Release Notes for Cisco ASDM, 7.4(x)

First Published: 2015-03-23

Last Modified: 2016-06-21

Release Notes for Cisco ASDM, 7.4(x)

This document contains release information for Cisco ASDM Version 7.4(x) for the Cisco ASA series.

Important Notes

- Potential Traffic Outage (9.4(3.11) through 9.4(4))—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.
- For the ASA 5506H-X, when you upgrade to ASA Version 9.5(2), the correct licensing level is applied. Earlier ASA versions apply the same licensing as the ASA 5506-X base license. For earlier versions, you can contact Cisco to receive the ASA 5506-X Security Plus license, which is equivalent to the correct ASA 5506H-X base license; or simply upgrade to 9.5(2).
- Unified Communications Phone Proxy and Intercompany Media Engine Proxy are deprecated—In ASA Version 9.4, the Phone Proxy and IME Proxy are no longer supported.
- Elliptic curve cryptography for SSL/TLS—When an elliptic curve-capable SSL VPN client connects to the ASA, the elliptic curve cipher suite will be negotiated, and the ASA will present the SSL VPN client with an elliptic curve certificate, even when the corresponding interface has been configured with an RSA-based trustpoint. To avoid having the ASA present a self-signed SSL certificate, the administrator needs to remove the corresponding cipher suites using the **ssl cipher** command. For example, for an interface configured with an RSA trustpoint, the administrator can execute the following command so that only RSA based ciphers are negotiated:

  ```
  ssl cipher tlsv1.2 custom
  "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:DES-CBC3-SHA:
  DES-CBC-SHA:RC4-SHA:RC4-MD5"
  ```

- 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.

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

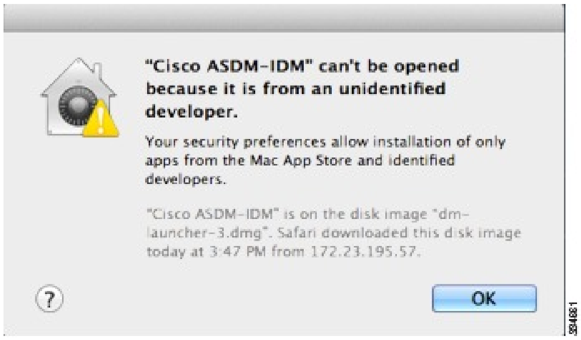
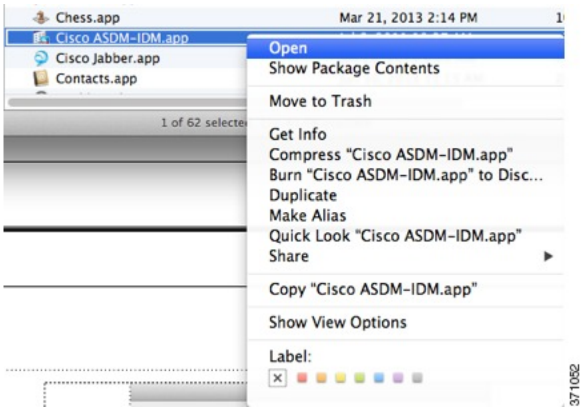
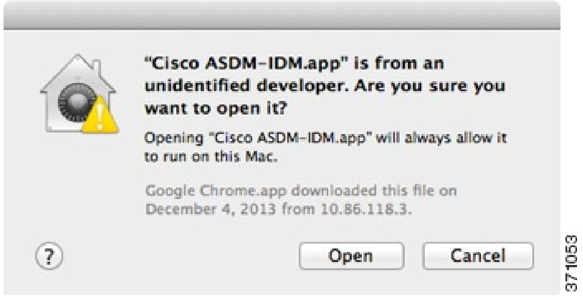
Operating System	Browser				Oracle JRE
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): 8 7 Server 2012 Server 2008	Yes	Yes	No support	Yes	8.0
Apple OS X 10.4 and later	No support	Yes	Yes	Yes (64-bit version only)	8.0
Ubuntu Linux 14.04 Debian Linux 7	N/A	Yes	N/A	Yes	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.

