

Release Notes for Cisco ASDM, 7.7(x)

First Published: 2017-01-23

Last Modified: 2017-03-09

Release Notes for Cisco ASDM, 7.7(x)

This document contains release information for Cisco ASDM Version 7.7(x) for the Cisco ASA series.

Important Notes

- 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.

- Potential Traffic Outage (9.7(1) through 9.7(1.2))—Due to bug [CSCvd78303](#), the ASA may stop passing traffic after 213 days of uptime. The effect on each network will be different, but it could range from an issue of limited connectivity to something more extensive like an outage. You must upgrade to a new version without this bug, when available. In the meantime, you can reboot the ASA to gain another 213 days of uptime. Other workarounds may be available. See Field Notice [FN-64291](#) for affected versions and more information.
- AnyConnect remote access VPN IPv6 DTLS tunnels in a scaled/stress environment may cause the ASA to traceback (for example: you have a large number of tunnels; or tunnels are continually connecting and disconnecting from the ASA headend). **Workaround:** Use IPv6 AnyConnect IKEv2 or IPv4 AnyConnect DTLS VPN remote access session types. (CSCvc77123)
- 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."
- When the ASA acts as a TLS server in a TLS proxy configuration, if the client proposes the TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 or

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ciphers and those are chosen, the TLS handshake might fail. You cannot control the cipher selection when the ASA acts as a server in this release, as there is a bug whereby the global **ssl encryption** command no longer takes effect as the default set of ciphers. In 9.8(1), you can use the new **server cipher-suite** command in the TLS proxy configuration to control the cipher. If you encounter this problem, please upgrade to 9.8(1). Alternatively, you can change the configuration of the client so that it does not propose those ciphers.

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.

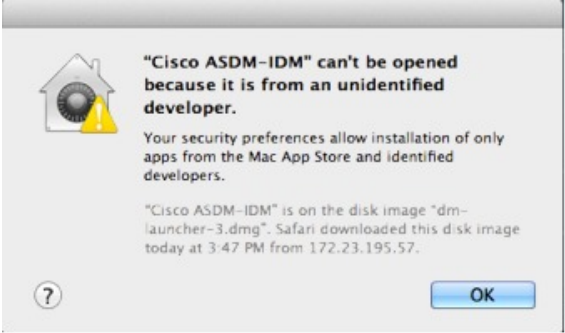
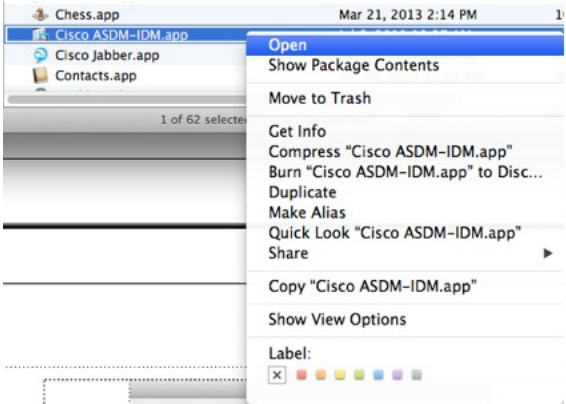

