12 or earlier, you will not be able to configure new interfaces or edit existing interfaces in FXOS (note that 9.12 and earlier only supports Platform mode). You either need to restore your version to 9.13 or later, or you need to clear your configuration using the FXOS erase configuration command. This problem does not occur if you originally upgraded to 9.13 or 9.14 from an earlier release; only fresh installations are affected, such as a new device or a re-imaged device. (CSCvr19755)
- **The tls-proxy keyword, and support for SCCP/Skinny encrypted inspection, was removed** from the **inspect skinny** command.
- **ASDM Upgrade Wizard**—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. Note that ASDM 7.13 and 7.14 did not support the ASA 5512-X, 5515-X, 5585-X, or ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.

9.13 Guidelines

- **ASAv requires 2GB memory in 9.13(1) and later**—Beginning with 9.13(1), the minimum memory requirement for the ASAv is 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version. You must adjust the memory size before upgrading. See the ASAv Getting Started Guide for information about the resource allocations (vCPU and memory) supported in version 9.13(1).
- **Downgrade issue for the Firepower 2100 in Platform mode from 9.13 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 that you converted to Platform mode: If you downgrade to 9.12 or earlier, you will not be able to configure new interfaces or edit existing interfaces in FXOS (note that 9.12 and earlier only supports Platform mode). You either need to restore your version to 9.13, or you need to clear your configuration using the FXOS erase configuration command. This problem does not occur if you originally upgraded to 9.13 from an earlier release; only fresh installations are affected, such as a new device or a re-imaged device. (CSCvr19755)
- **Cluster control link MTU change in 9.13(1)**—Starting in 9.13(1), many cluster control packets are larger than they were in previous releases. The recommended MTU for the cluster control link has always been 1600 or greater, and this value is appropriate. However, if you set the MTU to 1600 but then failed to match the MTU on connecting switches (for example, you left the MTU as 1500 on the switch), then you will start seeing the effects of this mismatch with dropped cluster control packets. Be sure to set all devices on the cluster control link to the same MTU, specifically 1600 or higher.
- **Beginning with 9.13(1), the ASA establishes an LDAP/SSL connection only if one of the following certification criteria is satisfied**:
  - The LDAP server certificate is trusted (exists in a trustpoint or the ASA trustpool) and is valid.
  - A CA certificate from servers issuing chain is trusted (exists in a trustpoint or the ASA trustpool) and all subordinate CA certificates in the chain are complete and valid.
- **Local CA server is removed in 9.13(1)**—When the ASA is configured as local CA server, it can issue digital certificates, publish Certificate Revocation Lists (CRLs), and securely revoke issued certificates. This feature has become obsolete and hence the **crypto ca server** command is removed.
- **Removal of CRL Distribution Point commands**—The static CDP URL configuration commands, namely **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. The CDP URL was moved to match certificate command.

Note The CDP URL configuration was enhanced to allow multiple instances of the CDP override for a single map (refer CSCvu05216).

- **Removal of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was removed.

  The following subcommands are removed:
  - **revocation-check crl none**
  - **revocation-check ocsp none**
  - **revocation-check crl ocsp none**
  - **revocation-check ocsp crl none**

Thus, after an upgrade, any revocation-check command that is no longer supported will transition to the new behavior by ignoring the trailing none.

Note These commands were restored later (refer CSCtb41710).

- **Low-Security Cipher Deprecation**— Several encryption ciphers used by the ASA IKE, IPsec, and SSH modules are considered insecure and have been deprecated. They will be removed in a later release.

  IKEv1: The following subcommands are deprecated:

  - **crypto ikev1 policy** *priority*:
    - **hash md5**
    - **encryption 3des**
    - **encryption des**
    - **group 2**
    - **group 5**

  IKEv2: The following subcommands are deprecated:

  - **crypto ikev2 policy** *priority*
    - **integrity md5**
    - **prf md5**
    - **group 2**
    - **group 5**
    - **group 24**
    - **encryption 3des**
    - **encryption des** (this command is still available when you have the DES encryption license only)
    - **encryption null**

  IPsec: The following commands are deprecated:

  - **crypto ipsec ikev1 transform-set** ***name*** **esp-3des esp-des esp-md5-hmac**
  - **crypto ipsec ikev2 ipsec-proposal** ***name***
    - **protocol esp integrity md5**
    - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
  - **crypto ipsec profile** ***name***
    - **set pfs group2 group5 group24**

SSH: The following commands are deprecated:

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
- **ssh key-exchange group dh-group1-sha1**

SSL: The following commands are deprecated:

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

Crypto Map: The following commands are deprecated:

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group5**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group5**

- **In 9.13(1), Diffie-Hellman Group 14 is now the default** for the **group** command under **crypto ikev1 policy**, **ssl dh-group**, and **crypto ikev2 policy**for IPsec PFS using **crypto map set pfs**, **crypto ipsec profile**, **crypto dynamic-map set pfs**, and **crypto map set ikev1 phase1-mode**. The former default Diffie-Hellman group was Group 2.

