



# Release Notes for Cisco ASDM, Version 6.2, for ASA and PIX

---

## November 2009

This document contains release information for Cisco ASDM Version 6.2 on Cisco ASA 5500 series and Cisco PIX 500 series security appliances. It includes the following sections:

- [Important Notes, page 1](#)
- [ASDM Client Operating System and Browser Requirements, page 2](#)
- [Supported Platforms and SSMs, page 3](#)
- [New ASDM Features, page 4](#)
- [New Features by Platform Release, page 4](#)
- [Upgrading the Security Appliance, page 26](#)
- [Unsupported Commands, page 27](#)
- [Open and Resolved Caveats for Software Version 6.2, page 30](#)
- [End-User License Agreement, page 36](#)
- [Related Documentation, page 36](#)
- [Obtaining Documentation and Submitting a Service Request, page 36](#)

## Important Notes

This section describes new enhancements or procedures or documentation issues that have been implemented since the last release, and includes the following topics:

- [AIP SSC Setup Screen in ASDM](#)
- [ASDM Launcher Upgrade Failure](#)



---

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

© 2009 Cisco Systems, Inc. All rights reserved.

## AIP SSC Setup Screen in ASDM

AIP (IPS) users will be unable to use ASDM to set up SSC if you mistype a password in the SSC-setup screen.

## ASDM Launcher Upgrade Failure

Upgrading from a previous version of ASDM, such as ASDM 6.1.5.51, which includes ASDM Launcher 1.5.30, sometimes fails in the following two ways on Windows XP or Vista:

- CSCsy75722: When using the ASDM Launcher to upgrade a Launcher installer wizard appears. After clicking the Install button on the Ready to Install the Program dialog, the status bar does not progress and a Cisco ASDM-IDM Launcher Installer Information dialog appears with the following: "The system cannot open the device or file specified". Pressing Retry does not help.
- CSCsz35267: When using a web browser, clicking the "Install ASDM Launcher and Run ASDM" button downloads the dm-launcher.msi installer. Running dm-launcher.msi may produce an error 1307 or 1316 dialog giving the full pathname of the file that either cannot be found or for which a network error occurred.

**Workaround** : To recover from such events, use the Add or Remove Programs control panel to remove the Cisco ASDM Launcher or Cisco ASDM-IDM Launcher. (Any of the ASDM on *IP address* programs do not need to be removed.) Afterwards, evoke a web browser; access ASDM with a URL such as `https://<IP_Address >/admin`; and install the new ASDM-IDM Launcher with the "Install ASDM Launcher and Run ASDM" button.

## 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	Version	Browser <sup>1</sup>	Other Requirements
Microsoft Windows	Windows 7 Windows Vista Windows 2003 Server (English or Japanese version) Windows XP	Internet Explorer 6.0, 7.0, 8.0 with Sun Java SE <sup>2</sup> Plug-in 5.0 (1.5.0), or 6.0 Firefox 1.5, 2.0, 3.0, and 3.5 with Java SE Plug-in 5.0 (1.5.0), or 6.0	<b>SSL Encryption Settings</b> —All available encryption options are enabled for SSL in the browser preferences.
<b>Note</b>	ASDM supports both the English and Japanese versions of Windows.	<b>Note</b>	<b>HTTP 1.1</b> —Settings for <b>Internet Options &gt; Advanced &gt; HTTP 1.1</b> should use HTTP 1.1 for both proxy and non-proxy connections.
Apple Macintosh	Apple Macintosh OS X, 10.4, 10.5, 10.6	Firefox 1.5, 2.0, 3.0, and 3.5, or Safari 2.0 with Java SE Plug-in 5.0 (1.5.0), or 6.0 <sup>3 4</sup>	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 5 running GNOME or KDE	Firefox 1.5, 2.0, 3.0, and 3.5 with Java SE Plug-in 5.0 (1.5.0), or 6.0	

1. The recommended minimal resolution for your browser should be 1024 x 768.

2. Obtain Sun Java from [java.sun.com](http://java.sun.com).
3. With Apple Macintosh, only 32-bit Java SE will be supported. Currently, this also excludes Java 6. The 32-bit Java can run on a 64-bit Mac OS.
4. If you are trying to launch ASDM on a Macintosh, be aware that recent Java upgrades do not automatically register the changed location of the Java Web Start application, which should handle JNLP extension files. To reconcile this problem, simply go to the directory /System/Library/CoreServices in the Mac Finder. After you have opened the folder in this directory, when you select Run ASDM and Run Startup Wizard, a dialog appears that allows you to associate JNLP files with Java Web Start.

**Note**

After upgrading ASDM, to restore normal memory usage on a Mac, existing ASDM desktop applications must be deleted and a new ASDM desktop application installed in its place. The following instructions avoid CSCsu31299.

**Important:** This procedure is not needed with operating systems that correct CSCsv28869: ASA/PIX 8.0(4.11), ASA 8.1(2.5), or ASA 8.2 or later.

On the Mac, go to **Applications > Utilities > Java > Java Preferences**. From the **Java Preferences** dialog, select **View**. The Java Cache Viewer dialog appears. Select **Applications** from the **Show** pull-down menu. Select the ASDM on *ip\_addr* row in the table that you want to delete, select 'X' to remove the selected item, and click **OK**.

Next, from the **Java Preferences** dialog, select **Settings**. Then select **Delete Files**. Choose all options from this pop-up dialog and click **Delete**. On the **Temporary Files Setting** dialog, click **OK**.

Go to the **Java Preferences** menu and select **Quit Java Preferences**. If the deleted desktop IP address application still appears on the desktop, drag and drop the application into the trash. Launch ASDM from a web browser, either Safari or Firefox, and, if desired, install a new ASDM desktop application when prompted.

**Note**

ASDM supports up to a maximum of a 512 KB configuration. If you exceed this amount, you may experience performance issues.

## Supported Platforms and SSMs

**Note**

ASDM 6.2(1) and higher is not supported on the PIX platforms. The last release that ASDM is supported on is 6.1(5).

ASDM Version 6.2 supports the following platforms and releases:

- ASA 5505, software Version 8.0(2), 8.0(3), 8.0(4), 8.0(5), and 8.2(1)
- ASA 5510, software Version 8.0(2), 8.0(3), 8.0(4), 8.0(5), and 8.2(1)
- ASA 5520, software Version 8.0(2), 8.0(3), 8.0(4), 8.0(5), and 8.2(1)
- ASA 5540, software Version 8.0(2), 8.0(3), 8.0(4), 8.0(5), and 8.2(1)
- ASA 5550, software Version 8.0(2), 8.0(3), 8.0(4), 8.0(5), and 8.2(1)
- ASA 5580, software Version 8.1(1), 8.1(2), and 8.2(1)

ASDM Version 6.2(3) supports the following SSMs and releases:

- Advanced Inspection and Prevention (AIP) SSM, software Version 5.0, 5.1, 6.0, 6.1, and 6.2
- Content Security and Control (CSC) SSM, software Version 6.1 and 6.2

- Advanced Inspection and Prevention (AIP) SSC, Version 6.2

## New ASDM Features

Table 2 lists the new features for ASDM Version 6.2.3

**Table 2**      **New Features for ASDM Version 6.2.3**

Feature	Description
Support for ASA 8.0(5)	ASDM 6.2(3) supports the new features in ASA 8.0(5).
CSC 6.3 Support in ASDM	ASDM displays Web Reputation, User Group Policies, and User ID Settings in the Plus License listing on the main home page. CSC 6.3 security event enhancements are included, such as the new Web Reputation events and user and group identifications.



