Release Notes for Cisco Secure Firewall ASDM, 7.19(x)

First Published: 2022-11-29

Last Modified: 2023-07-20

Release Notes for Cisco Secure Firewall ASDM, 7.19(x)

This document contains release information for ASDM Version 7.19(x) for the Secure Firewall ASA series.

Important Notes

- **No support in ASA 9.19(1) and later for the Firepower 4110, 4120, 4140, 4150, and Security Modules SM-24, SM-36, and SM-44 for the Firepower 9300**—ASA 9.18(x) is the last supported version.
- **ASDM 7.19(1) requires Oracle Java version 8u261 or later**—Before you upgrade to ASDM 7.19, be sure to update Oracle Java (if used) to version 8u261 or later. This version supports TLSv1.3, which is required to upgrade the ASDM Launcher. OpenJRE is not affected.
- **ASDM Upgrade Wizard**—Due to an internal change, starting in March 2022 the upgrade wizard will no longer work with pre-ASDM 7.17(1.150) versions. You must manually upgrade to 7.17(1.150) or later to use the wizard.

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): • 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

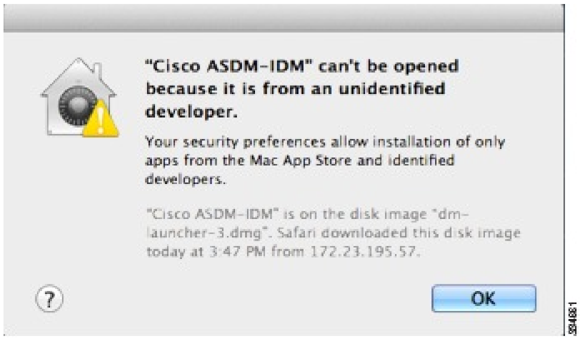
The following table lists compatibility caveats for ASDM.

Conditions	Notes
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.

Conditions	Notes
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.

<table>
<tr><th>Conditions</th><th>Notes</th></tr>
<tr><td>OS X 10.8 and later</td><td>

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.

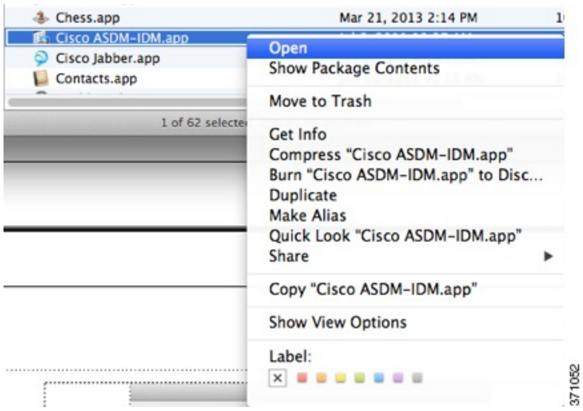


"Cisco ASDM-IDM" can't be opened because it is from an unidentified developer.

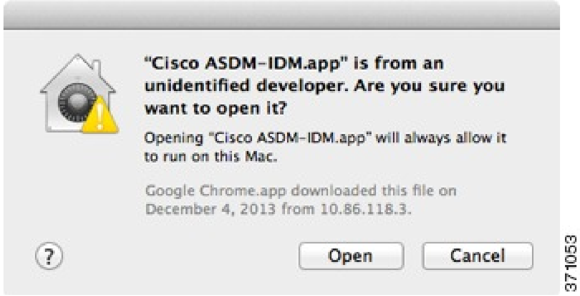
Your security preferences allow installation of only apps from the Mac App Store and identified developers.

"Cisco ASDM-IDM" is on the disk image "dm-launcher-3.dmg". Safari downloaded this disk image today at 3:47 PM from 172.23.195.57.

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.



"Cisco ASDM-IDM.app" is from an unidentified developer. Are you sure you want to open it?

Opening "Cisco ASDM-IDM.app" will always allow it to run on this Mac.

Google Chrome.app downloaded this file on December 4, 2013 from 10.86.118.3.

</td></tr>
</table>

Conditions	Notes
Requires Strong Encryption license (3DES/AES) on ASA **Note** Smart licensing models allow initial access with ASDM without the Strong Encryption license.	ASDM requires an SSL connection to the ASA. You can request a 3DES license from Cisco: **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.
• 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. You can use Java Web Start to launch ASDM until you install a 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.