Table 1: ASA and ASA FirePOWER: ASDM Operating System and Browser Requirements

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
<p>Requires Strong Encryption license (3DES/AES) on ASA</p> <p>Note Smart licensing models allow initial access with ASDM without the Strong Encryption license.</p>	<p>ASDM requires an SSL connection to the ASA. You can request a 3DES license from Cisco:</p> <ol style="list-style-type: none"> 1. Go to www.cisco.com/go/license. 2. Click Continue to Product License Registration. 3. In the Licensing Portal, click Get Other Licenses next to the text field. 4. Choose IPS, Crypto, Other... from the drop-down list. 5. Type ASA in to the Search by Keyword field. 6. Select Cisco ASA 3DES/AES License in the Product list, and click Next. 7. Enter the serial number of the ASA, and follow the prompts to request a 3DES/AES license for the ASA.
<ul style="list-style-type: none"> • Self-signed certificate or an untrusted certificate • IPv6 • Firefox and Safari 	<p>When the ASA uses a self-signed certificate or an untrusted certificate, Firefox and Safari are unable to add security exceptions when browsing using HTTPS over IPv6. See https://bugzilla.mozilla.org/show_bug.cgi?id=633001. This caveat affects all SSL connections originating from Firefox or Safari to the ASA (including ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority.</p>
<ul style="list-style-type: none"> • SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 or disable SSL false start in Chrome. • Chrome 	<p>If you change the SSL encryption on the ASA to exclude both RC4-MD5 and RC4-SHA1 algorithms (these algorithms are enabled by default), then Chrome cannot launch ASDM due to the Chrome “SSL false start” feature. We suggest re-enabling one of these algorithms (see the Configuration > Device Management > Advanced > SSL Settings pane); or you can disable SSL false start in Chrome using the --disable-ssl-false-start flag according to Run Chromium with flags.</p>
IE9 for servers	<p>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.</p>
OS X	<p>On OS X, you may be prompted to install Java the first time you run ASDM; follow the prompts as necessary. ASDM will launch after the installation completes.</p>

Conditions	Notes
OS X 10.8 and later	<p>You need to allow ASDM to run because it is not signed with an Apple Developer ID. If you do not change your security preferences, you see an error screen.</p>  <p>1. To allow ASDM to run, right-click (or Ctrl-Click) the Cisco ASDM-IDM Launcher icon, and choose Open.</p>  <p>2. You see a similar error screen; however, you can open ASDM from this screen. Click Open. The ASDM-IDM Launcher opens.</p> 

Conditions	Notes
Windows 10	<p>"This app can't run on your PC" error message.</p> <p>When you install the ASDM Launcher, Windows 10 might replace the ASDM shortcut target with the Windows Scripting Host path, which causes this error. To fix the shortcut target:</p> <ol style="list-style-type: none"> 1. Choose Start > Cisco ASDM-IDM Launcher, and right-click the Cisco ASDM-IDM Launcher application. 2. Choose More > Open file location. Windows opens the directory with the shortcut icon. 3. Right click the shortcut icon, and choose Properties. 4. Change the Target to: C:\Windows\System32\wscript.exe invisible.vbs run.bat 5. Click OK.

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 ASDM 7.7(1.151)

Released: April 28, 2017



Note ASDM 7.7(1.150) was removed from Cisco.com due to bug [CSCvd90344](#).

Feature	Description
Admin Features	
New background service for the ASDM upgrade tool	ASDM uses a new background service for Tools > Check for ASA/ASDM Upgrades . The older service used by earlier versions of ASDM will be discontinued by Cisco in the future.

New Features in ASA 9.7(1.4)/ASDM 7.7(1)

Released: April 4, 2017



Note Verion 9.7(1) was removed from Cisco.com due to bug [CSCvd78303](#).

