



Release Notes for Cisco ASDM, Version 7.0(x)

Released: October 29, 2012

Updated: January 27, 2014

This document contains release information for Cisco ASDM Version 7.0(x) for the Cisco ASA series. This document includes the following sections:

- [Important Notes, page 1](#)
- [Limitations and Restrictions, page 4](#)
- [System Requirements, page 4](#)
- [ASDM Client Operating System and Browser Requirements, page 4](#)
- [New Features, page 10](#)
- [ACL Migration in Version 9.0, page 25](#)
- [Upgrading the Software, page 25](#)
- [Unsupported Commands, page 39](#)
- [Open Caveats, page 41](#)
- [Resolved Caveats, page 43](#)
- [End-User License Agreement, page 46](#)
- [Related Documentation, page 46](#)
- [Obtaining Software, Documentation, and Submitting a Service Request, page 46](#)

Important Notes

- Downgrading issues—Upgrading to ASA Version 9.0 includes ACL migration (see the [“ACL Migration in Version 9.0” section on page 25](#)). Therefore, you cannot downgrade from 9.0 with a migrated configuration. Be sure to make a backup copy of your configuration before you upgrade so you can downgrade using the old configuration if required.



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2012 Cisco Systems, Inc. All rights reserved.

- Per-session PAT disabled when upgrading— Starting in Version 9.0, by default, all TCP PAT traffic and all UDP DNS traffic use per-session PAT. If you upgrade to Version 9.0 from an earlier release, to maintain the existing functionality of multi-session PAT, the per-session PAT feature is disabled during configuration migration.

To enable per-session PAT after you upgrade:

- a. Choose **Configuration > Firewall > Advanced > Per-Session NAT Rules**.

- b. Select each Deny rule in the table, and click **Delete**.

After you delete the Deny rules, only the default permit rules are still in place, thus enabling per-session PAT.

- c. Click **Apply**.

- No Payload Encryption for export—You can purchase some models with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA series. The ASA software senses a No Payload Encryption model, and disables the following features:

- Unified Communications
- VPN

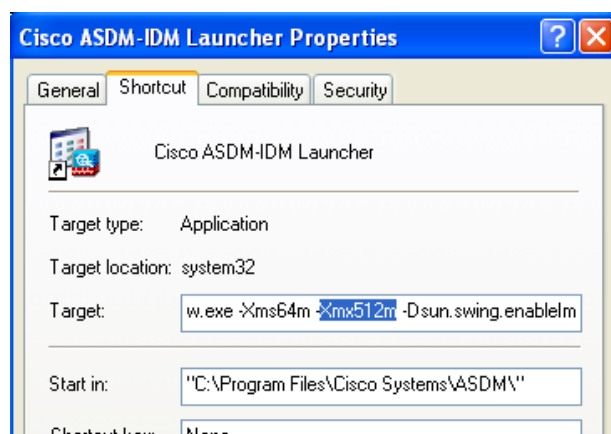
You can still install the Strong Encryption (3DES/AES) license for use with management connections and encrypted route messages for OSPFv3. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL) and redirect traffic to Cloud Web Security.

- Maximum Configuration Size—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 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.

To increase the ASDM heap memory size, download the ASDM-IDM Launcher, and then modify the ASDM-IDM Launcher shortcut by performing the following steps.

Windows:

- a. Right click the shortcut for the Cisco ASDM-IDM Launcher, and choose **Properties**.
- b. Click the **Shortcut** tab.
- c. In the Target field, 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.



Macintosh:

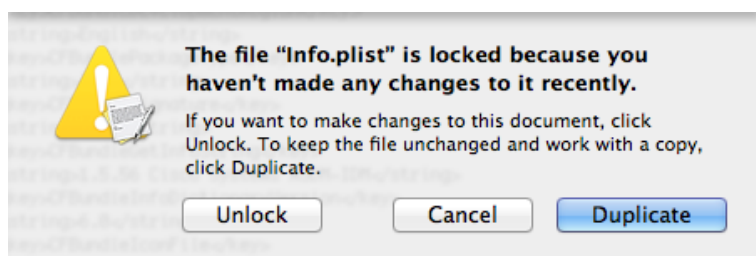
- Right click the Cisco ASDM-IDM icon, and choose **Show Package Contents**.
- In the Contents folder, double-click the Info.plist file. If you have Developer tools installed, it opens in the Property List Editor. Otherwise it opens in TextEdit.
- Under Java > VMOptions, change the string prefixed with “-Xmx” to specify your desired heap size. For example, change it to -Xmx768M for 768 MB or -Xmx1G for 1 GB.

```

<key>Java</key>
<dict>
    <key>WorkingDirectory</key>
    <string>${APP_PACKAGE}/Contents/Resources/Java</string>
    <key>VMOptions</key>
    <string>-Xms64m -Xmx512m</string>
    <key>MainClass</key>
    <string>com.cisco.launcher.Launcher</string>
    <key>JVMVersion</key>
    <string>1.5+</string>

```

- If this file is locked, you see an error such as the following:



- 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.

- Changes to VPN Certificate Maps in ASDM 7.x—You can create a certificate map in ASDM under *Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps* (for SSL) or under *Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules* (for IPsec). When you create a certificate map on either pane, it appears under both the IPsec and the SSL

certificate map lists in ASDM. When you assign a connection profile to a certificate map, it is listed only under the corresponding certificate map list. For example, if you create a certificate map, and assign it to an SSL Connection Profile, that map now only displays the SSL certificate map list (*Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps*).

In ASDM 6.4, assigning a profile to a certificate map acted somewhat differently:

If you assign an SSL Connection Profile to Certificate Map Name, that certificate map is not displayed under the SSL certificate map list (*Configuration > Remote Access VPN > Advanced > Certificate to AnyConnect and Clientless SSL VPN Connection Profile Maps*); it is displayed under the IPsec certificate map list (*Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Certificate to Connection Profile Maps > Rules*).

Limitations and Restrictions

Clientless SSL VPN with a self-signed certificate on the ASA—When the ASA uses a self-signed certificate or an untrusted certificate, Firefox 4 and later and Safari are unable to add security exceptions when browsing using an IPv6 address HTTPS URL (FQDN URL is OK): the “Confirm Security Exception” button is disabled. 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 clientless SSL VPN connections, and ASDM connections). To avoid this caveat, configure a proper certificate for the ASA that is issued by a trusted certificate authority. For Internet Explorer 9 and later, use compatibility mode.

System Requirements

For information about ASA/ASDM requirements and compatibility, see *Cisco ASA Compatibility*: <http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html>



Note

ASDM supports many ASA versions. The ASDM documentation and online help includes all of the latest features supported by the ASA. If you are running an older version of ASA software, the documentation might include features that are not supported in your version. Similarly, if a feature was added into a maintenance release for an older major or minor version, then the ASDM documentation includes the new feature even though that feature might not be available in all later ASA releases. Please refer to the new features tables to determine when features were added. For the minimum supported version of ASDM for each ASA version, see *Cisco ASA Compatibility*.

For VPN compatibility, see the *Supported VPN Platforms, Cisco ASA 5500 Series*: <http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html>

ASDM Client Operating System and Browser Requirements

Table 1 lists the supported and recommended client operating systems and Java for ASDM.

Table 1 **Operating System and Browser Requirements**

Operating System	Browser				Java SE Plug-in
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows (English and Japanese): <ul style="list-style-type: none"> • 7 • Vista • 2008 Server • XP 	6.0 or later	1.5 or later	No support	18.0 or later	6.0 or later
Apple Macintosh OS X: <ul style="list-style-type: none"> • 10.8 • 10.7 • 10.6 • 10.5 • 10.4 	No support	1.5 or later	2.0 or later	18.0 or later	6.0 or later
Red Hat Enterprise Linux 5 (GNOME or KDE): <ul style="list-style-type: none"> • Desktop • Desktop with Workstation 	N/A	1.5 or later	N/A	18.0 or later	6.0 or later

Table 2 lists compatibility caveats for Java, ASDM, and browser compatibility.

Table 2 **Caveats for ASDM Compatibility**

Java Version	Conditions	Notes
7 update 51	<ul style="list-style-type: none"> ASDM Launcher requires trusted certificate Java Web Start requires newer ASDM version <i>or</i> workaround 	<p>To continue using the Launcher, either install a trusted certificate (from a known CA; a self-signed certificate will not work) on the ASA or downgrade Java to 7 update 45 or earlier. You can alternatively use Java Web Start.</p> <p>To use Java Web Start, do one of the following:</p> <ul style="list-style-type: none"> Upgrade ASDM to Version 7.1(5.100) or later. This ASDM version includes the Permissions attribute in the JAR manifest, which is required as of Java 7 Update 51. To use ASDM 7.1(5) or earlier, add a security exception in the Java Control Panel for each ASA you want to manage with ASDM. See the “Workaround” section at: http://java.com/en/download/help/java_blocked.xml <p>If you already upgraded Java, and can no longer launch ASDM in order to upgrade it to Version 7.1(5.100) or later, then you can either use the CLI to upgrade ASDM, or you can use the above security exception workaround to launch the older ASDM, after which you can upgrade to a newer version.</p>
7 update 45	ASDM shows a yellow warning about the missing Permissions attribute	<p>Java 7 update 45 shows a warning when an application does not have the Permissions attribute in the JAR manifest. It is safe to ignore this warning. To prevent this warning from appearing, upgrade to ASDM 7.1(5.100) or later; this ASDM version includes the Permissions attribute, which will be required as of Java 7 Update 51.</p> <p>Note Due to a bug in Java, even if you upgrade to ASDM 7.1(5.100) or later, if you also do not have a trusted certificate installed on the ASA, you continue to see the yellow warning about the missing Permissions attribute. To prevent the warning from appearing, install a trusted certificate (from a known CA); or generate a self-signed certificate on the ASA by choosing Configuration > Device Management > Certificates > Identity Certificates. Launch ASDM, and when the certificate warning is shown, check the Always trust connections to websites checkbox.</p>

