Release Notes for Cisco Secure Firewall ASDM, 7.20(x)

First Published: 2023-09-07

Last Modified: 2026-09-18

Release Notes for Cisco Secure Firewall ASDM, 7.20(x)

This document contains release information for ASDM version 7.20(x) for the Secure Firewall ASA.

Note ASA 9.20(1) is only supported on the Secure Firewall 4200. Later releases are supported on the other models.

Important Notes

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

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

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

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

- **ASA version 9.20(1) only supports the Secure Firewall 4200**—ASDM 7.20(1) supports the Secure Firewall 4200 on 9.20(1), but is also backwards-compatible with earlier releases on other platforms.

- **During a software upgrade of ASA cluster, the VPN load-balancing cluster does not form if members run different ASA versions.** You must perform one of the following operations:
  - Upgrade all members to the same version. The VPN load-balancing cluster re-forms automatically after all members run the same version. VPN load balancing is unavailable during the mixed-version window.
  - For a hitless upgrade, temporarily remove the cluster keys from all members. Keep the interval without cluster keys as short as possible. Upgrade all members and then reconfigure the cluster keys on all members. VPN load balancing remains available during the upgrade.

    When you perform this operation, syslog 718089 is logged:

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

- **ASDM's self-signed certificate not valid due to a time and date mismatch with ASA**—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. See ASDM Compatibility Notes, on page 3 for more information.

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**).

The Oracle version of ASDM is included in the ASA package; if you want to use the OpenJRE version, you will need to copy it to the ASA and configure the ASA to use that version of ASDM.



Note ASDM is not supported on Linux.

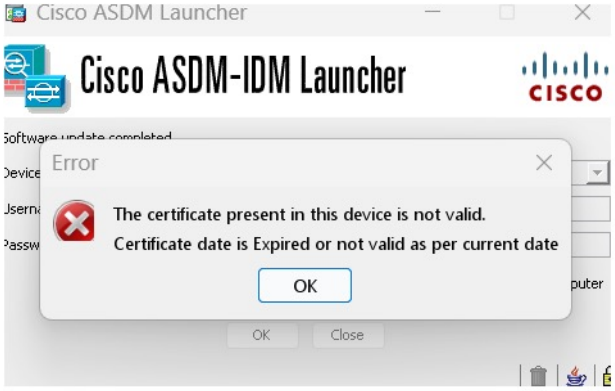
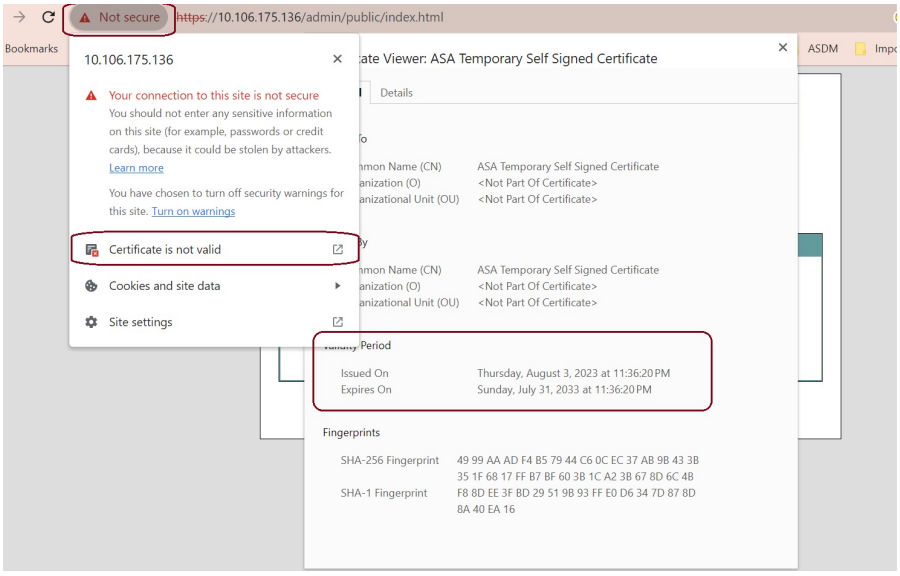
Table 1: ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): • 11 • 10 **Note** See Windows 10 in ASDM Compatibility Notes, on page 3 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