Feature	Description
Platform Features	

Feature	Description
New default configuration for the ASA 5506-X series using Integrated Routing and Bridging	<p>A new default configuration will be used for the ASA 5506-X series. The Integrated Bridging and Routing feature provides an alternative to using an external Layer 2 switch. For users replacing the ASA 5505, which includes a hardware switch, this feature lets you replace the ASA 5505 with an ASA 5506-X or other ASA model without using additional hardware.</p> <p>The new default configuration includes:</p> <ul style="list-style-type: none"> • outside interface on GigabitEthernet 1/1, IP address from DHCP • inside bridge group BVI 1 with GigabitEthernet ½ (inside1) through 1/8 (inside7), IP address 192.168.1.1 • inside --> outside traffic flow • inside ---> inside traffic flow for member interfaces • (ASA 5506W-X) wifi interface on GigabitEthernet 1/9, IP address 192.168.10.1 • (ASA 5506W-X) wifi <--> inside, wifi --> outside traffic flow • DHCP for clients on inside and wifi. The access point itself and all its clients use the ASA as the DHCP server. • Management 1/1 interface is Up, but otherwise unconfigured. The ASA FirePOWER module can then use this interface to access the ASA inside network and use the inside interface as the gateway to the Internet. • ASDM access—inside and wifi hosts allowed. • NAT—Interface PAT for all traffic from inside, wifi, and management to outside. <p>If you are upgrading, you can either erase your configuration and apply the default using the configure factory-default command, or you can manually configure a BVI and bridge group members to suit your needs. Note that to easily allow intra-bridge group communication, you need to enable the same-security-traffic permit inter-interface command (this command is already present for the ASA 5506W-X default configuration).</p>
Alarm ports support on the ISA 3000	<p>The ISA 3000 supports two alarm input interfaces and one alarm out interface. External sensors such as door sensors can be connected to the alarm inputs. External devices like buzzers can be connected to the alarm out interface. Alarms triggered are conveyed through two LEDs, syslogs, SNMP traps, and through devices connected to the alarm out interface. You can configure descriptions of external alarms. You can also specify the severity and trigger, for external and internal alarms. All alarms can be configured for relay, monitoring and logging.</p> <p>We introduced the following screens:</p> <p>Configuration > Device Management > Alarm Port > Alarm Contact</p> <p>Configuration > Device Management > Alarm Port > Redundant Power Supply</p> <p>Configuration > Device Management > Alarm Port > Temperature</p> <p>Monitoring > Properties > Alarm > Alarm Settings</p> <p>Monitoring > Properties > Alarm > Alarm Contact</p> <p>Monitoring > Properties > Alarm > Facility Alarm Status</p>

Feature	Description
Microsoft Azure Security Center support on the ASAv10	<p>Microsoft Azure is a public cloud environment that uses a private Microsoft Hyper V Hypervisor. Microsoft Azure Security Center is a Microsoft orchestration and management layer on top of Azure that simplifies the deployment of a highly secure public cloud infrastructure. Integration of the ASAv into Azure Security Center allows the ASAv to be offered as a firewall option to protect Azure environments.</p>
Precision Time Protocol (PTP) for the ISA 3000	<p>The ISA 3000 supports PTP, a time synchronization protocol for nodes distributed across a network. It provides greater accuracy than other time synchronization protocols, such as NTP, due to its hardware timestamp feature. The ISA 3000 supports PTP forward mode, as well as the one-step, end-to-end transparent clock. We added the following commands to the default configuration to ensure that PTP traffic is not sent to the ASA FirePOWER module for inspection. If you have an existing deployment, you need to manually add these commands:</p> <pre data-bbox="537 709 1533 783"> object-group service bypass_sfr_inspect service-object udp destination range 319 320 access-list sfrAccessList extended deny object-group bypass_sfr_inspect any any </pre> <p>We introduced the following screens:</p> <p>Configuration > Device Management > PTP</p> <p>Monitoring > Properties > PTP</p>
Automatic Backup and Restore for the ISA 3000	<p>You can enable auto-backup and/or auto-restore functionality using pre-set parameters in the backup and restore commands. The use cases for these features include initial configuration from external media; device replacement; roll back to an operable state.</p> <p>We introduced the following screen: Configuration > Device Management > Auto Backup & Restore Configuration</p>
Firewall Features	
Support for SCTP multi-streaming reordering and reassembly and fragmentation. Support for SCTP multi-homing, where the SCTP endpoints have more than one IP address.	<p>The system now fully supports SCTP multi-streaming reordering, reassembly, and fragmentation, which improves Diameter and M3UA inspection effectiveness for SCTP traffic. The system also supports SCTP multi-homing, where the endpoints have more than one IP address each. For multi-homing, the system opens pinholes for the secondary addresses so that you do not need to write access rules to allow them. SCTP endpoints must be limited to 3 IP addresses each.</p> <p>We did not modify any screens.</p>
M3UA inspection improvements.	<p>M3UA inspection now supports stateful failover, semi-distributed clustering, and multihoming. You can also configure strict application server process (ASP) state validation and validation for various messages. Strict ASP state validation is required for stateful failover and clustering.</p> <p>We modified the following screens: Configuration > Firewall > Objects > Inspection Maps > M3UA Add/Edit dialog boxes.</p>
Support for TLSv1.2 in TLS proxy and Cisco Unified Communications Manager 10.5.2.	<p>You can now use TLSv1.2 with TLS proxy for encrypted SIP or SCCP inspection with the Cisco Unified Communications Manager 10.5.2. The TLS proxy supports the additional TLSv1.2 cipher suites added as part of the client cipher-suite command.</p> <p>We did not modify any screens.</p>