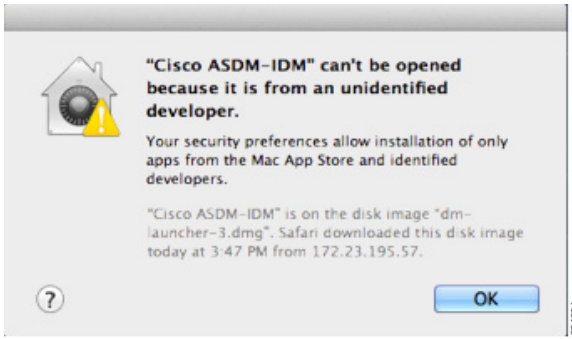
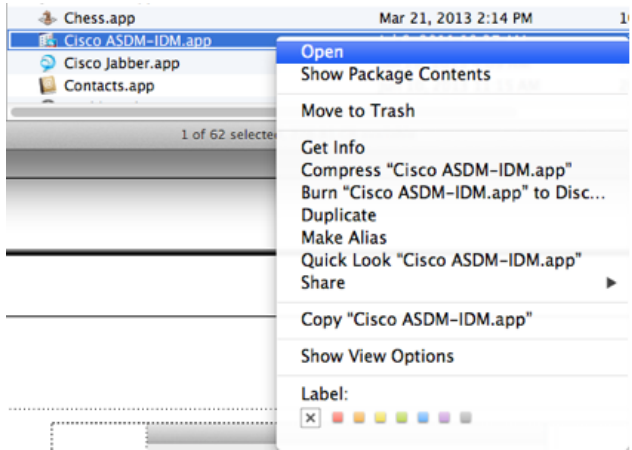

Table 2 **Caveats for ASDM Compatibility**

Java Version	Conditions	Notes
7	Requires strong encryption license (3DES/AES) on ASA	ASDM requires an SSL connection to the ASA. If the ASA has only the base encryption license (DES), and therefore has weak encryption ciphers for the SSL connection, you cannot launch ASDM. You must uninstall Java 7, and install Java 6 (http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html). Note that a workaround is required for weak encryption and Java 6 (see below, in this table).
	MacOS	<p>You may see the following error message when opening the ASDM Launcher:</p> <p>Cannot launch Cisco ASDM-IDM. No compatible version of Java 1.5+ is available.</p> <p>In this case, Java 7 is the currently-preferred Java version. Either upgrade ASDM to 7.1(4) or later, or you need to set Java 6 as the preferred Java version: Open the Java Preferences application (under Applications > Utilities), select the preferred Java version, and drag it up to be the first line in the table.</p>
6	No usernames longer than 50 characters	Due to a Java bug, ASDM does not support usernames longer than 50 characters when using Java 6. Longer usernames work correctly for Java 7.
	Requires strong encryption license (3DES/AES) on ASA <i>or</i> workaround	<p>When you initially connect a browser to the ASA to load the ASDM splash screen, the browser attempts to make an SSL connection to the ASA. If the ASA has only the base encryption license (DES), and therefore has weak encryption ciphers for the SSL connection, you may not be able to access the ASDM splash screen; most current browsers do not support weak encryption ciphers. Therefore, without the strong encryption license (3DES/AES), use one of the following workarounds:</p> <ul style="list-style-type: none"> • If available, use an already downloaded ASDM launcher or Java Web Start shortcut. The Launcher and Web Start shortcut work with Java 6 and weak encryption, even if the browsers do not. • For Windows Internet Explorer, you can enable DES as a workaround. See http://support.microsoft.com/kb/929708 for details. • For Firefox on any operating system, you can enable the security.ssl3.dhe_dss_des_sha setting as a workaround. See http://kb.mozillazine.org/About:config to learn how to change hidden configuration preferences.

Table 2 **Caveats for ASDM Compatibility**

Java Version	Conditions	Notes
All	<ul style="list-style-type: none"> Self-signed certificate or an untrusted certificate IPv6 Firefox and Safari 	When the ASA uses a self-signed certificate or an untrusted certificate, Firefox 4 and later 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.
	<ul style="list-style-type: none"> SSL encryption on the ASA must include both RC4-MD5 and RC4-SHA1 <i>or</i> 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 http://www.chromium.org/developers/how-tos/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.
	MacOS	On MacOS, 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.

Table 2 **Caveats for ASDM Compatibility**

Java Version	Conditions	Notes
All	MacOS 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> 

New Features

- [New Features in ASA Version 7.0\(2.9\), page 10](#)
- [New Features in ASA Version 7.0\(2\), page 10](#)
- [New Features in ASA Version 7.0\(1\), page 11](#)

New Features in ASA Version 7.0(2.9)

Released: November 6, 2012

There are no new features in Version 7.0(2.9).

New Features in ASA Version 7.0(2)

Released: October 31, 2012

[Table 3](#) lists the new features for ASA Version 8.4(5).

Table 3 **New Features for ASA Version 8.4(5)**

Feature	Description
Firewall Features	
EtherType ACL support for IS-IS traffic (transparent firewall mode)	<p>In transparent firewall mode, the ASA can now pass IS-IS traffic using an EtherType ACL. We modified the following command: access-list ethertype {permit deny} is-is.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
ARP cache additions for non-connected subnets	<p>The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.</p> <p>You may want to use this feature if you use:</p> <ul style="list-style-type: none"> • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
Increased maximum connection limits for service policy rules	<p>The maximum number of connections for service policy rules was increased from 65535 to 2000000.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), or 8.7(1).</i></p>
Remote Access Features	
Improved Host Scan and ASA Interoperability	<p>Host Scan and the ASA use an improved process to transfer posture attributes from the client to the ASA. This gives the ASA more time to establish a VPN connection with the client and apply a dynamic access policy.</p> <p><i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i></p>
Monitoring Features	

Table 3 **New Features for ASA Version 8.4(5) (continued)**

Feature	Description
NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to allow polling for Xlate count.	Support was added for the NAT-MIB cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs to support xlate_count and max_xlate_count for SNMP. This data is equivalent to the show xlate count command. <i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i>
NSEL	Flow-update events have been introduced to provide periodic byte counters for flow traffic. You can change the time interval at which flow-update events are sent to the NetFlow collector. You can filter to which collectors flow-update records will be sent. <i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i>
Hardware Features	
ASA 5585-X DC power supply support	Support was added for the ASA 5585-X DC power supply. <i>This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), or 9.1(1).</i>

New Features in ASA Version 7.0(1)

Released: October 29, 2012

[Table 4](#) lists the new features for ASA Version 9.0(1)/ASDM Version 7.0(1).



Note

Features added in 8.4(4.x), 8.4(5), and 8.4(6) are not included in 9.0(1) unless they are explicitly listed in this table.

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1)***

Feature	Description
Firewall Features	
Cisco TrustSec integration	<p>Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions.</p> <p>In this release, the ASA integrates with Cisco TrustSec to provide security group based policy enforcement. Access policies within the Cisco TrustSec domain are topology-independent, based on the roles of source and destination devices rather than on network IP addresses.</p> <p>The ASA can utilize the Cisco TrustSec solution for other types of security group based policies, such as application inspection; for example, you can configure a class map containing an access policy based on a security group.</p> <p>We introduced the following MIB: CISCO-TRUSTSEC-SXP-MIB.</p> <p>We introduced or modified the following screens:</p> <p>Configuration > Firewall > Identity by TrustSec Configuration > Firewall > Objects > Security Groups Object Groups Configuration > Firewall > Access Rules > Add Access Rules Monitoring > Properties > Identity by TrustSec > PAC Monitoring > Properties > Identity by TrustSec > Environment Data Monitoring > Properties > Identity by TrustSec > SXP Connections Monitoring > Properties > Identity by TrustSec > IP Mappings Monitoring > Properties > Connections Tools > Packet Tracer</p>
Cisco Cloud Web Security (ScanSafe)	<p>Cisco Cloud Web Security provides content scanning and other malware protection service for web traffic. It can also redirect and report about web traffic based on user identity.</p> <p>Note Clientless SSL VPN is not supported with Cloud Web Security; be sure to exempt any clientless SSL VPN traffic from the ASA service policy for Cloud Web Security.</p> <p>We introduced or modified the following screens:</p> <p>Configuration > Device Management > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security > Add/Edit Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security > Add/Edit Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security > Add/Edit > Manage Cloud Web Security Class Maps Configuration > Firewall > Identity Options Configuration > Firewall > Service Policy Rules Monitoring > Properties > Cloud Web Security</p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Extended ACL and object enhancement to filter ICMP traffic by ICMP code	<p>ICMP traffic can now be permitted/denied based on ICMP code.</p> <p>We introduced or modified the following screens:</p> <p>Configuration > Firewall > Objects > Service Objects/Groups</p> <p>Configuration > Firewall > Access Rule</p>
Unified communications support on the ASA SM	The ASA SM now supports all Unified Communications features.
NAT support for reverse DNS lookups	NAT now supports translation of the DNS PTR record for reverse DNS lookups when using IPv4 NAT, IPv6 NAT, and NAT64 with DNS inspection enabled for the NAT rule.
Per-session PAT	<p>The per-session PAT feature improves the scalability of PAT and, for ASA clustering, allows each member unit to own PAT connections; multi-session PAT connections have to be forwarded to and owned by the master unit. At the end of a per-session PAT session, the ASA sends a reset and immediately removes the xlate. This reset causes the end node to immediately release the connection, avoiding the TIME_WAIT state. Multi-session PAT, on the other hand, uses the PAT timeout, by default 30 seconds. For “hit-and-run” traffic, such as HTTP or HTTPS, the per-session feature can dramatically increase the connection rate supported by one address. Without the per-session feature, the maximum connection rate for one address for an IP protocol is approximately 2000 per second. With the per-session feature, the connection rate for one address for an IP protocol is 65535/<i>average-lifetime</i>.</p> <p>By default, all TCP traffic and UDP DNS traffic use a per-session PAT xlate. For traffic that can benefit from multi-session PAT, such as H.323, SIP, or Skinny, you can disable per-session PAT by creating a per-session deny rule.</p> <p>We introduced the following screen: Configuration > Firewall > Advanced > Per-Session NAT Rules.</p>
ARP cache additions for non-connected subnets	<p>The ASA ARP cache only contains entries from directly-connected subnets by default. You can now enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.</p> <p>You may want to use this feature if you use:</p> <ul style="list-style-type: none"> • Secondary subnets. • Proxy ARP on adjacent routes for traffic forwarding. <p>We modified the following screen: Configuration > Device Management > Advanced > ARP > ARP Static Table.</p> <p><i>Also available in 8.4(5).</i></p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
SunRPC change from dynamic ACL to pin-hole mechanism	<p>Previously, Sun RPC inspection does not support outbound access lists because the inspection engine uses dynamic access lists instead of secondary connections.</p> <p>In this release, when you configure dynamic access lists on the ASA, they are supported on the ingress direction only and the ASA drops egress traffic destined to dynamic ports. Therefore, Sun RPC inspection implements a pinhole mechanism to support egress traffic. Sun RPC inspection uses this pinhole mechanism to support outbound dynamic access lists.</p> <p><i>Also available in 8.4(4.1).</i></p>
Inspection reset action change	<p>Previously, when the ASA dropped a packet due to an inspection engine rule, the ASA sent only one RST to the source device of the dropped packet. This behavior could cause resource issues.</p> <p>In this release, when you configure an inspection engine to use a reset action and a packet triggers a reset, the ASA sends a TCP reset under the following conditions:</p> <ul style="list-style-type: none"> • The ASA sends a TCP reset to the inside host when the service resetoutbound command is enabled. (The service resetoutbound command is disabled by default.) • The ASA sends a TCP reset to the outside host when the service resetinbound command is enabled. (The service resetinbound command is disabled by default.) <p>For more information, see the service command in the <i>ASA Cisco Security Appliance Command Reference</i>.</p> <p>This behavior ensures that a reset action will reset the connections on the ASA and on inside servers; therefore countering denial of service attacks. For outside hosts, the ASA does not send a reset by default and information is not revealed through a TCP reset.</p> <p><i>Also available in 8.4(4.1).</i></p>
Increased maximum connection limits for service policy rules	<p>The maximum number of connections for service policy rules was increased from 65535 to 2000000.</p> <p>We modified the following screen: Configuration > Firewall > Service Policy Rules > Connection Settings.</p> <p><i>Also available in 8.4(5)</i></p>