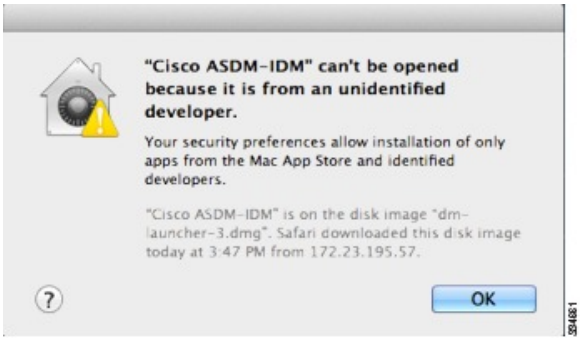
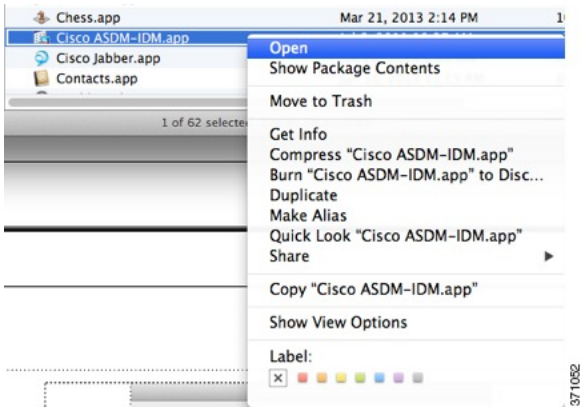
ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

Conditions	Notes
ASDM Launcher compatibility with ASDM version	"**Unable to Launch Device Manager**" error message. If you upgrade to a new ASDM version and then get this error, you may need to re-install the latest Launcher. **1.** Open the ASDM web page on the ASA: https://<asa_ip_address>. **2.** Click **Install ASDM Launcher**. ***Figure 1: Install ASDM Launcher***  **3.** Leave the username and password fields empty (for a new installation), and click **OK**. 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.

Conditions	Notes
Self-signed certificate not valid due to a time and date mismatch with ASA	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: ***Figure 2: Certificate Not Valid***  **To fix the issue:** Set the correct time on the ASA and reload. To check the certificate dates, (example shown is Chrome): **1.** Go to https://*device_ip*. **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. ***Figure 3: Certificate Viewer*** 

Conditions	Notes
Windows Active Directory directory access	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: • Desktop folder • C:\Windows\System32C:\Users\<username>\.asdm • C:\Program Files (x86)\Cisco Systems If your Active Directory is restricting directory access, you need to request access from your Active Directory administrator.
Windows 10	"**This app can't run on your PC**" error message. 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: **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	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.

Conditions	Notes
OS X 10.8 and later	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.  1. To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose **Open**.  2. You see a similar error screen; however, you can open ASDM from this screen. Click **Open**. The ASDM-IDM Launcher opens. 

Conditions	Notes
(ASA 5500 and ISA 3000) Requires Strong Encryption license (3DES/AES) on ASA **Note** Smart licensing models allow access with ASDM without the Strong Encryption license.	ASDM requires an SSL connection to the ASA. You can request a 3DES PAK license from Cisco: **1.** Go to https://www.cisco.com/go/license. **2.** Under **Traditional Licenses**, click **Access LRP**. **3.** Click **Get Licenses** and then choose **IPS, Crypto, Other...** from the drop-down list. **4.** Type **ASA** in to the **Search by Keyword** field. **5.** Select **Cisco ASA 3DES/AES License** in the **Product** list, and click **Next**. **6.** Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.
• Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari	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.
• SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome	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.

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.

In addition, we recommend reducing your configuration size if possible, for example, by removing unused objects.

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.

For very large configurations, you may need to specify a heap size up to 2 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.

