Release Notes for Cisco ASDM, 7.9(x)

First Published: 2017-12-04

Last Modified: 2018-05-09

Release Notes for Cisco ASDM, 7.9(x)

This document contains release information for Cisco ASDM Version 7.9(x) for the Cisco ASA series.

Important Notes

- 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.

- 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.

- ASA 5506-X memory issues with large configurations on 9.9(2)—If you upgrade to 9.9(2), parts of a very large configuration might be rejected due to insufficient memory with the following message: "ERROR: Insufficient memory to install the rules". One option is to enter the **object-group-search access-control** command to improve memory usage for ACLs; your performance might be impacted, however. Alternatively, you can downgrade to 9.9(1).

- New ROMMON Version 1.1.12 for the ASA 5506-X, 5508-X, and 5516-X—We recommend that you upgrade your ROMMON for several crucial fixes. See https://www.cisco.com/go/asa-firepower-sw, choose your *model* > ASA Rommon Software > 1.1.12. Refer to the release notes on the software download page for more information. To upgrade the ROMMON, see Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X). Note that the ASA running Firepower Threat Defense does not yet support upgrading to this ROMMON version; you can, however, successfully upgrade it in ASA and then reimage to Firepower Threat Defense.

- 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.

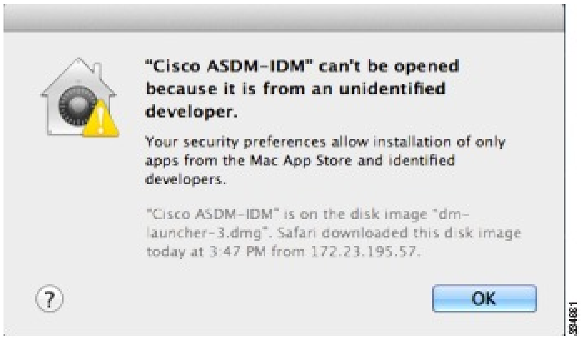
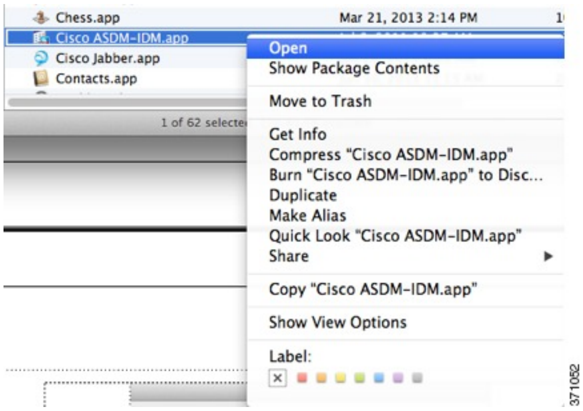
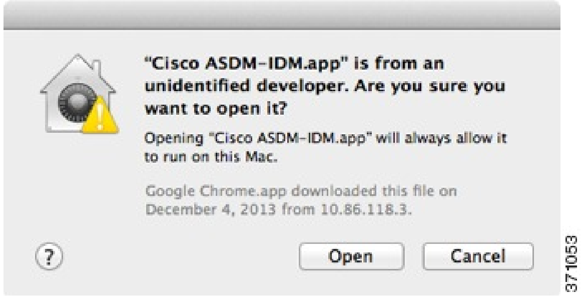
Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

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

ASDM Compatibility Notes

The following table lists compatibility caveats for ASDM.

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.
IE9 for servers	For Internet Explorer 9.0 for servers, the "**Do not save encrypted pages to disk**" option is enabled by default (See **Tools** > **Internet Options** > **Advanced**). This option causes the initial ASDM download to fail. Be sure to disable this option to allow ASDM to download.
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
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**.

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

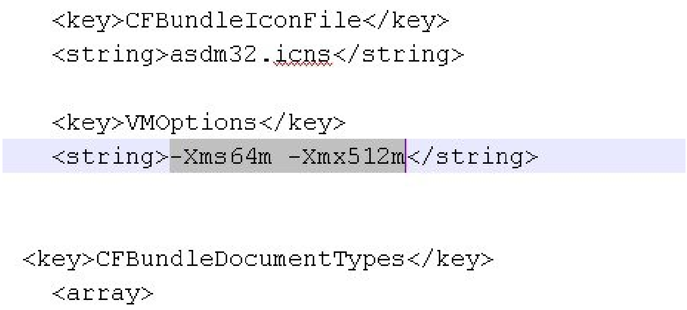
To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

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.