High Availability and Scalability Features

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
ASA Clustering for the ASA 5580 and 5585-X	<p>ASA Clustering lets you group multiple ASAs together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. ASA clustering is supported for the ASA 5580 and the ASA 5585-X; all units in a cluster must be the same model with the same hardware specifications. See the configuration guide for a list of unsupported features when clustering is enabled.</p> <p>We introduced or modified the following screens:</p> <ul style="list-style-type: none"> Home > Device Dashboard Home > Cluster Dashboard Home > Cluster Firewall Dashboard Configuration > Device Management > Advanced > Address Pools > MAC Address Pools Configuration > Device Management > High Availability and Scalability > ASA Cluster Configuration > Device Management > Logging > Syslog Setup > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > IPv6 Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface > Advanced Configuration > Firewall > Advanced > Per-Session NAT Rules Monitoring > ASA Cluster Monitoring > Properties > System Resources Graphs > Cluster Control Link Tools > Preferences > General Tools > System Reload Tools > Upgrade Software from Local Computer Wizards > High Availability and Scalability Wizard Wizards > Packet Capture Wizard Wizards > Startup Wizard
OSPF, EIGRP, and Multicast for clustering	<p>For OSPFv2 and OSPFv3, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment.</p> <p>For EIGRP, bulk synchronization, route synchronization, and spanned EtherChannels are supported in the clustering environment.</p> <p>Multicast routing supports clustering.</p>
Packet capture for clustering	<p>To support cluster-wide troubleshooting, you can enable capture of cluster-specific traffic on the master unit using the cluster exec capture command, which is then automatically enabled on all of the slave units in the cluster. The cluster exec keywords are the new keywords that you place in front of the capture command to enable cluster-wide capture.</p> <p>We modified the following screen: Wizards > Packet Capture Wizard.</p>

Table 4 **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
Logging for clustering	<p>Each unit in the cluster generates syslog messages independently. You can use the logging device-id command to generate syslog messages with identical or different device IDs to make messages appear to come from the same or different units in the cluster.</p> <p>We modified the following screen: Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration.</p>
Configure the connection replication rate during a bulk sync	<p>You can now configure the rate at which the ASA replicates connections to the standby unit when using Stateful Failover. By default, connections are replicated to the standby unit during a 15 second period. However, when a bulk sync occurs (for example, when you first enable failover), 15 seconds may not be long enough to sync large numbers of connections due to a limit on the maximum connections per second. For example, the maximum connections on the ASA is 8 million; replicating 8 million connections in 15 seconds means creating 533 K connections per second. However, the maximum connections allowed per second is 300 K. You can now specify the rate of replication to be less than or equal to the maximum connections per second, and the sync period will be adjusted until all the connections are synchronized.</p> <p><i>Also available in 8.4(4.1) and 8.5(1.7).</i></p>
IPv6 Features	
IPv6 Support on the ASA's outside interface for VPN Features.	<p>This release of the ASA adds support for IPv6 VPN connections to its outside interface using SSL and IKEv2/IPsec protocols.</p> <p>This release of the ASA continues to support IPv6 VPN traffic on its inside interface using the SSL protocol as it has in the past. This release does not provide IKEv2/IPsec protocol on the inside interface.</p>
Remote Access VPN support for IPv6: IPv6 Address Assignment Policy	<p>You can configure the ASA to assign an IPv4 address, an IPv6 address, or both an IPv4 and an IPv6 address to an AnyConnect client by creating internal pools of addresses on the ASA or by assigning a dedicated address to a local user on the ASA.</p> <p>The endpoint must have the dual-stack protocol implemented in its operating system to be assigned both types of addresses.</p> <p>Assigning an IPv6 address to the client is supported for the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following screens:</p> <p>Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy Configuration > Remote Access VPN > AAA/Local Users > Local Users > (Edit local user account) > VPN Policy</p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Remote Access VPN support for IPv6: Assigning DNS Servers with IPv6 Addresses to group policies	<p>DNS servers can be defined in a Network (Client) Access internal group policy on the ASA. You can specify up to four DNS server addresses including up to two IPv4 addresses and up to two IPv6 addresses.</p> <p>DNS servers with IPv6 addresses can be reached by VPN clients when they are configured to use the SSL protocol. This feature is not supported for clients configured to use the IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Servers.</p>
Remote Access VPN support for IPv6: Split tunneling	<p>Split tunneling enables you to route some network traffic through the VPN tunnel (encrypted) and to route other network traffic outside the VPN tunnel (unencrypted or “in the clear”). You can now perform split tunneling on IPv6 network traffic by defining an IPv6 policy which specifies a unified access control rule.</p> <p>IPv6 split tunneling is reported with the telemetry data sent by the Smart Call Home feature. If either IPv4 or IPv6 split tunneling is enabled, Smart Call Home reports split tunneling as “enabled.” For telemetry data, the VPN session database displays the IPv6 data typically reported with session management.</p> <p>You can include or exclude IPv6 traffic from the VPN “tunnel” for VPN clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Advanced > Split Tunneling.</p>
Remote Access VPN support for IPv6: AnyConnect Client Firewall Rules	<p>Access control rules for client firewalls support access list entries for both IPv4 and IPv6 addresses.</p> <p>ACLs containing IPv6 addresses can be applied to clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Advanced > AnyConnect Client > Client Firewall.</p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Remote Access VPN support for IPv6: Client Protocol Bypass	<p>The Client Protocol Bypass feature allows you to configure how the ASA manages IPv4 traffic when it is expecting only IPv6 traffic or how it manages IPv6 traffic when it is expecting only IPv4 traffic.</p> <p>When the AnyConnect client makes a VPN connection to the ASA, the ASA could assign it an IPv4, IPv6, or both an IPv4 and IPv6 address. If the ASA assigns the AnyConnect connection only an IPv4 address or only an IPv6 address, you can now configure the Client Bypass Protocol to drop network traffic for which the ASA did not assign an IP address, or allow that traffic to bypass the ASA and be sent from the client unencrypted or “in the clear.”</p> <p>For example, assume that the ASA assigns only an IPv4 address to an AnyConnect connection and the endpoint is dual stacked. When the endpoint attempts to reach an IPv6 address, if Client Bypass Protocol is disabled, the IPv6 traffic is dropped; however, if Client Bypass Protocol is enabled, the IPv6 traffic is sent from the client in the clear.</p> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Group Policy) Advanced > AnyConnect Client > Client Bypass Protocol.</p>
Remote Access VPN support for IPv6: IPv6 Interface ID and prefix	<p>You can now specify a dedicated IPv6 address for local VPN users.</p> <p>This feature benefits users configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > AAA/Local Users > Local Users > (Edit User) > VPN Policy.</p>
Remote Access VPN support for IPv6: Sending ASA FQDN to AnyConnect client	<p>You can return the FQDN of the ASA to the AnyConnect client to facilitate load balancing and session roaming.</p> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Network (Client) Access > Group Policies > (Edit group policy) > Advanced > AnyConnect.</p>
Remote Access VPN support for IPv6: ASA VPN Load Balancing	<p>Clients with IPv6 addresses can make AnyConnect connections through the public-facing IPv6 address of the ASA cluster or through a GSS server. Likewise, clients with IPv6 addresses can make AnyConnect VPN connections through the public-facing IPv4 address of the ASA cluster or through a GSS server. Either type of connection can be load-balanced within the ASA cluster.</p> <p>For clients with IPv6 addresses to successfully connect to the ASAs public-facing IPv4 address, a device that can perform network address translation from IPv6 to IPv4 needs to be in the network.</p> <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Load Balancing.</p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Remote Access VPN support for IPv6: Dynamic Access Policies support IPv6 attributes	<p>When using ASA 9.0 or later with ASDM 6.8 or later, you can now specify these attributes as part of a dynamic access policy (DAP):</p> <ul style="list-style-type: none"> • IPv6 addresses as a Cisco AAA attribute • IPv6 TCP and UDP ports as part of a Device endpoint attribute • Network ACL Filters (client) <p>This feature can be used by clients configured to use the SSL or IKEv2/IPsec protocol.</p> <p>We modified the following screens:</p> <p>Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add > Cisco AAA attribute</p> <p>Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add > Device > Add Endpoint Attribute</p> <p>Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Network ACL Filters (client)</p> <p>Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Webtype ACL Filters (clientless)</p>
Remote Access VPN support for IPv6: Session Management	<p>Session management output displays the IPv6 addresses in Public/Assigned address fields for AnyConnect connections, site-to-site VPN connections, and Clientless SSL VPN connections. You can add new filter keywords to support filtering the output to show only IPv6 (outside or inside) connections. No changes to IPv6 User Filters exist.</p> <p>This feature can be used by clients configured to use the SSL protocol. This feature does not support IKEv2/IPsec protocol.</p> <p>We modified these screen: Monitoring > VPN > VPN Statistics > Sessions.</p>
NAT support for IPv6	<p>NAT now supports IPv6 traffic, as well as translating between IPv4 and IPv6 (NAT64). Translating between IPv4 and IPv6 is not supported in transparent mode.</p> <p>We modified the following screens:</p> <p>Configuration > Firewall > Objects > Network Objects/Group</p> <p>Configuration > Firewall > NAT Rules</p>
DHCPv6 relay	<p>DHCP relay is supported for IPv6.</p> <p>We modified the following screen: Configuration > Device Management > DHCP > DHCP Relay.</p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
OSPFv3	<p>OSPFv3 routing is supported for IPv6. Note the following additional guidelines and limitations for OSPFv2 and OSPFv3:</p> <p>Clustering</p> <ul style="list-style-type: none"> • OSPFv2 and OSPFv3 support clustering. • When clustering is configured, OSPFv3 encryption is not supported. An error message appears if you try to configure OSPFv3 encryption in a clustering environment. • When using individual interfaces, make sure that you establish the master and slave units as either OSPFv2 or OSPFv3 neighbors. • When using individual interfaces, OSPFv2 adjacencies can only be established between two contexts on a shared interface on the master unit. Configuring static neighbors is supported only on point-to-point links; therefore, only one neighbor statement is allowed on an interface. <p>Other</p> <ul style="list-style-type: none"> • OSPFv2 and OSPFv3 support multiple instances on an interface. • The ESP and AH protocol is supported for OSPFv3 authentication. • OSPFv3 supports Non-Payload Encryption. <p>We introduced the following screens:</p> <p>Configuration > Device Setup > Routing > OSPFv3 > Setup Configuration > Device Setup > Routing > OSPFv3 > Interface Configuration > Device Setup > Routing > OSPFv3 > Redistribution Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix Configuration > Device Setup > Routing > OSPFv3 > Virtual Link Monitoring > Routing > OSPFv3 LSAs Monitoring > Routing > OSPFv3 Neighbors</p>
Unified ACL for IPv4 and IPv6	<p>ACLs now support IPv4 and IPv6 addresses. You can also specify a mix of IPv4 and IPv6 addresses for the source and destination. The IPv6-specific ACLs are deprecated. Existing IPv6 ACLs are migrated to extended ACLs.</p> <p>ACLs containing IPv6 addresses can be applied to clients configured to use the SSL protocol. This feature is not supported for the IKEv2/IPsec protocol.</p> <p>We modified the following screens:</p> <p>Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options</p>

