



Release Notes for Cisco Secure Firewall ASDM, 7.18(x)

First Published: 2022-06-06

Last Modified: 2023-12-15

Release Notes for Cisco Secure Firewall ASDM, 7.18(x)

This document contains release information for ASDM Version 7.18(x) for the Secure Firewall ASA series.

Important Notes

- **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](#))
- **Downgrade issue from 9.18 or later**—There is a behavior change in 9.18 where the **access-group** command will be listed before its **access-list** commands. If you downgrade, the **access-group** command will be rejected because it has not yet loaded the **access-list** commands. This outcome occurs even if you had previously enabled the **forward-reference enable** command, because that command is now removed. Before you downgrade, be sure to copy all **access-group** commands manually, and then after downgrading, re-enter them.
- **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](#))
- **Behavior change for Secure Firewall 3100 in 9.18(2.7)**—When you set the FEC to Auto using the **fec** command on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. ([CSCwc75082](#))
- **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.
- **ASDM 7.18 ending support for Java Web Launch**—Starting with ASDM 7.18, ASDM will no longer support Java Web Start due to Oracle’s end of support for JRE 8 and Java Network Launching Protocol (JNLP). You will have to install the ASDM Launcher to launch ASDM.

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**).



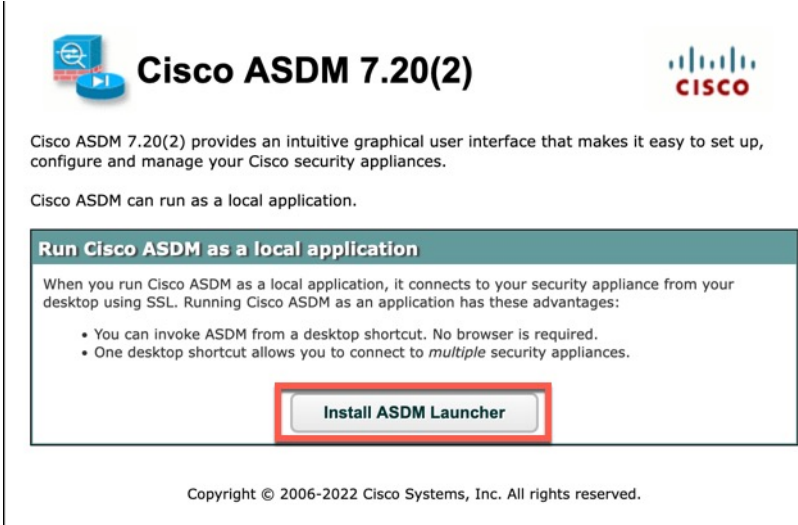
Note ASDM is not tested on Linux.

Table 1: ASDM Operating System and Browser Requirements


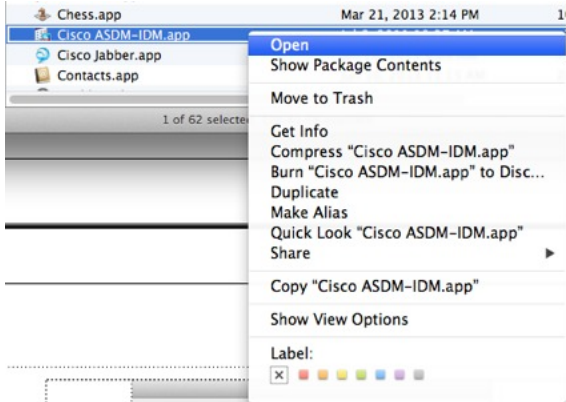

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): <ul style="list-style-type: none"> • 10 • 8 • 7 • Server 2016 and Server 2019 • Server 2012 R2 • Server 2012 • Server 2008 <p>Note See Windows 10 in ASDM Compatibility Notes, on page 2 if you have problems with the ASDM shortcut.</p>	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>
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\System32C:\Users\<username>\.asdm • 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>

Conditions	Notes
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>371081</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>371082</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

