Release Notes for Cisco ASDM, 7.8(x)

First Published: 2017-05-15

Last Modified: 2017-10-12

Release Notes for Cisco ASDM, 7.8(x)

This document contains release information for Cisco ASDM Version 7.8(x) for the Cisco ASA series.

Important Notes

- **ASDM signed-image support in 9.8(4.45)/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)
- Upgrade ROMMON for ASA 5506-X, 5508-X, and 5516-X to Version 1.1.15—There is a new ROMMON version for these ASA models (May 15, 2019); we highly recommend that you upgrade to the latest version. To upgrade, see the instructions in the ASA configuration guide.

Caution The ROMMON upgrade for 1.1.15 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- If you are using SAML authentication with AnyConnect 4.4 or 4.5 and you deploy ASA version 9.7.1.24, 9.8.2.28, or 9.9.2.1 (Release Date: 18-APR-2018), the defaulted SAML behavior is the embedded browser, which is not supported on AnyConnect 4.4 and 4.5. Therefore, you must enable the **saml external-browser** command in tunnel group configuration in order for AnyConnect 4.4 and 4.5 clients to authenticate with SAML using the external (native) browser.

Note The **saml external-browser** command is for migration purposes for those upgrading to AnyConnect 4.6 or later. Because of security limitations, use this solution only as part of a temporary migration while upgrading AnyConnect software. The command itself will be depreciated in the future.

- Do not upgrade to 9.8(1) for ASAv on Amazon Web Services--Due to CSCve56153, you should not upgrade to 9.8(1). After upgrading, the ASAv becomes unreachable. Upgrade to 9.8(1.5) or later instead.
- ASAv5 memory issues—Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling AnyConnect or downloading files to the ASAv fail. The following bugs were fixed in 9.8(1.5) to transparently improve memory function and to optionally allow you to assign more memory to the ASAv5 if necessary: CSCvd90079 and CSCvd90071.
- The RSA toolkit version used in ASA 9.x is different from what was used in ASA 8.4, which causes differences in PKI behavior between these two versions.

  For example, ASAs running 9.x software allow you to import certificates with an Organizational Name Value (OU) field length of 73 characters. ASAs running 8.4 software allow you to import certificates with an OU field name of 60 characters. Because of this difference, certificates that can be imported in ASA 9.x will fail to be imported to ASA 8.4. If you try to import an ASA 9.x certificate to an ASA running version 8.4, you will likely receive the error, "ERROR: Import PKCS12 operation failed.

System Requirements

This section lists the system requirements to run this release.

ASDM Java Requirements

You can install ASDM using Oracle JRE 8.0. OpenJRE is not supported.

Note ASDM is not tested on Linux.

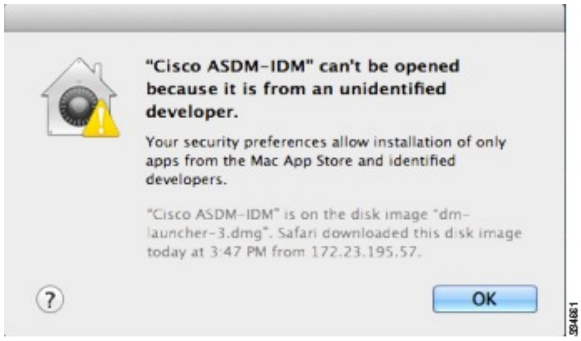
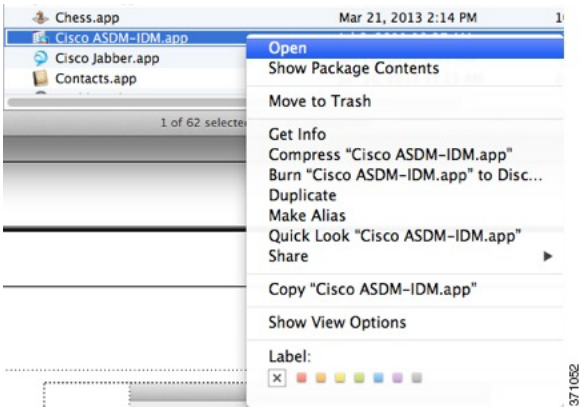
Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

Operating System	Browser			Oracle JRE
	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): • 10 • 8 • 7 • Server 2012 R2 • Server 2012 • Server 2008	Yes	No support	Yes	8.0
Apple OS X 10.4 and later	Yes	Yes	Yes (64-bit version only)	8.0

ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

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.

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
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**.