Table 4 **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
Mixed IPv4 and IPv6 object groups	<p>Previously, network object groups could only contain all IPv4 addresses or all IPv6 addresses. Now network object groups can support a mix of both IPv4 and IPv6 addresses.</p> <p>Note You cannot use a mixed object group for NAT.</p> <p>We modified the following screen: Configuration > Firewall > Objects > Network Objects/Groups.</p>
Range of IPv6 addresses for a Network object	<p>You can now configure a range of IPv6 addresses for a network object.</p> <p>We modified the following screen: Configuration > Firewall > Objects > Network Objects/Groups.</p>
Inspection support for IPv6 and NAT64	<p>We now support DNS inspection for IPv6 traffic.</p> <p>We also support translating between IPv4 and IPv6 for the following inspections:</p> <ul style="list-style-type: none"> • DNS • FTP • HTTP • ICMP <p>You can now also configure the service policy to generate a syslog message (767001) when unsupported inspections receive and drop IPv6 traffic.</p> <p>We modified the following screen: Configuration > Firewall > Service Policy Rules > Add Service Policy Rule Wizard - Service Policy.</p>
Remote Access Features	
Clientless SSL VPN: Additional Support	<p>We have added additional support for these browsers, operating systems, web technologies and applications:</p> <p>Internet browser support: Microsoft Internet Explorer 9, Firefox 4, 5, 6, 7, and 8</p> <p>Operating system support: Mac OS X 10.7</p> <p>Web technology support: HTML 5</p> <p>Application Support: Sharepoint 2010</p>
Clientless SSL VPN: Enhanced quality for rewriter engines	<p>The clientless SSL VPN rewriter engines were significantly improved to provide better quality and efficacy. As a result, you can expect a better end-user experience for clientless SSL VPN users.</p> <p>We did not add or modify any ASDM screens for this feature.</p> <p><i>Also available in 8.4(4.1).</i></p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Clientless SSL VPN: Citrix Mobile Receiver	<p>This feature provides secure remote access for Citrix Receiver applications running on mobile devices to XenApp and XenDesktop VDI servers through the ASA.</p> <p>For the ASA to proxy Citrix Receiver to a Citrix Server, when users try to connect to Citrix virtualized resource, instead of providing the Citrix Server's address and credentials, users enter the ASA's SSL VPN IP address and credentials.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policy > Edit > More Options > VDI Access > Add VDI Server.</p>
Clientless SSL VPN: Enhanced Auto-sign-on	<p>This feature improves support for web applications that require dynamic parameters for authentication.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks.</p>
Clientless SSL VPN: Clientless Java Rewriter Proxy Support	<p>This feature provides proxy support for clientless Java plug-ins when a proxy is configured in client machines' browsers.</p> <p>We did not add or modify any ASDM screens for this feature.</p>
Clientless SSL VPN: Remote File Explorer	<p>The Remote File Explorer provides users with a way to browse the corporate network from their web browser. When users click the Remote File System icon on the Cisco SSL VPN portal page, an applet is launched on the user's system displaying the remote file system in a tree and folder view.</p> <p>We did not add or modify any ASDM screens for this feature.</p>
Clientless SSL VPN: Server Certificate Validation	<p>This feature enhances clientless SSL VPN support to enable SSL server certificate verification for remote HTTPS sites against a list of trusted CA certificates.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Certificate Management > Trusted Certificate Pool.</p>
AnyConnect Performance Improvements	<p>This feature improves throughput performance for AnyConnect TLS/DTLS traffic in multi-core platforms. It accelerates the SSL VPN datapath and provides customer-visible performance gains in AnyConnect, smart tunnels, and port forwarding.</p> <p>We modified the following screen: Configuration > Remote Access VPN > Advanced > Crypto Engine.</p>
Custom Attributes	<p>Custom attributes define and configure AnyConnect features that have not yet been added to ASDM. You add custom attributes to a group policy, and define values for those attributes.</p> <p>For AnyConnect 3.1, custom attributes are available to support AnyConnect Deferred Upgrade.</p> <p>Custom attributes can benefit AnyConnect clients configured for either IKEv2/IPsec or SSL protocols.</p> <p>A new screen was added: Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes.</p>

Table 4 ***New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)***

Feature	Description
Next Generation Encryption	<p>The National Standards Association (NSA) specified a set of cryptographic algorithms that devices must support to meet U.S. federal standards for cryptographic strength. RFC 6379 defines the Suite B cryptographic suites. Because the collective set of algorithms defined as NSA Suite B are becoming a standard, the AnyConnect IPsec VPN (IKEv2 only) and public key infrastructure (PKI) subsystems now support them. The next generation encryption (NGE) includes a larger superset of this set adding cryptographic algorithms for IPsec V3 VPN, Diffie-Hellman Groups 14 and 24 for IKEv2, and RSA certificates with 4096 bit keys for DTLS and IKEv2.</p> <p>The following functionality is added to ASA to support the Suite B algorithms:</p> <ul style="list-style-type: none"> • AES-GCM/GMAC support (128-, 192-, and 256-bit keys) <ul style="list-style-type: none"> – IKEv2 payload encryption and authentication – ESP packet encryption and authentication – Hardware supported only on multi-core platforms • SHA-2 support (256-, 384-, and 512-bit hashes) <ul style="list-style-type: none"> – ESP packet authentication – Hardware and software supported only on multi-core platforms • ECDH support (groups 19, 20, and 21) <ul style="list-style-type: none"> – IKEv2 key exchange – IKEv2 PFS – Software only supported on single- or multi-core platforms • ECDSA support (256-, 384-, and 521-bit elliptic curves) <ul style="list-style-type: none"> – IKEv2 user authentication – PKI certificate enrollment – PKI certificate generation and verification – Software only supported on single- or multi-core platforms <p>New cryptographic algorithms are added for IPsecV3.</p> <p>Note Suite B algorithm support requires an AnyConnect Premium license for IKEv2 remote access connections, but Suite B usage for other connections or purposes (such as PKI) has no limitations. IPsecV3 has no licensing restrictions.</p> <p>We introduced or modified the following screens:</p> <p>Monitor > VPN > Sessions Monitor > VPN > Encryption Statistics Configuration > Site-to-Site VPN > Certificate Management > Identity Certificates Configuration > Site-to-Site VPN > Advanced > System Options Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > Crypto Maps</p>
Support for VPN on the ASA SM	The ASA SM now supports all VPN features.

Table 4 **New Features for ASA Version 9.0(1)/ASDM Version 7.0(1) (continued)**

Feature	Description
Multiple Context Mode Features	
Site-to-Site VPN in multiple context mode	Site-to-site VPN tunnels are now supported in multiple context mode.
New resource type for site-to-site VPN tunnels	<p>New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.</p> <p>We modified the following screen: Configuration > Context Management > Resource Class > Add Resource Class.</p>
Dynamic routing in Security Contexts	EIGRP and OSPFv2 dynamic routing protocols are now supported in multiple context mode. OSPFv3, RIP, and multicast routing are not supported.
New resource type for routing table entries	<p>A new resource class, routes, was created to set the maximum number of routing table entries in each context.</p> <p>We modified the following screen: Configuration > Context Management > Resource Class > Add Resource Class.</p>
Mixed firewall mode support in multiple context mode	<p>You can set the firewall mode independently for each security context in multiple context mode, so some can run in transparent mode while others run in routed mode.</p> <p>You cannot set the firewall mode in ASDM; you must use the command-line interface.</p> <p><i>Also available in Version 8.5(1).</i></p>
Module Features	
ASA Services Module support on the Cisco 7600 switch	<p>The Cisco 7600 series now supports the ASASM. For specific hardware and software requirements, see: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html.</p>
ASA 5585-X support for the ASA CX SSP-10 and -20	<p>The ASA CX module lets you enforce security based on the complete context of a situation. This context includes the identity of the user (who), the application or website that the user is trying to access (what), the origin of the access attempt (where), the time of the attempted access (when), and the properties of the device used for the access (how). With the ASA CX module, you can extract the full context of a flow and enforce granular policies such as permitting access to Facebook but denying access to games on Facebook or permitting finance employees access to a sensitive enterprise database but denying the same to other employees.</p> <p>We introduced the following screens:</p> <p>Home > ASA CX Status Wizards > Startup Wizard > ASA CX Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA CX Inspection</p> <p><i>Also available in 8.4(4.1).</i></p>
ASA 5585-X Dual SSP support for the SSP-10 and SSP-20 (in addition to the SSP-40 and SSP-60); VPN support for Dual SSPs	<p>The ASA 5585-X now supports dual SSPs using all SSP models (you can use two SSPs of the same level in the same chassis). VPN is now supported when using dual SSPs.</p> <p>We did not modify any screens.</p>

ACL Migration in Version 9.0

The following ACL configurations will be migrated when upgrading to Version 9.0.