Conditions	Notes
- 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

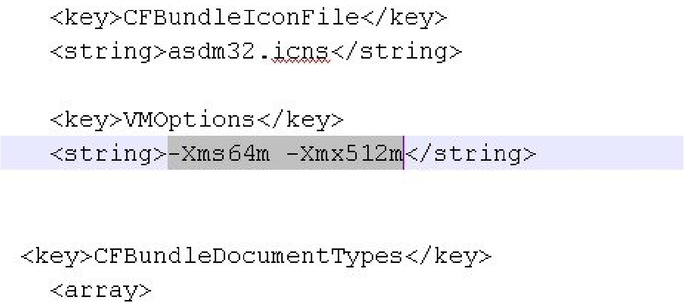
To increase the ASDM heap memory size, edit the **Info.plist** file by performing the following procedure.

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.

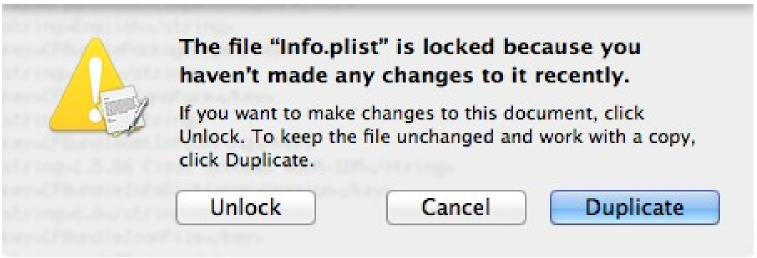


```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

    <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 ASA 9.4(4.5)/ASDM 7.6(2)

Released: April 3, 2017

> **Note** Verion 9.4(4) was removed from Cisco.com due to bug CSCvd78303.

There are no new features in this release.

New Features in ASA 9.4(3)/ASDM 7.6(1)

Released: April 25, 2016

Feature	Description
Firewall Features	
Connection holddown timeout for route convergence	You can now configure how long the system should maintain a connection when the route used by the connection no longer exists or is inactive. If the route does not become active within this holddown period, the connection is freed. You can reduce the holddown timer to make route convergence happen more quickly. However, the 15 second default is appropriate for most networks to prevent route flapping. We modified the following screen: **Configuration** > **Firewall** > **Advanced** > **Global Timeouts**
Remote Access Features	
Configurable SSH encryption and HMAC algorithm.	Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. We introduced the following screen: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** *Also available in 9.1(7).*
HTTP redirect support for IPv6	When you enable HTTP redirect to HTTPS for ASDM access or clientless SSL VPN, you can now redirect traffic sent an to IPv6 address. We added functionality to the following screen: **Configuration** > **Device Management** > **HTTP Redirect** *Also available in 9.1(7).*
Monitoring Features	

Feature	Description
SNMP engineID sync for Failover	In a failover pair, the SNMP engineIDs of the paired ASAs are synced on both units. Three sets of engineIDs are maintained per ASA—synced engineID, native engineID and remote engineID. An SNMPv3 user can also specify the engineID of the ASA when creating a profile to preserve localized **snmp-server user** authentication and privacy options. If a user does not specify the native engineID, the **show running config** output will show two engineIDs per user. We modified the following command: **snmp-server user** No ASDM support.
show tech support enhancements	The **show tech support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the following cases: • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail**. We did not add or modify any screens. *Also available in 9.1(7).*
Support for the cempMemPoolTable in the CISCO-ENHANCED-MEMPOOL-MIB	The cempMemPoolTable of the CISCO-ENHANCED-MEMPOOL-MIB is now supported. This is a table of memory pool monitoring entries for all physical entities on a managed system. **Note** The CISCO-ENHANCED-MEMPOOL-MIB uses 64-bit counters and supports reporting of memory on platforms with more than 4GB of RAM. We did not add or modify any screens. *Also available in 9.1(7).*

New Features in ASA 9.4(2.145)/ASDM 7.5(1)

Released: November 13, 2015

There are no new features in this release.

Note This release supports only the Firepower 9300 ASA security module.

New Features in ASA 9.4(2)/ASDM 7.5(1)

Released: September 24, 2015

There are no new features in this release.

Note ASAv 9.4(1.200) features are not included in this release.

Note This version does not support the ISA 3000.

New Features in ASA 9.4(1.225)/ASDM 7.5(1)

Released: September 17, 2015

Note This release supports only the Cisco ISA 3000.

Feature	Description
Platform Features	
Cisco ISA 3000 Support	The Cisco ISA 3000 is a DIN Rail mounted, ruggedized, industrial security appliance. It is low-power, fan-less, with Gigabit Ethernet and a dedicated management port. This model comes with the ASA Firepower module pre-installed. Special features for this model include a customized transparent mode default configuration, as well as a hardware bypass function to allow traffic to continue flowing through the appliance when there is a loss of power. We introduced the following screen: **Configuration** > **Device Management** > **Hardware Bypass** The **hardware-bypass boot-delay** command is not available in ASDM 7.5(1). *This feature is not available in Version 9.5(1).*

New Features in ASA 9.4(1.152)/ASDM 7.4(3)

Released: July 13, 2015

Note This release supports only the ASA on the Firepower 9300.

Feature	Description
Platform Features	
ASA security module on the Firepower 9300	We introduced the ASA security module on the Firepower 9300. **Note** Firepower Chassis Manager 1.1.1 does not support any VPN features (site-to-site or remote access) for the ASA security module on the Firepower 9300.
High Availability Features	

Feature	Description