Feature	Description
Integrated Routing and Bridging	<p>Integrated Routing and Bridging provides the ability to route between a bridge group and a routed interface. A bridge group is a group of interfaces that the ASA bridges instead of routes. The ASA is not a true bridge in that the ASA continues to act as a firewall: access control between interfaces is controlled, and all of the usual firewall checks are in place. Previously, you could only configure bridge groups in transparent firewall mode, where you cannot route between bridge groups. This feature lets you configure bridge groups in routed firewall mode, and to route between bridge groups and between a bridge group and a routed interface. The bridge group participates in routing by using a Bridge Virtual Interface (BVI) to act as a gateway for the bridge group. Integrated Routing and Bridging provides an alternative to using an external Layer 2 switch if you have extra interfaces on the ASA to assign to the bridge group. In routed mode, the BVI can be a named interface and can participate separately from member interfaces in some features, such as access rules and DHCP server.</p> <p>The following features that are supported in transparent mode are not supported in routed mode: multiple context mode, ASA clustering. The following features are also not supported on BVIs: dynamic routing and multicast routing.</p> <p>We modified the following screens:</p> <p>Configuration > Device Setup > Interface Settings > Interfaces</p> <p>Configuration > Device Setup > Routing > Static Routes</p> <p>Configuration > Device Management > DHCP > DHCP Server</p> <p>Configuration > Firewall > Access Rules</p> <p>Configuration > Firewall > EtherType Rules</p>
VM Attributes	<p>You can define network objects to filter traffic according to attributes associated with one or more Virtual Machines (VMs) in an VMware ESXi environment managed by VMware vCenter. You can define access control lists (ACLs) to assign policies to traffic from groups of VMs sharing one or more attributes.</p> <p>We added the following screen:</p> <p>Configuration > Firewall > VM Attribute Agent</p>
Stale route timeout for interior gateway protocols	<p>You can now configure the timeout for removing stale routes for interior gateway protocols such as OSPF.</p> <p>We modified the following screen: Configuration > Firewall > Advanced > Global Timeouts.</p>
Network object limitations for object group search.	<p>You can reduce the memory required to search access rules by enabling object group search with the the object-group-search access-control command. When enabled, object group search does not expand network or service objects, but instead searches access rules for matches based on those group definitions.</p> <p>Starting with this release, the following limitation is applied: For each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped.</p> <p>This check is to prevent performance degradation. Configure your rules to prevent an excessive number of matches.</p>