**Note**

In ASDM Version 6.2, the VPN Wizard (accessible by choosing Wizards > IPsec VPN Wizard) was updated. The step to select IPsec Encryption and Authentication (formerly Step 9 of 11) was removed because the Wizard now generates default values for these settings. In addition, the step to select IPsec Settings (Optional) now includes new fields to enable perfect forwarding secrecy (PFS) and set the Diffie-Hellman Group. The ASDM Help and the *Cisco ASA 5580 Adaptive Security Appliance Getting Started Guide, 8.1* were updated to reflect these changes.

## New Features by Platform Release

This section lists the new features available in each supported platform release. Because ASDM supports multiple platform releases, and the ASDM documentation includes features for all releases, you should see these sections to determine if a feature is in your release. This section includes the following topics:

- [New Features in Version 8.2\(1\), page 5](#)
- [New Features in Version 8.1\(2\), page 10](#)
- [New Features in Version 8.1\(1\), page 13](#)
- [New Features in Version 8.0\(5\), page 14](#)
- [New Features in Version 8.0\(4\), page 15](#)
- [New Features in Version 8.0\(3\), page 19](#)
- [New Features in Version 8.0\(2\), page 20](#)

## New Features in Version 8.2(1)

Table 3 lists the new features for Version 8.2(1).

**Table 3**      *New Features for ASA Version 8.2(1)*

Feature	Description
<b>Remote Access Features</b>	
One Time Password Support for ASDM Authentication	<p>ASDM now supports administrator authentication using one time passwords (OTPs) supported by RSA SecurID (SDI). This feature addresses security concerns about administrators authenticating with static passwords.</p> <p>New session controls for ASDM users include the ability to limit the session time and the idle time. When the password used by the ASDM administrator times out, ASDM prompts the administrator to re-authenticate.</p> <p>The following commands were introduced: <b>http server idle-timeout</b> and <b>http server session-timeout</b>. The <b>http server idle-timeout</b> default is 20 minutes, and can be increased up to a maximum of 1440 minutes.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; ASDM/HTTPD/Telnet/SSH.</p>
Customizing Secure Desktop	<p>You can use ASDM to customize the Secure Desktop windows displayed to remote users, including the Secure Desktop background (the lock icon) and its text color, and the dialog banners for the Desktop, Cache Cleaner, Keystroke Logger, and Close Secure Desktop windows.</p> <p>In ASDM, see Configuration &gt; CSD Manager &gt; Secure Desktop Manager.</p>
Pre-fill Username from Certificate	<p>The pre-fill username feature enables the use of a username extracted from a certificate for username/password authentication. With this feature enabled, the username is “pre-filled” on the login screen, with the user being prompted only for the password. To use this feature, you must configure both the <b>pre-fill username</b> and the <b>username-from-certificate</b> commands in tunnel-group configuration mode.</p> <p>The double-authentication feature is compatible with the pre-fill username feature, as the pre-fill username feature can support extracting a primary username and a secondary username from the certificate to serve as the usernames for double authentication when two usernames are required. When configuring the pre-fill username feature for double authentication, the administrator uses the following new tunnel-group general-attributes configuration mode commands:</p> <ul style="list-style-type: none"> <li>• <b>secondary-pre-fill-username</b>—Enables username extraction for Clientless or AnyConnect client connection.</li> <li>• <b>secondary-username-from-certificate</b>—Allows for extraction of a few standard DN fields from a certificate for use as a username.</li> </ul> <p>In ASDM, see In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect or Clientless SSL VPN Connection Profiles &gt; Advanced. Settings are in Authentication, Secondary Authentication, and Authorization panels.</p>

Table 3 New Features for ASA Version 8.2(1) (continued)

Feature	Description
Double Authentication	<p>The double authentication feature implements two-factor authentication for remote access to the network, in accordance with the Payment Card Industry Standards Council Data Security Standard. This feature requires that the user enter two separate sets of login credentials at the login page. For example, the primary authentication might be a one-time password, and the secondary authentication might be a domain (Active Directory) credential. If either authentication fails, the connection is denied.</p> <p>Both the AnyConnect VPN client and Clientless SSL VPN support double authentication. The AnyConnect client supports double authentication on Windows computers (including supported Windows Mobile devices and Start Before Logon), Mac computers, and Linux computers. The IPsec VPN client, SVC client, cut-through-proxy authentication, hardware client authentication, and management authentication do not support double authentication.</p> <p>Double authentication requires the following new tunnel-group general-attributes configuration mode commands:</p> <ul style="list-style-type: none"> <li>• <b>secondary-authentication-server-group</b>—Specifies the secondary AAA server group, which cannot be an SDI server group.</li> <li>• <b>secondary-username-from-certificate</b>—Allows for extraction of a few standard DN fields from a certificate for use as a username.</li> <li>• <b>secondary-pre-fill-username</b>—Enables username extraction for Clientless or AnyConnect client connection.</li> <li>• <b>authentication-attr-from-server</b>—Specifies which authentication server authorization attributes are applied to the connection.</li> <li>• <b>authenticated-session-username</b>—Specifies which authentication username is associated with the session.</li> </ul> <p><b>Note</b> The RSA/SDI authentication server type cannot be used as the secondary username/password credential. It can only be used for primary authentication.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access or Clientless SSL VPN &gt; AnyConnect Connection Profiles &gt; Add/Edit &gt; Advanced &gt; Secondary Authentication.</p>

Table 3 New Features for ASA Version 8.2(1) (continued)

Feature	Description
AnyConnect Essentials	<p>AnyConnect Essentials is a separately licensed SSL VPN client, entirely configured on the security appliance, that provides the full AnyConnect capability, with the following exceptions:</p> <ul style="list-style-type: none"> <li>• No CSD (including HostScan/Vault/Cache Cleaner)</li> <li>• No clientless SSL VPN</li> <li>• Optional Windows Mobile Support</li> </ul> <p>The AnyConnect Essentials client provides remote end users running Microsoft Windows Vista, Windows Mobile, Windows XP or Windows 2000, Linux, or Macintosh OS X, with the benefits of a Cisco SSL VPN client.</p> <p>To configure AnyConnect Essentials, the administrator uses the following command:</p> <p><b>anyconnect-essentials</b>—Enables the AnyConnect Essentials feature. If this feature is disabled (using the <b>no</b> form of this command), the SSL Premium license is used. This feature is enabled by default.</p> <p><b>Note</b> This license cannot be used at the same time as the shared SSL VPN premium license.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; AnyConnect Essentials License. The AnyConnect Essentials license must be installed for ASDM to show this pane.</p>
Disabling Cisco Secure Desktop per Connection Profile	<p>When enabled, Cisco Secure Desktop automatically runs on all computers that make SSL VPN connections to the security appliance. This new feature lets you exempt certain users from running Cisco Secure Desktop on a per connection profile basis. It prevents the detection of endpoint attributes for these sessions, so you might need to adjust the Dynamic Access Policy (DAP) configuration.</p> <p>CLI: <b>[no] without-csd command</b></p> <p><b>Note</b> “Connect Profile” in ASDM is also known as “Tunnel Group” in the CLI. Additionally, the <b>group-url</b> command is required for this feature. If the SSL VPN session uses connection-alias, this feature will not take effect.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Connection Profiles &gt; Add or Edit &gt; Advanced, Clientless SSL VPN Configuration.</p> <p>or</p> <p>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add or Edit &gt; Advanced &gt; SSL VPN.</p>
Certificate Authentication Per Connection Profile	<p>Previous versions supported certificate authentication for each security appliance interface, so users received certificate prompts even if they did not need a certificate. With this new feature, users receive a certificate prompt only if the connection profile configuration requires a certificate. This feature is automatic; the <b>ssl certificate authentication</b> command is no longer needed, but the security appliance retains it for backward compatibility.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add/Edit &gt; Basic.</p> <p>or</p> <p>Configuraiton &gt; Remote Access VPN &gt; Clientless SSL VPN &gt; Connection Profiles &gt; Add/Edit&gt;Basic.</p>