  When you upgrade from a pre-9.13(1) release, if you need to use the old default (Diffie-Hellman Group 2), then you must *manually* configure the DH group as **group 2** or else your tunnels will default to Group 14. Because group 2 will be removed in a future release, you should move your tunnels to group 14 as soon as possible.

9.12 Guidelines

- **ASDM signed-image support in 9.12(4.50)/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)
- ASDM Upgrade Wizard—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.
- SSH security improvements and new defaults in 9.12(1)—See the following SSH security improvements:
  - SSH version 1 is no longer supported; only version 2 is supported. The **ssh version 1** command will be migrated to **ssh version 2**.
  - Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default (**ssh key-exchange group dh-group14-sha256**). The former default was Group 1 SHA1. Make sure that your SSH client supports Diffie-Hellman Group 14 SHA256. If it does not, you may see an

error such as "Couldn't agree on a key exchange algorithm." For example, OpenSSH supports Diffie-Hellman Group 14 SHA256.

- HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha1 and hmac-sha2-256 as defined by the **ssh cipher integrity high** command). The former default was the medium set.

- The NULL-SHA TLSv1 cipher is deprecated and removed in 9.12(1)—Because NULL-SHA doesn't offer encryption and is no longer considered secure against modern threats, it will be removed when listing supported ciphers for TLSv1 in the output of **tls-proxy** mode commands/options and **show ssl ciphers all**. The **ssl cipher tlsv1 all** and **ssl cipher tlsv1 custom NULL-SHA** commands will also be deprecated and removed.
- The default trustpool is removed in 9.12(1)—In order to comply with PSB requirement, SEC-AUT-DEFROOT, the "default" trusted CA bundle is removed from the ASA image. As a result, **crypto ca trustpool import default** and **crypto ca trustpool import clean default** commands are also removed along with other related logic. However, in existing deployments, certificates that were previously imported using these command will remain in place.
- The **ssl encryption** command is removed in 9.12(1)—In 9.3(2) the deprecation was announced and replaced by **ssl cipher**. In 9.12(1), **ssl encryption** is removed and no longer supported.

9.10 Guidelines

- Due to an internal change, the ASDM Upgrade 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.

9.9 Guidelines

- ASA 5506-X memory issues with large configurations on 9.9(2) and later—If you upgrade to 9.9(2) or later, parts of a very large configuration might be rejected due to insufficient memory with the following message: "ERROR: Insufficient memory to install the rules". One option is to enter the **object-group-search access-control** command to improve memory usage for ACLs; your performance might be impacted, however. Alternatively, you can downgrade to 9.9(1).

9.8 Guidelines

- **ASDM signed-image support in 9.8(4.45)/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)
- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- Do not upgrade to 9.8(1) for ASAv on Amazon Web Services--Due to CSCve56153, you should not upgrade to 9.8(1). After upgrading, the ASAv becomes unreachable. Upgrade to 9.8(1.5) or later instead.

9.7 Guidelines

- Upgrade issue with 9.7(1) to 9.7(1.x) and later for VTI and VXLAN VNI—If you configure both Virtual Tunnel Interfaces (VTIs) and VXLAN Virtual Network Identifier (VNI) interfaces, then you cannot perform a zero downtime upgrade for failover; connections on these interface types will not replicate to the standby unit until both units are on the same version. (CSCvc83062)

9.6 Guidelines

- (ASA 9.6(2) through 9.7(x)) Upgrade impact when using SSH public key authentication—Due to updates to SSH authentication, additional configuration is required to enable SSH public key authentication; as a result, existing SSH configurations using public key authentication no longer work after upgrading. Public key authentication is the default for the ASAv on Amazon Web Services (AWS), so AWS users will see this issue. To avoid loss of SSH connectivity, you can update your configuration *before* you upgrade. Or you can use ASDM after you upgrade (if you enabled ASDM access) to fix the configuration.

Note The original behavior was restored in 9.8(1).

Sample original configuration for a username "admin":

```
username admin nopassword privilege 15
username admin attributes
  ssh authentication publickey 55:06:47:eb:13:75:fc:5c:a8:c1:2c:bb:
  07:80:3a:fc:d9:08:a9:1f:34:76:31:ed:ab:bd:3a:9e:03:14:1e:1b hashed
```

To use the **ssh authentication** command, before you upgrade, enter the following commands:

```
aaa authentication ssh console LOCAL
username admin password <password> privilege 15
```

We recommend setting a password for the username as opposed to keeping the **nopassword** keyword, if present. The **nopassword** keyword means that *any* password can be entered, not that *no* password can be entered. Prior to 9.6(2), the **aaa** command was not required for SSH public key authentication, so the **nopassword** keyword was not triggered. Now that the **aaa** command is required, it automatically also allows regular password authentication for a **username** if the **password** (or **nopassword**) keyword is present.

