



Release Notes for Cisco Secure Firewall ASDM, 7.22(x)

First Published: 2024-09-16

Last Modified: 2024-09-16

Release Notes for Cisco Secure Firewall ASDM, 7.22(x)

This document contains release information for ASDM version 7.22(x) for the Secure Firewall ASA.

Important Notes

- **No support in ASA 9.22(1) and later for the Firepower 2100**—ASA 9.20(x) is the last supported version.
- **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**.

System Requirements

ASDM requires a computer with a CPU with at least 4 cores. Fewer cores can result in high memory usage.

ASDM Java Requirements


You can install ASDM using Oracle JRE 8.0 (**asdm-version.bin**) or OpenJRE 1.8.x (**asdm-openjre-version.bin**).

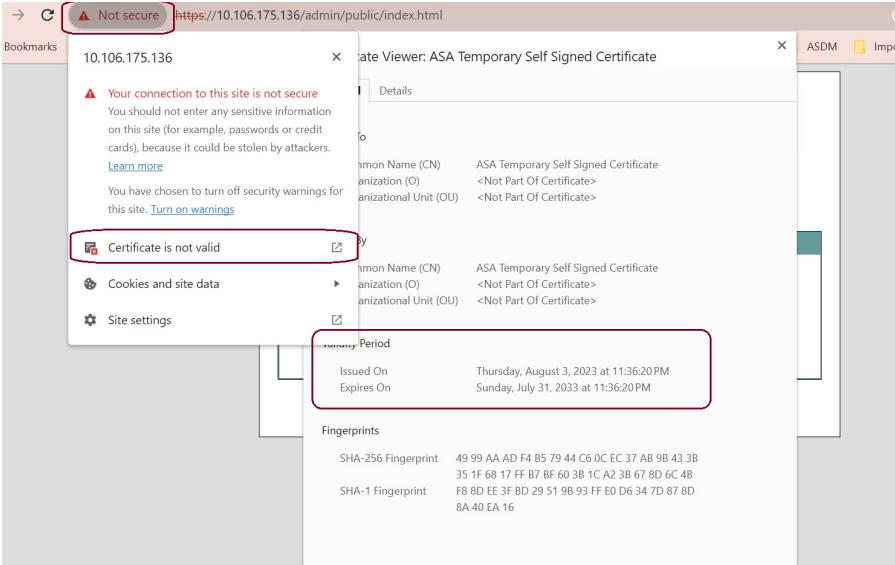
Table 1: ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): <ul style="list-style-type: none"> • 11 • 10 Note See Windows 10 in ASDM Compatibility Notes, on page 2 if you have problems with the ASDM shortcut. • 8 • 7 • Server 2016 and Server 2019 • Server 2012 R2 • Server 2012 • Server 2008 	Yes	No support	Yes	8.0 version 8u261 or later	1.8 Note No support for Windows 7 or 10 32-bit
Apple OS X 10.4 and later	Yes	Yes	Yes (64-bit version only)	8.0 version 8u261 or later	1.8

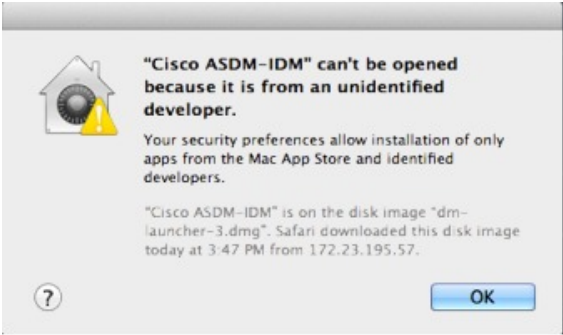
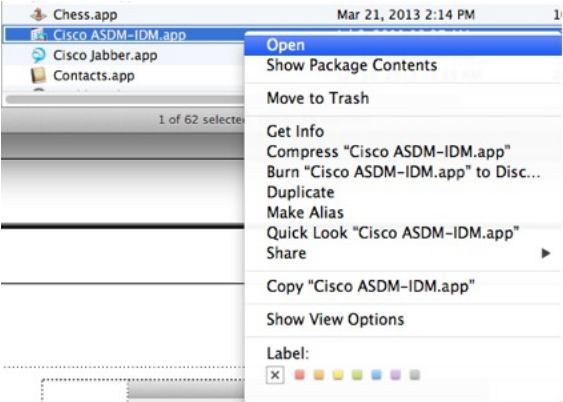

ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
ASDM Launcher compatibility with ASDM version	<p>"Unable to Launch Device Manager" error message.</p> <p>If you upgrade to a new ASDM version and then get this error, you may need to re-install the latest Launcher.</p> <ol style="list-style-type: none"> 1. Open the ASDM web page on the ASA: <a href="https://<asa_ip_address>">https://<asa_ip_address>. 2. Click Install ASDM Launcher. <p><i>Figure 1: Install ASDM Launcher</i></p>  <p>Copyright © 2006-2022 Cisco Systems, Inc. All rights reserved.</p> <ol style="list-style-type: none"> 3. Leave the username and password fields empty (for a new installation), and click OK. <p>With no HTTPS authentication configured, you can gain access to ASDM with no username and the enable password, which is blank by default. When you enter the enable command at the CLI for the first time, you are prompted to change the password; this behavior is not enforced when you log into ASDM. We suggest that you change the enable password as soon as possible so that it does not remain blank. Note: If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.</p>

Conditions	Notes
<p>Self-signed certificate not valid due to a time and date mismatch with ASA</p>	<p>ASDM validates the self-signed SSL certificate, and if the ASA's date is not within the certificate's Issued On and Expires On date, ASDM will not launch. If there is a time and date mismatch, you will see the following error:</p> <p>Figure 2: Certificate Not Valid</p>  <p>To fix the issue: Set the correct time on the ASA and reload.</p> <p>To check the certificate dates, (example shown is Chrome):</p> <ol style="list-style-type: none"> 1. Go to <code>https://device_ip</code>. 2. Click the Not secure text in the menu bar. 3. Click Certificate is not valid to open the Certificate Viewer. 4. Check the Validity Period. <p>Figure 3: Certificate Viewer</p> 

Conditions	Notes
Windows Active Directory directory access	<p>In some cases, Active Directory settings for Windows users may restrict access to program file locations needed to successfully launch ASDM on Windows. Access is needed to the following directories:</p> <ul style="list-style-type: none"> • Desktop folder • C:\Windows\System32\Users\<username>\.asdm</username> • C:\Program Files (x86)\Cisco Systems <p>If your Active Directory is restricting directory access, you need to request access from your Active Directory administrator.</p>
Windows 10	<p>"This app can't run on your PC" error message.</p> <p>When you install the ASDM Launcher, Windows 10 might replace the ASDM shortcut target with the Windows Scripting Host path, which causes this error. To fix the shortcut target:</p> <ol style="list-style-type: none"> 1. Choose Start > Cisco ASDM-IDM Launcher, and right-click the Cisco ASDM-IDM Launcher application. 2. Choose More > Open file location. Windows opens the directory with the shortcut icon. 3. Right click the shortcut icon, and choose Properties. 4. Change the Target to: C:\Windows\System32\wscript.exe invisible.vbs run.bat 5. Click OK.
OS X	<p>On OS X, you may be prompted to install Java the first time you run ASDM; follow the prompts as necessary. ASDM will launch after the installation completes.</p>

Conditions	Notes
OS X 10.8 and later	<p>You need to allow ASDM to run because it is not signed with an Apple Developer ID. If you do not change your security preferences, you see an error screen.</p>  <p>371051</p> <ol style="list-style-type: none"> To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose Open.  <p>371052</p> <ol style="list-style-type: none"> You see a similar error screen; however, you can open ASDM from this screen. Click Open. The ASDM-IDM Launcher opens.  <p>371053</p>