Table 3 New Features for ASA Version 8.2(1) (continued)

Feature	Description
EKU Extensions for Certificate Mapping	<p>This feature adds the ability to create certificate maps that look at the Extended Key Usage extension of a client certificate and use these values in determining what connection profile the client should use. If the client does not match that profile, it uses the default group. The outcome of the connection then depends on whether or not the certificate is valid and the authentication settings of the connection profile.</p> <p>The following command was introduced: <b>extended-key-usage</b>.</p> <p>In ASDM, use the IPsec Certificate to Connection Maps &gt; Rules pane, or Certificate to SSL VPN Connections Profile Maps pane.</p>
SSL VPN SharePoint Support for Win 2007 Server	Clientless SSL VPN sessions now support Microsoft Office SharePoint Server 2007.
Shared license for SSL VPN sessions	<p>You can purchase a shared license with a large number of SSL VPN sessions and share the sessions as needed among a group of security appliances by configuring one of the security appliances as a shared license server, and the rest as clients. The following commands were introduced: <b>license-server</b> commands (various), <b>show shared license</b>.</p> <p><b>Note</b> This license cannot be used at the same time as the AnyConnect Essentials license.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Licensing &gt; Shared SSL VPN Licenses. Also see, Monitoring &gt; VPN &gt; Clientless SSL VPN &gt; Shared Licenses.</p>
<b>Firewall Features</b>	
TCP state bypass	<p>If you have asymmetric routing configured on upstream routers, and traffic alternates between two security appliances, then you can configure TCP state bypass for specific traffic. The following command was introduced: <b>set connection advanced tcp-state-bypass</b>.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Rule Actions &gt; Connection Settings.</p>
Per-Interface IP Addresses for the Media-Termination Instance Used by the Phone Proxy	<p>In Version 8.0(4), you configured a global media-termination address (MTA) on the security appliance. In Version 8.2, you can now configure MTAs for individual interfaces (with a minimum of two MTAs). As a result of this enhancement, the old CLI has been deprecated. You can continue to use the old configuration if desired. However, if you need to change the configuration at all, only the new configuration method is accepted; you cannot later restore the old configuration.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; Media Termination Address.</p>
Displaying the CTL File for the Phone Proxy	<p>The Cisco Phone Proxy feature includes the <b>show ctl-file</b> command, which shows the contents of the CTL file used by the phone proxy. Using the <b>show ctl-file</b> command is useful for debugging when configuring the phone proxy instance.</p> <p>This command is not supported in ASDM.</p>
Clearing Secure-phone Entries from the Phone Proxy Database	<p>The Cisco Phone Proxy feature includes the <b>clear phone-proxy secure-phones</b> command, which clears the secure-phone entries in the phone proxy database. Because secure IP phones always request a CTL file upon bootup, the phone proxy creates a database that marks the IP phones as secure. The entries in the secure phone database are removed after a specified configured timeout (via the <b>timeout secure-phones</b> command). Alternatively, you can use the <b>clear phone-proxy secure-phones</b> command to clear the phone proxy database without waiting for the configured timeout.</p> <p>This command is not supported in ASDM.</p>

Table 3 New Features for ASA Version 8.2(1) (continued)

Feature	Description
H.239 Message Support in H.323 Application Inspection	<p>In this release, the security appliance supports the H.239 standard as part of H.323 application inspection. H.239 is a standard that provides the ability for H.300 series endpoints to open an additional video channel in a single call. In a call, an endpoint (such as a video phone), sends a channel for video and a channel for data presentation. The H.239 negotiation occurs on the H.245 channel. The security appliance opens a pinhole for the additional media channel. The endpoints use open logical channel message (OLC) to signal a new channel creation. The message extension is part of H.245 version 13. The decoding and encoding of the telepresentation session is enabled by default. H.239 encoding and decoding is preformed by ASN.1 coder.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard &gt; Rule Actions &gt; Protocol Inspection &gt; H.323 H.225. Click <b>Configure</b> and then choose the H.323 Inspect Map.</p>
Processing H.323 Endpoints When the Endpoints Do Not Send OLCAck	<p>H.323 application inspection has been enhanced to process common H.323 endpoints. The enhancement affects endpoints using the extendedVideoCapability OLC with the H.239 protocol identifier. Even when an H.323 endpoint does not send OLCAck after receiving an OLC message from a peer, the security appliance propagates OLC media proposal information into the media array and opens a pinhole for the media channel (extendedVideoCapability).</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add Service Policy Rule Wizard &gt; Rule Actions &gt; Protocol Inspection &gt; H.323 H.225.</p>
IPv6 in transparent firewall mode	<p>Transparent firewall mode now participates in IPv6 routing. Prior to this release, the security appliance could not pass IPv6 traffic in transparent mode. You can now configure an IPv6 management address in transparent mode, create IPv6 access lists, and configure other IPv6 features; the security appliance recognizes and passes IPv6 packets.</p> <p>All IPv6 functionality is supported unless specifically noted.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Management Access &gt; Management IP Address.</p>
Botnet Traffic Filter	<p>Malware is malicious software that is installed on an unknowing host. Malware that attempts network activity such as sending private data (passwords, credit card numbers, key strokes, or proprietary data) can be detected by the Botnet Traffic Filter when the malware starts a connection to a known bad IP address. The Botnet Traffic Filter checks incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity. You can also supplement the dynamic database with a static database by entering IP addresses or domain names in a local “blacklist” or “whitelist.”</p> <p><b>Note</b> This feature requires the Botnet Traffic Filter license. See the following licensing document for more information:</p> <p><a href="http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html">http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html</a></p> <p>The following commands were introduced: <b>dynamic-filter</b> commands (various), and the <b>inspect dns dynamic-filter-snoop</b> keyword.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Botnet Traffic Filter.</p>
AIP SSC card for the ASA 5505	<p>The AIP SSC offers IPS for the ASA 5505 security appliance. Note that the AIP SSM does not support virtual sensors. The following commands were introduced: <b>allow-ssc-mgmt</b>, <b>hw-module module ip</b>, and <b>hw-module module allow-ip</b>.</p> <p>In ASDM, see Configuration &gt; Device Setup &gt; SSC Setup and Configuration &gt; IPS.</p>

**Table 3** *New Features for ASA Version 8.2(1) (continued)*

Feature	Description
IPv6 support for IPS	You can now send IPv6 traffic to the AIP SSM or SSC when your traffic class uses the <b>match any</b> command, and the policy map specifies the <b>ips</b> command.  In ASDM, see Configuration > Firewall > Service Policy Rules.
<b>Management Features</b>	
SNMP version 3 and encryption	This release provides DES, 3DES, or AES encryption and support for SNMP Version 3, the most secure form of the supported security models. This version allows you to configure authentication characteristics by using the User-based Security Model (USM).  The following commands were introduced: <ul style="list-style-type: none"> <li>• <b>show snmp engineid</b></li> <li>• <b>show snmp group</b></li> <li>• <b>show snmp-server group</b></li> <li>• <b>show snmp-server user</b></li> <li>• <b>snmp-server group</b></li> <li>• <b>snmp-server user</b></li> </ul> The following command was modified: <ul style="list-style-type: none"> <li>• <b>snmp-server host</b></li> </ul> In ASDM, see Configuration > Device Management > Management Access > SNMP.
<b>Routing Features</b>	
Multicast NAT	The security appliance now offers Multicast NAT support for group addresses.
<b>Troubleshooting Features</b>	
Coredump functionality	A coredump is a snapshot of the running program when the program has terminated abnormally. Coredumps are used to diagnose or debug errors and save a crash for later or off-site analysis. Cisco TAC may request that users enable the coredump feature to troubleshoot application or system crashes on the security appliance.  To enable coredump, see the <b>coredump enable</b> command.