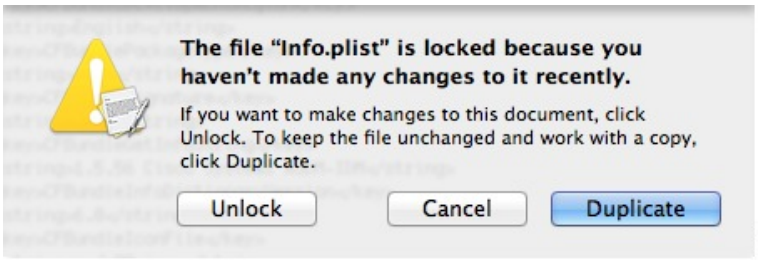
Step 3 Under **Java** > **VMOptions**, change the string prefixed with "-Xmx" to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

```
    <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:



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 ASA 9.8(4)

Released: April 24, 2019

Feature	Description
VPN Features	
Add subdomains to webVPN HSTS	Allows domain owners to submit what domains should be included in the HSTS preload list for web browsers. New/Modified screens: **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Advanced** > **Proxies** > **Enable HSTS Subdomains**field *Also in 9.12(1).*
Administrative Features	

Feature	Description
Allow non-browser-based HTTPS clients to access the ASA	You can allow non-browser-based HTTPS clients to access HTTPS services on the ASA. By default, ASDM, CSM, and REST API are allowed. Many specialty clients (for example, python libraries, curl, and wget) do not support Cross-site request forgery (CSRF) token-based authentication, so you need to specifically allow these clients to use the ASA basic authentication method. For security purposes, you should only allow required clients. New/Modified screens. **Configuration** > **Device Management** > **Management Access** > **HTTP Non-Browser Client Support** *Also in 9.12(1).*
show tech-support includes additional output	The output of the **show tech-support** is enhanced to display the output of the following: • **show ipv6 interface** • **show aaa-server** • **show fragment** New/Modified commands: **show tech-support** *Also in 9.12(1).*
Support to enable and disable the results for free memory and used memory statistics during SNMP walk operations	To avoid overutilization of CPU resources, you can enable and disable the query of free memory and used memory statistics collected through SNMP walk operations. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP** *Also in 9.10(1).*

New Features in ASA 9.8(3)/ASDM 7.9(2.152)

Released: July 2, 2018

Feature	Description
Platform Features	
Firepower 2100 Active LED now lights amber when in standby mode	Formerly, the Active LED was unlit in standby mode.
Firewall Features	
Support for removing the logout button from the cut-through proxy login page.	If you configure the cut-through proxy to obtain user identity information (the AAA authentication listener), you can now remove the logout button from the page. This is useful in case where users connect from behind a NAT device and cannot be distinguished by IP address. When one user logs out, it logs out all users of the IP address. New/Modified commands: **aaa authentication listener no-logout-button**. No ASDM support.

Feature	Description
Trustsec SXP connection configurable delete hold down timer	The default SXP connection hold down timer is 120 seconds. You can now configure this timer, between 120 to 64000 seconds. New/Modified commands: **cts sxp delete-hold-down period**, **show cts sxp connection brief**, **show cts sxp connections** No ASDM support.
VPN Features	
Support for legacy SAML authentication	If you deploy an ASA with the fix for CSCvg65072, then the default SAML behavior is to use the embedded browser, which is not supported on AnyConnect 4.4 or 4.5. Therefore, to continue to use AnyConnect 4.4 or 4.5, you must enable the legacy external browser SAML authentication method. Because of security limitations, use this option only as part of a temporary plan to migrate to AnyConnect 4.6. This option will be deprecated in the near future. New/Modified screens: **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles** page **>** **Connection Profiles** area **>** **Add** button **>** **Add AnyConnect Connection Profile** dialog box **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** > page **>** **Connection Profiles** area **>** **Add** button **>** **Add Clientless SSL VPN Connection Profile** dialog box New/Modified options: **SAML External Browser** check box
Interface Features	
Unique MAC address generation for single context mode	You can now enable unique MAC address generation for VLAN subinterfaces in single context mode. Normally, subinterfaces share the same MAC address with the main interface. Because IPv6 link-local addresses are generated based on the MAC address, this feature allows for unique IPv6 link-local addresses. New or modified command: **mac-address auto** No ASDM support. *Also in 9.9(2) and later.*

New Features in ASDM 7.8(2.151)

Released: October 12, 2017

Feature	Description
Firewall Features	

Feature	Description
Ethertype access control list changes	EtherType access control lists now support Ethernet II IPX (EII IPX). In addition, new keywords are added to the DSAP keyword to support common DSAP values: BPDU (0x42), IPX (0xE0), Raw IPX (0xFF), and ISIS (0xFE). Consequently, existing EtherType access contol entries that use the BPDU or ISIS keywords will be converted automatically to use the DSAP specification, and rules for IPX will be converted to 3 rules (DSAP IPX, DSAP Raw IPX, and EII IPX). In addition, packet capture that uses IPX as an EtherType value has been deprecated, because IPX corresponds to 3 separate EtherTypes. This feature is supported in 9.8(2.9) and other interim releases. For more information, see CSCvf57908. We modified the following screens: **Configuration** > **Firewall** > **Ethertype Rules**.