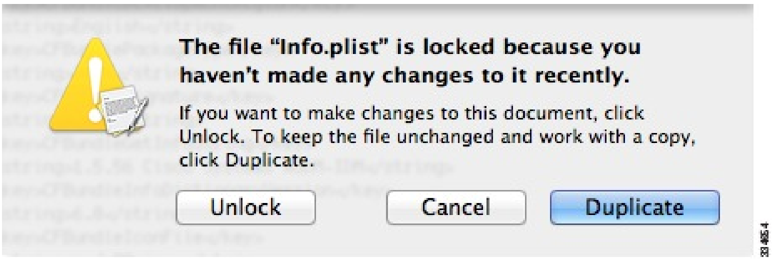


```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <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 7.9(2.152)

Released: May 9, 2018

Feature	Description
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

New Features in ASA 9.9(2)/ASDM 7.9(2)

Released: March 26, 2018

Feature	Description
Platform Features	
ASAv support for VMware ESXi 6.5	The ASAv virtual platform supports hosts running on VMware ESXi 6.5. New VMware hardware versions have been added to the *vi.ovf* and *esxi.ovf* files to enable optimal performance and usability of the ASAv on ESXi 6.5. We did not modify any screens.
ASAv support for VMXNET3 interfaces	The ASAv virtual platform supports VMXNET3 interfaces on VMware hypervisors. We did not modify any screens.
ASAv support for virtual serial console on first boot	You can now configure the ASAv to use the virtual serial console on first boot, instead of the virtual VGA console, to access and configure the ASAv.

Feature	Description
ASAv support to update user-defined routes in more than one Azure subscription for High Availability on Microsoft Azure	You can now configure the ASAv in an Azure High Availability configuration to update user-defined routes in more than one Azure subscription. New or modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** > **Route-Table**
VPN Features	
Remote Access VPN multi-context support extended to IKEv2 protocol	Support for configuring ASA to allow Anyconnect and third party Standards-based IPSec IKEv2 VPN clients to establish Remote Access VPN sessions to ASA operating in multi-context mode.
IPv6 connectivity to Radius Servers	ASA 9.9.2 now supports IPv6 connectivity to external AAA Radius Servers.
Easy VPN Enhancements for BVI Support	Easy VPN has been enhanced to support a Bridged Virtual Interface (BVI) as its internal secure interface, and you can now directly configure which interface to use as the internal secure interface. Otherwise, the ASA chooses its internal secure interface using security levels. Also, management services, such as **telnet**, **http**, and **ssh**, can now be configured on a BVI if VPN **management-access** has been enabled on that BVI. For non-VPN management access, you should continue to configure these services on the bridge group member interfaces.
Distributed VPN Session Improvements	• The Active Session Redistribution logic, which balances Distributed S2S VPN active and backup sessions, has been improved. Also, the balancing process may be repeated up to eight times in the background for a single **cluster redistribute vpn-sessiondb** command entered by the administrator. • The handling of dynamic Reverse Route Injections (RRI) across the cluster has been improved.
High Availability and Scalability Features	
Automatically rejoin the cluster after an internal failure	Formerly, many error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals by default: 5 minutes, 10 minutes, and then 20 minutes. These values are configurable. Internal failures include: application sync timeout; inconsistent application statuses; and so on. New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster** > **Auto Rejoin**
Configurable debounce time to mark an interface as failed for the ASA 5000-X series	You can now configure the debounce time before the ASA considers an interface to be failed and the unit is removed from the cluster on the ASA 5500-X series. 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. This feature was previously available for the Firepower 4100/9300. New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**

Feature	Description
Show transport related statistics for cluster reliable transport protocol messages	You can now view per-unit cluster reliable transport buffer usage so you can identify packet drop issues when the buffer is full in the control plane. New or modified command: **show cluster info transport cp detail**
Show failover history from peer unit	You can now view failover history from the peer unit, using the **details** keyword . This includes failover state changes and reason for the state change. New or modified command: **show failover**
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 9.8(3) and 9.8(4).*
Administrative Features	
RSA key pair supports 3072-bit keys	You can now set the modulus size to 3072. New or modified screen: **Configuration** > **Device Management** > **Certificate Management** > **Identity Certificates**
The FXOS bootstrap configuration now sets the enable password	When you deploy the ASA on the Firepower 4100/9300, the password setting in the bootstrap configuration now sets the enable password as well as the admin user password. Requires FXOS Version 2.3.1.
Monitoring and Troubleshooting Features	