## New Features in Version 8.1(2)

Table 4 lists the new features for Version 8.1(2).



### Note

Version 8.1(x) is only supported on the Cisco ASA 5580 adaptive security appliance.

Table 4 New Features for ASA Version 8.1(2)

Feature	Description
<b>Remote Access Features</b>	
Auto Sign-On with Smart Tunnels for IE	<p>This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it is not supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature.</p> <p>Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host.</p> <p>To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature is not supported with Dynamic Access Policy.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; ACL Manager.</p>
Entrust Certificate Provisioning	<p>ASDM 6.1.3 (which lets you manage security appliances running Versions 8.0x and 8.1x) includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Certificate Management &gt; Identity Certificates &gt; Enroll ASA SSL VPN head-end with Entrust.</p>
Extended Time for User Reauthentication on IKE Rekey	<p>You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Certificate Management &gt; Identity Certificates.</p>
Persistent IPsec Tunneled Flows	<p>With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a hardware client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the <b>sysopt connection preserve-vpn-flows</b> command. This option is disabled by default.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; System Options. Check the <b>Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)</b> checkbox to enable persistent IPsec tunneled flows.</p>
Show Active Directory Groups	<p>The CLI command <b>show ad-groups</b> was added to list the active directory groups. ASDM Dynamic Access Policy uses this command to present the administrator with a list of MS AD groups that can be used to define the VPN policy.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Dynamic Access Policies &gt; Add/Edit DAP &gt; Add/Edit AAA Attribute.</p>

**Table 4**      ***New Features for ASA Version 8.1(2) (continued)***

<b>Feature</b>	<b>Description</b>
Smart Tunnel over Mac OS	<p>Smart tunnels now support Mac OS.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Smart Tunnels.</p>
<b>Firewall Features</b>	
NetFlow Filtering	<p>You can filter NetFlow events based on traffic and event-type, and then send records to different collectors. For example, you can log all flow-create events to one collector, but log flow-denied events to a different collector. See the <b>flow-export event-type</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; NetFlow.</p>
NetFlow Delay Flow Creation Event	<p>For short-lived flows, NetFlow collecting devices benefit from processing a single event as opposed to seeing two events: flow creation and teardown. You can now configure a delay before sending the flow creation event. If the flow is torn down before the timer expires, only the flow teardown event will be sent. See the <b>flow-export delay flow-create</b> command.</p> <p><b>Note</b>    The teardown event includes all information regarding the flow; there is no loss of information.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Logging &gt; NetFlow.</p>
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as the security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the <b>shape</b> command.</p> <p>See also the <b>crypto ipsec security-association replay</b> command, which lets you configure the IPsec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPsec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p>

**Table 4**      **New Features for ASA Version 8.1(2) (continued)**

Feature	Description
TCP Normalization Enhancements	<p>You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets.</p> <ul style="list-style-type: none"> <li>• TCP invalid ACK check (the <b>invalid-ack</b> command)</li> <li>• TCP packet sequence past window check (the <b>seq-past-window</b> command)</li> <li>• TCP SYN-ACK with data check (the <b>synack-data</b> command)</li> </ul> <p>You can also set the TCP out-of-order packet buffer timeout (the <b>queue</b> command <b>timeout</b> keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value.</p> <p>The default action for packets that exceed MSS has changed from drop to allow (the <b>exceed-mss</b> command).</p> <p>The following non-configurable actions have changed from drop to clear for these packet types:</p> <ul style="list-style-type: none"> <li>• Bad option length in TCP</li> <li>• TCP Window scale on non-SYN</li> <li>• Bad TCP window scale value</li> <li>• Bad TCP SACK ALLOW option</li> </ul> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; TCP Maps.</p>
TCP Intercept statistics	<p>You can enable collection for TCP Intercept statistics using the <b>threat-detection statistics tcp-intercept</b> command, and view them using the <b>show threat-detection statistics</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Threat Detection.</p>
Threat detection shun timeout	<p>You can now configure the shun timeout for threat detection using the <b>threat-detection scanning-threat shun duration</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Threat Detection.</p>
Threat detection host statistics fine tuning	<p>You can now reduce the amount of host statistics collected, thus reducing the system impact of this feature, by using the <b>threat-detection statistics host number-of-rate</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Threat Detection.</p>
<b>Platform Features</b>	
Increased VLANs	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.

## New Features in Version 8.1(1)

Table 5 lists the new features for Version 8.1(1).



### Note

Version 8.1(x) is only supported on the Cisco ASA 5580 adaptive security appliance.

**Table 5** *New Features for ASA Version 8.1(1)*

Feature	Description
Introduction of the Cisco ASA 5580	<p>The Cisco ASA 5580 comes in two models:</p> <ul style="list-style-type: none"> <li>The ASA 5580-20 delivers 5 Gigabits per second of TCP traffic and UDP performance is even greater. Many features in the system have been made multi-core capable to achieve this high throughput. In addition the system delivers greater than 60,000 TCP connections per second and supports up to 1 million connections.</li> <li>The ASA 5580-40 will deliver 10 Gigabits per second of TCP traffic and similar to ASA 5580-20 the UDP performance will be even greater. The ASA 5580-40 delivers greater than 120,000 TCP connections per second and up to 2 million connections in total.</li> </ul> <p>In ASDM, see Home &gt; System Resource Status and Home &gt; Device Information &gt; Environment Status.</p>
NetFlow	<p>The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. For detailed information on this feature and the new CLI commands, see the <i>Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide</i>.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Logging &gt; Netflow.</p>
Timeout for SIP Provisional Media	<p>You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Global Timeouts.</p>
Details about the activation key	<p>You can now view the permanent and temporary activation keys with their enabled features, including all previously installed temporary keys and their expiration dates using the <b>show activation key detail</b> command.</p> <p>In ASDM in single context mode, see Configuration &gt; Device Management &gt; System Image/Configuration &gt; Activation Key. In ASDM in multiple context mode, see System &gt; Configuration &gt; Device Management &gt; Activation Key.</p>

## New Features in Version 8.0(5)

Table 6 lists the new features for Version 8.0(5).



**Note**

Version 8.0(5) is not supported on the PIX security appliance.