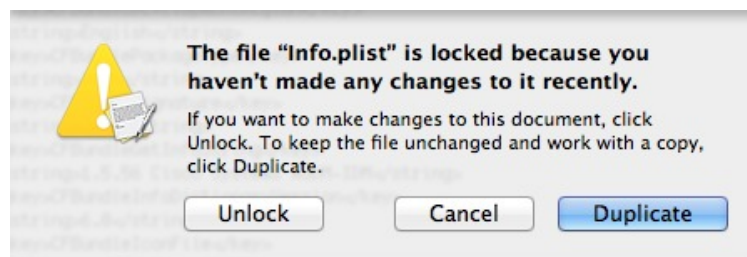
-
- Step 1** Right-click the **Cisco ASDM-IDM** icon, and choose **Show Package Contents**.
 - Step 2** In the **Contents** folder, double-click the **Info.plist** file. If you have Developer tools installed, it opens in the **Property List Editor**. Otherwise, it opens in **TextEdit**.
 - Step 3** Under **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 ASDM 7.18(1.161)

Released: July 3, 2023

There are no new features in this release.

New Features in ASA 9.18(4)/ASDM 7.20(1)

Released: October 3, 2023

Feature	Description
High Availability and Scalability Features	
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. <i>Also in 9.20(1).</i>
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 dp-clients <i>Also in 9.20(2).</i>

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 <i>Also in 9.20(2).</i>
Interface Features	
FXOS local-mgmt show command improvements	See the following additions for interface show commands in FXOS local-mgmt: <ul style="list-style-type: none"> • Added the show portmanager switch tail-drop-allocated buffers all command • Include Ethernet port ID in show portmanager switch status command • For the Secure Firewall 3100, added the show portmanager switch default-rule-drop-counter command New/Modified FXOS commands: show portmanager switch tail-drop-allocated buffers all , show portmanager switch status , show portmanager switch default-rule-drop-counter
Administrative, Monitoring, and Troubleshooting Features	
show tech support improvements	Added output to show tech support for: <ul style="list-style-type: none"> • show storage detail, show slot expand detail for the Secure Firewall 3100 in show tech support brief • Recent messages from dpdk.log in the flash for the ASA Virtual • Control link state for the Firepower 1010 • show failover statistics • FXOS local-mgmt show portmanager switch tail-drop-allocated buffers all • show controller • DPDK mbuf pool statistics New/Modified commands: show tech support

New Features in ASA 9.18(3)/ASDM 7.19(1.90)

Released: February 16, 2023

Feature	Description
Interface Features	

Feature	Description
Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers	When you set the FEC to Auto on the Secure Firewall 3100 fixed ports, the default type is now set to cl108-rs instead of cl74-fc for 25 GB SR, CSR, and LR transceivers. New/Modified screens: Configuration > Device Setup > Interface Settings > Interfaces > Edit Interface > Configure Hardware Properties > FEC Mode <i>Also in 9.19(1) and 9.18(2.7).</i>
VPN Features	
AnyConnect 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 Features in ASA 9.18(2)/ASDM 7.18(1.152)

Released: August 10, 2022

Feature	Description
Interface Features	
Loopback interface support for BGP and management traffic	You can now add a loopback interface and use it for the following features: <ul style="list-style-type: none"> • AAA • BGP • SNMP • SSH • Syslog • Telnet New/Modified commands: interface loopback , logging host , neighbor update-source , snmp-server host , ssh , telnet No ASDM support.
ping command changes	To support pinging a loopback interface, the ping command now has changed behavior. If you specify the interface in the command, the source IP address matches the specified interface IP address, but the actual egress interface is determined by a route lookup using the data routing table. New/Modified commands: ping

New Features in ASDM 7.18(1.152)

Released: August 2, 2022

There are no new features in this release.