Conditions	Notes
<p>Requires Strong Encryption license (3DES/AES) on ASA</p> <p>Note Smart licensing models allow initial access with ASDM without the Strong Encryption license.</p>	<p>ASDM requires an SSL connection to the ASA. You can request a 3DES license from Cisco:</p> <ol style="list-style-type: none"> 1. Go to www.cisco.com/go/license. 2. Click Continue to Product License Registration. 3. In the Licensing Portal, click Get Other Licenses next to the text field. 4. Choose IPS, Crypto, Other... from the drop-down list. 5. Type ASA in to the Search by Keyword field. 6. Select Cisco ASA 3DES/AES License in the Product list, and click Next. 7. Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.
<ul style="list-style-type: none"> • Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari 	<p>When the ASA uses a self-signed certificate or an untrusted certificate, Firefox and Safari are unable to add security exceptions when browsing using HTTPS over IPv6. See https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority.</p>
<ul style="list-style-type: none"> • SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome 	<p>If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome "SSL false start" feature. We suggest re-enabling one of these algorithms (see the Configuration > Device Management > Advanced > SSL Settings pane); or you can disable SSL false start in Chrome using the --disable-ssl-false-start flag according to Run Chromium with flags.</p>

Install an Identity Certificate for ASDM

When using Java 7 update 51 and later, the ASDM Launcher requires a trusted certificate. An easy approach to fulfill the certificate requirements is to install a self-signed identity certificate.

See [Install an Identity Certificate for ASDM](#) to install a self-signed identity certificate on the ASA for use with ASDM, and to register the certificate with Java.

Increase the ASDM Configuration Memory

ASDM supports a maximum configuration size of 512 KB. If you exceed this amount you may experience performance issues. For example, when you load the configuration, the status dialog box shows the percentage of the configuration that is complete, yet with large configurations it stops incrementing and appears to suspend operation, even though ASDM might still be processing the configuration. If this situation occurs, we recommend that you consider increasing the ASDM system heap memory. To confirm that you are experiencing memory exhaustion, monitor the Java console for the "java.lang.OutOfMemoryError" message.

Increase the ASDM Configuration Memory in Windows

To increase the ASDM heap memory size, edit the **run.bat** file by performing the following procedure.

Procedure

-
- Step 1** Go to the ASDM installation directory, for example C:\Program Files (x86)\Cisco Systems\ASDM.
 - Step 2** Edit the **run.bat** file with any text editor.
 - Step 3** In the line that starts with “start javaw.exe”, change the argument prefixed with “-Xmx” to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.
 - Step 4** Save the **run.bat** file.
-

Increase the ASDM Configuration Memory in Mac OS

To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

Procedure

-
- Step 1** Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.
 - Step 2** In the **Contents** folder, double-click the **Info.plist** file. If you have Developer tools installed, it opens in the **Property List Editor**. Otherwise, it opens in **TextEdit**.
 - Step 3** Under **Java > VMOptions**, change the string prefixed with “-Xmx” to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>
```