- [IPv6 ACLs, page 25](#)
- [Any Keyword, page 25](#)

IPv6 ACLs

IPv6 ACLs (**ipv6 access-list**) will be migrated to extended ACLs (**access-list extended**); IPv6 ACLs are no longer supported.

If IPv4 and IPv6 ACLs are applied on the same direction of an interface (**access-group** command), then the ACLs are merged:

- If both IPv4 and IPv6 ACLs are not used anywhere other than the access-group, then the name of the IPv4 ACL is used for the merged ACL; the IPv6 access-list is removed.
- If at least one of the ACLs is used in another feature, then a new ACL is created with the name *IPv4-ACL-name_IPv6-ACL-name*; the in-use ACL(s) continue to be used for other features. ACLs not in use are removed. If the IPv6 ACL is in use for another feature, it is migrated to an extended ACL of the same name.

Any Keyword

Now that ACLs support both IPv4 and IPv6, the **any** keyword now represents “all IPv4 and IPv6 traffic.” Any existing ACLs that use the **any** keyword will be changed to use the **any4** keyword, which denotes “all IPv4 traffic.”

In addition, a separate keyword was introduced to designate “all IPv6 traffic”: **any6**.



Note

The **any4** and **any6** keywords are not available for all commands that use the **any** keyword. For example, the NAT feature uses only the **any** keyword; **any** represents IPv4 traffic or IPv6 traffic depending on the context within the command.

Upgrading the Software

This section describes how to upgrade to the latest version and includes the following topics:

- [Upgrade Path and Migrations, page 26](#)
- [Viewing Your Current Version, page 27](#)
- [Downloading the Software from Cisco.com, page 27](#)
- [Upgrading a Standalone Unit, page 28](#)
- [Upgrading a Failover Pair or ASA Cluster, page 33](#)



Note

For CLI procedures, see the ASA documentation.

Upgrade Path and Migrations

- If you are upgrading from a pre-8.3 release:
 - See the [Cisco ASA 5500 Migration Guide to Version 8.3 and Later](#) for important information about migrating your configuration.
 - You cannot upgrade directly to 9.0 or later. You must first upgrade to Version 8.3 or 8.4 for a successful migration.
- When upgrading to Version 9.0, because of ACL migration, you cannot later perform a downgrade; be sure to back up your configuration file in case you want to downgrade. See the ACL migration section in the release notes for more information.

- Software Version Requirements for Zero Downtime Upgrading:



The units in a failover configuration or ASA cluster should have the same major (first number) and minor (second number) software version. However, you do not need to maintain version parity on the units during the upgrade process; you can have different versions on the software running on each unit and still maintain failover support. To ensure long-term compatibility and stability, we recommend upgrading all units to the same version as soon as possible.

[Table 1-5](#) shows the supported scenarios for performing zero-downtime upgrades.

Table 1-5 Zero-Downtime Upgrade Support

Type of Upgrade	Support
Maintenance Release	<p>You can upgrade from any maintenance release to any other maintenance release within a minor release.</p> <p>For example, you can upgrade from 8.4(1) to 8.4(6) without first installing the maintenance releases in between.</p>

Table 1-5 **Zero-Downtime Upgrade Support (continued)**

Type of Upgrade	Support
Minor Release	<p>You can upgrade from a minor release to the next minor release. You cannot skip a minor release.</p> <p>For example, you can upgrade from 8.2 to 8.3. Upgrading from 8.2 directly to 8.4 is not supported for zero-downtime upgrades; you must first upgrade to 8.3. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.2 to 8.4 (the model is not supported on 8.3).</p> <p> Note Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.2 to 8.3.</p>
Major Release	<p>You can upgrade from the last minor release of the previous version to the next major release.</p> <p>For example, you can upgrade from 8.6 to 9.0, assuming that 8.6 is the last minor version in the 8.x release series for your model. Upgrading from 8.6 directly to 9.1 is not supported for zero-downtime upgrades; you must first upgrade to 9.0. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.4 to 9.0 (the model is not supported on 8.5 or 8.6).</p> <p> Note Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.4 to 9.0.</p>

Viewing Your Current Version

The software version appears on the ASDM home page; view the home page to verify the software version of your ASA.

Downloading the Software from Cisco.com

If you are using the ASDM Upgrade Wizard, you do not have to pre-download the software. If you are manually upgrading, for example for a failover upgrade, download the images to your local computer.

If you have a Cisco.com login, you can obtain the OS and ASDM images from the following website:

<http://www.cisco.com/cisco/software/navigator.html?mdfid=279513386>

Upgrading a Standalone Unit



Note

This section describes how to install the ASDM and operating system (OS) images. If the ASA is running Version 8.0 or later, then you can upgrade to the latest version of ASDM (and disconnect and reconnect to start running it) before upgrading the OS. The exception is for ASA versions that are not supported by the latest ASDM version; for example, ASA 8.5. In that case, follow the instructions for pre-8.0 versions (ASDM 5.2 and earlier).

If the ASA is running a version earlier than 8.0, then use the already installed version of ASDM to upgrade both the OS and ASDM to the latest versions, and then reload.

- [Upgrading from Your Local Computer \(ASDM 6.0 or Later\), page 28](#)
- [Upgrading Using the Cisco.com Wizard \(ASDM 6.3 or Later\), page 30](#)
- [Upgrading Using the Cisco.com Wizard \(ASDM 6.0 Through ASDM 6.2\), page 31](#)
- [Upgrading from Your Local Computer \(ASDM 5.2 or Earlier\), page 32](#)

Upgrading from Your Local Computer (ASDM 6.0 or Later)

The Upgrade Software from Local Computer tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

To upgrade software from your computer, perform the following steps:

- Step 1** (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.
- Step 2** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software dialog box appears.



- Step 3** From the Image to Upload drop-down list, choose **ASDM**.
- Step 4** In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.
- Step 5** In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 6** Click **Upload Image**. The uploading process might take a few minutes.

- Step 7** Repeat [Step 2](#) through [Step 6](#), choosing **ASA** from the Image to Upload drop-down list. You can also use this procedure to upload other file types.
- Step 8** Configure the ASA to use the new images.
- Choose **Configuration > Device Management > System/Image Configuration > Boot Image/Configuration**.

Configuration > Device Management > System Image/Configuration > Boot Image/Configuration

Boot Configuration

Configure boot images from a flash file system. Up to four boot images can be configured for the boot system.

Boot Order	Boot Image Location
1	disk0:/cdisk.bin

Buttons: Add, Edit, Delete, Move Up, Move Down

Boot Configuration File Path: Browse Flash...

ASDM Image Configuration

ASDM Image File Path: Browse Flash...

- In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.
- If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.
- Click **Browse Flash**, choose the OS image, and click **OK**.
 - Click **OK** to return to the Boot Image/Configuration pane.
 - Make sure the new image is the first image in the table by using the **Move Up** button as needed.
 - In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.
 - Click **Apply**.
- Step 9** Choose **File > Save Running Configuration to Flash** to save your configuration changes.
- Step 10** Choose **Tools > System Reload** to reload the ASA.
- A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.
- Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.
- Step 11** After the ASA reloads, restart ASDM.

Upgrading Using the Cisco.com Wizard (ASDM 6.3 or Later)

The Upgrade Software from Cisco.com Wizard lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.



Note

ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 8.4(2), the download might be 8.4(2.8). This behavior is expected, so you may proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, restart the ASA to save the configuration and complete the upgrade.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 Choose **Tools > Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The Cisco.com Authentication dialog box appears.

Step 3 Enter your assigned Cisco.com username and the Cisco.com password, and then click **Login**.

The Cisco.com Upgrade Wizard appears.



Note

If there are no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

Step 4 Click **Next** to display the Select Software screen.

The current ASA version and ASDM version appear.

Step 5 To upgrade the ASA version and ASDM version, perform the following steps:

- In the ASA area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.
- In the ASDM area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.

Step 6 Click **Next** to display the Review Changes screen.

Step 7 Verify the following items:

- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
- The ASA image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASA boot image has been selected.

Step 8 Click **Next** to start the upgrade installation.

You can then view the status of the upgrade installation as it progresses.

The Results screen appears, which provides additional details, such as the upgrade installation status (success or failure).

During the upgrade process from Version 8.2(1) to Version 8.3(1), the following files are automatically saved to flash memory:

- The startup configuration
- The per-context configuration
- The bootup error log, which includes any migration messages

If there is insufficient memory to save the configuration files, an error message appears on the console of the ASA and is saved in the bootup error log file. All previously saved configuration files are also removed.

Step 9 If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.

Step 10 Click **Finish** to exit the wizard and save the configuration changes that you have made.



Note To upgrade to the next higher version, if any, you must restart the wizard.

Upgrading Using the Cisco.com Wizard (ASDM 6.0 Through ASDM 6.2)

Detailed Steps

- Step 1** (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.
- Step 2** From the Tools menu, choose **Tools > Upgrade Software from Cisco.com**.
In multiple context mode, access this menu from the System.
The Upgrade Software from Cisco.com Wizard appears.
- Step 3** Click **Next**.
The Authentication screen appears.
- Step 4** Enter your Cisco.com username and password, and click **Next**.
The Image Selection screen appears.
- Step 5** Check the **Upgrade the ASA version** check box and the **Upgrade the ASDM version** check box to specify the most current images to which you want to upgrade, and click **Next**.
The Selected Images screen appears.
- Step 6** Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.
The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.
The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the ASA.