Intra-chassis ASA Clustering for the Firepower 9300	You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster. We introduced the following screen: **Configuration** > **Device Management** > **High Availability and Scalability** > **ASA Cluster Replication**
Licensing Features	
Cisco Smart Software Licensing for the ASA on the Firepower 9300	We introduced Smart Software Licensing for the ASA on the Firepower 9300. We modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**

New Features in ASAv 9.4(1.200)/ASDM 7.4(2)

Released: May 12, 2015

Note This release supports only the ASAv.

Feature	Description
Platform Features	
ASAv on VMware no longer requires vCenter support	You can now install the ASAv on VMware without vCenter using the vSphere client or the OVFTool using a Day 0 configuration.
ASAv on Amazon Web Services (AWS)	You can now use the ASAv with Amazon Web Services (AWS) and the Day 0 configuration. **Note** Amazon Web Services only supports models ASAv10 and ASAv30.

New Features in ASDM 7.4(2)

Released: May 6, 2015

Feature	Description
Remote Access Features	
AnyConnect Version 4.1 support	ASDM now supports AnyConnect Version 4.1. We modified the following screen: **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile** (a new profile called **AMP Enabler Service Profile**)

New Features in ASA 9.4(1)/ASDM 7.4(1)

Released: March 30, 2015

Feature	Description
Platform Features	
ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X	We introduced the ASA 5506W-X with wireless access point, hardened ASA 5506H-X, ASA 5508-X, and ASA 5516-X models. We did not modify any ASDM screens.
Certification Features	
Department of Defense Unified Capabilities Requirements (UCR) 2013 Certification	The ASA was updated to comply with the DoD UCR 2013 requirements. See the rows in this table for the following features that were added for this certification: • Periodic certificate authentication • Certificate expiration alerts • Enforcement of the basic constraints CA flag • ASDM Username From Certificate Configuration • ASDM management authorization • IKEv2 invalid selectors notification configuration • IKEv2 pre-shared key in Hex
FIPS 140-2 Certification compliance updates	When you enable FIPS mode on the ASA, additional restrictions are put in place for the ASA to be FIPS 140-2 compliant. Restrictions include: • RSA and DH Key Size Restrictions—Only RSA and DH keys 2K (2048 bits) or larger are allowed. For DH, this means groups 1 (768 bit), 2 (1024 bit), and 5 (1536 bit) are not allowed. **Note** The key size restrictions disable use of IKEv1 with FIPS. • Restrictions on the Hash Algorithm for Digital Signatures—Only SHA256 or better is allowed. • SSH Cipher Restrictions—Allowed ciphers: aes128-cbc or aes256-cbc. MACs: SHA1 To see the FIPS certification status for the ASA, see: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf This PDF is updated weekly. See the Computer Security Division Computer Security Resource Center site for more information: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html We modified the following command: **fips enable**

Feature	Description
Firewall Features	
Improved SIP inspection performance on multiple core ASAs.	If you have multiple SIP signaling flows going through an ASA with multiple cores, SIP inspection performance has been improved. However, you will not see improved performance if you are using a TLS, phone, or IME proxy. We did not modify any screens.
SIP inspection support for Phone Proxy and UC-IME Proxy was removed.	You can no longer use Phone Proxy or UC-IME Proxy when configuring SIP inspection. Use TLS Proxy to inspect encrypted traffic. We removed Phone Proxy and UC-IME Proxy from the **Select SIP Inspect Map** service policy dialog box.
DCERPC inspection support for ISystemMapper UUID message RemoteGetClassObject opnum3.	The ASA started supporting non-EPM DCERPC messages in release 8.3, supporting the ISystemMapper UUID message RemoteCreateInstance opnum4. This change extends support to the RemoteGetClassObject opnum3 message. We did not modify any screens.
Unlimited SNMP server trap hosts per context	The ASA supports an unlimited number of SNMP server trap hosts per context. The **show snmp-server host** command output displays only the active hosts that are polling the ASA, as well as the statically configured hosts. We did not modify any screens.
VXLAN packet inspection	The ASA can inspect the VXLAN header to enforce compliance with the standard format. We modified the following screen: **Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > Protocol Inspection**
DHCP monitoring for IPv6	You can now monitor DHCP statistics and DHCP bindings for IPv6. We introduced the following screens: **Monitoring > Interfaces > DHCP > IPV6 DHCP Statistics Monitoring > Interfaces > DHCP > IPV6 DHCP Binding**.