Feature	Description
Routing Features	
31-bit Subnet Mask	<p>For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. The 31-bit subnet includes only 2 addresses; normally, the first and last address in the subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4. For example, the failover link between 2 ASAs only requires 2 addresses; any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog. This feature is not supported with BVIs for bridge groups or multicast routing.</p> <p>We modified the following screens:</p> <p>Configuration > Device Setup > Interface Settings > Interfaces > Add Interface > General</p>
High Availability and Scalability Features	
Inter-site clustering improvement for the ASA on the Firepower 4100/9300 chassis	<p>You can now configure the site ID for each Firepower 4100/9300 chassis when you deploy the ASA cluster. Previously, you had to configure the site ID within the ASA application; this new feature eases initial deployment. Note that you can no longer set the site ID within the ASA configuration. Also, for best compatibility with inter-site clustering, we recommend that you upgrade to ASA 9.7(1) and FXOS 2.1.1, which includes several improvements to stability and performance.</p> <p>We modified the following screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Configuration</p>
Director localization: inter-site clustering improvement for data centers	<p>To improve performance and keep traffic within a site for inter-site clustering for data centers, you can enable director localization. New connections are typically load-balanced and owned by cluster members within a given site. However, the ASA assigns the director role to a member at <i>any</i> site. Director localization enables additional director roles: a local director at the same site as the owner, and a global director that can be at any site. Keeping the owner and director at the same site improves performance. Also, if the original owner fails, the local director chooses a new connection owner at the same site. The global director is used if a cluster member receives packets for a connection that is owned on a different site.</p> <p>We modified the following screen: Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Configuration</p>
Interface link state monitoring polling for failover now configurable for faster detection	<p>By default, each ASA in a failover pair checks the link state of its interfaces every 500 msec. You can now configure the polling interval, between 300 msec and 799 msec; for example, if you set the polltime to 300 msec, the ASA can detect an interface failure and trigger failover faster.</p> <p>We modified the following screen: Configuration > Device Management > High Availability and Scalability > Failover > Criteria</p>

Feature	Description
Bidirectional Forwarding Detection (BFD) support for Active/Standby failover health monitoring on the Firepower 9300 and 4100	<p>You can enable Bidirectional Forwarding Detection (BFD) for the failover health check between two units of an Active/Standby pair on the Firepower 9300 and 4100. Using BFD for the health check is more reliable than the default health check method and uses less CPU.</p> <p>We modified the following screen: Configuration > Device Management > High Availability and Scalability > Failover > Setup</p>
VPN Features	
Dynamic RRI for IKEv2 static crypto maps	<p>Dynamic Reverse Route Injection occurs upon the successful establishment of IPsec Security Associations (SA's) when dynamic is specified for a crypto map. Routes are added based on the negotiated selector information. The routes will be deleted after the IPsec SA's are deleted. Dynamic RRI is supported on IKEv2 based static crypto maps only.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps > Add/Edit > Tunnel Policy (Crypto Maps) - Advanced</p>
Virtual Tunnel Interface (VTI) support for ASA VPN module	<p>The ASA VPN module is enhanced with a new logical interface called Virtual Tunnel Interface (VTI), used to represent a VPN tunnel to a peer. This supports route based VPN with IPsec profiles attached to each end of the tunnel. Using VTI does away with the need to configure static crypto map access lists and map them to interfaces.</p> <p>We introduced the following screens:</p> <p>Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets) > IPsec Profile</p> <p>Configuration > Site-to-Site VPN > Advanced > IPsec Proposals (Transform Sets) > IPsec Profile > Add > Add IPsec Profile</p> <p>Configuration > Device Setup > Interface Settings > Interfaces > Add > VTI Interface</p> <p>Configuration > Device Setup > Interface Settings > Interfaces > Add > VTI Interface > General</p> <p>Configuration > Device Setup > Interface Settings > Interfaces > Add > VTI Interface > Advanced</p>
SAML 2.0 based SSO for AnyConnect	<p>SAML 2.0-based service provider IdP is supported in a private network. With the ASA as a gateway between the user and services, authentication on IdP is handled with a restricted anonymous webvpn session, and all traffic between IdP and the user is translated.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers > Add SSO Server.</p>
CMPv2	<p>To be positioned as a security gateway device in wireless LTE networks, the ASA now supports certain management functions using the Certificate Management Protocol (CMPv2).</p> <p>We modified the following screens: Configuration > Remote Access VPN > Certificate Management > Identity Certificates > Add an Identity Certificate</p>