If you upgraded the ASA version and the upgrade succeeded, an option to save the configuration and reload the ASA appears.

Step 7 Click **Yes**.

For the upgrade versions to take effect, you must save the configuration, reload the ASA, and restart ASDM.

Step 8 Click **Finish** to exit the wizard when the upgrade is finished.

Step 9 After the ASA reloads, restart ASDM.

Upgrading from Your Local Computer (ASDM 5.2 or Earlier)

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration. For example, choose **File > Show Running Configuration in New Window** to open the configuration as an HTML page. You can also use one of the **File > Save Running Configuration** options.

Step 2 Choose **Tools > Upgrade Software**.

Step 3 From the Image to Upload drop-down list, choose **ASDM**.

Step 4 Click **Browse Local Files**, and browse to the ASDM image you downloaded from Cisco.com.

Step 5 Click **Browse Flash** to determine where to install the new ASDM image.

The Browse Flash dialog box appears. Choose the new location, and click **OK**. If you do not have room for both the current image and the new image, you can install over the current image.

Step 6 Click **Upload Image**.

Wait for the image to upload. An information window appears that indicates a successful upload.

Step 7 Repeat [Step 2](#) through [Step 6](#), choosing **ASA** from the Image to Upload drop-down list.

Step 8 Click **Close** to exit the Upgrade Software dialog box.

Step 9 Configure the ASA to use the new images.

- a. Choose **Configuration > Properties > Device Administration > Boot Image/Configuration**.
- b. In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.
If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.
- c. Click **Browse Flash**, choose the OS image, and click **OK**.
- d. Click **OK** to return to the Boot Image/Configuration pane.
- e. Make sure the new image is the first image in the table by using the **Move Up** button as needed.
- f. In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.
- g. Click **Apply**.

Step 10 Choose **File > Save Running Configuration to Flash** to save your configuration changes.

Step 11 Choose **Tools > System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 12 After the ASA reloads, restart ASDM.

Upgrading a Failover Pair or ASA Cluster

- [Upgrading an Active/Standby Failover Pair, page 33](#)
- [Upgrading an Active/Active Failover Pair, page 35](#)
- [Upgrading an ASA Cluster, page 37](#)

Upgrading an Active/Standby Failover Pair

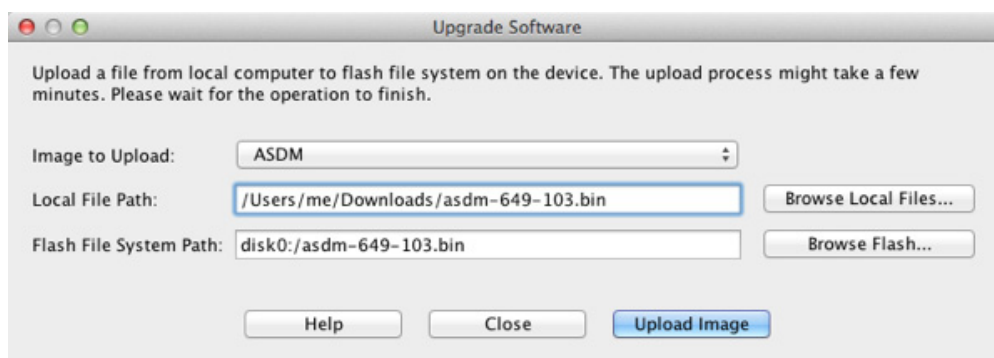
To upgrade the Active/Standby failover pair, perform the following steps.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 On the active unit, in the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



Step 3 From the Image to Upload drop-down list, choose **ASDM**.

Step 4 In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

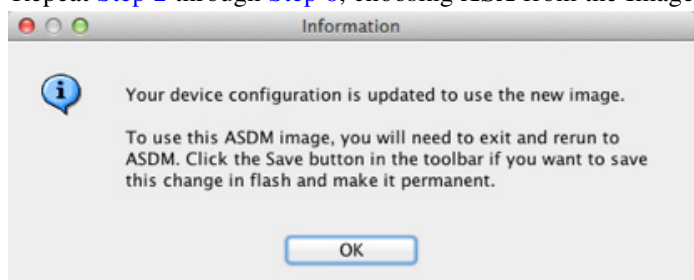
Step 6 Click **Upload Image**. The uploading process might take a few minutes.

Step 7 You are prompted to set this image as the ASDM image. Click **Yes**.



Step 8 You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 9 Repeat [Step 2](#) through [Step 8](#), choosing **ASA** from the Image to Upload drop-down list.



Step 10 Click the **Save** icon on the toolbar to save your configuration changes.

Step 11 Connect ASDM to the *standby* unit, and upload the ASA and ASDM software according to [Step 2](#) through [Step 9](#), using the same file locations you used on the active unit.

Step 12 Choose **Tools > System Reload** to reload the standby ASA.

A new window appears that asks you to verify the details of the reload.

- Click the **Save the running configuration at the time of reload** radio button (the default).
- Choose a time to reload (for example, **Now**, the default).
- Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 13 After the standby ASA reloads, restart ASDM and connect to the standby unit to make sure it is running.

Step 14 Connect ASDM to the *active* unit again.

Step 15 Force the active unit to fail over to the standby unit by choosing **Monitoring > Properties > Failover > Status**, and clicking **Make Standby**.

Step 16 Choose **Tools > System Reload** to reload the (formerly) active ASA.

A new window appears that asks you to verify the details of the reload.

- Click the **Save the running configuration at the time of reload** radio button (the default).
- Choose a time to reload (for example, **Now**, the default).
- Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

After the ASA comes up, it will now be the standby unit.

Upgrading an Active/Active Failover Pair

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Requirements

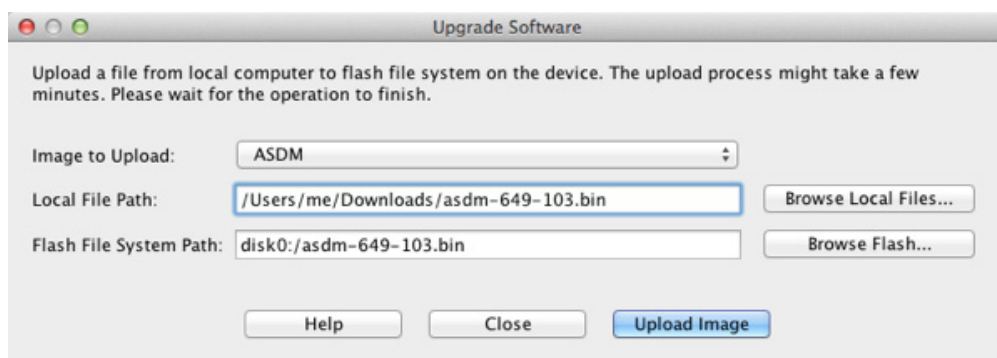
Perform these steps in the system execution space.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 On the primary unit, in the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



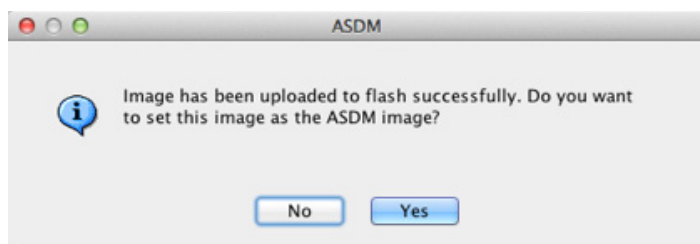
Step 3 From the Image to Upload drop-down list, choose **ASDM**.

Step 4 In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.

Step 5 In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.

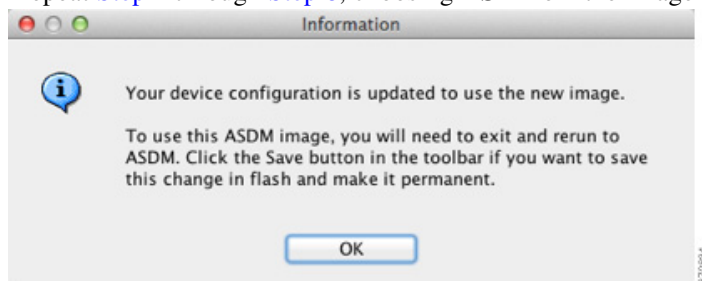
Step 6 Click **Upload Image**. The uploading process might take a few minutes.

Step 7 You are prompted to set this image as the ASDM image. Click **Yes**.



Step 8 You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

Step 9 Repeat [Step 2](#) through [Step 8](#), choosing **ASA** from the Image to Upload drop-down list.



Step 10 Click the **Save** icon on the toolbar to save your configuration changes.

Step 11 Make both failover groups active on the primary unit by choosing **Monitoring > Failover > Failover Group #**, where # is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 12 Connect ASDM to the *secondary* unit, and upload the ASA and ASDM software according to [Step 2](#) through [Step 9](#), using the same file locations you used on the active unit.

Step 13 Choose **Tools > System Reload** to reload the secondary ASA.

A new window appears that asks you to verify the details of the reload.

- a. Click the **Save the running configuration at the time of reload** radio button (the default)
- b. Choose a time to reload (for example, **Now**, the default).
- c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 14 Connect ASDM to the *primary* unit, and check when the secondary unit reloads by choosing **Monitoring > Failover > System**.

Step 15 After the secondary unit comes up, force the primary unit to fail over to the secondary unit by choosing **Monitoring > Properties > Failover > System**, and clicking **Make Standby**.

Step 16 Choose **Tools > System Reload** to reload the (formerly) active ASA.

A new window appears that asks you to verify the details of the reload.