**Table 6** *New Features for ASA Version 8.0(5)*

Feature	Description
<b>Remote Access Features</b>	
Scalable Solutions for Waiting-to-Resume VPN Sessions	<p>An administrator can now keep track of the number of users in the active state and can look at the statistics. The sessions that have been inactive for the longest time are marked as idle (and are automatically logged off) so that license capacity is not reached and new users can log in</p> <p>The following ASDM screen was modified: Monitoring &gt; VPN &gt; VPN Statistics &gt; Sessions.</p>

Table 6 New Features for ASA Version 8.0(5) (continued)

Feature	Description
<b>Application Inspection Features</b>	
Enabling Call Set up Between H.323 Endpoints	<p>You can enable call setup between H.323 endpoints when the Gatekeeper is inside the network. The security appliance includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages.</p> <p>Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the security appliance opens a pinhole through source IP address/port 0/0. By default, this option is disabled.</p> <p>The following commands were introduced: <b>ras-enhancement enable</b>, <b>show running-configuration ras-enhancement</b>, <b>clear configure ras-enhancement</b>.</p> <p>The following ASDM screen was modified: Configuration &gt; Firewall &gt; Objects &gt; Inspect Maps &gt; H.323 &gt; Details &gt; State Checking.</p>
<b>Interface Features</b>	
In multiple context mode, auto-generated MAC addresses now use a user-configurable prefix, and other enhancements	<p>The MAC address format was changed to allow use of a prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair.</p> <p>The MAC addresses are also now persistent across reloads.</p> <p>The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2.</p> <p>The following command was modified: <b>mac-address auto prefix prefix</b>.</p> <p>The following ASDM screen was modified: Configuration &gt; Context Management &gt; Security Contexts.</p>
<b>High Availability Features</b>	
No notifications when interfaces are brought up or brought down during a switchover event	To distinguish between link up/down transitions during normal operation from link up/down transitions during failover, no link up/link down traps are sent during a failover. Also, no syslog messages about link up/down transitions during failover are sent.
<b>Routing Features</b>	
DHCP RFC compatibility (rfc3011, rfc3527) to resolve routing issues	<p>This enhancement introduces security appliance support for DHCP RFCs 3011 (The IPv4 Subnet Selection Option) and 3527 (Link Selection Sub-option for the Relay Agent Information Option). For each DHCP server that is configured using the <b>dhcp-server</b> command, you can now configure the security appliance to send the <b>subnet-selection</b> option, and the <b>link-selection</b> option or neither.</p> <p>The following ASDM screen was modified: Remote Access VPN &gt; Network Access &gt; IPsec connection profiles &gt; Add/Edit.</p>

## New Features in Version 8.0(4)



### Note

These features are not available in Version 8.1(1). See the [“New Features in Version 8.1\(2\)”](#) section on page 10 for many, but not all, of these features. For example, Unified Communications features are not supported in 8.1(2) or lower.

Table 7 lists the new features for Version 8.0(4).

**Table 7** *New Features for ASA and PIX Version 8.0(4)*

Feature	Description
<b>Unified Communications Features<sup>1</sup></b>	
Phone Proxy	<p>Phone Proxy functionality is supported. ASA Phone Proxy provides similar features to those of the Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced security. The ASA Phone Proxy has the following key features:</p> <ul style="list-style-type: none"> <li>• Secures remote IP phones by forcing the phones to encrypt signaling and media</li> <li>• Performs certificate-based authentication with remote IP phones</li> <li>• Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified Mobility Advantage servers</li> <li>• Terminates SRTP and initiates RTP/SRTP to the called party</li> </ul> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; Phone Proxy.</p>
Mobility Proxy	<p>Secure connectivity (mobility proxy) between Cisco Unified Mobility Advantage clients and servers is supported.</p> <p>Cisco Unified Mobility Advantage solutions include the Cisco Unified Mobile Communicator, an easy-to-use software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage server. The mobility solution streamlines the communication experience, enabling real-time collaboration across the enterprise.</p> <p>The ASA in this solution delivers inspection for the MMP (formerly called OLWP) protocol, the proprietary protocol between Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage. The ASA also acts as a TLS proxy, terminating and reoriginating the TLS signaling between the Cisco Unified Mobile Communicator and Cisco Unified Mobility Advantage.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; TLS Proxy.</p>
Presence Federation Proxy	<p>Secure connectivity (presence federation proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers is supported. With the Presence solution, businesses can securely connect their Cisco Unified Presence clients back to their enterprise networks, or share Presence information between Presence servers in different enterprises.</p> <p>The ASA delivers functionality to enable Presence for Internet and intra-enterprise communications. An SSL-enabled Cisco Unified Presence client can establish an SSL connection to the Presence Server. The ASA enables SSL connectivity between server to server communication including third-party Presence servers communicating with Cisco Unified Presence servers. Enterprises share Presence information, and can use IM applications. The ASA inspects SIP messages between the servers.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; Protocol Inspection or Configuration &gt; Firewall &gt; Advanced &gt; Encrypted Traffic Inspection &gt; TLS Proxy &gt; Add &gt; Client Configuration.</p>
<b>Remote Access Features</b>	

**Table 7**      **New Features for ASA and PIX Version 8.0(4) (continued)**

Feature	Description
Auto Sign-On with Smart Tunnels for IE <sup>1</sup>	<p>This feature lets you enable the replacement of logon credentials for WININET connections. Most Microsoft applications use WININET, including Internet Explorer. Mozilla Firefox does not, so it is not supported by this feature. It also supports HTTP-based authentication, therefore form-based authentication does not work with this feature.</p> <p>Credentials are statically associated to destination hosts, not services, so if initial credentials are wrong, they cannot be dynamically corrected during runtime. Also, because of the association with destinations hosts, providing support for an auto sign-on enabled host may not be desirable if you want to deny access to some of the services on that host.</p> <p>To configure a group auto sign-on for smart tunnels, you create a global list of auto sign-on sites, then assign the list to group policies or user names. This feature is not supported with Dynamic Access Policy.</p> <p>In ASDM, see Firewall &gt; Advanced &gt; ACL Manager.</p>
Entrust Certificate Provisioning <sup>1</sup>	<p>ASDM includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Certificate Management &gt; Identity Certificates. Click <b>Enroll ASA SSL VPN head-end with Entrust</b>.</p>
Extended Time for User Reauthentication on IKE Rekey	<p>You can configure the security appliance to give remote users more time to enter their credentials on a Phase 1 SA rekey. Previously, when reauthenticate-on-rekey was configured for IKE tunnels and a phase 1 rekey occurred, the security appliance prompted the user to authenticate and only gave the user approximately 2 minutes to enter their credentials. If the user did not enter their credentials in that 2 minute window, the tunnel would be terminated. With this new feature enabled, users now have more time to enter credentials before the tunnel drops. The total amount of time is the difference between the new Phase 1 SA being established, when the rekey actually takes place, and the old Phase 1 SA expiring. With default Phase 1 rekey times set, the difference is roughly 3 hours, or about 15% of the rekey interval.</p> <p>In ASDM, see Configuration &gt; Device Management &gt; Certificate Management &gt; Identity Certificates.</p>
Persistent IPsec Tunneled Flows	<p>With the persistent IPsec tunneled flows feature enabled, the security appliance preserves and resumes stateful (TCP) tunneled flows after the tunnel drops, then recovers. All other flows are dropped when the tunnel drops and must reestablish when a new tunnel comes up. Preserving the TCP flows allows some older or sensitive applications to keep working through a short-lived tunnel drop. This feature supports IPsec LAN-to-LAN tunnels and Network Extension Mode tunnels from a Hardware Client. It does not support IPsec or AnyConnect/SSL VPN remote access tunnels. See the <b>[no] sysopt connection preserve-vpn-flows</b> command. This option is disabled by default.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Advanced &gt; IPsec &gt; System Options. Check the <b>Preserve stateful VPN flows when the tunnel drops for Network Extension Mode (NEM)</b> checkbox to enable persistent IPsec tunneled flows.</p>
Show Active Directory Groups	<p>The CLI command <b>show ad-groups</b> was added to list the active directory groups. ASDM Dynamic Access Policy uses this command to present the administrator with a list of MS AD groups that can be used to define the VPN policy.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Dynamic Access Policies &gt; Add/Edit DAP &gt; Add/Edit AAA Attribute.</p>