After you upgrade, the **username** command no longer requires the **password** or **nopassword** keyword; you can require that a user cannot enter a password. Therefore, to force public key authentication only, re-enter the **username** command:

```
username admin privilege 15
```

- Upgrade impact when upgrading the ASA on the Firepower 9300— Due to license entitlement naming changes on the back-end, when you upgrade to ASA 9.6(1)/FXOS 1.1(4), the startup configuration may not parse correctly upon the initial reload; configuration that corresponds to add-on entitlements is rejected.

For a standalone ASA, after the unit reloads with the new version, wait until all the entitlements are processed and are in an "Authorized" state (**show license all** or **Monitoring > Properties > Smart License**), and simply reload again (**reload** or **Tools > System Reload**) *without* saving the configuration. After the reload, the startup configuration will be parsed correctly.

For a failover pair if you have any add-on entitlements, follow the upgrade procedure in the FXOS release notes, but reset failover after you reload each unit (**failover reset** or **Monitoring > Properties > Failover > Status**, **Monitoring > Failover > System**, or **Monitoring > Failover > Failover Group**, and then click **Reset Failover**).

For a cluster, follow the upgrade procedure in the FXOS release notes; no additional action is required.

9.5 Guidelines and Migration

- 9.5(2) New Carrier License—The new Carrier license replaces the existing GTP/GPRS license, and also includes support for SCTP and Diameter inspection. For the Firepower 9300 ASA security module, the **feature mobile-sp** command will automatically migrate to the **feature carrier** command.
- 9.5(2) E-mail proxy commands deprecated—In ASA Version 9.5(2), the e-mail proxy commands (**imap4s**, **pop3s**, **smtps**) and subcommands are no longer supported.
- 9.5(2) CSD commands deprecated or migrated—In ASA Version 9.5(2), the CSD commands (**csd image**, **show webvpn csd image**, **show webvpn csd**, **show webvpn csd hostscan**, **show webvpn csd hostscan image**) are no longer supported.

  The following CSD commands will migrate: **csd enable** migrates to **hostscan enable**; **csd hostscan image** migrates to **hostscan image**.
- 9.5(2) Select AAA commands deprecated—In ASA Version 9.5(2), these AAA commands and subcommands (**override-account-disable**, **authentication crack**) are no longer supported.
- 9.5(1) We deprecated the following command: **timeout gsn**
- ASA 5508-X and 5516-X upgrade issue when upgrading to 9.5(x) or later—Before you upgrade to ASA Version 9.5(x) or later, if you never enabled jumbo frame reservation then you must check the maximum memory footprint. Due to a manufacturing defect, an incorrect software memory limit might have been applied. If you upgrade to 9.5(x) or later before performing the below fix, then your device will crash on bootup; in this case, you must downgrade to 9.4 using ROMMON (Load an Image for the ASA 5500-X Series Using ROMMON), perform the below procedure, and then upgrade again.

  1. Enter the following command to check for the failure condition:

     ```
     ciscoasa# show memory detail | include Max memory footprint
     Max memory footprint        =    456384512
     Max memory footprint        =            0
     Max memory footprint        =    456384512
     ```

     If a value less than **456,384,512** is returned for “Max memory footprint,” then the failure condition is present, and you must complete the remaining steps before you upgrade. If the memory shown is 456,384,512 or greater, then you can skip the rest of this procedure and upgrade as normal.

  2. Enter global configuration mode:

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

3. Temporarily enable jumbo frame reservation:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: This command will take effect after the running-config
is saved and the system has been rebooted. Command accepted.
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```

Note Do not reload the ASA.

4. Save the configuration:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. Disable jumbo frame reservation:

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```

Note Do not reload the ASA.

6. Save the configuration again:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. You can now upgrade to Version 9.5(x) or later.

9.4 Guidelines and Migration

- 9.4(1) Unified Communications Phone Proxy and Intercompany Media Engine Proxy are deprecated—In ASA Version 9.4, the Phone Proxy and IME Proxy are no longer supported.

9.3 Guidelines and Migration

- 9.3(2) Transport Layer Security (TLS) version 1.2 support—We now support TLS version 1.2 for secure message transmission for ASDM, Clientless SSVPN, and AnyConnect VPN. We introduced or modified the following commands: ssl client-version, ssl server-version, ssl cipher, ssl trust-point, ssl dh-group. We deprecated the following command: ssl encryption

- 9.3(1) Removal of AAA Windows NT domain authentication—We removed NTLM support for remote access VPN users. We deprecated the following command: aaa-server protocol nt

9.2 Guidelines and Migration

Auto Update Server certificate verification

9.2(1) Auto Update Server certificate verification enabled by default. The Auto Update Server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning:

```
WARNING: The certificate provided by the auto-update servers will not be verified. In order
to verify this certificate please use the verify-certificate option.
```

The configuration will be migrated to explicitly configure no verification:

auto-update server no-verification

Upgrade impact for ASDM login

Upgrade impact for ASDM login when upgrading from a pre-9.2(2.4) release to 9.2(2.4) or later. If you upgrade from a pre-9.2(2.4) release to ASA Version 9.2(2.4) or later and you use command authorization and ASDM-defined user roles, users with Read Only access will not be able to log in to ASDM. You must change the **more** command either before or after you upgrade to be at privilege level 5; only Admin level users can make this change. Note that ASDM version 7.3(2) and later includes the **more** command at level 5 for defined user roles, but preexisting configurations need to be fixed manually.