- a. Click the **Save the running configuration at the time of reload** radio button (the default)
- b. Choose a time to reload (for example, **Now**, the default).
- c. Click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

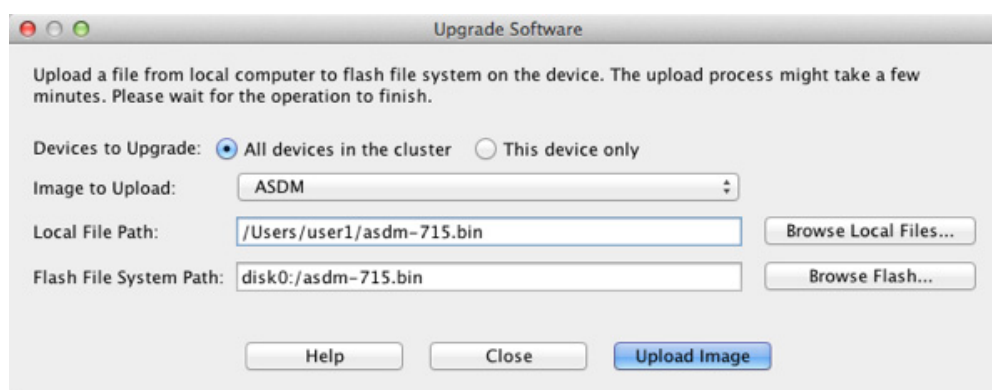
If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the **Monitoring > Failover > Failover Group #** pane.

Upgrading an ASA Cluster

To upgrade all units in an ASA cluster, perform the following steps on the master unit. For multiple context mode, perform these steps in the system execution space.

Detailed Steps

- Step 1** Launch ASDM on the master unit.
- Step 2** (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.
- Step 3** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software from Local Computer dialog box appears.
- Step 4** Click the **All devices in the cluster** radio button. The Upgrade Software dialog box appears.

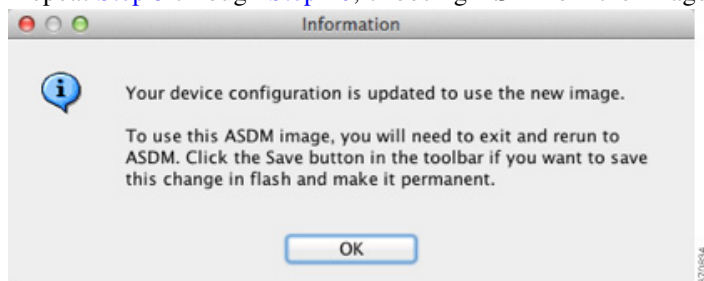


- Step 5** From the Image to Upload drop-down list, choose **ASDM**.
- Step 6** In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.
- Step 7** In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 8** Click **Upload Image**. The uploading process might take a few minutes.
- Step 9** You are prompted to set this image as the ASDM image. Click **Yes**.



- Step 10** You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.

- Step 11** Repeat [Step 3](#) through [Step 10](#), choosing **ASA** from the Image to Upload drop-down list.

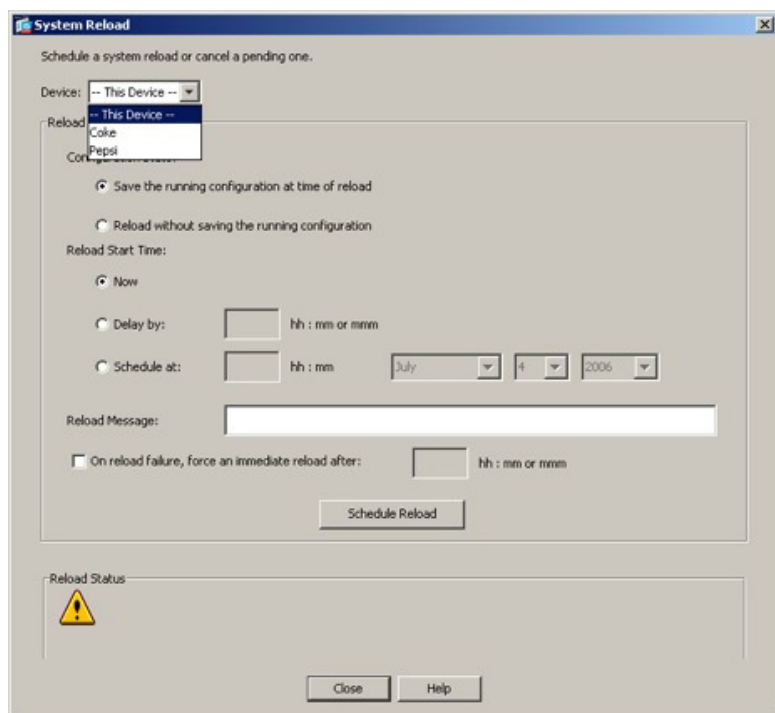


- Step 12** Click the **Save** icon on the toolbar to save your configuration changes.

- Step 13** Choose **Tools > System Reload**.

The System Reload dialog box appears.

- Step 14** Reload each slave unit one at a time by choosing a slave unit name in the Device drop-down list, and then clicking **Schedule Reload** to reload the unit now.



To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up (approximately 5 minutes) before reloading the next unit. To view when a unit rejoins the cluster, see the **Monitoring > ASA Cluster > Cluster Summary** pane.

- Step 15** After all slave units have reloaded, disable clustering on the master unit by choosing **Configuration > Device Management > High Availability and Scalability > ASA Cluster**, uncheck the **Participate in ASA cluster** check box, and click **Apply**.

Wait for 5 minutes for a new master to be selected and traffic to stabilize. When the former master unit rejoins the cluster, it will be a slave.

Do not save the configuration; when the master unit reloads, you want clustering to be enabled on it.

- Step 16** Choose **Tools > System Reload** and reload the master unit from the System Reload dialog box by choosing **--This Device--** from the Device drop-down list.
- Step 17** Quit and restart ASDM; you will reconnect to the new master unit.

Unsupported Commands

ASDM supports almost all commands available for the adaptive ASA, but ASDM ignores some commands in an existing configuration. Most of these commands can remain in your configuration; see **Tools > Show Commands Ignored by ASDM on Device** for more information.

This section includes the following topics:

- [Ignored and View-Only Commands, page 39](#)
- [Effects of Unsupported Commands, page 40](#)
- [Discontinuous Subnet Masks Not Supported, page 40](#)
- [Interactive User Commands Not Supported by the ASDM CLI Tool, page 40](#)

Ignored and View-Only Commands

[Table 6](#) lists commands that ASDM supports in the configuration when added through the CLI, but that cannot be added or edited in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it appears in the GUI, but you cannot edit it.

Table 6 *List of Unsupported Commands*

Unsupported Commands	ASDM Behavior
capture	Ignored.
coredump	Ignored. This can be configured only using the CLI.
crypto engine large-mod-accel	Ignored.
dhcp-server (tunnel-group name general-attributes)	ASDM only allows one setting for all DHCP servers.
eject	Unsupported.
established	Ignored.
failover timeout	Ignored.
fips	Ignored.
nat-assigned-to-public-ip	Ignored.
pager	Ignored.
pim accept-register route-map	Ignored. You can configure only the list option using ASDM.

Table 6 *List of Unsupported Commands (continued)*

Unsupported Commands	ASDM Behavior
service-policy global	Ignored if it uses a match access-list class. For example: <pre>access-list myacl extended permit ip any any class-map mycm match access-list myacl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>
set metric	Ignored.
sysopt nodnsalias	Ignored.
sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
threat-detection rate	Ignored.

Effects of Unsupported Commands

If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, choose **Tools > Show Commands Ignored by ASDM on Device**.

Discontinuous Subnet Masks Not Supported

ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Interactive User Commands Not Supported by the ASDM CLI Tool

The ASDM CLI tool does not support interactive user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter “[yes/no]” but does not recognize your input. ASDM then times out waiting for your response.

For example:

1. Choose **Tools > Command Line Interface**.
2. Enter the **crypto key generate rsa** command.
ASDM generates the default 1024-bit RSA key.
3. Enter the **crypto key generate rsa** command again.

Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
ke00000000000000$A key
Input line must be less than 16 characters in length.
```



```
%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

Workaround:

- You can configure most commands that require user interaction by means of the ASDM panes.
- For CLI commands that have a **noconfirm** option, use this option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

Open Caveats

This section contains open caveats in ASDM software Version 7.0, and includes the following topics:

- [Open Caveats in Version 7.0\(2.9\), page 41](#)
- [Open Caveats in Version 7.0\(2\), page 42](#)
- [Open Caveats in Version 7.0\(1\), page 42](#)

Open Caveats in Version 7.0(2.9)

Table 8 contains open caveats in ASDM software Version 7.0(2.9).

Registered Cisco.com users can view more information about each caveat by using the Bug Toolkit at the following website:

<http://tools.cisco.com/Support/BugToolkit/>

Table 7 **Open Caveats in ASDM Version 7.0(2.9)**

Caveat	Description
CSCtq19131	Clientless WebVPN-Delete bookmark which in use-error msg not consistent
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCub14386	Upgrade image to whole cluster: sometime fail to copy images
CSCuc39101	ASDM: AnyConnect Script: no 'linux-64' option (see CSCuc39071)
CSCuc45845	ASDM Launcher does not work with JAVA version 7 on Mac OS
CSCuc47316	asdm_handler returns wrong value for CONN for system context
CSCuc59446	IPv6/IPv4 option missing when configuring network object
CSCuc63622	AnyConnect Web Sec. profile creation not completed
CSCuc63797	Static policy nat is not working in ASDM 6.49-103
CSCuc68351	ASDM truncates regular expression in username-from-certificate script
CSCuc77445	Do not allow cluster configuration without cluster license
CSCuc81697	ASDM changes AES to DES in IKEv1 policy

Open Caveats in Version 7.0(2)

Table 8 contains open caveats in ASDM software Version 7.0(2).

Registered Cisco.com users can view more information about each caveat by using the Bug Toolkit at the following website:

<http://tools.cisco.com/Support/BugToolkit/>

Table 8 *Open Caveats in ASDM Version 7.0(2)*

Caveat	Description
CSCtq19131	Clientless WebVPN-Delete bookmark which in use-error msg not consistent
CSCtt24721	False Error when Manually Enabling Anonymous Reporting the First Time
CSCub14386	Upgrade image to whole cluster: sometime fail to copy images
CSCuc39101	ASDM: AnyConnect Script: no 'linux-64' option (see CSCuc39071)
CSCuc45845	ASDM Launcher does not work with JAVA version 7 on Mac OS
CSCuc47316	asdm_handler returns wrong value for CONN for system context
CSCuc59446	IPv6/IPv4 option missing when configuring network object
CSCuc63622	AnyConnect Web Sec. profile creation not completed
CSCuc63797	Static policy nat is not working in ASDM 6.49-103
CSCuc68351	ASDM truncates regular expression in username-from-certificate script
CSCuc77445	Do not allow cluster configuration without cluster license
CSCuc81697	ASDM changes AES to DES in IKEv1 policy
CSCud03838	ASDM 7.0 warning "uploaded file is not a valid ASA-SM image" on 9.0.1

Open Caveats in Version 7.0(1)

Table 9 contains open caveats in ASDM software Version 7.0(1).