**Table 7** *New Features for ASA and PIX Version 8.0(4) (continued)*

Feature	Description
Smart Tunnel over Mac OS <sup>1</sup>	<p>Smart tunnels now support Mac OS.</p> <p>In ASDM, see Configuration &gt; Remote Access VPN &gt; Clientless SSL VPN Access &gt; Portal &gt; Smart Tunnels.</p>
<b>Firewall Features</b>	
QoS Traffic Shaping	<p>If you have a device that transmits packets at a high speed, such as the security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the <b>shape</b> command. See also the <b>crypto ipsec security-association replay</b> command, which lets you configure the IPsec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPsec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms.</p> <p>In ASDM, see Configuration &gt; Firewall &gt; Security Policy &gt; Service Policy Rules &gt; Add/Edit Service Policy Rule &gt; Rule Actions &gt; QoS. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p>
TCP Normalization Enhancements	<p>You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets.</p> <ul style="list-style-type: none"> <li>• TCP invalid ACK check (the <b>invalid-ack</b> command)</li> <li>• TCP packet sequence past window check (the <b>seq-past-window</b> command)</li> <li>• TCP SYN-ACK with data check (the <b>synack-data</b> command)</li> </ul> <p>You can also set the TCP out-of-order packet buffer timeout (the <b>queue</b> command <b>timeout</b> keyword). Previously, the timeout was 4 seconds. You can now set the timeout to another value.</p> <p>The default action for packets that exceed MSS has changed from drop to allow (the <b>exceed-mss</b> command).</p> <p>The following non-configurable actions have changed from drop to clear for these packet types:</p> <ul style="list-style-type: none"> <li>• Bad option length in TCP</li> <li>• TCP Window scale on non-SYN</li> <li>• Bad TCP window scale value</li> <li>• Bad TCP SACK ALLOW option</li> </ul> <p>In ASDM, see Configuration &gt; Firewall &gt; Objects &gt; TCP Maps.</p>
TCP Intercept statistics	<p>You can enable collection for TCP Intercept statistics using the <b>threat-detection statistics tcp-intercept</b> command, and view them using the <b>show threat-detection statistics</b> command.</p> <p>In ASDM 6.1(5) and later, see Configuration &gt; Firewall &gt; Threat Detection. This command was not supported in ASDM 6.1(3).</p>
Threat detection shun timeout	<p>You can now configure the shun timeout for threat detection using the <b>threat-detection scanning-threat shun duration</b> command.</p> <p>In ASDM 6.1(5) and later, see Configuration &gt; Firewall &gt; Threat Detection. This command was not supported in ASDM 6.1(3).</p>

**Table 7**      **New Features for ASA and PIX Version 8.0(4) (continued)**

Feature	Description
Timeout for SIP Provisional Media	You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.  In ASDM, see Configuration > Firewall > Advanced > Global Timeouts.
<b>Platform Features</b>	
Native VLAN support for the ASA 5505	You can now include the native VLAN in an ASA 5505 trunk port using the <b>switchport trunk native vlan</b> command.  In ASDM, see Configuration > Device Setup > Interfaces > Switch Ports > Edit dialog.
SNMP support for unnamed interfaces	Previously, SNMP only provided information about interfaces that were configured using the <b>nameif</b> command. For example, SNMP only sent traps and performed walks on the IF MIB and IP MIB for interfaces that were named. Because the ASA 5505 has both unnamed switch ports and named VLAN interfaces, SNMP was enhanced to show information about all physical interfaces and logical interfaces; a <b>nameif</b> command is no longer required to display the interfaces using SNMP. These changes affect all models, and not just the ASA 5505.

1. This feature is not supported on the PIX security appliance.

## New Features in Version 8.0(3)

[Table 8](#) lists the new features for Version 8.0(3).

**Table 8**      **New Features for ASA and PIX Version 8.0(3)**

Feature	Description
AnyConnect RSA SoftID API Integration	Provides support for AnyConnect VPN clients to communicate directly with RSA SoftID for obtaining user token codes. It also provides the ability to specify SoftID message support for a connection profile (tunnel group), and the ability to configure SDI messages on the security appliance that match SDI messages received through a RADIUS proxy. This feature ensures the prompts displayed to the remote client user are appropriate for the action required during authentication and the AnyConnect client responds successfully to authentication challenges.
IP Address Reuse Delay	Delays the reuse of an IP address after it has been returned to the IP address pool. Increasing the delay prevents problems the security appliance may experience when an IP address is returned to the pool and reassigned quickly.  In ASDM, see Configure > Remote Access VPN > Network (Client) Access > Address Assignment > Assignment Policy.
WAAS Inspection	Added support for Wide Area Application Services (WAAS) inspection. WAAS gives branch and remote offices LAN-like access to WAN and MAN services. See the <b>inspect waas</b> command.  In ASDM, see Configuration > Firewall > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > Protocol Inspection.
DNS Guard Enhancement	Added an option to enable or disable DNS guard. When enabled, this feature allows only one DNS response back from a DNS request.  In ASDM, see Configuration > Firewall > Objects > Inspect maps > DNS.

**Table 8** *New Features for ASA and PIX Version 8.0(3) (continued)*

Feature	Description
Fully Qualified Domain Name Support Enhancement	Added option in the <b>redirect-fqdn</b> command to send either the fully qualified domain name (FQDN) or the IP address to the client in a VPN load balancing cluster. In ASDM, see Configuration > Device Management > High Availability > VPN Load Balancing or Configuration > Remote Access VPN > Load Balancing.
Clientless SSL VPN Caching Static Content Enhancement	Added a new command to allow clientless SSL VPN users to cache the static content, <b>cache-static-content</b> enable. In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Cache.
DHCP Client Enhancements	Added two new items for the DHCP client. The first option configures DHCP Option 61 to send either the MAC or the string "cisco-<MAC>-<interface>-<hostname>", where < > represents the corresponding values as the client identifier. The second option either sets or clears the broadcast flag for DHCP discover when the DHCP request has the broadcast flag enabled. In ASDM, see Configuration > Device Management > DHCP > DHCP Server; then click on Advanced button.
ASDM Banner	When you start ASDM, new banner text appears in a dialog box with the option to continue or disconnect. See the <b>banner asdm</b> command. In ASDM, see Configuration > Properties > Device Administration > Banner.
ESMTP Enhancement	Added an option for Extended Simple Mail Transfer Protocol (ESMTP) inspection to work over Transport Layer Security (TLS). In ASDM, see Configuration > Firewall > Objects > Inspect Map > ESMTP.
Smart Card Removal Enhancement	Added option in the VPN group policy to specify whether tunnels stay connected or not when the Smart Card is removed. Previously, the tunnels were always disconnected. See the <b>smartcard-removal-disconnect</b> command. In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Internal/External Group Policies > More Options.

## New Features in Version 8.0(2)

Table 1-9 lists the new features for Version 8.0(2).



**Note**

There was no ASA or PIX 8.0(1) release.

**Table 1-9** *New Features for ASA and PIX Version 8.0(2)*

ASA Feature Type	Feature	Description
<b>General Features</b>		
Routing	EIGRP routing	The security appliance supports EIGRP or EIGRP stub routing.