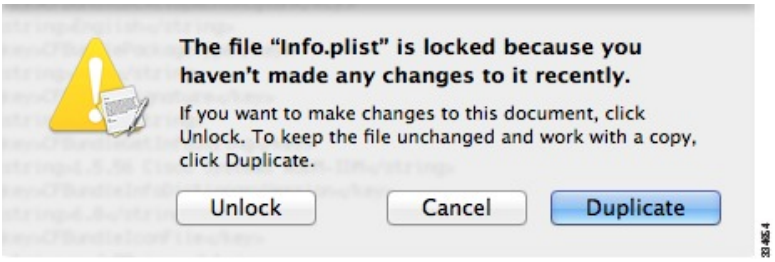
```
<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

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


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

For very large configurations, you may need to specify a heap size up to 2 GB.

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 9.20(4)/ASDM 7.20(4)

Released: July 2, 2025

Feature	Description
License Features	
Smart Transport is the default Smart Licensing transport	Smart Licensing now uses Smart Transport as the default transport. You can optionally enable the former type, Smart Call Home, if necessary. New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing** *Also in 9.22(1).*
Administrative, Monitoring, and Troubleshooting Features	

Feature	Description
SSH X.509 certificate authentication	You can now use an X.509v3 certificate to authenticate a user for SSH (RFC 6187). For the Firepower 4100/9300, you need FXOS version 2.16(2.109+) or 2.18+. **Note** The bundled version of ASDM 7.20(4) does not include support for this feature. Download and install ASDM 7.20(4) from Cisco.com for feature support. Be sure to change the image name to asdm.bin if you want to overwrite the bundled version. New/Modified screens: • **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization** • **Configuration** > **Device Management** > **Certificate Management** > **CA Certificates** > **Add/Edit Trustpoint** > **Advanced** • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** *Also in 9.22(3), 9.24(1).*
AES-256-GCM SSH cipher	The ASA supports the AES-256-GCM cipher for SSH. It is enabled by default for **all** and **high** encryption levels. New/Modified screens: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** *Also in 9.22(3), 9.24(1).*
Display of UDP's initiator and responder values in connection status output	For UDP traffic flows, the ASA displays the initiator and responder field values in the connection detail status. These field values indicate the direction of communication, which helps in troubleshooting network connectivity issues.

New Features in ASA 9.20(3)

Released: July 31, 2024

Feature	Description
Platform Features	

Feature	Description
ASA Virtual AWS IMDSv2 support	AWS Instance Metadata Service version 2 (IMDSv2) API is now supported on ASA Virtual, which allows you to retrieve and validate instance metadata. IMDSv2 provides additional security against vulnerabilities targeting the Instance Metadata Service. When deploying ASA Virtual on AWS, you can now configure the Metadata version for ASA Virtual as follows: • ASA Virtual 9.20(3) and later supports IMDSv2 only (token required) – Set "V2 only (token required)" to enable IMDSv2. • Earlier ASA Virtual versions support only IMDSv1 APIs via the IMDS option - 'IMDSv1 or IMDSv2 (token optional)' – Set "V1 and V2 (token optional). If you have an existing ASA Virtual deployment, you can migrate to "IMDSv2 Required" mode after upgrading to 9.20(3) and later. See AWS documentation, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-options.html For more information, see Cisco Secure Firewall ASA Virtual Getting Started Guide, 9.20.
Firewall Features	
Threat Detection for VPN services	You can configure threat detection for VPN services to protect against the following types of VPN attack from IPv4 addresses: • Excessive failed authentication attempts to a remote access VPN, for example brute-force username/password scanning. • Client initiation attacks, where the attacker starts but does not complete repeated connection attempts to a remote access VPN head-end from a single host. • Access attempts to invalid VPN services, that is, services that are for internal use only. These attacks, even when unsuccessful in their attempt to gain access, can consume computational resources and in some cases result in Denial of Service. The following commands were introduced or changed: **clear threat-detection service**, **show threat-detection service**, **shun**, **threat-detection service**.
VPN Features	
Multiple IdP certificates in a webvpn configuration and a tunnel-group	You can now configure tunnel-group-specific IdP certificates and multiple IdP certificates in a webvpn configuration. This feature lets you trust an old certificate as well as a new certificate, making migration to the new certificate easier. New/Modified commands: **saml idp-trustpoint**, **trustpoint idp** No ASDM support
Rate Limit for Preauthenticated SSL Connections	ASA Virtual can rate-limit preauthenticated SSL connections. This limit is calculated as three times the VPN connection limit of the device. When this limit exceeds, no new SSL connections are allowed. The device allows new SSL connections only after the preauthenticated SSL connections count becomes zero. However, this restriction is not valid for management connections. New/Modified commands: **show counters** No ASDM support

New Features in ASA 9.20(2)/ASDM 7.20(2)

Released: December 13, 2023

Feature	Description
Platform Features	
100GB network module support for the Secure Firewall 3100	You can now use the 100GB network module for the Secure Firewall 3100. This module is also supported for the Secure Firewall 4200.
Increased connection limits for the Secure Firewall 4200	Connection limits have been increased: • 4215: 15M → **40M** • 4225: 30M → **80M** • 4245: 60M → **80M**
ASAv on OCI: Additional instances	ASA Virtual instances on OCI now supports additional shapes to achieve the highest performance and throughput level.
High Availability and Scalability Features	
ASAv on Azure: Clustering with Gateway Load Balancing	We now support the ASA virtual clustering deployment on Azure using the Azure Resource Manager (ARM) template and then configure the ASAv clusters to use the Gateway Load Balancer (GWLB) for load balancing the network traffic. New/Modified screens:
ASAv on AWS: Resiliency for clustering with Gateway Load Balancing	You can configure the Target Failover option in the Target Groups service of AWS, which helps GWLB to forward existing flows to a healthy target in the event of virtual instance failover. In the ASAv clustering, each instance is associated with a Target Group, where the Target Failover option is enabled. It helps GWLB to identify an unhealthy target and redirect or forward the network traffic to a healthy instance identified or registered as a target node in the target group.
Configurable delay to rejoin cluster after chassis heartbeat failure (Firepower 4100/9300)	By default, if the chassis heartbeat fails and then recovers, the node rejoins the cluster immediately. However, if you configure the **health-check chassis-heartbeat-delay-rejoin** command, it will rejoin according to the settings of the **health-check system auto-rejoin** command. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Auto Rejoin**
show failover statistics includes client statistics	The failover client packet statistics are now enhanced to improve debuggability. The **show failover statistics** command is enhanced to display **np-clients** (data-path clients) and **cp-clients** (control-plane clients) information. Modified commands: **show failover statistics cp-clients**, **show failover statistics np-clients** *Also in 9.18(4).*

Feature	Description
show failover statistics events includes new events	The **show failover statistics events** command is now enhanced to identify the local failures notified by the App agent: failover link uptime, supervisor heartbeat failures, and disk full issues. Modified commands: **show failover statistics events** *Also in 9.18(4).*
VPN Features	
Support for RSA PSS-based certificate	ASA now supports certificates signed with RSA Probabilistic Signature Scheme (RSA-PSS) method.

New Features in ASA 9.20(1)/ASDM 7.20(1)

Released: September 7, 2023

Note This release is only supported on the Secure Firewall 4200.

Feature	Description
Platform Features	
Secure Firewall 4200	We introduced the ASA for the Secure Firewall 4215, 4225, and 4245. The Secure Firewall 4200 supports up to 8 units for Spanned EtherChannel clustering. You can hot swap a network module of the same type while the firewall is powered up without having to reboot; making other module changes requires a reboot. Secure Firewall 4200 25 Gbps and higher interfaces support Forward Error Correction as well as speed detection based on the SFP installed. The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. There are two Management interfaces.
Firewall Features	
ASDM support for the **sysopt connection tcp-max-unprocessed-seg** command	You can set the maximum number of TCP unprocessed segments, from 6 to 24. The default is 6. If you find that SIP phones are not connecting to the call manager, you can try increasing the maximum number of unprocessed TCP segments. New/Modified screens: **Configuration** > **Firewall** > **Advanced** > **TCP Options**.
ASP rule engine compilation offloaded to the data plane.	By default, ASP rule engine compilation is offloaded to the data plane (instead of the control plane) when any rule-based policy (for example, ACL, NAT, VPN) has more than 100 rule updates. The offload leaves more time for the control plane to perform other tasks. We added or modified the following commands: **asp rule-engine compile-offload**, **show asp rule-engine**.
High Availability and Scalability Features	

Feature	Description
Reduced false failovers for ASA high availability	We now introduced an additional heartbeat module in the data plane of the ASA high availability. This heartbeat module helps to avoid false failovers or split-brain scenarios that can happen due to traffic congestion in the control plain or CPU overload. *Also in 9.18(4).*
Configurable cluster keepalive interval for flow status	The flow owner sends keepalives (clu_keepalive messages) and updates (clu_update messages) to the director and backup owner to refresh the flow state. You can now set the keepalive interval. The default is 15 seconds, and you can set the interval between 15 and 55 seconds. You may want to set the interval to be longer to reduce the amount of traffic on the cluster control link. New/Modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Cluster Configuration**
Routing Features	
EIGRPv6	You can now configure EIGRP for IPv6 and manage them separately. You must explicitly enable IPv6 when configuring EIGRP on each interface. New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **EIGRPv6** , **Setup**, **Filter Rules**,**Interface**,**Passive Interface**, **Redistribution**, **Static Neighbor** tabs.
Path monitoring through HTTP client	PBR can now use the performance metrics (RTT, jitter, packet-lost, and MOS) collected by path monitoring through HTTP client on the application domain rather than the metrics on a specific destination IP. HTTP-based application monitoring option is enabled by default for the interface. HTTP based path-monitoring can be configured on the interface using Network Service Group objects. You can configure a PBR policy with match ACL having the monitored applications and interface ordering for path determination. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Path Monitoring**
Interface Features	
VXLAN VTEP IPv6 support	You can now specify an IPv6 address for the VXLAN VTEP interface. IPv6 is not supported for the ASA Virtual cluster control link or for Geneve encapsulation. New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **VXLAN** • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VNI Interface**
Loopback interface support for DNS, HTTP, ICMP, and IPsec Flow Offload	You can now add a loopback interface and use it for: • DNS • HTTP • ICMP • IPsec Flow Offload

Feature	Description
License Features	
IPv6 for Cloud services such as Smart Licensing and Smart Call Home	ASA now supports IPv6 for Cloud services such as Smart Licensing and Smart Call Home.
Certificate Features	