SNMP IPv6 support	The ASA now supports SNMP over IPv6, including communicating with SNMP servers over IPv6, allowing the execution of queries and traps over IPv6, and supporting IPv6 addresses for existing MIBs. We added the following new SNMP IPv6 MIB objects as described in RFC 8096. • ipv6InterfaceTable (OID: 1.3.6.1.2.1.4.30)—Contains per-interface IPv6-specific information. • ipAddressPrefixTable (OID:1.3.6.1.2.1.4.32)—Includes all the prefixes learned by this entity. • ipAddressTable (OID: 1.3.6.1.2.1.4.34)—Contains addressing information relevant to the entity's interfaces. • ipNetToPhysicalTable (OID: 1.3.6.1.2.1.4.35)—Contains the mapping from IP addresses to physical addresses. New or modified screen: **Configuration** > **Device Management** > **Management Access** > **SNMP**

Feature	Description
Conditional Debugging to troubleshoot a single user session	Conditional debugging feature now assists you to verify the logs of specific ASA VPN sessions based on the filter conditions that are set. Support for "any, any" for IPv4 and IPv6 subnets is provided.

New Features in ASDM 7.9(1.151)

Released: February 14, 2018

There are no new features in this release.

New Features in ASA 9.9(1)/ASDM 7.9(1)

Released: December 4, 2017

Feature	Description
Firewall Features	
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. New or modified screen: **Configuration** > **Firewall** > **Ethertype Rules**.
VPN Features	

Feature	Description
Distributed Site-to-Site VPN with clustering on the Firepower 9300	An ASA cluster on the Firepower 9300 supports Site-to-Site VPN in distributed mode. Distributed mode provides the ability to have many Site-to-Site IPsec IKEv2 VPN connections distributed across members of an ASA cluster, not just on the control unit (as in centralized mode). This significantly scales VPN support beyond Centralized VPN capabilities and provides high availability. Distributed S2S VPN runs on a cluster of up to two chassis, each containing up to three modules (six total cluster members), each module supporting up to 6K active sessions (12K total), for a maximum of approximately 36K active sessions (72K total). New or modified screens: **Monitoring > ASA Cluster > ASA Cluster > VPN Cluster Summary** **Monitoring > VPN > VPN Statistics > Sessions** **Configuration > Device Management > High Availablility and Scalability > ASA Cluster** **Wizards > Site-to-Site** **Monitoring > VPN > VPN Statistics > Sessions** **Monitoring > ASA Cluster > ASA Cluster > VPN Cluster Summary** **Monitoring > ASA Cluster > ASA Cluster > System Resource Graphs > CPU/Memory** **Monitoring > Logging > Real-Time Log Viewer**
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. New or modified screens: **Configuration** > **Device Management** > **High Availability and Scalability** > **Failover** **Monitoring** > **Properties** > **Failover** > **Status** **Monitoring** > **Properties** > **Failover** > **History** *Also in 9.8(1.200).*
Improved chassis health check failure detection for the Firepower chassis	You can now configure a lower holdtime for the chassis health check: 100 ms. The previous minimum was 300 ms. New or modified command: **app-agent heartbeat interval** No ASDM support.
Inter-site redundancy for clustering	Inter-site redundancy ensures that a backup owner for a traffic flow will always be at the other site from the owner. This feature guards against site failure. New or modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**

Feature	Description
cluster remove unit command behavior matches **no enable** behavior	The **cluster remove unit** command now removes a unit from the cluster until you manually reenable clustering or reload, similar to the **no enable** command. Previously, if you redeployed the bootstrap configuration from FXOS, clustering would be reenabled. Now, the disabled status persists even in the case of a bootstrap configuration redeployment. Reloading the ASA, however, will reenable clustering. New/Modified screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster**
Administrative, Monitoring, and Troubleshooting Features	
SSH version 1 has been deprecated	SSH version 1 has been deprecated, and will be removed in a future release. The default setting has changed from both SSH v1 and v2 to just SSH v2. New/Modified screens: • **Configuration** > **Device Management** > **Management Access** > **ASDM/HTTPS/Telnet/SSH**