ASDM:

1. Choose **Configuration > Device Management > Users/AAA > AAA Access > Authorization**, and click **Configure Command Privileges**.
2. Select **more**, and click **Edit**.

3. Change the **Privilege Level** to 5, and click **OK**.
4. Click **OK**, and then **Apply**.

CLI:

```
ciscoasa(config)# privilege cmd level 5 mode exec command more
```

9.1 Guidelines and Migration

- Maximum MTU Is Now 9198 Bytes—If your MTU was set to a value higher than 9198, then the MTU is automatically lowered when you upgrade. In some cases, this MTU change can cause an MTU mismatch; be sure to set any connecting equipment to use the new MTU value. The maximum MTU that the ASA can use is 9198 bytes (check for your model's exact limit at the CLI help). This value does not include the Layer 2 header. Formerly, the ASA let you specify the maximum MTU as 65535 bytes, which was inaccurate and could cause problems.

9.0 Guidelines and Migration

- **IPv6 ACL Migration**—IPv6 ACLs (**ipv6 access-list**) will be migrated to extended ACLs (**access-list extended**); IPv6 ACLs are no longer supported.

  If IPv4 and IPv6 ACLs are applied on the same direction of an interface (**access-group** command), then the ACLs are merged:

  - If both IPv4 and IPv6 ACLs are not used anywhere other than the access-group, then the name of the IPv4 ACL is used for the merged ACL; the IPv6 access-list is removed.
  - If at least one of the ACLs is used in another feature, then a new ACL is created with the name *IPv4-ACL-name_IPv6-ACL-name*; the in-use ACL(s) continue to be used for other features. ACLs not in use are removed. If the IPv6 ACL is in use for another feature, it is migrated to an extended ACL of the same name.

- **ACL Any Keyword Migration**—Now that ACLs support both IPv4 and IPv6, the **any** keyword now represents "all IPv4 and IPv6 traffic." Any existing ACLs that use the **any** keyword will be changed to use the **any4** keyword, which denotes "all IPv4 traffic."

  In addition, a separate keyword was introduced to designate "all IPv6 traffic": **any6**.

  The **any4** and **any6** keywords are not available for all commands that use the **any** keyword. For example, the NAT feature uses only the **any** keyword; any represents IPv4 traffic or IPv6 traffic depending on the context within the specific NAT command.

- **Static NAT-with-port-translation Requirement Before Upgrading**—In Version 9.0 and later, static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. This behavior is also true for Twice NAT. Moreover, traffic that does not match the source IP address of the Twice NAT rule will be dropped if it matches the destination IP address, regardless of the destination port. Therefore, before you upgrade, you must add additional rules for all other traffic allowed to the destination IP address.

  For example, you have the following Object NAT rule to translate HTTP traffic to the inside server between port 80 and port 8080:

  ```
  object network my-http-server
    host 10.10.10.1
    nat (inside,outside) static 192.168.1.1 80 8080
  ```

  If you want any other services to reach the server, such as FTP, then you must explicitly allow them:

  ```
  object network my-ftp-server
    host 10.10.10.1
    nat (inside,outside) static 192.168.1.1 ftp ftp
  ```

  Or, to allow traffic to other ports of the server, you can add a general static NAT rule that will match all other ports:

  ```
  object network my-server-1
    host 10.10.10.1
    nat (inside,outside) static 192.168.1.1
  ```

For Twice NAT, you have the following rule to allow HTTP traffic from 192.168.1.0/24 to the inside server and translate between port 80 and port 8080:

```
object network my-real-server
  host 10.10.10.1
object network my-mapped-server
  host 192.168.1.1
object network outside-real-hosts
  subnet 192.168.1.0 255.255.255.0
object network outside-mapped-hosts
  subnet 10.10.11.0 255.255.255.0
object service http-real
  service tcp destination eq 80
object service http-mapped
  service tcp destination eq 8080
object service ftp-real
  service tcp destination eq 21
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server service http-mapped http-real
```

If you want the outside hosts to reach another service on the inside server, add another NAT rule for the service, for example FTP:

```
nat (outside,inside) source static outside-real-hosts outside-mapped-hosts destination
 static my-mapped-server my-real-server ftp-real ftp-real
```

If you want other source addresses to reach the inside server on any other ports, you can add another NAT rule for that specific IP address or for any source IP address. Make sure the general rule is ordered after the specific rule.

```
nat (outside,inside) source static any any destination static my-mapped-server
my-real-server
```

8.4 Guidelines and Migration

- Configuration Migration for Transparent Mode—In 8.4, all transparent mode interfaces now belong to a bridge group. When you upgrade to 8.4, the existing two interfaces are placed in bridge group 1, and the management IP address is assigned to the Bridge Group Virtual Interface (BVI). The functionality remains the same when using one bridge group. You can now take advantage of the bridge group feature to configure up to four interfaces per bridge group and to create up to eight bridge groups in single mode or per context.