ESMTP inspection change in default behavior for TLS sessions.	The default for ESMTP inspection was changed to allow TLS sessions, which are not inspected. However, this default applies to new or reimaged systems. If you upgrade a system that includes **no allow-tls**, the command is not changed. The change in default behavior was also made in these older versions: 8.4(7.25), 8.5(1.23), 8.6(1.16), 8.7(1.15), 9.0(4.28), 9.1(6.1), 9.2(3.2) 9.3(1.2), 9.3(2.2).
High Availability Features	
Blocking syslog generation on a standby ASA	You can now block specific syslogs from being generated on a standby unit. We did not modify any screens.

Feature	Description
Enable and disable ASA cluster health monitoring per interface	You can now enable or disable health monitoring per interface. Health monitoring is enabled by default on all port-channel, redundant, and single physical interfaces. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored. You might want to disable health monitoring of non-essential interfaces, for example, the management interface. We introduced the following screen: **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Interface Health Monitoring**
ASA clustering support for DHCP relay	You can now configure DHCP relay on the ASA cluster. Client DHCP requests are load-balanced to the cluster members using a hash of the client MAC address. DHCP client and server functions are still not supported. We did not modify any screens.
SIP inspection support in ASA clustering	You can now configure SIP inspection on the ASA cluster. A control flow can be created on any unit (due to load balancing), but its child data flows must reside on the same unit. TLS Proxy configuration is not supported. We did not modify any screens.
Routing Features	
Policy Based Routing	Policy Based Routing (PBR) is a mechanism by which traffic is routed through specific paths with a specified QoS using ACLs. ACLs let traffic be classified based on the content of the packet's Layer 3 and Layer 4 headers. This solution lets administrators provide QoS to differentiated traffic, distribute interactive and batch traffic among low-bandwidth, low-cost permanent paths and high-bandwidth, high-cost switched paths, and allows Internet service providers and other organizations to route traffic originating from various sets of users through well-defined Internet connections. We introduced or modified the following screens: **Configuration > Device Setup > Routing > Route Maps > Policy Based Routing** **Configuration > Device Setup > Routing > Interface Settings > Interfaces.**
Interface Features	
VXLAN support	VXLAN support was added, including VXLAN tunnel endpoint (VTEP) support. You can define one VTEP source interface per ASA or security context. We introduced the following screens: **Configuration > Device Setup > Interface Settings > Interfaces > Add > VNI Interface** **Configuration > Device Setup > Interface Settings > VXLAN**
Monitoring Features	
Memory tracking for the EEM	We have added a new debugging feature to log memory allocations and memory usage, and to respond to memory logging wrap events. We modified the following screen: **Configuration > Device Management > Advanced > Embedded Event Manager > Add Event Manager Applet > Add Event Manager Applet Event**

Feature	Description
Troubleshooting crashes	The **show tech-support** command output and **show crashinfo** command output includes the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.
Remote Access Features	
Support for ECDHE-ECDSA ciphers	TLSv1.2 added support for the following ciphers: • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES256-SHA384 • ECDHE-RSA-AES256-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • RSA-AES128-GCM-SHA256 • ECDHE-ECDSA-AES128-SHA256 • ECDHE-RSA-AES128-SHA256 **Note** ECDSA and DHE ciphers are the highest priority. We modified the following screen: **Configuration > Remote Access VPN > Advanced > SSL Settings.**

Feature	Description
Clientless SSL VPN session cookie access restriction	You can now prevent a Clientless SSL VPN session cookie from being accessed by a third party through a client-side script such as Javascript. **Note** Use this feature only if Cisco TAC advises you to do so. Enabling this command presents a security risk because the following Clientless SSL VPN features will not work without any warning. • Java plug-ins • Java rewriter • Port forwarding • File browser • Sharepoint features that require desktop applications (for example, MS Office applications) • AnyConnect Web launch • Citrix Receiver, XenDesktop, and Xenon • Other non-browser-based and browser plugin-based applications We introduced the following screen: **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > HTTP Cookie**. *This feature is also in 9.2(3).*