New Features in ASA 9.8(2)/ASDM 7.8(2)

Released: August 28, 2017

Feature	Description
Platform Features	
ASA for the Firepower 2100 series	We introduced the ASA for the Firepower 2110, 2120, 2130, and 2140. Similar to the Firepower 4100 and 9300, the Firepower 2100 runs the base FXOS operating system and then the ASA operating system as an application. The Firepower 2100 implementation couples FXOS more closely with the ASA than the Firepower 4100 and 9300 do (pared down FXOS functions, single device image bundle, easy management access for both ASA and FXOS). FXOS owns configuring hardware settings for interfaces, including creating EtherChannels, as well as NTP services, hardware monitoring, and other basic functions. You can use the Firepower Chassis Manager or the FXOS CLI for this configuration. The ASA owns all other functionality, including Smart Licensing (unlike the Firepower 4100 and 9300). The ASA and FXOS each have their own IP address on the Management 1/1 interface, and you can configure management of both the ASA and FXOS instances from any data interface. We introduced the following screens: **Configuration** > **Device Management** > **Management Access** > **FXOS Remote Management**
Department of Defense Unified Capabilities Approved Products List	The ASA was updated to comply with the Unified Capabilities Approved Products List (UC APL) requirements. In this release, when you enter the **fips enable** command, the ASA will reload. Both failover peers must be in the same FIPS mode before you enable failover. We modified the following command: **fips enable**
ASAv for Amazon Web Services M4 instance support	You can now deploy the ASAv as an M4 instance. We did not modify any screens.
ASAv5 1.5 GB RAM capability	Starting in Version 9.7(1), the ASAv5 may experience memory exhaustion where certain functions such as enabling AnyConnect or downloading files to the ASAv fail. You can now assign 1.5 GB (up from 1 GB) of RAM to the ASAv5. We did not modify any screens.

Feature	Description
VPN Features	
HTTP Strict Transport Security (HSTS) header support	HSTS protects websites against protocol downgrade attacks and cookie hijacking on clientless SSL VPN. It lets web servers declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. HSTS is an IETF standards track protocol and is specified in RFC 6797. We modified the following screens: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Proxies**
Interface Features	
VLAN support for the ASAv50	The ASAv50 now supports VLANs on the ixgbe-vf vNIC for SR-IOV interfaces. We did not modify any screens.

New Features in ASA 9.8(1.200)

Released: July 30, 2017

Note This release is only supported on the ASAv for Microsoft Azure. These features are not supported in Version 9.8(2).

Feature	Description
High Availability and Scalability Features	
Active/Backup High Availability for ASAv on Microsoft Azure	A stateless Active/Backup solution that allows for a failure of the active ASAv to trigger an automatic failover of the system to the backup ASAv in the Microsoft Azure public cloud. We introduced the following commands: **failover cloud** No ASDM support.

New Features in ASDM 7.8(1.150)

Released: June 20, 2017

There are no new features in this release.

New Features in ASA 9.8(1)/ASDM 7.8(1)

Released: May 15, 2017

Feature	Description
Platform Features	

Feature	Description
ASAv50 platform	The ASAv platform has added a high-end performance ASAv50 platform that provides 10 Gbps Firewall throughput levels. The ASAv50 requires ixgbe-vf vNICs, which are supported on VMware and KVM only.
SR-IOV on the ASAv platform	The ASAv platform supports Single Root I/O Virtualization (SR-IOV) interfaces, which allows multiple VMs to share a single PCIe network adapter inside a host. ASAv SR-IOV support is available on VMware, KVM, and AWS only.
Automatic ASP load balancing now supported for the ASAv	Formerly, you could only manually enable and disable ASP load balancing. We modified the following screen: **Configuration > Device Management > Advanced > ASP Load Balancing**
Firewall Features	
Support for setting the TLS proxy server SSL cipher suite	You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA on the **Configuration** > **Device Management** > **Advanced** > **SSL Settings** > **Encryption** page. We modified the following screen: **Configuration** > **Firewall** > **Unified Communications** > **TLS Proxy**, Add/Edit dialog boxes, **Server Configuration** page.