**Table 1-9**      **New Features for ASA and PIX Version 8.0(2) (continued)**

<b>ASA Feature Type</b>	<b>Feature</b>	<b>Description</b>
High Availability	Remote command execution in Failover pairs	You can execute commands on the peer unit in a failover pair without having to connect directly to the peer. This works for both Active/Standby and Active/Active failover.
	CSM configuration rollback support	Adds support for the Cisco Security Manager configuration rollback feature in failover configurations.
	Failover pair Auto Update support	You can use an Auto Update server to update the platform image and configuration in failover pairs.
	Stateful Failover for SIP signaling	SIP media and signaling connections are replicated to the standby unit.
	Redundant interfaces	A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to eight redundant interface pairs.
SSMs	Password reset	You can reset the password on the SSM hardware module.
<b>VPN Features<sup>1</sup></b>		
Authentication Enhancements	Combined certificate and username/password login	An administrator requires a username and password in addition to a certificate for login to SSL VPN connections.
	Internal domain username/password	Provides a password for access to internal resources for users who log in with credentials other than a domain username and password, for example, with a one-time password. This is a password in addition to the one a user enters when logging in.
	Generic LDAP support	This includes OpenLDAP and Novell LDAP. Expands LDAP support available for authentication and authorization.
	Onscreen keyboard	The security appliance includes an onscreen keyboard option for the login page and subsequent authentication requests for internal resources. This provides additional protection against software-based keystroke loggers by requiring a user to use a mouse to click characters in an onscreen keyboard for authentication, rather than entering the characters on a physical keyboard.
	SAML SSO verified with RSA Access Manager	The security appliance supports Security Assertion Markup Language (SAML) protocol for Single Sign On (SSO) with RSA Access Manager (Cleartrust and Federated Identity Manager).
	NTLMv2	Version 8.0(2) adds support for NTLMv2 authentication for Windows-based clients.
Certificates	Local certificate authority	Provides a certificate authority on the security appliance for use with SSL VPN connections, both browser- and client-based.
	OCSP CRL	Provides OCSP revocation checking for SSL VPN.

**Table 1-9** *New Features for ASA and PIX Version 8.0(2) (continued)*

<b>ASA Feature Type</b>	<b>Feature</b>	<b>Description</b>
Cisco Secure Desktop	Host Scan	<p>As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connection, the remote computer scans for a greatly expanded collection of antivirus and antispymware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the security appliance. The security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP).</p> <p>With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements.</p> <p>Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.</p>
	Simplified prelogin assessment and periodic checks	<p>Cisco Secure Desktop now simplifies the configuration of prelogin and periodic checks to perform on remote Microsoft Windows computers. Cisco Secure Desktop lets you add, modify, remove, and place conditions on endpoint checking criteria using a simplified, graphical view of the checks. As you use this graphical view to configure sequences of checks, link them to branches, deny logins, and assign endpoint profiles, Cisco Secure Desktop Manager records the changes to an XML file. You can configure the security appliance to use returned results in combination with many other types of data, such as the connection type and multiple group settings, to generate and apply a DAP to the session.</p>
Access Policies	Dynamic access policies (DAP)	<p>VPN gateways operate in dynamic environments. Multiple variables can affect each VPN connection, for example, intranet configurations that frequently change, the various roles each user may inhabit within an organization, and logins from remote access sites with different configurations and levels of security. The task of authorizing users is much more complicated in a VPN environment than it is in a network with a static configuration.</p> <p>Dynamic Access Policies (DAP) on the security appliance let you configure authorization that addresses these many variables. You create a dynamic access policy by setting a collection of access control attributes that you associate with a specific user tunnel or session. These attributes address issues of multiple group membership and endpoint security. That is, the security appliance grants access to a particular user for a particular session based on the policies you define. It generates a DAP at the time the user connects by selecting and/or aggregating attributes from one or more DAP records. It selects these DAP records based on the endpoint security information of the remote device and the AAA authorization information for the authenticated user. It then applies the DAP record to the user tunnel or session.</p>
	Administrator differentiation	<p>Lets you differentiate regular remote access users and administrative users under the same database, either RADIUS or LDAP. You can create and restrict access to the console via various methods (TELNET and SSH, for example) to administrators only. It is based on the IETF RADIUS service-type attribute.</p>

**Table 1-9**      **New Features for ASA and PIX Version 8.0(2) (continued)**

<b>ASA Feature Type</b>	<b>Feature</b>	<b>Description</b>
Platform Enhancements	VLAN support for remote access VPN connections	Provides support for mapping (tagging) of client traffic at the group or user level. This feature is compatible with clientless as well as IPsec and SSL tunnel-based connections.
	VPN load balancing for the ASA 5510	Extends load balancing support to ASA 5510 security appliances that have a Security Plus license.
	Crypto conditional debug	Lets users debug an IPsec tunnel on the basis of predefined crypto conditions such as the peer IP address, connection-ID of a crypto engine, and security parameter index (SPI). By limiting debug messages to specific IPsec operations and reducing the amount of debug output, you can better troubleshoot the security appliance with a large number of tunnels.
Browser-based SSL VPN Features	Enhanced portal design	Version 8.0(2) includes an enhanced end user interface that is more cleanly organized and visually appealing.
	Customization	Supports administrator-defined customization of all user-visible content.
	Support for FTP	You can provide file access via FTP in addition to CIFS (Windows-based).
	Plugin applets	Version 8.0(2) adds a framework for supporting TCP-based applications without requiring a pre-installed client application. Java applets let users access these applications from the browser-enabled SSL VPN portal. Initial support is for TELNET, SSH, RDP, and VNC.
	Smart tunnels	<p>A smart tunnel is a connection between an application and a remote site, using a browser-based SSL VPN session with the security appliance as the pathway. Version 8.0(2) lets you identify the applications to which you want to grant smart tunnel access, and lets you specify the path to the application and the SHA-1 hash of its checksum to check before granting it access. Lotus SameTime and Microsoft Outlook Express are examples of applications to which you might want to grant smart tunnel access.</p> <p>The remote host originating the smart tunnel connection must be running Microsoft Windows Vista, Windows XP, or Windows 2000, and the browser must be enabled with Java, Microsoft ActiveX, or both.</p>
	RSS newsfeed	Administrators can populate the clientless portal with RSS newsfeed information, which lets company news or other information display on a user screen.

Table 1-9 New Features for ASA and PIX Version 8.0(2) (continued)

ASA Feature Type	Feature	Description
Browser-based SSL VPN Features (continued)	Personal bookmark support	Users can define their own bookmarks. These bookmarks are stored on a file server.
	Transformation enhancements	Adds support for several complex forms of web content over clientless connections, including Adobe flash and Java WebStart.
	IPv6	Allows access to IPv6 resources over a public IPv4 connection.
	Web folders	Lets browser-based SSL VPN users connecting from Windows operating systems browse shared file systems and perform the following operations: view folders, view folder and file properties, create, move, copy, copy from the local host to the remote host, copy from the remote host to the local host, and delete. Internet Explorer indicates when a web folder is accessible. Accessing this folder launches another window, providing a view of the shared folder, on which users can perform web folder functions, assuming the properties of the folders and documents permit them.
	Microsoft Sharepoint enhancement	Extends Web Access support for Microsoft Sharepoint, integrating Microsoft Office applications available on the machine with the browser to view, change, and save documents shared on a server. Version 8.0(2) supports Windows Sharepoint Services 2.0 in Windows Server 2003.
HTTP Proxy	PAC support	Lets you specify the URL of a proxy autoconfiguration file (PAC) to download to the browser. Once downloaded, the PAC file uses a JavaScript function to identify a proxy for each URL.
HTTPS Proxy	Proxy exclusion list	Lets you configure a list of URLs to exclude from the HTTP requests the security appliance can send to an external proxy server.
NAC	SSL VPN tunnel support	The security appliance provides NAC posture validation of endpoints that establish AnyConnect VPN client sessions.
	Support for audit services	You can configure the security appliance to pass the IP address of the client to an optional audit server if the client does not respond to a posture validation request. The audit server uses the host IP address to challenge the host directly to assess its health. For example, it might challenge the host to determine whether its virus checking software is active and up-to-date. After the audit server completes its interaction with the remote host, it passes a token to the posture validation server, indicating the health of the remote host. If the token indicates the remote host is healthy, the posture validation server sends a network access policy to the security appliance for application to the traffic on the tunnel.