Virtual desktop access control using security group tagging	The ASA now supports security group tagging-based policy control for Clientless SSL remote access to internal applications and websites. This feature uses Citrix's virtual desktop infrastructure (VDI) with XenDesktop as the delivery controller and the ASA's content transformation engine. See the following Citrix product documentation for more information: • Policies for XenDesktop and XenApp: http://support.citrix.com/proddocs/topic/infocenter/ic-how-to-use.html • Managing policies in XenDesktop 7: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-wrapper-rho.html • Using group policy editor for XenDesktop 7 policies: http://support.citrix.com/proddocs/topic/xendesktop-7/cds-policies-use-gpmc.html
OWA 2013 feature support has been added for Clientless SSL VPN	Clientless SSL VPN supports the new features in OWA 2013 except for the following: • Support for tablets and smartphones • Offline mode • Active Directory Federation Services (AD FS) 2.0. The ASA and AD FS 2.0 can't negotiate encryption protocols. We did not modify any screens.

Feature	Description
Citrix XenDesktop 7.5 and StoreFront 2.5 support has been added for Clientless SSL VPN	Clientless SSL VPN supports the access of XenDesktop 7.5 and StoreFront 2.5. See http://support.citrix.com/proddocs/topic/xenapp-xendesktop-75/cds-75-about-whats-new.html for the full list of XenDesktop 7.5 features, and for more details. See http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-about.html for the full list of StoreFront 2.5 features, and for more details. We did not modify any screens.
Periodic certificate authentication	When you enable periodic certificate authentication, the ASA stores certificate chains received from VPN clients and re-authenticates them periodically. We modified the following screens: **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
Certificate expiration alerts	The ASA checks all CA and ID certificates in the trust points for expiration once every 24 hours. If a certificate is nearing expiration, a syslog will be issued as an alert. You can configure the reminder and recurrence intervals. By default, reminders will start at 60 days prior to expiration and recur every 7 days. We modified the following screens: **Configuration > Device Management > Certificate Management > Identity Certificates** **Configuration > Device Management > Certificate Management > CA Certificates**
Enforcement of the basic constraints CA flag	Certificates without the CA flag now cannot be installed on the ASA as CA certificates by default. The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate. You can configure the ASA to allow installation of these certificates if desired. We modified the following screens: **Configuration > Device Management > Certificate Management > CA Certificates**
IKEv2 invalid selectors notification configuration	Currently, if the ASA receives an inbound packet on an SA, and the packet's header fields are not consistent with the selectors for the SA, then the ASA discards the packet. You can now enable or disable sending an IKEv2 notification to the peer. Sending this notification is disabled by default. **Note** This feature is supported with AnyConnect 3.1.06060 and later.
IKEv2 pre-shared key in Hex	You can now configure the IKEv2 pre-shared keys in hex.
Administrative Features	
ASDM management authorization	You can now configure management authorization separately for HTTP access vs. Telnet and SSH access. We modified the following screen: **Configuration > Device Management > Users/AAA > AAA Access > Authorization**

Feature	Description
ASDM Username From Certificate Configuration	When you enable ASDM certificate authentication, you can configure how ASDM extracts the username from the certificate; you can also enable pre-filling the username at the login prompt. We introduced the following screen: **Configuration > Device Management > Management Access > HTTP Certificate Rule.**
terminal interactive command to enable or disable help when you enter **?** at the CLI	Normally, when you enter **?** at the ASA CLI, you see command help. To be able to enter **?** as text within a command (for example, to include a ? as part of a URL), you can disable interactive help using the **no terminal interactive** command. We introduced the following command: terminal interactive
REST API Features	
REST API Version 1.1	We added support for the REST API Version 1.1.
Support for token-based authentication (in addition to existing basic authentication)	Client can send log-in request to a specific URL; if successful, a token is returned (in response header). Client then uses this token (in a special request header) for sending additional API calls. The token is valid until explicitly invalidated, or the idle/session timeout is reached.
