Release Notes for Cisco ASDM, 7.17(x)

Release Notes for Cisco ASDM, 7.17(x)

This document contains release information for Cisco ASDM Version 7.17(x) for the Cisco ASA series.

Important Notes

- **ASDM signed-image support in 9.17(1.13)/7.18(1.152) and later**—The ASA now validates whether the ASDM image is a Cisco digitally signed image. If you try to run an older ASDM image with an ASA version with this fix, ASDM will be blocked and the message "%ERROR: Signature not valid for file disk0:/<filename>" will be displayed at the ASA CLI. ASDM release 7.18(1.152) and later are backwards compatible with all ASA versions, even those without this fix. (CSCwb05291, CSCwb05264)
- **No support for the ASA 5506-X, 5506H-X, 5506W-X, ASA 5508-X, and ASA 5516-X in 9.17(1) and later**—ASA 9.16(x) is the last supported version. For the ASA FirePOWER module on the ASA 5508-X and 5516-X, the last supported combination is 9.16/7.0.
- **No support for the ASA FirePOWER module on the ISA 3000 in 9.17(1) and later**—The ISA 3000 continues to be supported in ASA 9.17 and later; however, the last supported combination for the ASA FirePOWER module is 9.16/7.0.
- **No support for Clientless SSL VPN in 9.17(1) and later**—Clientless SSL VPN is no longer supported.
    - **webvpn**—The following subcommands are removed:
        - **apcf**
        - **java-trustpoint**
        - **onscreen-keyboard**
        - **port-forward**
        - **portal-access-rule**
        - **rewrite**
        - **smart-tunnel**
    - **group-policy webvpn**—The following subcommands are removed:
        - **port-forward**
        - **smart-tunnel**
        - **ssl-clientless**
- **ASDM Upgrade Wizard**—Due to an internal change, starting in March 2022 the upgrade wizard will no longer work with pre-ASDM 7.17(1.152) versions. You must manually upgrade to 7.17(1.152) to use the wizard.

- **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**).

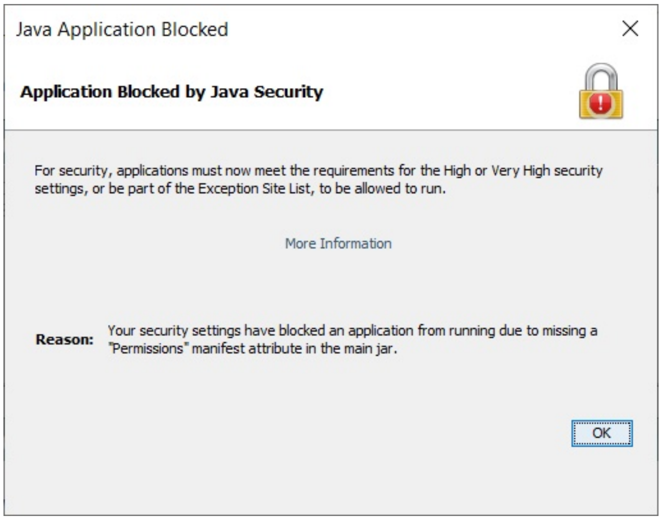
Note ASDM is not tested on Linux.