```
<key>CFBundleDocumentTypes</key>
<array>
```

- Step 4** If this file is locked, you see an error such as the following:



- Step 5** Click **Unlock** and save the file.

If you do not see the **Unlock** dialog box, exit the editor, right-click the **Cisco ASDM-IDM** icon, choose **Copy Cisco ASDM-IDM**, and paste it to a location where you have write permissions, such as the Desktop. Then change the heap size from this copy.

ASA and ASDM Compatibility

For information about ASA/ASDM software and hardware requirements and compatibility, including module compatibility, see [Cisco Secure Firewall ASA Compatibility](#).

VPN Compatibility

For VPN compatibility, see [Supported VPN Platforms, Cisco ASA 5500 Series](#).

New Features

This section lists new features for each release.



Note New, changed, and deprecated syslog messages are listed in the syslog message guide.

New Features in ASA 9.22(1.1)/ASDM 7.22(1)

Released: September 16, 2024



Note 9.22(1) was not released.

Feature	Description
Platform Features	

Feature	Description
ASA Virtual Supports Dual-Arm Deployment Mode on AWS with GWLB	<p>ASA Virtual now supports the dual-arm deployment mode on AWS with GWLB. This mode enables ASA Virtual to directly forward internet-bound traffic to the internet through the internet gateway after traffic inspection, while also performing network address translation (NAT).</p> <p>The dual-arm mode differs from the single-arm mode, which helps in routing inspected outbound traffic back to the GWLB, and then to the internet through the internet gateway.</p> <p>The dual-arm mode supports forwarding of inspected traffic from ASA Virtual to the internet in both single VPC and multiple VPC network environments.</p> <p>The advantages of the dual-arm mode in ASA Virtual are:</p> <ul style="list-style-type: none"> • Minimize traffic hops, thereby reducing traffic latency and improving throughput performance. • Consolidate and inspect outbound traffic from multiple VPCs before forwarding it to the internet. • Provide a cost-effective solution because of reduced infrastructure requirements. <p>For more information, see Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.22.</p>
Deploy the Cisco Secure Firewall ASA container (ASAc) in a Kubernetes or Docker Environment	<p>A container is a software package that bundles up code and associated requirements such as system libraries, system tools, default settings, and so on, to ensure that the application runs successfully in a computing environment. You can deploy the ASA container (ASAc) in an open-source Kubernetes or Docker environment running on any cloud platform.</p>
Firewall Features	
Object group search optimization.	<p>The object group search feature has been enhanced to reduce object lookup time when evaluating access control rules to match connections and to reduce CPU overhead. There are no changes to configuring object group search, the optimized behavior happens automatically.</p> <p>We added the following commands in the device CLI, or enhanced command output: clear asp table network-object, debug ac logs, packet-tracer, show access-list, show asp table network-group, show object-group.</p>
High Availability and Scalability Features	
Secure Firewall 3100 and 4200 maximum cluster nodes increased to 16.	<p>For the Secure Firewall 3100 and 4200, the maximum nodes were increased from 8 to 16.</p>
Secure Firewall 3100 and 4200 cluster Individual interface mode	<p>Individual interfaces are normal routed interfaces, each with their own <i>Local IP address</i> used for routing. The <i>Main cluster IP address</i> for each interface is a fixed address that always belongs to the control node. When the control node changes, the Main cluster IP address moves to the new control node, so management of the cluster continues seamlessly.</p> <p>Load balancing must be configured separately on the upstream switch.</p> <p>New/Modified commands: cluster interface-mode individual</p> <p>New/Modified screens: Wizards > > High Availability and Scalability Wizard</p>

Feature	Description
ASA Virtual Clustering deployment support on the AWS Multi-Availability Zone	<p>You can now deploy and configure the ASA virtual cluster across multiple availability zones in an AWS region. The cluster also has dynamic scaling capability (Autoscale), which helps in scaling up or scaling down virtual devices based on demand.</p> <p>Extending the ASA virtual cluster across multiple availability zones in an AWS region enables continuous traffic inspection and dynamic scaling during disaster recovery.</p> <p>For more information, see Deploy a Cluster for the ASA Virtual in a Public Cloud.</p>
License Features	
Smart Transport is the default Smart Licensing transport	<p>Smart Licensing now uses Smart Transport as the default transport. You can optionally enable the former type, Smart Call Home, if necessary.</p> <p>New/Modified screens: Configuration > Device Management > Licensing > Smart Licensing</p>
ASAvU (Unlimited) license to deploy ASA virtuals with 32 cores and 64 cores	<p>ASAvU license achieves maximum throughput on deployments with 32 cores and 64 cores and is supported only on VMware and KVM.</p> <p>New/Modified screens: Configuration > Device Management > Licensing > Smart Licensing.</p>
Administrative, Monitoring, and Troubleshooting Features	
Disable the USB port (disk1)	<p>By default, the type-A USB port (disk1) is enabled and could not be disabled. You can now disable USB port access for security purposes on the following models:</p> <ul style="list-style-type: none"> • Firepower 1000 • Secure Firewall 3100 • Secure Firewall 4200 <p>This setting is stored in firmware and requires a reload. Moreover, if the USB port is disabled and you downgrade to a version that does not support this feature, the port will remain disabled and you cannot re-enable it without erasing the NVRAM.</p> <p>Note This feature does not affect the type-B USB console port, if present.</p> <p>New/Modified screens: .</p> <ul style="list-style-type: none"> • Configuration > Device Management > Advanced > Enable/Disable USB Port • Monitoring > Properties > USB Port > USB Port Info