Limited multiple-context support	The REST API agent can now be enabled in multi-context mode; the CLI commands can be issued only in system-context mode (same commands as single-context mode). Pass-through CLI API commands can be used to configure any context, as follows. `https://<asa_admin_context_ip>/api/cli?context=<context_name>` If the **context** parameter is not present, it is assumed that the request is directed to the **admin** context.
Advanced (granular) inspection	Granular inspection of these protocols is supported: • DNS over UDP • HTTP • ICMP • ICMP ERROR • RTSP • SIP • FTP • DCERPC • IP Options • NetBIOS Name Server over IP • SQL*Net

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**.

Current Version	Interim Upgrade Version	Target Version
9.3(x)	—	Any of the following: → 9.4(x) → 9.3(x)
9.2(x)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(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: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.1(1)	→ 9.1(2)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
9.0(2), 9.0(3), or 9.0(4)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
9.0(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.6(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.5(1)	→ 9.0(2), 9.0(3), or 9.0(4)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.4(5+)	—	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)

Current Version	Interim Upgrade Version	Target Version
8.4(1) through 8.4(4)	Any of the following: → 9.0(2), 9.0(3), or 9.0(4) → 8.4(6)	→ 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.3(x)	→ 8.4(6)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 9.1(7.4)
8.2(x) and earlier	→ 8.4(6)	Any of the following: → 9.4(x) → 9.3(x) → 9.2(x) → 9.1(3), 9.1(4), 9.1(5), 9.1(6), 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 7.4(1)

If you have a Cisco support contract, use the following dynamic search for all open bugs severity 3 and higher for Version 7.4(1):

- 7.4(1) open bug search.

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

Identifier	Description
CSCuz92899	Prelogin Policies changes not getting saved

Open Bugs in Version 7.4(2)

There are no open bugs for Version 7.4(2).

Open Bugs in Version 7.4(1)

If you have a Cisco support contract, use the following dynamic search for all open bugs severity 3 and higher for Version 7.4(1):

- 7.4(1) open bug search.

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

Identifier	Description
CSCuz92899	Prelogin Policies changes not getting saved

Resolved Bugs

This section lists resolved bugs per release.

Resolved Bugs in Version 7.4(3)

If you have a Cisco support contract, use the following search for all resolved bugs:

- 7.4(3) fixed bug search.

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

Identifier	Description
CSCut74372	asdm: Issues in loading the home page due to Core Usage output
CSCuu29995	DOC: ASDM: 'DM_INLINE_NETWORK' is default name of object-group

Resolved Bugs in Version 7.4(2)

If you have a Cisco support contract, use the following search for all resolved bugs:

- 7.4(2) fixed bug search.

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

Identifier	Description
CSCut49785	ASDM 7.4.X gets stuck in "software update completed"
CSCut50204	ASDM: NPE when parsing ssl command
CSCut57751	ASDM 7.4.1 hangs at 87% while validating running configuration

Resolved Bugs in Version 7.4(1)

If you have a Cisco support contract, use the following search for all resolved bugs:

- 7.4(1) fixed bug search.

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

Identifier	Description
CSCup27452	ASDM persistently polling ASA with CX installed
CSCuq59377	ASDM:Botnet Traffic Filter not working for Real-time-Reports on ASDM 7.3
CSCur16710	VXLAN: interface cli is missing while sending nve-only
CSCur21416	Null pointer Exception thrown in Failover panel
CSCur23947	ASDM 7.3.2 doesn't display the "Endpoint Attribute Type: Policy" in DAP
CSCur45190	ASDM: IPv6 DHCP Relay panel is missing
CSCur60489	ASDM Identity Certificate Wizard error due to usage-keys
CSCur90915	ASDM DAP: Need to add Windows 10 to Endpoint OS Attribute list
CSCur96423	ASDM unable to add subinterfaces for ASA with SFR module
CSCus05440	ASDM: Unableto display correct NAT Rules using specific object name
CSCus11684	ASDM goes unresponsive with HPM enabled
CSCus14883	ASDM polls for FirePOWER module status continuously
CSCus26083	Syslog server table shows tcp protocol as udp and vice versa
CSCus30737	ASDM 7.3.2 becomes slow when hpm topN is enabled
CSCus54556	ASDM 7.3.2 hangs when loading "All Remote Access" filter
CSCus56092	Add max TLS session values for 5506, 5508 and 5516
CSCus86770	ASDM corrupts ACL which leads to traffic failures
CSCus87127	ASDM shows error while creating more than 32 named int in Transparent FW
CSCut04386	Trafic Capture Wizard: ACL created for Ingress doesn't show for Egress

Identifier	Description
CSCut04499	Traffic Capture Wizard: changing match criteria resets interface

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.