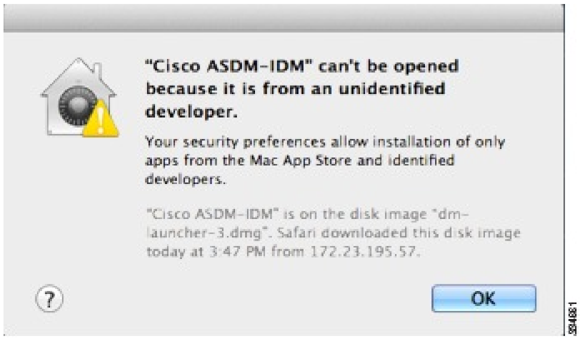
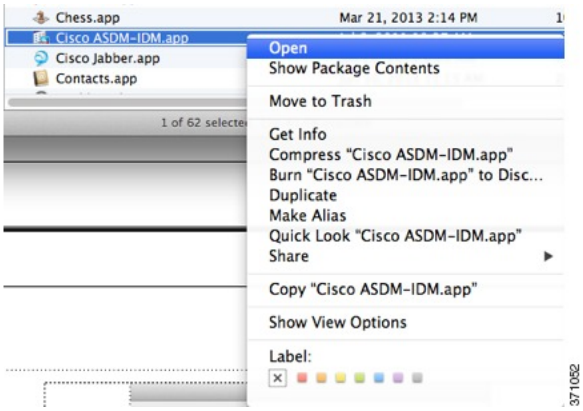
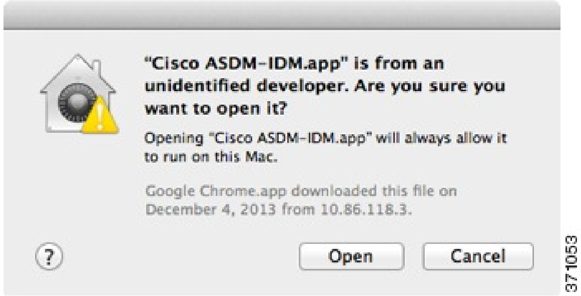
Table 1: ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE	OpenJRE
	Firefox	Safari	Chrome		
Microsoft Windows (English and Japanese): • 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 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	"**Java Application blocked**" error message. When you launch the ASDM Web Launcher, Oracle might block the application from running and prompt you to set the application's security level. The popup notification includes a link to Java's web page, where workaround steps are provided.  Java Application Blocked **Application Blocked by Java Security** For security, applications must now meet the requirements for the High or Very High security settings, or be part of the Exception Site List, to be allowed to run. More Information **Reason:** Your security settings have blocked an application from running due to missing a "Permissions" manifest attribute in the main jar.
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.  **“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**.  Chess.app Mar 21, 2013 2:14 PM Cisco ASDM-IDM.app Cisco Jabber.app Contacts.app 1 of 62 selecte Open Show Package Contents Move to Trash Get Info Compress “Cisco ASDM-IDM.app” Burn “Cisco ASDM-IDM.app” to Disc... Duplicate Make Alias Quick Look “Cisco ASDM-IDM.app” Share Copy “Cisco ASDM-IDM.app” Show View Options Label: 371052 **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.

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

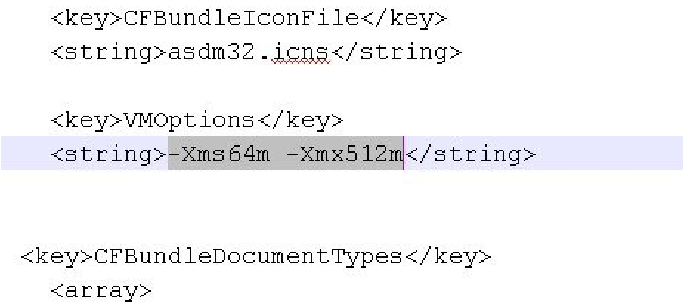
To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

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.