Feature	Description
Multiple certificate authentication	<p>You can now validate multiple certificates per session with AnyConnect SSL and IKEv2 client protocols. The Aggregate Authentication protocol has been extended to define the protocol exchange for multiple-certificate authentication and utilize this for both session types.</p> <p>We modified the following screens:</p> <p>Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Edit AnyConnect Connection Profile</p> <p>Configuration > Remote Access VPN > Network Client Access > AnyConnect Connection Profiles > Edit AnyConnect Connection Profiles</p>
Increase split-tunneling routing limit	<p>The limit for split-tunneling routes for AC-SSL and AC-IKEv2 was increased from 200 to 1200. The IKEv1 limit was left at 200.</p>
Smart Tunnel Support on Chrome	<p>A new method for smart-tunnel support in the Chrome browser on Mac and Windows devices was created. A Chrome Smart Tunnel Extension has replaced Netscape Plugin Application Program Interfaces (NPAPIs) that are no longer supported on Chrome. If you click on the smart tunnel enabled bookmark in Chrome without the extension already being installed, you are redirected to the Chrome Web Store to obtain the extension. New Chrome installations will direct the user to the Chrome Web Store to download the extension. The extension downloads the binaries from ASA that are required to run smart tunnel. Your usual bookmark and application configuration while using smart tunnel is unchanged other than the process of installing the new extension.</p>
Clientless SSL VPN: Session information for all web interfaces	<p>All web interfaces will now display details of the current session, including the user name used to login, and user privileges which are currently assigned. This will help the user be aware of the current user session and will improve user security.</p>
Clientless SSL VPN: Validation of all cookies for web applications' sessions	<p>All web applications will now grant access only after validating all security-related cookies. In each request, each cookie with an authentication token or a session ID will be verified before granting access to the user session. Multiple session cookies in the same request will result in the connection being dropped. Cookies with failed validations will be treated as invalid and the event will be added to the audit log.</p>
AnyConnect: Maximum Connect Time Alert Interval is now supported in the Group Policy for AnyConnect VPN Client connections.	<p>The alert interval is the interval of time before max connection time is reached that a message will be displayed to the user warning them of termination. Valid time interval is 1-30 minutes. Default is 30 minutes. Previously supported for clientless and site-to-site VPN connections.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options, adding a Maximum Connect Time Alert Interval field</p>
AAA Features	
IPv6 address support for LDAP and TACACS+ Servers for AAA	<p>You can now use either IPv4 or IPv6 addresses for LDAP and TACACS+ servers used for AAA.</p> <p>We modified the following screen: Configuration > Device Management > Users/AAA > AAA Server Groups > Add AAA Server Group</p>
Administrative Features	

Feature	Description
PBKDF2 hashing for all local username and enable passwords	<p>Local username and enable passwords of all lengths are stored in the configuration using a PBKDF2 (Password-Based Key Derivation Function 2) hash. Previously, passwords 32 characters and shorter used the MD5-based hashing method. Already existing passwords continue to use the MD5-based hash unless you enter a new password. See the "Software and Configurations" chapter in the General Operations Configuration Guide for downgrading guidelines.</p> <p>We modified the following screens:</p> <p>Configuration > Device Setup > Device Name/Password > Enable Password</p> <p>Configuration > Device Management > Users/AAA > User Accounts > Add/Edit User Account > Identity</p>
Licensing Features	
Licensing changes for failover pairs on the Firepower 4100/9300 chassis	Only the active unit requests the license entitlements. Previously, both units requested license entitlements. Supported with FXOS 2.1.1.
Monitoring and Troubleshooting Features	
IPv6 address support for traceroute	<p>The traceroute command was modified to accept an IPv6 address.</p> <p>We modified the following screen: Tools > Traceroute</p>
Support for the packet tracer for bridge group member interfaces	<p>You can now use the packet tracer for bridge group member interfaces.</p> <p>We added VLAN ID and Destination MAC Address fields in the packet-tracer screen: Tools > Packet Tracer</p>
IPv6 address support for syslog servers	<p>You can now configure syslog servers with IPv6 addresses to record and send syslogs over TCP and UDP.</p> <p>We modified the following screen: Configuration > Device Management > Logging > Syslog Servers > Add Syslog Server</p>
SNMP OIDs and MIBs	<p>The ASA now supports SNMP MIB objects corresponding to the end-to-end transparent clock mode as part of the Precision Time Protocol (PTP) for the ISA 3000. The following SNMP MIB objects are supported:</p> <ul style="list-style-type: none"> • ciscoPtpMIBSystemInfo • cPtpClockDefaultDSTable • cPtpClockTransDefaultDSTable • cPtpClockPortTransDSTable
Manually stop and start packet captures	<p>You can now manually stop and start the capture.</p> <p>Added/Modified screens: Wizards > Packet Capture Wizard > Run Captures</p> <p>Added/Modified options: Start button, Stop button</p>