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

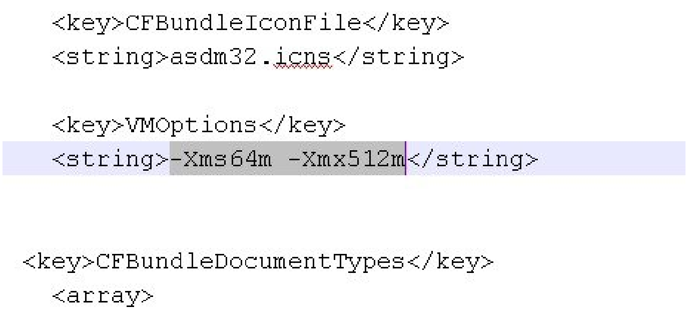
To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

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.

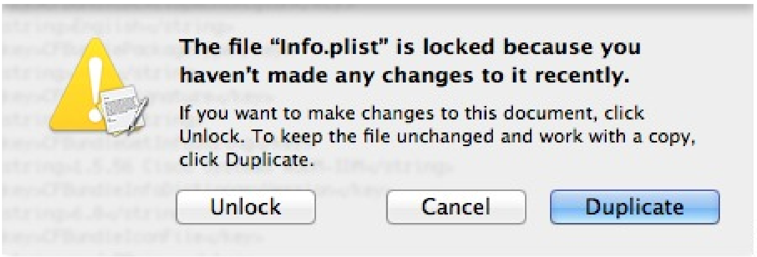


```
  <key>CFBundleIconFile</key>
  <string>asdm32.icns</string>

  <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:


The file "Info.plist" is locked because you haven't made any changes to it recently.

If you want to make changes to this document, click Unlock. To keep the file unchanged and work with a copy, click Duplicate.

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 7.19(1.95)

Released: July 5, 2023

There are no new features in this release.

New Features in ASA 9.19(1)/ASDM 7.19(1)

Released: November 29, 2022

Feature	Description
Platform Features	
Secure Firewall 3105	We introduced the ASA for the Secure Firewall 3105.

Feature	Description
ASA virtual Auto Scale solution with Azure Gateway Load Balancer	You can now deploy the ASA virtual Auto Scale Solution with Gateway Load Balancer on Microsoft Azure. See the Interfaces features for more information.
Firewall Features	
Network service groups support	You can now define a maximum of 1024 network service groups.
High Availability and Scalability Features	
Removal of biased language	Commands, command output, and syslog messages that contained the terms "Master" and "Slave" have been changed to "Control" and "Data." New/Modified commands: **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
ASA virtual Amazon Web Services (AWS) clustering	The ASA virtual supports Individual interface clustering for up to 16 nodes on AWS. You can use clustering with or without the AWS Gateway Load Balancer. No ASDM support.
Routing Features	
BGP graceful restart support for IPv6	We added BGP graceful restart support for IPv6 address family. New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv6 Family** > **Neighbour**
ASDM support for loopback interfaces for BGP traffic	ASDM now supports setting a loopback interface as the source interface for BGP neighborship. The loopback interface helps to overcome path failures. New/Modified screens: **Configuration** > **Device Setup** > **Routing** > **BGP** > **IPv4 Family / IPv6 Family** > **Neighbor** > **Add** > **General**
Interface Features	
ASA virtual support for IPv6	ASAv to support IPv6 network protocol on Private and Public Cloud platforms. Users can now: • Enable and configure an IPv6 management address via day0 configuration. • Assign IPv6 addresses using DHCP and static methods.
Paired proxy VXLAN for the ASA virtual for the Azure Gateway Load Balancer	You can configure a paired proxy mode VXLAN interface for the ASA virtual in Azure for use with the Azure Gateway Load Balancer (GWLB). The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy. New/Modified commands: **external-port, external-segment-id, internal-port, internal-segment-id, proxy paired** No ASDM support.

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**
ASDM support for loopback interfaces	ASDM now supports loopback interfaces. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add Loopback Interface**
License Features	
ASA virtual permanent license reservation support for the ASAv5 on KVM and VMware	A new command is available that you can execute to override the default PLR license entitlement and request the Cisco Smart Software Manager (SSM) to issue an ASAv5 PLR license when you are deploying ASAv with 2GB RAM on KVM and VMware. You can modify the same command by adding the <*no*> form to revert the license entitlement from ASAv5 to the default PLR license in correspondence to the RAM configuration.
VPN Features	
VTI loopback interface support	You can now set a loopback interface as the source interface for a VTI. Support has also been added to inherit the IP address from a loopback interface instead of a statically configured IP address. The loopback interface helps to overcome path failures. If an interface goes down, you can access all interfaces through the IP address assigned to the loopback interface. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add VTI Interface** > **Advanced**
Dynamic Virtual Tunnel Interface (dynamic VTI) support	The ASA is enhanced with dynamic VTI. A single dynamic VTI can replace several static VTI configurations on the hub. You can add new spokes to a hub without changing the hub configuration. Dynamic VTI supports dynamic (DHCP) spokes. New/Modified screens: **Configuration > Device Setup > Interface Settings > Interfaces > Add > DVTI Interface**