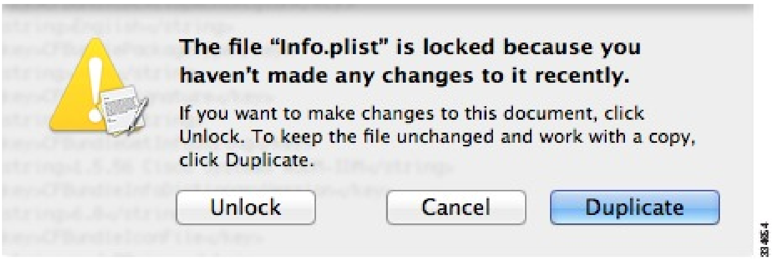


```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <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 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 7.17(1.155)

Released: June 28, 2022

There are no new features in this release.

New Features in ASDM 7.17(1.152)

Released: February 8, 2022

There are no new features in this release.

New Features in ASA 9.17(1)/ASDM 7.17(1)

Released: December 1, 2021

Feature	Description
Platform Features	
Secure Firewall 3100	We introduced the ASA for the Secure Firewall 3110, 3120, 3130, and 3140. The Secure Firewall 3100 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 3100 25 Gbps 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. New/Modified commands: **fec, netmod, speed sfp-detect, raid, show raid, show ssd** New/Modified screens: • **Configuration** > **Device Management** > **Advanced** > **EPM** • **Configuration** > **Device Settings** > **Interfaces** > **Edit Interface** > **Configure Hardware Properties**
ASAv support for Autoscale	The ASAv now supports Autoscale for the following Public Cloud offerings: • Google Cloud Platform (GCP) • Oracle Cloud Infrastructure (OCI) Autoscaling increases or decreases the number of ASAv application instances based on capacity requirements.
ASAv for AWS expanded instance support	The ASAv on the AWS Public Cloud now supports AWS Nitro System instances from different Nitro instance families. ASAv for AWS adds support for these instances: • c5a.large, c5a.xlarge, c5a.2xlarge, c5a.4xlarge • c5d.large, c5d.xlarge, c5d.2xlarge, c5d.4xlarge • c5ad.large, c5ad.xlarge, c5ad.2xlarge, c5ad.4xlarge • m5n.large, m5n.xlarge, m5n.2xlarge, m5n.4xlarge • m5zn.large, m5zn.xlarge, m5zn.2xlarge For a detailed list of supported instances, see the Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet.

Feature	Description
ASAv for Azure expanded instance support	ASAv on the Azure Public Cloud now supports these instances: • Standard_D8s_v3 • Standard_D16s_v3 • Standard_F8s_v2 • Standard_F16s_v2 For a detailed list of supported instances, see the Cisco Adaptive Security Virtual Appliance (ASAv) Data Sheet.
Intel QuickAssist Technology (QAT) on ASAv	The ASAv supports hardware crypto acceleration for ASAv deployments that use the Intel QuickAssist (QAT) 8970 PCI adapter. Hardware crypto acceleration for the ASAv using QAT is supported on VMware ESXi and KVM only.
Single Root I/O Virtualization (SR-IOV) support for ASAv on OCI.	You can now implement Single Root Input/Output Virtualization (SR-IOV) for ASAv on OCI. SR-IOV can provide performance improvements for ASAv. Mellanox 5 as vNICs are not supported in SR-IOV mode.
Firewall Features	
Twice NAT support for fully-qualified domain name (FQDN) objects as the translated (mapped) destination	You can use an FQDN network object, such as one specifying www.example.com, as the translated (mapped) destination address in twice NAT rules. The system configures the rule based on the IP address returned from the DNS server.
Network-service objects and their use in policy-based routing and access control	You can configure network-service objects and use them in extended access control lists for use in policy-based routing route maps and access control groups. Network-service objects include IP subnet or DNS domain name specifications, and optionally protocol and port specifications, that essentially combine network and service objects. This feature also includes the ability to define trusted DNS servers, to ensure that any DNS domain name resolutions acquire IP addresses from trusted sources. We added or modified the following screens. • **Configuration** > **Device Setup** > **Routing** > **Route Maps**, Add/Edit dialog boxes. • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces**, Add/Edit dialog boxes. • **Configuration** > **Firewall** > **Objects** > **Network Services Objects/Groups**. • **Configuration** > **Device Management** > **DNS** > **DNS Client**.
High Availability and Scalability Features	

Feature	Description
ASAv30, ASAv50, and ASAv100 clustering for VMware and KVM	ASAv clustering lets you group up to 16 ASAvs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. ASAv clustering supports Individual Interface mode in routed firewall mode; Spanned EtherChannels are not supported. The ASAv uses a VXLAN virtual interface (VNI) for the cluster control link. New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** • **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
Clearing routes in a high availability group or cluster	In previous releases, the **clear route** command cleared the routing table on the unit only. Now, when operating in a high availability group or cluster, the command is available on the active or control unit only, and clears the routing table on all units in the group or cluster. We changed the **clear route** command.
Interface Features	