New Features in ASA 9.18(1)/ASDM 7.18(1)

Released: June 6, 2022

Feature	Description
Platform Features	
ASAv-AWS Security center integration for AWS GuardDuty	You can now integrate Amazon GuardDuty service with ASAv. The integration solution helps you to capture and process the threat analysis data or results (malicious IP addresses) reported by Amazon GuardDuty. You can configure and feed these malicious IP addresses in the ASAv to protect the underlying networks and applications.
Firewall Features	
Forward referencing of ACLs and objects is always enabled. In addition, object group search for access control is now enabled by default.	<p>You can refer to ACLs or network objects that do not yet exist when configuring access groups or access rules.</p> <p>In addition, object group search is now enabled by default for access control for <i>new</i> deployments. Upgrading devices will continue to have this command disabled. If you want to enable it (recommended), you must do so manually.</p> <p>Caution If you downgrade, the access-group command will be rejected because it has not yet loaded the access-list commands. This outcome occurs even if you had previously enabled the forward-reference enable command, because that command is now removed. Before you downgrade, be sure to copy all access-group commands manually, and then after downgrading, re-enter them.</p> <p>We removed the forward-reference enable command and changed the default for new deployments for object-group-search access-control to enabled.</p>
Routing Features	
Path monitoring metrics in PBR.	<p>PBR uses the metrics to determine the best path (egress interface) for forwarding the traffic. Path monitoring periodically notifies PBR with the monitored interface whose metric got changed. PBR retrieves the latest metric values for the monitored interfaces from the path monitoring database and updates the data path.</p> <p>New/Modified screens: Configuration > Device Setup > Interface Settings > Interfaces</p>
Interface Features	
Pause Frames for Flow Control for the Secure Firewall 3100	<p>If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue.</p> <p>New/Modified screens: Configuration > Device Settings > Interfaces > General</p>

Feature	Description
Breakout ports for the Secure Firewall 3130 and 3140	You can now configure four 10GB breakout ports for each 40GB interface on the Secure Firewall 3130 and 3140. New/Modified screens: Configuration > Device Management > Advanced > EPM
License Features	
Secure Firewall 3100 support for the Carrier license	The Carrier license enables Diameter, GTP/GPRS, SCTP inspection. New/Modified screens: Configuration > Device Management > Licensing > Smart Licensing.
Certificate Features	
Mutual LDAPS authentication.	You can configure a client certificate for the ASA to present to the LDAP server when it requests a certificate to authenticate. This feature applies when using LDAP over SSL. If an LDAP server is configured to require a peer certificate, the secure LDAP session will not complete and authentication/authorization requests will fail. New/Modified screens: Configuration > Device Management > Users/AAA > > AAA Server Groups , Add/Edit LDAP server.
Authentication: Validate certificate name or SAN	When a feature specific reference-identity is configured, the peer certificate identity is validated with the matching criteria specified under crypto ca reference-identity <name> submode commands. If there is no match found in the peer certificate Subject Name/SAN or if the FQDN specified with reference-identity submode command fail to resolve, the connection is terminated The reference-identity CLI is configured as a submode command for aaa-server host configuration and ddns configuration. New/Modified screens: <ul style="list-style-type: none"> • Configuration > Device Management > Users/AAA > > AAA Server Groups > LDAP Parameters for authentication/authorization • Configuration > Device Management > DNS > Dynamic DNS > Update Methods
Administrative, Monitoring, and Troubleshooting Features	
Multiple DNS server groups	You can now use multiple DNS server groups: one group is the default, while other groups can be associated with specific domains. A DNS request that matches a domain associated with a DNS server group will use that group. For example, if you want traffic destined to inside eng.cisco.com servers to use an inside DNS server, you can map eng.cisco.com to an inside DNS group. All DNS requests that do not match a domain mapping will use the default DNS server group, which has no associated domains. For example, the DefaultDNS group can include a public DNS server available on the outside interface. New/Modified screens: Configuration > Device Management > DNS > DNS Client
Dynamic Logging Rate-limit	A new option to limit logging rate when block usage exceeds a specified threshold value was added. It dynamically limits the logging rate as the rate limiting is disabled when the block usage returns to normal value. New/Modified screens: Configuration > Device Management > Logging > Rate Limit

Feature	Description
Packet Capture for Secure Firewall 3100 devices	The provision to capture switch packets was added. This option can be enabled only for Secure Firewall 3100 devices. New/Modified screens: Wizards > Packet Capture Wizard > Buffers & Captures
VPN Features	
IPsec flow offload.	On the Secure Firewall 3100, IPsec flows are offloaded by default. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. New/Modified screens: Configuration > Firewall > Advanced > IPsec Offload
Certificate and SAML for Authentication	You can configure remote access VPN connection profiles for certificate and SAML authentication. Users can configure VPN settings to authenticate a machine certificate or user certificate before a SAML authentication/authorization is initiated. This can be done using DAP certificate attributes along with user specific SAML DAP attributes. New/Modified screens: Configuration > Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles > Add/Edit > Basic

Upgrade the Software

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

ASA Upgrade Path

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**.