Note Note In 8.3 and earlier, as an unsupported configuration, you could configure a management interface without an IP address, and you could access the interface using the device management address. In 8.4, the device management address is assigned to the BVI, and the management interface is no longer accessible using that IP address; the management interface requires its own IP address.

- When upgrading to 8.4(2) from 8.3(1), 8.3(2), and 8.4(1), all identity NAT configurations will now include the **no-proxy-arp** and **route-lookup** keywords, to maintain existing functionality. The **unidirectional** keyword is removed.

8.3 Guidelines and Migration

See the following guide that describes the configuration migration process when you upgrade from a pre-8.3 version of the Cisco ASA 5500 operating system (OS) to Version 8.3:

Cisco ASA 5500 Migration to Version 8.3

Clustering Guidelines

There are no special requirements for Zero Downtime Upgrades for ASA clustering with the following exceptions.

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

- Firepower 4100/9300 Failover and Clustering hitless upgrade requirements for flow offload—Due to bug fixes in the flow offload feature, some combinations of FXOS and ASA do not support flow offload (see the Firepower 4100/9300 Compatibility with ASA and Threat Defense). Flow offload is disabled by default for ASA. To perform a Failover or Clustering hitless upgrade when using flow offload, you need to follow the below upgrade paths to ensure that you are always running a compatible combination when upgrading to FXOS 2.3.1.130 or later:

  1. Upgrade ASA to 9.8(3) or later
  2. Upgrade FXOS to 2.3.1.130 or later
  3. Upgrade ASA to your final version

  For example, you are on FXOS 2.2.2.26/ASA 9.8(1), and you want to upgrade to FXOS 2.6.1/ASA 9.12(1), then you can:

  1. Upgrade ASA to 9.8(4)
  2. Upgrade FXOS to 2.6.1
  3. Upgrade ASA to 9.12(1)

- Firepower 4100/9300 Cluster Upgrade to FXOS 2.3/ASA 9.9(2)—Data units on ASA 9.8 and earlier cannot rejoin a cluster where the control unit is on FXOS 2.3/9.9(2) or later; they will join after you upgrade the ASA version to 9.9(2)+ [CSCvi54844].
- Distributed Site-to-Site VPN—Distributed Site-to-Site VPN sessions on a failed unit require up to 30 minutes to stabilize on other units. During this time, additional unit failures might result in lost sessions. Therefore, during a cluster upgrade, to avoid traffic loss, follow these steps. Refer to the FXOS/ASA cluster upgrade procedure so you can integrate these steps into your upgrade task.

Note Zero Downtime Upgrade is not supported with Distributed Site-to-Site VPN when upgrading from 9.9(1) to 9.9(2) or later. In 9.9(2), due to Active Session Redistribution enhancements, you cannot run some units on 9.9(2) and other units on 9.9(1).

1. On the chassis *without* the control unit, disable clustering on one module using the ASA console.

cluster group *name*

no enable

If you are upgrading FXOS on the chassis as well as ASA, save the configuration so clustering will be disabled after the chassis reboots:

write memory

2. Wait for the cluster to stabilize; verify all backup sessions have been created.

   show cluster vpn-sessiondb summary

3. Repeat steps 1 and 2 for each module on this chassis.
4. Upgrade FXOS on the chassis using the FXOS CLI or Firepower Chassis Manager.
5. After the chassis comes online, update the ASA image on each module using the FXOS CLI or Firepower Chassis Manager.
6. After the modules come online, re-enable clustering on each module at the ASA console.

   cluster group *name*

   enable

   write memory

7. Repeat steps 1 through 6 on the second chassis, being sure to disable clustering on the data units first, and then finally the control unit.

   A new control unit will be chosen from the upgraded chassis.

8. After the cluster has stabilized, redistribute active sessions among all modules in the cluster using the ASA console on the control unit.

   cluster redistribute vpn-sessiondb

- Upgrade issue for 9.9(1) and later with clustering—9.9(1) and later includes an improvement in the backup distribution. You should perform your upgrade to 9.9(1) or later as follows to take advantage of the new backup distribution method; otherwise upgraded units will continue to use the old method.
  1. Remove all secondary units from the cluster (so the cluster consists only of the primary unit).
  2. Upgrade 1 secondary unit, and rejoin the cluster.
  3. Disable clustering on the primary unit; upgrade it, and rejoin the cluster.
  4. Upgrade the remaining secondary units, and join them back to the cluster, one at a time.

- Firepower 4100/9300 Cluster Upgrade to ASA 9.8(1) and earlier—When you disable clustering on a data unit (**no enable**), which is part of the upgrade process, traffic directed to that unit can drop for up to three seconds before traffic is redirected to a new owner [CSCvc85008].