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
9.6(x)	—	Any of the following: → 9.6(x)
9.5(x)	—	Any of the following: → 9.6(x)
9.4(x)	—	Any of the following: → 9.6(x)
9.3(x)	—	Any of the following: → 9.6(x)
9.2(x)	—	Any of the following: → 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: → 9.6(x) → 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.1(1)	→ 9.1(2)	Any of the following: → 9.6(x) → 9.1(7.4)
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.6(x) → 9.1(7.4)
9.0(1)	→ 9.0(4)	Any of the following: → 9.6(x) → 9.1(7.4)
8.6(1)	→ 9.0(4)	Any of the following: → 9.6(x) → 9.1(7.4)
8.5(1)	→ 9.0(4)	Any of the following: → 9.6(x) → 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.6(x) → 9.1(7.4) → 9.0(4)
8.4(1) through 8.4(4)	→ 9.0(4)	→ 9.6(x) → 9.1(7.4)
8.3(x)	→ 9.0(4)	Any of the following: → 9.6(x) → 9.1(7.4)
8.2(x) and earlier	→ 9.0(4)	Any of the following: → 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 7.7(1.151)

There are no new open bugs for version 7.7(1.151). See [Open Bugs in Version 7.7\(1\)](#), on page 17.

Open Bugs in Version 7.7(1)

If you have a Cisco support contract, use the following dynamic search for all open bugs severity 3 and higher for Version 7.7(1):

- [7.7\(1\) open bug search](#).

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

Caveat ID Number	Description
CSCvc73791	SNMPv3 user from asdm configuration is failing.

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.7(1.151)

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

Caveat ID Number	Description
CSCvd90344	ASDM 7.7.150 Upload wizard not working

Resolved Bugs in Version 7.7(1)

If you have a Cisco support contract, use the following search for severity 3 and higher resolved bugs:

- [7.7\(1\) fixed bug search](#).

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

Caveat ID Number	Description
CSCva50676	ASDM replacing network IP with host based object in access-list
CSCva89785	ASDM: TCP timeout values under service-policy pushes wrong values to ASA
CSCva91507	ASDM does not allow port range from 0 to 65535
CSCva99049	ASDM: Wrong Service object added after reordering the list
CSCvb16663	ASDM 7.6.2 can't display VPN sessions - stuck @ 97% loading
CSCvb24760	ASDM: Remove demo functionality from Launcher and from cisco.com
CSCvb37828	ASDM 7.6.x not showing "pre-fill-username" option
CSCvb48973	ASDM: VPN Wizard Incorrectly Combining configuration
CSCvb49232	ASDM: VPN remove crypto access-list
CSCvb53989	ASDM not allows to correct non-contiguous object subnet mask
CSCvb63008	ASDM 7.6.2 Not displaying active anyconnect clients
CSCvb68442	ASDM File Management does not display Disk1
CSCvb99770	ASDM not removing identical remarks from different line #s in an ACL
CSCvb99824	ASDM adding duplicate remarks when removing object groups from an ACE
CSCvc10201	ASDM 7.6.2 can't display IPsec RA VPN sessions - stuck @ 97% loading

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](#).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017 Cisco Systems, Inc. All rights reserved.