VPN Features	
DTLS Crypto Acceleration	<p>Cisco Secure Firewall 4200 and 3100 series support DTLS cryptographic acceleration. The hardware performs DTLS encryption and decryption, and improves the throughput of the DTLS-encrypted and DTLS-decrypted traffic. The hardware also performs optimization of the egress-encrypted packets to improve latency.</p> <p>New/Modified screens: Configuration > Firewall > Advanced > DTLS Offload > DTLS Offload and Egress Optimization for DTLS Offload check boxes.</p>

Upgrade the Software

This section provides the upgrade path information and a link to complete your upgrade.

Upgrade Link

To complete your upgrade, see the [ASA upgrade guide](#).

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.

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 2: 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

Current Version	Interim Upgrade Version	Target Version
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
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

Current Version	Interim Upgrade Version	Target Version
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
9.10	—	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
9.9	—	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
9.7	—	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
9.6	—	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
9.4	—	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
9.3	—	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
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)

Current Version	Interim Upgrade Version	Target Version
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)
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)

Current Version	Interim Upgrade Version	Target Version
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 Logical Devices for the Firepower 4100/9300

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

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

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

FXOS Version	Model	ASA Version	Threat Defense Version		
2.11	Firepower 4112	9.17 (recommended)	7.1 (recommended)		
		9.16	7.0		
		9.14	6.6		
	Firepower 4145 Firepower 4125 Firepower 4115	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.17 (recommended)	7.1 (recommended)	
			9.16	7.0	
			9.14	6.6	
		9.12	6.4		
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.17 (recommended)	7.1 (recommended)
				9.16	7.0
	9.14			6.6	
	9.12		6.4		
	9.8				
	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)	7.0 (recommended)	
			9.14	6.6	
Firepower 4145 Firepower 4125 Firepower 4115		Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	9.16 (recommended)	7.0 (recommended)	
			9.14	6.6	
			9.12	6.4	
		Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.16 (recommended)	7.0 (recommended)
				9.14	6.6
				9.12	6.4
9.8					

FXOS Version	Model	ASA Version	Threat Defense Version
2.9	Firepower 4112	9.14	6.6
	Firepower 4145	9.14	6.6
	Firepower 4125	9.12	6.4
	Firepower 4115		
	Firepower 9300 SM-56		
	Firepower 9300 SM-48		
	Firepower 9300 SM-40		
	Firepower 4150	9.14	6.6
	Firepower 4140	9.12	6.4
	Firepower 4120	9.8	
Firepower 4110			
	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	9.14 (recommended)	6.6 (recommended)
	Firepower 4125	9.12	Note 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4115	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	9.14 (recommended)	6.6 (recommended)
	Firepower 4140	9.12	Note 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4120	9.8	6.4
Firepower 4110		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 Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.8 Note 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	
2.2	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110 Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.8	Threat Defense versions are EoL

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.

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.



Note You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can [register for an account](#). If you do not have a Cisco support contract, you can only look up bugs by ID; you cannot run searches.

For more information about the Cisco Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

Open Bugs in Version 7.22(1)

There are no open bugs in this release.

Resolved Bugs in Version 7.22(1)

The following table lists select resolved bugs at the time of this Release Note publication.

Identifier	Headline
CSCwa87515	ASDM session disconnects while switching between the context
CSCwh18177	ASDM backup restore replaces custom policy-map with default class inspect options
CSCwh50291	Checkbox of Enable autogeneration of MAC addresses not working properly
CSCwi11925	Unable to use 'any' keyword as an object when editing object-group through ASDM
CSCwj14147	ASDM fails to load access-group config if L2 and L3 acl's are mixed.
CSCwj14498	Source & Destination file extension error pop-up from ASDM GUI
CSCwj17213	Change in Application Client Type attribute
CSCwj28481	ASDM applies new rules in the incorrect order when "forward-referenced" lines are present
CSCwj66085	ASA is unable to export NAT rules via ASDM in .csv format
CSCwk64399	ASDM- Unable to edit Secure Client Profile

Cisco General Terms

The Cisco General Terms (including other related terms) governs the use of Cisco software. You can request a physical copy from Cisco Systems, Inc., P.O. Box 641387, San Jose, CA 95164-1387. Non-Cisco software purchased from Cisco is subject to applicable vendor license terms. See also: <https://cisco.com/go/generalterms>.

Related Documentation

For additional information on the ASA, see [Navigating the Cisco Secure Firewall ASA Series Documentation](#).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024 Cisco Systems, Inc. All rights reserved.