- Zero Downtime Upgrade may not be supported when upgrading to the following releases with the fix for CSCvb24585. This fix moved 3DES from the default (medium) SSL ciphers to the low cipher set. If you set a custom cipher that only includes 3DES, then you may have a mismatch if the other side of the connection uses the default (medium) ciphers that no longer include 3DES.
  - 9.1(7.12)

- 9.2(4.18)
- 9.4(3.12)
- 9.4(4)
- 9.5(3.2)
- 9.6(2.4)
- 9.6(3)
- 9.7(1)
- 9.8(1)

- Upgrade issues for fully-qualified domain name (FQDN) ACLs—Due to CSCuv92371, ACLs containing FQDNs might result in incomplete ACL replication to secondary units in a cluster or failover pair. This bug is present in 9.1(7), 9.5(2), 9.6(1), and some interim releases. We suggest that you upgrade to a version that includes the fix for CSCuy34265: 9.1(7.6) or later, 9.5(3) or later, 9.6(2) or later. However, due to the nature of configuration replication, zero downtime upgrade is not available. See CSCuy34265 for more information about different methods of upgrading.
- Firepower Threat Defense Version 6.1.0 clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in 6.2.0). If you deployed or re-deployed a 6.1.0 cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, then you must remove the site ID (set it to **0**) on each unit in FXOS before you upgrade to 6.2.3. Otherwise, the units will not be able to rejoin the cluster after the upgrade. If you already upgraded, change the site ID to **0** on each unit to resolve the issue. See the FXOS configuration guide to view or change the site ID
- Upgrade to 9.5(2) or later (CSCuv82933)—Before you upgrade the control unit, if you enter **show cluster info**, the upgraded data units show as "DEPUTY_BULK_SYNC"; other mismatched states are also shown. You can ignore this display; the status will show correctly when you upgrade all units.
- Upgrade from 9.0(1) or 9.1(1) (CSCue72961)—Zero Downtime Upgrade is not supported.

Failover Guidelines

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

- For the Firepower 1010, invalid VLAN IDs can cause problems—Before you upgrade to 9.15(1), make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See CSCvw33057 for more information.
- Firepower 4100/9300 Failover and Clustering hitless upgrade requirements for flow offload—Due to bug fixes in the flow offload feature, some combinations of FXOS and ASA do not support flow offload (see the Firepower 4100/9300 Compatibility with ASA and Threat Defense). Flow offload is disabled by default for ASA. To perform a Failover or Clustering hitless upgrade when using flow offload, you need to follow the below upgrade paths to ensure that you are always running a compatible combination when upgrading to FXOS 2.3.1.130 or later:

  1. Upgrade ASA to 9.8(3) or later
  2. Upgrade FXOS to 2.3.1.130 or later

3. Upgrade ASA to your final version

For example, you are on FXOS 2.2.2.26/ASA 9.8(1), and you want to upgrade to FXOS 2.6.1/ASA 9.12(1), then you can:

1. Upgrade ASA to 9.8(4)
2. Upgrade FXOS to 2.6.1
3. Upgrade ASA to 9.12(1)

- Upgrade issues with 8.4(6), 9.0(2) , and 9.1(2)—Due to CSCug88962, you cannot perform a Zero Downtime Upgrade to 8.4(6), 9.0(2), or 9.1(3). You should instead upgrade to 8.4(5) or 9.0(3). To upgrade 9.1(1), you cannot upgrade directly to the 9.1(3) release due to CSCuh25271, so there is no workaround for a Zero Downtime Upgrade; you must upgrade to 9.1(2) before you upgrade to 9.1(3) or later.
- Upgrade issues for fully-qualified domain name (FQDN) ACLs—Due to CSCuv92371, ACLs containing FQDNs might result in incomplete ACL replication to secondary units in a cluster or failover pair. This bug is present in 9.1(7), 9.5(2), 9.6(1), and some interim releases. We suggest that you upgrade to a version that includes the fix for CSCuy34265: 9.1(7.6) or later, 9.5(3) or later, 9.6(2) or later. However, due to the nature of configuration replication, zero downtime upgrade is not available. See CSCuy34265 for more information about different methods of upgrading.
- Upgrade issue with 9.7(1) to 9.7(1.x) and later for VTI and VXLAN VNI—If you configure both Virtual Tunnel Interfaces (VTIs) and VXLAN Virtual Network Identifier (VNI) interfaces, then you cannot perform a zero downtime upgrade for failover; connections on these interface types will not replicate to the standby unit until both units are on the same version. (CSCvc83062)
- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- 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.

Additional Guidelines

- Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability—Multiple vulnerabilities have been fixed for clientless SSL VPN in ASA software, so you should upgrade your software to a fixed version. See http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa for details about the vulnerability and a list of fixed ASA versions. Also, if you ever ran an earlier ASA version that had a vulnerable configuration, then regardless of the version you are currently running, you should verify that the portal customization was not compromised. If an attacker compromised a customization object in the past, then the compromised object stays persistent after you upgrade the ASA to a fixed version. Upgrading the ASA prevents this vulnerability from being exploited further, but it will not modify any customization objects that were already compromised and are still present on the system.