Enhanced packet tracer and packet capture capabilities	The packet tracer has been enhanced with the following features: • Trace a packet when it passes between cluster units. • Allow simulated packets to egress the ASA. • Bypass security checks for a similated packet. • Treat a simulated packet as an IPsec/SSL decrypted packet. The packet capture has been enhanced with the following features: • Capture packets after they are decrypted. • Capture traces and retain them in the persistent list. New or modified screens: **Tools** > **Packet Tracer** We added **Cluster Capture** field to support these options: **decrypted**, **persist**, **bypass-checks**, **transmit** We added two new options in the **Filter By** view under the **All Sessions** drop-down list: **Origin** and **Origin-ID** **Monitoring** > **VPN** > **VPN Statistics** > **Packet Tracer and Capture** We added **ICMP Capture** field in the Packet Capture Wizard screen:**Wizards** > **Packet Capture Wizard** We added two options **include-decrypted** and **persist** to support ICMP Capture.

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:

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

See the following table for the upgrade path for your version. Some older versions require an intermediate upgrade before you can upgrade to a newer version. Recommended versions are in **bold**.

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
9.8(x)	—	Any of the following: → 9.9(x) → **9.8(x)**
9.7(x)	—	Any of the following: → 9.9(x) → **9.8(x)**
9.6(x)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x)

Current Version	Interim Upgrade Version	Target Version
9.4(x)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x)
9.3(x)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(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: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.0(1)	→ 9.0(4)	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.2(x) and earlier	→ 9.0(4)	Any of the following: → 9.9(x) → **9.8(x)** → 9.6(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 7.9(2.152)

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

Caveat ID Number	Description
CSCvh80794	Configuring Multicast Route with interface throwing - Error : Required Validation
CSCvi23649	EasyVpnRemote - Allows Removing Interface Name of VPN Secure Client associated Interface.

Open Bugs in Version 7.9(2)

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

Caveat ID Number	Description
CSCvh80794	Configuring Multicast Route with interface throwing - Error : Required Validation
CSCvi23649	EasyVpnRemote - Allows Removing Interface Name of VPN Secure Client associated Interface.

Open Bugs in Version 7.9(1.151)

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
CSCvg34789	SecGwy:ASDM long delay-mins to retrieve session details for 1000s of VPN S2S tunnels
CSCvg88749	EtherType - Delete EtherType - After Edit

Open Bugs in Version 7.9(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
CSCvg34789	SecGwy:ASDM long delay-mins to retrieve session details for 1000s of VPN S2S tunnels
CSCvg88749	EtherType - Delete EtherType - After Edit

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.9(2.152)

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

Caveat ID Number	Description
CSCvi21519	ASDM 7.8(2)151 "Specified remark does not exist" when editing multiple ACL remarks
CSCvi43311	Inclusion of new CLI under Tunnel group webvpn attributes on ASDM
CSCvi54306	ASDM shows vxlan as udp-1 when creating an object service or object group service

Resolved Bugs in Version 7.9(2)

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

Caveat ID Number	Description
CSCvg44558	ASDM creates UDP port range service object as TCP service object
CSCvg81125	ASDM 7.8.2.151 : VPN Statistics->Sessions show incorrect values
CSCvg88749	EtherType - Delete EtherType - After Edit
CSCvg94453	ASDM ACL Manager: unable to remove multiple ACEs

Caveat ID Number	Description
CSCvh20595	ASDM 7.9(1) VPN Summary in Device Dashboard tab is incomplete
CSCvh48054	Basic access lists editing results in erroneous configuration
CSCvh56769	Can't change "set connection conn-max" value other than the default protocol in ASDM
CSCvh83068	Apply Button Not Enabled When "Enable Easy VPN Option" Box Checked & Outside Interface Uses DHCP

Resolved Bugs in Version 7.9(1.151)

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

Caveat ID Number	Description
CSCvg94453	ASDM ACL Manager: unable to remove multiple ACEs
CSCvh48054	Basic access lists editing results in erroneous configuration

Resolved Bugs in Version 7.9(1)

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

Caveat ID Number	Description
CSCvd68637	Unable to create or view more than one ipv6 prefix-list in ASDM
CSCvf82966	ASDM - Logging: Unable to View Real-Time logs
CSCvf91260	ASDM: Upgrade from CCO not working due to un-ignorable fields. "Meta data request failed"
CSCvg15782	ASDM - Unable to view modify SFR traffic redirection after upgrade to version 7.8(2)
CSCvg31344	DAP configuration is not visible in ASDM
CSCvg43291	ASDM adding duplicate random remarks when modifying an access rule
CSCvg51001	Local user password is changed automatically after enabling GroupLock setting

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.