VTI support for EIGRP and OSPF	EIGRP and OSPFv2/v3 routing is now supported on the Virtual Tunnel Interface. You can now use these routing protocol to share routing information and to route traffic flow through VTI-based VPN tunnel between peers
TLS 1.3 in Remote Access VPN	You can now use TLS 1.3 to encrypt remote access VPN connections. TLS 1.3 adds support for the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 This feature requires Cisco Secure Client, Version 5.0.01242 and above. New/Modified screens: **Configuration > Device Management > Advanced > SSL Settings**

Feature	Description
Dual Stack support for IKEv2 third-party clients	Secure Firewall ASA now supports dual stack IP request from IKEv2 third-party remote access VPN clients. If the third-party remote access VPN client requests for both IPv4 and IPv6 addresses, ASA can now assign both IP version addresses using multiple traffic selectors. This feature enables third-party remote access VPN clients to send IPv4 and IPv6 data traffic using the single IPsec tunnel.
Traffic selector for static VTI interface	You can now assign a traffic selector for a static VTI interface.

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

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

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

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

ASA 9.2(x) was the final version for the ASA 5505.

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

Current Version	Interim Upgrade Version	Target Version
9.18(x)	—	Any of the following: → **9.19(x)**
9.17(x)	—	Any of the following: → **9.19(x)** → **9.18(x)**
9.16(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x)
9.15(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)**
9.14(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x)
9.13(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)

Current Version	Interim Upgrade Version	Target Version
9.12(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.10(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.9(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)

Current Version	Interim Upgrade Version	Target Version
9.8(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.6(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.5(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.4(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.3(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)

Current Version	Interim Upgrade Version	Target Version
9.2(x)	—	Any of the following: → **9.19(x)** → **9.18(x)** → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
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(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.14(x) → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ **9.12(x)** → 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → **9.12(x)** → 9.8(x) → 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 7.19(1.95)

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

Identifier	Headline
CSCwc48458	Anyconnect authenticated user not showing in GET results for /api/monitoring/authusers

Open Bugs in Version 7.19(1.90)

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

Identifier	Headline
CSCwc48458	Anyconnect authenticated user not showing in GET results for /api/monitoring/authusers
CSCwd58653	ASDM initial connection/load time increased

Open Bugs in Version 7.19(1)

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

Identifier	Headline
CSCwc48458	Anyconnect authenticated user not showing in GET results for /api/monitoring/authusers
CSCwd58653	ASDM initial connection/load time increased

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.19(1.95)

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
CSCwf74697	ASDM version 7.19.1.94 openJRE version file in the backend still showing OracleJRE version

Resolved Bugs in Version 7.19(1.90)

There were no resolved bugs in this release.

Resolved Bugs in Version 7.19(1)

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

Identifier	Headline
CSCwc21296	Cisco ASDM MSI Installer Not Properly Signed
CSCwc63675	Some contexts of the ASA are not sending logs to the real time logs of the ASDM
CSCwc84975	SAML configuration is not persistent in ASDM.
CSCwd16386	ASDM:DAP config missing AAA Attributes type (Radius/LDAP)
CSCwd19658	ASDM incorrectly sets the default group to DH 5 for IKEv1 Site-to-Site VPN

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.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.