Note 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.



Note For guidance on security issues on the ASA, and which releases contain fixes for each issue, see the [ASA Security Advisories](#).



- Note** 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.

Current Version	Interim Upgrade Version	Target Version
9.17	—	Any of the following: → 9.18
9.16	—	Any of the following: → 9.18 → 9.17
9.15	—	Any of the following: → 9.18 → 9.17 → 9.16
9.14	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15
9.13	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14

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

Current Version	Interim Upgrade Version	Target Version
9.7	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.6	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.5	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8

Current Version	Interim Upgrade Version	Target Version
9.4	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.3	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 9.14 → 9.12 → 9.8
9.2	—	Any of the following: → 9.18 → 9.17 → 9.16 → 9.15 → 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)

Current Version	Interim Upgrade Version	Target Version
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)
8.4(5+)	—	Any of the following: → 9.12 → 9.8 → 9.1(7.4) → 9.0(4)

Current Version	Interim Upgrade Version	Target Version
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 Link

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

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 7.18(1.161)

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

Open Bugs in Version 7.18(1.152)

Identifier	Headline
CSCvu01215	Appliance mode : checksum does not match issue while downloading asa image from CCO
CSCvv83043	Cipher changes require in VPN wizard according to 9161/7161 CLIs

Open Bugs in Version 7.18(1.152)

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

Identifier	Headline
CSCvu01215	Appliance mode : checksum does not match issue while downloading asa image from CCO
CSCvv83043	Cipher changes require in VPN wizard according to 9161/7161 CLIs

Open Bugs in Version 7.18(1)

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

Identifier	Headline
CSCvu01215	Appliance mode : checksum does not match issue while downloading asa image from CCO
CSCvv83043	Cipher changes require in VPN wizard according to 9161/7161 CLIs

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.18(1.161)

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

Identifier	Headline
CSCwd58653	ASDM initial connection/load time increased
CSCwd85545	ASDM will delete all class-map configuration due delete class-map ACL that configured from CLI
CSCwd98702	"Where used" option in ASDM not working
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.
CSCwe52019	ASDM Fails to Launch with security exception error - invalid SHA1 signature file

Resolved Bugs in Version 7.18(1.152)

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

Identifier	Headline
CSCvw79912	Cisco Adaptive Security Device Manager Remote Code Execution Vulnerability
CSCwb05264	Cisco ASDM and ASA Software Client-side Arbitrary Code Execution Vulnerability

Resolved Bugs in Version 7.18(1)

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

Identifier	Headline
CSCvv17403	Check box not available for disable delete tunnel with no delay in simultaneous connection preempt
CSCvx31842	Hostscan 4.3.x to 4.6.x Migration steps should not be display when the SDM have the HS 4.10.x
CSCvy17527	"load balancing" item is not displayed on ASDM.
CSCvy38427	ASDM: Transforms file name must start with "_" underscore to take effect to multiple AC modules
CSCvz62261	Unable to restrict user access when using ASDM
CSCvz89126	ASDM session/quota count mismatch in ASA when multiple context switchover is done from ASDM
CSCwa48034	ASDM side changes for the ASA #CSCvz89126
CSCwa70482	ASDM on MAC popup remove hostscan/CSD pkg
CSCwa99370	ASDM:DAP config missing AAA Attributes type (Radius/LDAP)
CSCwb84225	Evaluation OpenJDK CVEs for ASDM & ASA REST API

End-User License Agreement

For information on the end-user license agreement, go to <http://www.cisco.com/go/warranty>.

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)

© 2023 Cisco Systems, Inc. All rights reserved.