Global timeout for ICMP errors	You can now set the idle time before the ASA removes an ICMP connection after receiving an ICMP echo-reply packet. When this timeout is disabled (the default), and you enable ICMP inspection, then the ASA removes the ICMP connection as soon as an echo-reply is received; thus any ICMP errors that are generated for the (now closed) connection are dropped. This timeout delays the removal of ICMP connections so you can receive important ICMP errors. We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**.
High Availability and Scalability Features	
Improved cluster unit health-check failure detection	You can now configure a lower holdtime for the unit health check: .3 seconds minimum. The previous minimum was .8 seconds. This feature changes the unit health check messaging scheme to *heartbeats* in the data plane from *keepalives* in the control plane. Using heartbeats improves the reliability and the responsiveness of clustering by not being susceptible to control plane CPU hogging and scheduling delays. Note that configuring a lower holdtime increases cluster control link messaging activity. We suggest that you analyze your network before you configure a low holdtime; for example, make sure a ping from one unit to another over the cluster control link returns within the *holdtime*/3, because there will be three heartbeat messages during one holdtime interval. If you downgrade your ASA software after setting the hold time to .3 - .7, this setting will revert to the default of 3 seconds because the new setting is unsupported. We modified the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**

Feature	Description
Configurable debounce time to mark an interface as failed for the Firepower 4100/9300 chassis	You can now configure the debounce time before the ASA considers an interface to be failed, and the unit is removed from the cluster. This feature allows for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the ASA waits the number of milliseconds specified before marking the interface as failed and the unit is removed from the cluster. The default debounce time is 500 ms, with a range of 300 ms to 9 seconds. New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
VPN Features	
Support for IKEv2, certificate based authentication, and ACL in VTI	Virtual Tunnel Interface (VTI) now supports BGP (static VTI). You can now use IKEv2 in standalone and high availability modes. You can use certificate based authentication by setting up a trustpoint in the IPsec profile. You can also apply access lists on VTI using access-group commands to filter ingress traffic. We introduced options to select the trustpoint for certificate based authentication in the following screen: **Configuration** > **Site-to-Site VPN** > **Advanced** > **IPsec Proposals (Transform Sets)** > **IPsec Profile** > **Add**
Mobile IKEv2 (MobIKE) is enabled by default	Mobile devices operating as remote access clients require transparent IP address changes while moving. Supporting MobIKE on ASA allows a current IKE security association (SA) to be updated without deleting the current SA. MobIKE is “always on.”
SAML 2.0 SSO Updates	The default signing method for a signature in a SAML request changed from SHA1 to SHA2, and you can configure which signing method you prefer: rsa-sha1, rsa-sha256, rsa-sha384, or rsa-sha512. We introduced changes to the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers > Add**.
Change for **tunnelgroup webvpn-attributes**	We changed the **pre-fill-username** and **secondary-pre-fill-username** value from **ssl-client** to **client**.
AAA Features	
Login history	By default, the login history is saved for 90 days. You can disable this feature or change the duration, up to 365 days. This feature only applies to usernames in the local database when you enable local AAA authentication for one or more of the management methods (SSH, ASDM, Telnet, and so on). We introduced the following screen: **Configuration** > **Device Management** > **Users/AAA** > **Login History**
Password policy enforcement to prohibit the reuse of passwords, and prohibit use of a password matching a username	You can now prohibit the reuse of previous passwords for up to 7 generations, and you can also prohibit the use of a password that matches a username. We modified the following screen: **Configuration** > **Device Management** > **Users/AAA** > **Password Policy**

Feature	Description
Separate authentication for users with SSH public key authentication and users with passwords	In releases prior to 9.6(2), you could enable SSH public key authentication (**ssh authentication**) without also explicitly enabling AAA SSH authentication with the Local user database (**aaa authentication ssh console LOCAL**). In 9.6(2), the ASA required you to explicitly enable AAA SSH authentication. In this release, you no longer have to explicitly enable AAA SSH authentication; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with *passwords*, and you can use any AAA server type (**aaa authentication ssh console radius_1**, for example). For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS. We did not modify any screens. *Also in Version 9.6(3).*
Monitoring and Troubleshooting Features	