Geneve interface support for the ASAv	Geneve encapsulation support was added for the ASAv30, ASAv50, and ASAv100 to support single-arm proxy for the AWS Gateway Load Balancer. New/Modified screens: • **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Add** > **VNI Interface** • **Configuration** > **Device Setup** > **Interface Settings** > **VXLAN**
Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces.	Secure Firewall 3100 auto-negotiation can be enabled or disabled for 1Gigabit and higher interfaces. For other model SFP ports, the **no speed nonegotiate** option sets the speed to 1000 Mbps; the new command means you can set auto-negotiation and speed independently. New/Modified screens: **Configuration** > **Device Setup** > **Interface Settings** > **Interfaces** > **Advanced**
Administrative and Troubleshooting Features	
Startup time and tmatch compilation status	The **show version** command now includes information on how long it took to start (boot) up the system. Note that the larger the configuration, the longer it takes to boot up the system. The new **show asp rule-engine** command shows status on tmatch compilation. Tmatch compilation is used for an access list that is used as an access group, the NAT table, and some other items. It is an internal process that can consume CPU resources and impact performance while in progress, if you have very large ACLs and NAT tables. Compilation time depends on the size of the access list, NAT table, and so forth.

Feature	Description
Enhancements to **show access-list element-count** output and **show tech-support** content	The output of the **show access-list element-count** has be enhanced to show the following: • When used in the system context in multiple-context mode, the output shows the element count for all access lists across all the contexts. • When used with object-group search enabled, the output includes details about the number of object groups in the element count. In addition, the **show tech-support** output now includes the output **show access-list element-count** and **show asp rule-engine**.
CiscoSSH stack	The ASA uses a proprietary SSH stack for SSH connections. You can now choose to use the CiscoSSH stack instead, which is based on OpenSSH. The default stack continues to be the ASA stack. Cisco SSH supports: • FIPS compliance • Regular updates, including updates from Cisco and the open source community Note that the CiscoSSH stack does not support: • SSH to a different interface over VPN (management-access) • EdDSA key pair • RSA key pair in FIPS mode If you need these features, you should continue to use the ASA SSH stack. There is a small change to SCP functionality with the CiscoSSH stack: to use the ASA **copy** command to copy a file to or from an SCP server, you have to enable SSH access on the ASA for the SCP server subnet/host. New/Modified screens: • Single context mode: **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH** • Multiple context mode: **Configuration** > **Device Management** > **SSH Stack**
PCAP support in packet tracer	You can replay a PCAP file in packet tracer tool and obtain the trace results. **pcap** and **force** are two new keywords that is used to support the usage of PCAP in packet tracer. New/Modified commands: **packet-tracer input** and **show packet-tracer**

Feature	Description
Stronger local user and enable password requirements	For local users and the enable password, the following password requirements were added: - Password length—Minimum 8 characters. Formerly, the minimum was 3 characters. - Repetitive and sequential characters—Three or more consecutive sequential or repetitive ASCII characters are disallowed. For example, the following passwords will be rejected: - **abc**user1 - user**543** - user**aaaa** - user2**666** New/Modified screens: - **Configuration** > **Device Management** > **Users/AAA** > **User Accounts** - **Configuration** > **Device Setup** > **Device Name/Password**
Local user lockout changes	The ASA can lock out local users after a configurable number of failed login attempts. This feature did not apply to users with privilege level 15. Also, a user would be locked out indefinitely until an admin unlocked their account. Now, users will be unlocked after 10 minutes unless an admin uses the **clear aaa local user lockout** command before then. Privilege level 15 users are also now affected by the lockout setting. New/Modified commands: **aaa local authentication attempts max-fail** , **show aaa local user**
SSH and Telnet password change prompt	The first time a local user logs into the ASA using SSH or Telnet, they are prompted to change their password. They will also be prompted for the first login after an admin changes their password. If the ASA reloads, however, users will not be prompted even if it is their first login. Note that any service that uses the local user database, such as VPN, will also have to use the new password if it was changed during an SSH or Telnet login. New/Modified commands: **show aaa local user**
Monitoring Features	
SNMP now supports IPv6 when grouping multiple hosts in the form of a network object	The **host-group** command of **snmp-server** now supports IPv6 host, range, and subnet objects.