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 40): _____

   Current ASA version (Upgrade Path: ASA Appliances, on page 40): _____

2. Check the ASA/ASDM compatibility per model (ASA and ASDM Compatibility Per Model, on page 22).

   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 47). 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 57).

   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 Threat Defense, on page 29).

      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 68).

   Download the intermediate ASA versions (Download ASA Software, on page 57).

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 36).

      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 models. For older versions and models, see Cisco ASA Compatibility.

ASA 9.20 and 9.19

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

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).
- 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 1: ASA and ASDM Compatibility: 9.20 and 9.19

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

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

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).
- 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 2: ASA and ASDM Compatibility: 9.18 to 9.17

ASA	ASDM	ASA Model							
		ASA Virtual	Firepower 1010 1120 1140 1150		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**
9.18(3)	7.18(1.152)	**YES**	**YES**		**YES**	**YES**	**YES**	**YES**	**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 to 9.15

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

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 3: ASA and ASDM Compatibility: 9.16 to 9.15

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**
9.15(1)	7.15(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

ASA 9.14 to 9.13

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

Note

- ASA 9.14(x) was the final version for the ASA 5525-X, 5545-X, and 5555-X.
- ASA 9.12(x) was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.
- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.13(1) can manage an ASA 5516-X on ASA 9.10(1). ASDM 7.13(1) and ASDM 7.14(1) did not support ASA 5512-X, 5515-X, 5585-X, and ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.
- 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 7.13 with ASA 9.14. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.14(1.2) with ASDM 7.14(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.
- ASA 9.14(4.14) 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: 9.14 to 9.13

ASA	ASDM	ASA Model							
		ASA 5506-X **5506H-X** **5506W-X** **5508-X** **5516-X**	**ASA 5525-X** **5545-X** **5555-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**
9.14(4.14)	7.18(1.152)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.14(4)	7.14(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.14(3)	7.14(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.14(2)	7.14(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.14(1.30)	7.14(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.14(1.6)	7.14(1.48)	—	—	**YES** (+ASAv100)	—	—	—	—	—
9.14(1)	7.14(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

ASA	ASDM	ASA Model							
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5525-X 5545-X 5555-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
9.13(1)	7.13(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES** (except 4112)	**YES**	**YES**

ASA 9.12 to 9.5

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

Note

- ASA 9.12(x) was the final version for the ASA 5512-X, 5515-X, 5585-X, and ASASM.
- ASDM versions are backwards compatible with all previous ASA versions, unless otherwise stated. For example, ASDM 7.12(1) can manage an ASA 5515-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 7.10 with ASA 9.12. For ASA maintenance releases and interims, you can continue to use the current ASDM version, unless otherwise stated. For example, you can use ASA 9.12(1.15) with ASDM 7.12(1). If an ASA maintenance release has significant new features, then usually there will be a new ASDM version required.
- ASA 9.8(4.45) and 9.12(4.50) and later require 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: 9.12 to 9.5

ASA	ASDM	ASA Model									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.12(4.50)	7.18(1.152)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(4)	7.12(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(3)	7.12(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(2)	7.12(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.12(1)	7.12(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
9.10(1)	7.10(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.9(2)	7.9(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.9(1)	7.9(1)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(4.45)	7.18(1.152)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(4)	7.8(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(3)	7.8(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(2)	7.8(2)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	**YES**
9.8(1.200)	No support	—	—	—	**YES**	—	—	—	—	—	—
9.8(1)	7.8(1)	**YES**	**YES**	**YES**	**YES** (+ASAv50)	**YES**	—	**YES**	—	**YES**	**YES**
9.7(1.4)	7.7(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(4)	7.9(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(3.1)	7.7(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(2)	7.6(2)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES**	—	**YES**	**YES**
9.6(1)	7.6(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	**YES** (except 4150)	—	**YES**	**YES**
9.5(3.9)	7.6(2)	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	**YES**

ASA	ASDM	ASA Model									
		ASA 5506-X 5506H-X 5506W-X 5508-X 5516-X	ASA 5512-X 5515-X 5525-X 5545-X 5555-X	ASA 5585-X	ASAv	ASASM	Firepower 2110 2120 2130 2140	Firepower 4110 4120 4140 4150	Firepower 4115 4125 4145	Firepower 9300	ISA 3000
9.5(2.200)	7.5(2.153)	—	—	—	**YES**	—	—	—	—	—	—
9.5(2.2)	7.5(2)	—	—	—	—	—	—	—	—	**YES**	—
9.5(2.1)	7.5(2)	—	—	—	—	—	—	—	—	**YES**	—
9.5(2)	7.5(2)	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	**YES**
9.5(1.200)	7.5(1)	—	—	—	**YES**	—	—	—	—	—	—
9.5(1.5)	7.5(1.112)	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	—
9.5(1)	7.5(1)	**YES**	**YES**	**YES**	**YES**	**YES**	—	—	—	—	—

Firepower 4100/9300 Compatibility with ASA and Threat Defense

The following table lists compatibility between the ASA and threat defense applications with the Firepower 4100/9300.