Saving currently-running packet captures when the ASA crashes	Formerly, active packet captures were lost if the ASA crashed. Now, packet captures are saved to disk 0 at the time of the crash with the filename [*context_name*.]*capture_name*.**pcap**. We did not modify any screens.

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 9.12(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
9.7(x)	—	Any of the following: → 9.8(x)
9.6(x)	—	Any of the following: → 9.8(x)
9.5(x)	—	Any of the following: → 9.8(x)
9.4(x)	—	Any of the following: → 9.8(x)
9.3(x)	—	Any of the following: → 9.8(x)
9.2(x)	—	Any of the following: → 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: → 9.8(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.8(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.8(x) → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.6(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.8(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ 9.8(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → 9.8(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → 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 7.8(2.151)

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

Caveat ID Number	Description
CSCvc44203	ONBOX: Need to remove the SFR module other than Admin Context
CSCvf74630	Incompatible button visibility in the DAP UI

Open Bugs in Version 7.8(2)

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

Caveat ID Number	Description
CSCvf74630	Incompatible button visibility in the DAP UI
CSCvc44203	ONBOX: Need to remove the SFR module other than Admin Context

Open Bugs in Version 7.8(1.150)

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

Caveat ID Number	Description
CSCvc44203	ONBOX: Need to remove the SFR module other than Admin Context

Open Bugs in Version 7.8(1)

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

Caveat ID Number	Description
CSCvc44203	ONBOX: Need to remove the SFR module other than Admin Context

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.8(2.151)

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

Caveat ID Number	Description
CSCvf67423	Reintroduce performance fix (introduced in ASDM 7.5.1 and backed out in ASDM 7.6.1)
CSCvf82966	ASDM - Logging: Unable to View Real-Time logs

Caveat ID Number	Description
CSCvf91260	ASDM: Upgrade from CCO not working due to un-ignorable fields. "Meta data request failed"

Resolved Bugs in Version 7.8(2)

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

Caveat ID Number	Description
CSCvc23816	ASDM user attributes change breaks user password
CSCvd58610	Selection Criteria in DAP disappears when using Multi Context mode
CSCvd81711	ASDM not detecting the default settings for netbios probe settings for user-identity feature
CSCvd83906	ASDM Unable to Find Usage for Pre-Defined Service Objects
CSCvd90344	ASDM 7.7.150 Upload wizard not working
CSCvd95382	ASDM shows default idle timer value as 1193:0:0 (49D17H) while making connection timer changes
CSCve02504	Unable to add more than 4 interfaces to a specific bridge group
CSCve26349	ASDM doesn't display Object Descriptions
CSCve55694	ASDM sets service as "service tcp destination eq -1" when configuring range on service object
CSCve64342	'Dynamic Access Policies' page is freezed and unable to access after HS image uninstalled.
CSCve69985	ASDM does not allow more than one static MAC address table entry per interface in transparent mode.
CSCve72433	ASDM error requesting to remove prefix-list used in route-maps for dynamic routing protocol
CSCve72787	"Where Used" function on object causes java.lang.NullPointerException if object in Manual NAT
CSCve76967	ASDM Where Used option not displaying results
CSCve93019	ASDM Hangs when editing crypto map associated to Dynamic Site-to-Site tunnel
CSCvf08411	Display of Cipher Algorithms at ASDM is incorrect,when TLS1.2's Cipher Security Level is "medium"

Resolved Bugs in Version 7.8(1.150)

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

Caveat ID Number	Description
CSCve66939	Don't offer 9.8.1 as an upgrade option for ASAs in AWS

Resolved Bugs in Version 7.8(1)

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

Caveat ID Number	Description
CSCvc65799	incorrect NAT exempt rule being pushed by ASDM
CSCvc75477	ASDM "Specified remark does not exist" when remarks are edited and a time range is added
CSCvc77732	Apply button not enabled on editing the Crypto Map
CSCvc86115	7.5.2.153 traceroute along with Command line utility does not work in ASDM.
CSCvc90621	ASDM not supporting Monitoring of VPN AnyConnect sessions
CSCvc92151	User and Security Group fields in ASDM show invalid content and random objects
CSCvd03071	Group policy locked for editing
CSCvd12493	ASDM gets stuck and does not load beyond Software update complete.
CSCvd24557	ASDM is pushing improper public servers configuration to ASA.
CSCvd90344	ASDM 7.7.150 Upload wizard not working

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.

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.