IPv6 PKI for OCSP and CRL	ASA now supports both IPv4 and IPv6 OCSP and CRL URLs. When using IPv6 in the URLs, it must be enclosed with square brackets. New/Modified screens: **Configuration** > **Site-to-Site VPN** > **Certificate Management** > **CA Certificates** > **Add**
Administrative, Monitoring, and Troubleshooting Features	
Rate limiting for SNMP syslogs	If you do not set system-wide rate limiting, you can now configure rate limiting separately for syslogs sent to an SNMP server. New/Modified commands: **logging history rate-limit**
Packet Capture for switches	You can now configure to capture egress and ingress traffic packets for a switch. This option is applicable only for Secure Firewall 4200 model devices. New/Modified screens: **Wizards** > **Packet Capture Wizard** > **Ingress Traffic Selector**and **Wizards** > **Packet Capture Wizard** > **Egress Traffic Selector**
VPN Features	
Crypto debugging enhancements	Following are the enhancements for crypto debugging: • Crypto archive is now available in two formats: text and binary format. • Additional SSL counters. • Stuck encrypt rules can be removed from the ASP table without rebooting the device.
Multiple Key Exchanges for IKEv2	ASA supports multiple key exchanges in IKEv2 to secure the IPsec communication from quantum computer attacks.
Secure Client connection authentication using SAML	In a DNS load balancing cluster, when SAML authentication is configured on ASAs, you can specify a local base URL that uniquely resolves to the device on which the configuration is applied. New/Modified screens: **Configuration > Remote Access VPN > Network (Client) Access > Secure Client Connection Profiles > Add/Edit > Basic > SAML Identity Provider > Manage > Add/Edit**
ASDM Features	
Windows 11 support	ASDM has been verified to operate on Windows 11.

Upgrade the Software

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

Upgrade Link

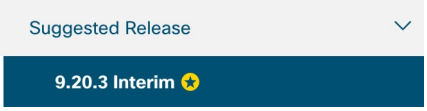
To complete your upgrade, see the ASA upgrade guide.

Upgrade Path: ASA Appliances

What Version Should I Upgrade To?

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

Figure 4: Suggested Release



View Your Current Version

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

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

Upgrade Guidelines

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

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

Upgrade Paths

This table provides upgrade paths for ASA.

Note ASA 9.18 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
9.19	—	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

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

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

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

Upgrade Path: ASA on Firepower 2100 in Platform Mode

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

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

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

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

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

Table 3: 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**

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

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

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

- FXOS: From FXOS 2.2.2 and later, you can upgrade directly to any higher version. (FXOS 2.0.1–2.2.1 can upgrade as far as 2.8.1. For versions earlier than 2.0.1, you need to upgrade to each intermediate version.) Note that you cannot upgrade FXOS to a version that does not support your current logical device version. You will need to upgrade in steps: upgrade FXOS to the highest version that supports your current logical device; then upgrade your logical device to the highest version supported with that FXOS version. For example, if you want to upgrade from FXOS 2.2/ASA 9.8 to FXOS 2.13/ASA 9.19, you would have to perform the following upgrades:

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

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

Table 4: Firepower 4100/9300 Compatibility with ASA and Firewall Threat Defense

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

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

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

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

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

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

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

Note on Downgrades

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

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

This section lists open bugs in each version.

Open Bugs in Version 7.20(4)

There are no open bugs in this release.

Open Bugs in Version 7.20(2)

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

Identifier	Headline
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

Open Bugs in Version 7.20(1)

There are no open bugs in this release.

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.20(4)

There are no resolved bugs in this release.

Resolved Bugs in Version 7.20(2)

There are no resolved bugs in this release.

Resolved Bugs in Version 7.20(1)

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

Identifier	Headline
CSCwc48458	Anyconnect authenticated user not showing in GET results for /api/monitoring/authusers
CSCwd23375	ASDM - SSL cert verification vulnerability
CSCwe00348	Unable to update hostscan file from ASDM ,Unable to edit the DAP if we install hostscan image
CSCwe34665	Unable to Edit the ACL objects if it is already in use, getting the exception.
CSCwf11170	Post Quantum key validation needs to be handled properly.
CSCwf71723	ASDM losing configured objects/object groups

Cisco General Terms

The Cisco General Terms (including other related terms) govern 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)

© 2026 Cisco Systems, Inc. All rights reserved.