VPN Features	
Local tunnel id support for IKEv2	Support has been added for local Tunnel id configuration for IKEv2. New/Modified commands: **set ikev2 local-identity**
Support for SAML Attributes with DAP constraint	Support has been added for SAML assertion attributes which can be used to make DAP policy selections. It also introduces the ability for a group-policy to be specified by the *cisco_group_policy* attribute.

Feature	Description
Multiple SAML trustpoints in IDP configuration	This feature supports adding multiple IDP trustpoints per SAML IDP configuration for applications that support multiple applications for the same Entity ID. New/Modified commands: **saml idp-trustpoint <trustpoint-name>**
AnyConnect Client VPN SAML External Browser	You can now configure VPN SAML External Browser to enable additional authentication choices, such as passwordless authentication, WebAuthN, FIDO2, SSO, U2F, and an improved SAML experience due to the persistence of cookies. When you use SAML as the primary authentication method for a remote access VPN connection profile, you can elect to have the AnyConnect Client use the client's local browser instead of the AnyConnect Client embedded browser to perform the web authentication. This option enables single sign-on (SSO) between your VPN authentication and other corporate logins. Also choose this option if you want to support web authentication methods, such as biometric authentication and Yubikeys, that cannot be performed in the embedded browser. New/Modified screens: **Remote Access VPN connection profile wizard** > **SAML Login Experience**.
VPN Load balancing with SAML	ASA now supports VPN load balancing with SAML authentication.

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(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
9.16(x)	—	Any of the following: → 9.17(x)
9.15(x)	—	Any of the following: → 9.17(x) → **9.16(x)**
9.14(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x)
9.13(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)
9.12(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x)

Current Version	Interim Upgrade Version	Target Version
9.10(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.9(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.8(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x)
9.7(x)	—	Any of the following: → 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
9.6(x)	—	Any of the following: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.5(x)	—	Any of the following: → 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: → 9.17(x) → **9.16(x)** → 9.15(x) → 9.14(x) → 9.12(x) → 9.8(x)
9.3(x)	—	Any of the following: → 9.17(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: → 9.17(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 7.17(1.155)

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
CSCvv17403	Check box not available for disable delete tunnel with no delay in simultaneous connection prempt
CSCvv83043	Cipher changes require in VPN wizard according to 9161/7161 CLIs

Open Bugs in Version 7.17(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
CSCvv17403	Check box not available for disable delete tunnel with no delay in simultaneous connection prempt
CSCvv83043	Cipher changes require in VPN wizard according to 9161/7161 CLIs

Open Bugs in Version 7.17(1)

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

Caveat ID Number	Description
CSCvu01215	Appliance mode : checksum does not match issue while downloading asa image from CCO
CSCvu60781	ASDM: Need support for MAC in Launcher 1.9.1
CSCvv17403	Check box not available for disable delete tunnel with no delay in simultaneous connection prempt
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 7.17(1.155)

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

Identifier	Headline
CSCwc13294	ASA: Cannot connect to ASA using ASDM with Java Web Launch

Resolved Bugs in Version 7.17(1.152)

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

Identifier	Headline
CSCvu60781	ASDM: Need support for MAC in Launcher 1.9.1
CSCwa48034	ASDM side changes for the ASA #CSCvz89126

Resolved Bugs in Version 7.17(1)

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

Caveat ID Number	Description
CSCvw39124	NSF wait interval warning popup is not showing when configuring wrong value
CSCvw61817	ASDM Display "n/a" for "Peak Usage (KB)" Under Tab "Context Usage" of Memory Status
CSCvw86103	ASA Cluster ASDM real-time log viewer showing same events on Master and Slave
CSCvx31769	ASDM session being abruptly terminated when switching between different admin and system contexts
CSCvx31842	Hostscan 4.3.x to 4.6.x Migration steps should not be display when the SDM have the HS 4.10.x
CSCvx40955	ASDM does not recognize SCTP port as per the parser Errors

Caveat ID Number	Description
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
CSCvz15404	ASA: Multiple context mode : ASDM logging stops, when switched to a different context

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 ASA Series Documentation.