Registered Cisco.com users can view more information about each caveat by using the Bug Toolkit at the following website:

<http://tools.cisco.com/Support/BugToolkit/>

Table 9 *Open Caveats in ASDM Version 7.0(1)*

Caveat	Description
CSCua80116	Removed slave unit is not removed from Monitoring->ASA Cluster->Summary
CSCub00490	New IPv6 addresses don't show up in the Interfaces panel
CSCub06744	ASDM doesn't launch with " java.lang.NoSuchFieldError: b"
CSCub14386	Upgrade image to whole cluster: sometime fail to copy images
CSCub22526	In multi-mode preview CLI should mask Scansafe key in user context
CSCub23960	PPPoE is not supported in cluster and should be removed from intf dialog
CSCub52100	ASDM: dynamic nat - fall through to interface pat enabled - L3 Cluster
CSCub56265	ASDM: IPV6 tab - Strict checking not done in IP Pool

Table 9 **Open Caveats in ASDM Version 7.0(1) (continued)**

Caveat	Description
CSCub68249	ASDM Completely Hangs if User Cancels Progress Dialogue
CSCub75956	ASDM takes an hour to time out and can't cancel
CSCub77143	ASDM no login button in auth prompt after idle time for less priv user
CSCub80506	WCCP service group accepts only IPv4 access rules
CSCub85377	When user is authenticated twice only one IP is shown in ASDM
CSCuc02307	Error message for AnyConnect Client Profile if user is not admin
CSCuc07375	ASDM Add User Account attribute stuck in loop
CSCuc09321	Interface allocation list: interface in use by cluster shouldn't show up
CSCuc13050	ETSG-J:-System CPU Usage Shows incorrect Value in ASDM
CSCuc13614	ETSG-J:- Unable to View or Activate the License in the ASDM
CSCuc14426	Enabling WebVPN on an interface results error even though it is success
CSCuc17092	Bookmarks- HTML Capture parameters are not visible if using small screen
CSCuc20354	Splash screen update and version mismatch resolution for 88.7
CSCuc21198	"DNS server ip address not valid" in ASDM when name is configured
CSCuc22711	Adv tab gray out when adding EC from interface panel
CSCuc23034	Update help for Ebay netflow enhancement
CSCuc23887	Deleting IPv6 ACL in ASDM sends wrong command to ASA 8.x
CSCuc30486	ASDM: Incorrect User message Length for DAP Help menu
CSCuc34859	ASDM: DAP attribute needed for iPhone 5
CSCuc37955	HA Wizard:hide ASA Cluster option when cluster is not available
CSCuc39101	ASDM: AnyConnect Script: no 'linux-64' option (see CSCuc39071)
CSCuc39218	Mix Mode transparent context - Scansafe monitor shows "invalid error"
CSCuc44572	ASDM: DAP attributes needed for iPhone 5 Vendors
CSCuc45845	ASDM Launcher does not work with JAVA version 7 on Mac OS
CSCuc47316	asdm_handler returns wrong value for CONN for system context
CSCuc53827	Unable to run S2S VPN wizard
CSCuc54924	ASDM:source any is not accepted for nat64 on asdm
CSCuc57947	ASDM: DAP attribute for iPhone is incorrect
CSCuc59446	IPv6/IPv4 option missing when configuring network object
CSCud03838	ASDM 7.0 warning "uploaded file is not a valid ASA-SM image" on 9.0.1

Resolved Caveats

This section contains the following topics:

- [Resolved Caveats in Version 7.0\(2.9\), page 44](#)
- [Resolved Caveats in Version 7.0\(2\), page 44](#)

Resolved Caveats in Version 7.0(2.9)

Table 10 contains the resolved caveats in ASDM software Version 7.0(2.9).

Registered Cisco.com users can view more information about each caveat by using the Bug Toolkit at the following website:

<http://tools.cisco.com/Support/BugToolkit/>

Table 10 **Resolved Caveats in ASDM Version 7.0(2.9)**

Caveat	Description
CSCuc99271	Update demo mode files
CSCud03838	ASDM 7.0 warning "uploaded file is not a valid ASA-SM image" on 9.0.1

Resolved Caveats in Version 7.0(2)

Table 11 contains the resolved caveats in ASDM software Version 7.0(2).

Registered Cisco.com users can view more information about each caveat by using the Bug Toolkit at the following website:

<http://tools.cisco.com/Support/BugToolkit/>

Table 11 **Resolved Caveats in ASDM Version 7.0(2)**

Caveat	Description
CSCtl23621	Add / Edit EtherChannel dialog default is too large for many laptops
CSCtl45001	Help-About Cisco ASA output has "null" text in 1st line of output.remove
CSCts96100	ASDM downgrade error: can't delete external portal page post parameters
CSCtt29947	ASDM startup wizard produces errors when IPv6 address already on BVI int
CSCtw60293	Apply button is not enabled in Filter Rules & Default Information screen
CSCtw69933	ASDM misleading popup when connecting to ASA with http server disabled
CSCtw73611	Manage CA server on TLS proxy
CSCtw92696	ASDM: Edit/Delete buttons should be disabled - when TLS Proxy empty
CSCty91785	ASDM asks for passphrase everytime local ca server is being enabled
CSCtz50654	Hint popup goes off the current screen boundaries
CSCua55800	OSPFv3: Improve proxy ARP to include IPv6 neighbor discovery
CSCua63832	Netflow enhancement for new CLI addition of report interval
CSCua64203	Different color icons needed for icmp & icmp6 service types
CSCua80116	Removed slave unit is not removed from Monitoring->ASA Cluster->Summary
CSCua86879	Clarify "IPv6 Enable" Option
CSCub00490	New IPv6 addresses don't show up in the Interfaces panel
CSCub05516	ASDM doesn't recognize windows 8 platform under operating system
CSCub06744	ASDM doesn't launch with " java.lang.NoSuchFieldError: b"
CSCub14070	When ASA is in L2/L3 mode, hide functionality incompatible with cluster

Table 11 *Resolved Caveats in ASDM Version 7.0(2) (continued)*

Caveat	Description
CSCub16930	ASDM support for CSCub02268-Maximum TCP intercept config values too low
CSCub23960	PPPoE is not supported in cluster and should be removed from intf dialog
CSCub29537	Double-clicking non-mgmt intf in L2 cluster wizard allows to edit intf
CSCub34361	ASDM File Management change request
CSCub35300	Support IS-IS routing protocol passthrough in transparent mode
CSCub35574	ASDM should alert when proxy arp is enabled for identity nat
CSCub40755	Support for Windows 8 on ASDM
CSCub52100	ASDM: dynamic nat - fall through to interface pat enabled - L3 Cluster
CSCub56265	ASDM: IPV6 tab - Strict checking not done in IP Pool
CSCub65157	NAT Rules: "Where used" fails to find rules with "DM_INLINE_NETWORK"
CSCub66231	ASDM Service policy screen missing SGT from rule view
CSCub68249	ASDM Completely Hangs if User Cancels Progress Dialogue
CSCub71148	ASDM: while creating AAA rules default src & dest add should be "any4"
CSCub77143	ASDM no login button in auth prompt after idle time for less priv user
CSCub80352	Some remaining issues with External Portal GUI panel enhancement
CSCub80506	WCCP service group accepts only IPv4 access rules
CSCub85377	When user is authenticated twice only one IP is shown in ASDM
CSCub96756	ASDM: ignored commands
CSCub99608	ASDM enhancement - new cli "ssl certificate-authentication fca-timeout"
CSCuc02307	Error message for AnyConnect Client Profile if user is not admin
CSCuc09185	DAP Attribute does not accept space in its device type name
CSCuc09321	Interface allocation list: interface in use by cluster shouldn't show up
CSCuc11760	Cluster: Need to allow nameif on port-channel subinterface in spanned md
CSCuc13614	ETSG-J:- Unable to View or Activate the License in the ASDM
CSCuc14426	Enabling WebVPN on an interface results error even though it is success
CSCuc17092	Bookmarks- HTML Capture parameters are not visible if using small screen
CSCuc20354	Splash screen update and version mismatch resolution for 88.7
CSCuc21198	"DNS server ip address not valid" in ASDM when name is configured
CSCuc22711	Adv tab gray out when adding EC from interface panel
CSCuc23887	Deleting IPv6 ACL in ASDM sends wrong command to ASA 8.x
CSCuc34859	ASDM: DAP attribute needed for iPhone 5
CSCuc37955	HA Wizard:hide ASA Cluster option when cluster is not configurable
CSCuc39218	Mix Mode transparent context - Scansafe monitor shows "invalid error"
CSCuc40313	Merge Torino to ASDM main branch
CSCuc43333	ASDM version detail at Help->About Cisco ASDM splash screen
CSCuc44572	ASDM: DAP attributes needed for iPhone 5 Vendors

Table 11 **Resolved Caveats in ASDM Version 7.0(2) (continued)**

Caveat	Description
CSCuc53827	Unable to run S2S VPN wizard, Conn Profile , Max IPsec proposals exceeded
CSCuc54733	Label for Enforce EUI-64 is shown as "E" only
CSCuc56688	ASDM version mismatch on running Benu
CSCuc57193	Can't add ipv6 address when adding/editing Bridge Group Interface
CSCuc57947	ASDM: DAP attribute for iPhone is incorrect
CSCuc63797	Static policy nat is not working in ASDM 6.49-103
CSCuc80086	ASDM Anyconnect wizard is unresponsive if no WINS server is entered

End-User License Agreement

For information about the end-user license agreement, go to:

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html

Related Documentation

For additional information about ASDM or its platforms, see *Navigating the Cisco ASA Series Documentation*:

<http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html>

Obtaining Software, Documentation, and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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: www.cisco.com/go/trademarks. 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. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

©2012 Cisco Systems, Inc. All rights reserved.