The **bold** versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.

For upgrading, see the following guidelines:

- FXOS—For 2.2.2 and later, you can upgrade directly to a higher version. When upgrading from versions earlier than 2.2.2, 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

- ASA—ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

Note This section applies only to the Firepower 4100/9300. Other models utilize FXOS only as an underlying operating system that is included in the ASA and threat defense unified image bundles. For the Secure Firewall 3100 in multi-instance mode, see the Threat Defense compatibility guide.

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.

Note FXOS 2.12/ASA 9.18/Threat Defense 7.2 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.

Table 6: ASA or Threat Defense, and Firepower 4100/9300 Compatibility

FXOS Version	Model	ASA Version	Threat Defense Version
2.16	Firepower 4112	**9.22** (recommended) 9.20 9.19 9.18 9.17 9.16 9.14	**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 9.16 9.14	**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	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 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**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
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 Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	**9.19** (recommended) 9.18 9.17 9.16 9.14	**7.3** (recommended) 7.2 7.1 7.0 6.6

FXOS Version	Model	ASA Version	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	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	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
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24		6.2.3

FXOS Version	Model	ASA Version	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	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**	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.

Table 7: Radware DefensePro Compatibility

FXOS Version	ASA	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

FXOS Version	ASA	Threat Defense	Radware DefensePro	Security Appliance Models
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
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

FXOS Version	ASA	Threat Defense	Radware DefensePro	Security Appliance Models
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
2.9.1	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

FXOS Version	ASA	Threat Defense	Radware DefensePro	Security Appliance Models
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
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

FXOS Version	ASA	Threat Defense	Radware DefensePro	Security Appliance Models
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
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

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 ASA. Some older 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.

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
9.20	—	Any of the following: → **9.22**
9.19	—	Any of the following: → **9.22** → **9.20**
9.18	—	Any of the following: → **9.22** → **9.20** → **9.19**
9.17	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18**
9.16	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17

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

Current Version	Interim Upgrade Version	Target Version
9.10	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.9	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12
9.8	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12

Current Version	Interim Upgrade Version	Target Version
9.7	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.6	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.5	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.4	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.3	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8
9.2	—	Any of the following: → **9.22** → **9.20** → **9.19** → **9.18** → 9.17 → **9.16** → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.1(2), 9.1(3), 9.1(4), 9.1(5), 9.1(6), or 9.1(7.4)	—	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14 → **9.12** → 9.8 → 9.6 → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.14 → **9.12** → 9.8 → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.4(5+)	—	Any of the following: → **9.12** → 9.8 → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12** → 9.8 → 9.1(7.4)
8.3	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)
8.2 and earlier	→ 9.0(4)	Any of the following: → **9.12** → 9.8 → 9.1(7.4)

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
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** → 9.15

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

Current Version	Interim Upgrade Version	Target Version
9.9	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**
9.9	—	Any of the following: → 9.17 → **9.16** → 9.15 → 9.14 → 9.12
9.8	→ 9.17	Any of the following: → **9.20** → **9.19** → **9.18**
9.8	—	Any of the following: → 9.17 → **9.16** → 9.15 → 9.14 → 9.12

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**.

For upgrading, see the following guidelines:

- FXOS—For 2.2.2 and later, you can upgrade directly to a higher version. When upgrading from versions earlier than 2.2.2, 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

- ASA—ASA lets you upgrade directly from your current version to any higher version, noting the FXOS requirements above.

Table 10: ASA or Threat Defense, and Firepower 4100/9300 Compatibility

FXOS Version	Model	ASA Version	Threat Defense Version
2.16	Firepower 4112	**9.22** (recommended) 9.20 9.19 9.18 9.17 9.16 9.14	**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 9.16 9.14	**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	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	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	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	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	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	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**	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

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.

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

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.

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**. **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.

ASA Model	Download Location	Packages
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**. **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-7171.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.

ASA Model	Download Location	Packages
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**. **Note** When you upgrade the ASA bundle in FXOS, 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-782.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.
	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**. **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-7201.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.

ASA Model	Download Location	Packages
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**. **Note** When you upgrade the ASA bundle in FXOS, 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-782.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.
	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 Services Module	**ASDM Software** http://www.cisco.com/go/asdm-software Choose **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.

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.

ASA Model	Download Location	Packages
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**. **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-782.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.
ASA Services Module	**ASA Software** http://www.cisco.com/go/asasm-software Choose your *version*.	The ASA software file has a filename like asa962-**smp-k8.bin**.
	ASDM Software http://www.cisco.com/go/asdm-software Choose **Adaptive Security Appliance (ASA) Device Manager** > *version*.	The ASDM software file has a filename like asdm-762**.bin**.

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.

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, ASA FirePOWER local management, Firepower Management Center, and FXOS configuration guides for more information.