Table 1-9 New Features for ASA and PIX Version 8.0(2) (continued)

ASA Feature Type	Feature	Description
<b>Firewall Features</b>		
Application Inspection	Modular policy framework inspect class map	Traffic can match one of multiple match commands in an inspect class map; formerly, traffic had to match all match commands in a class map to match the class map.
	AIC for encrypted streams and AIC Arch changes	Provides HTTP inspection into TLS, which allows AIC/MPF inspection in WebVPN HTTP and HTTPS streams.
	TLS Proxy for SCCP and SIP <sup>2</sup>	Enables inspection of encrypted traffic. Implementations include SSL encrypted VoIP signaling, namely Skinny and SIP, interacting with the Cisco CallManager.
	SIP enhancements for CCM	Improves interoperability with CCM 5.0 and 6.x with respect to signaling pinholes.
	Full RTSP PAT support	Provides TCP fragment reassembly support, a scalable parsing routine on RTSP, and security enhancements that protect RTSP traffic.
Access Lists	Enhanced service object group	Lets you configure a service object group that contains a mix of TCP services, UDP services, ICMP-type services, and any protocol. It removes the need for a specific ICMP-type object group and protocol object group. The enhanced service object group also specifies both source and destination services. The access list CLI now supports this behavior.
	Ability to rename access list	Lets you rename an access list.
	Live access list hit counts	Includes the hit count for ACEs from multiple access lists. The hit count value represents how many times traffic hits a particular access rule.
Attack Prevention	Set connection limits for management traffic to the security appliance	For a Layer 3/4 management class map, you can specify the <b>set connection</b> command.
	Threat detection	You can enable basic threat detection and scanning threat detection to monitor attacks such as DoS attacks and scanning attacks. For scanning attacks, you can automatically shun attacking hosts. You can also enable scan threat statistics to monitor both valid and invalid traffic for hosts, ports, protocols, and access lists.
NAT	Transparent firewall NAT support	You can configure NAT for a transparent firewall.
IPS	Virtual IPS sensors with the AIP SSM	The AIP SSM running IPS software Version 6.0 and above can run multiple virtual sensors, which means you can configure multiple security policies on the AIP SSM. You can assign each context or single mode security appliance to one or more virtual sensors, or you can assign multiple security contexts to the same virtual sensor. See the IPS documentation for more information about virtual sensors, including the maximum number of sensors supported.
Logging	Secure logging	You can enable secure connections to the syslog server using SSL or TLS with TCP, and encrypted system log message content. Not supported on the PIX series security appliance.
IPv6	IPv6 support for SIP	The SIP inspection engine supports IPv6 addresses. IPv6 addresses can be used in URLs, in the Via header field, and SDP fields.

1. Clientless SSL VPN features are not supported on the PIX security appliance.
2. TLS proxy is not supported on the PIX security appliance.

## Upgrading the Security Appliance

This section describes how to upgrade the security appliance to a new ASDM release. If you have a Cisco.com login, you can obtain ASDM from one of the following websites:

<http://www.cisco.com/cgi-bin/tablebuild.pl/asa>

or

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix>



**Note**

If you are upgrading from PIX Version 6.3, first upgrade to Version 7.0 according to *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*. Then upgrade PDM to ASDM according to the ASDM 5.0 release notes.

If you have a previous release of ASDM on your security appliance and want to upgrade to the latest release, you can do so from within ASDM. We recommend that you upgrade the ASDM image before the platform image. ASDM is backward compatible, so you can upgrade the platform image using the new ASDM; you cannot use an old ASDM with a new platform image.



**Note**

If the ASA or PIX is running a version earlier than 8.0, then ASA and ASDM must be upgraded at the same time as the ASA or PIX operating system using the existing version of ASDM. This should be compatible with the existing operating system. But, if ASA or PIX is running version 8.0 or later, then ASDM 6.2 is backward compatible and may be upgraded before the ASA or PIX operating system.

To upgrade ASDM, perform the following steps:

- 
- Step 1** Download the new ASDM image to your PC.  
Optionally, you can download a new platform image to your PC if the installed image is earlier than 8.0.
  - Step 2** Launch ASDM.
  - Step 3** From the Tools menu:
    - a. In ASDM 5.0 and 5.1, choose **Tools > Upload Image from Local PC**.
    - b. In ASDM 5.2, choose **Tools > Upgrade Software**.
    - c. In ASDM 6.0 or later, choose **Tools > Upload Software from Local Computer**.
  - Step 4** With ASDM selected, click **Browse Local** to select the new ASDM image.
  - Step 5** To specify the location in Flash memory where you want to install the new image, enter the directory path in the field or click **Browse Flash**.

If your security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.

If you have enough memory for both versions, you can specify a different name for the new version. If you need to revert to the old version, it is still in your Flash memory.

**Step 6** Click **Upload Image**.

When ASDM is finished uploading, the following message appears:

“ASDM Image is Uploaded to Flash Successfully.”

**Step 7** **For Version 5.x only:** If the new ASDM image has a different name than the old image, then you must configure the security appliance to load the new image. Use the **Configuration > Properties > Device Administration > Boot System/Configuration** pane.

**Step 8** If installing a new platform image, download the new platform image using the **Tools > Upgrade Software** tool with ASA or PIX selected.

If your security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.

**Step 9** If installing a new image, select ASA as the new image, and reload the security appliance using the **Tools > System Reload** tool.

Make sure to choose "Save the running configuration at time of reload".

**Step 10** To run the new ASDM image, exit ASDM and reconnect.

## Unsupported Commands

ASDM supports almost all commands available for the adaptive security appliance, 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 27](#)
- [Effects of Unsupported Commands, page 28](#)
- [Discontinuous Subnet Masks Not Supported, page 29](#)
- [Interactive User Commands Not Supported by the ASDM CLI Tool, page 29](#)

## Ignored and View-Only Commands

**Table 10** 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 10** *List of Unsupported Commands*

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used.
capture	Ignored.

**Table 10 List of Unsupported Commands (continued)**

Unsupported Commands	ASDM Behavior
<b>coredump</b>	Ignored. This can be configured only using the CLI.
<b>eject</b>	Unsupported.
<b>established</b>	Ignored.
<b>failover timeout</b>	Ignored.
<b>ipv6 nd prefix</b>	Unsupported.
<b>match-metric</b>	Ignored. This is a subcommand of route-map.
<b>match-interface</b>	Ignored. This is a subcommand of route-map.
<b>match route-type</b>	Ignored. This is a subcommand of route-map.
<b>pager</b>	Ignored.
<b>pim accept-register route-map</b>	Ignored. You can configure only the <b>list</b> option using ASDM.
<b>prefix-list</b>	Ignored if not used in an OSPF area.
<b>service-policy global</b>	Ignored if it uses a <b>match access-list</b> class. For example:  <pre>access-list myacl line 1 extended permit ip any any class-map mycm match access-list mycl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>
<b>set metric</b>	Ignored.
<b>sysopt nodnsalias</b>	Ignored.
<b>sysopt uauth allow-http-cache</b>	Ignored.
<b>terminal</b>	Ignored.
<b>tunnel-group name general-attributes dhcp-server</b>	The <b>dhcp-server</b> subcommand is unsupported. ASDM only allows one setting for all DHCP servers.

## 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.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.  
 Monitor-only mode allows access to the following functions:
  - The Monitoring area
  - The CLI tool (Tools > Command Line Interface), which lets you use the CLI commands

To exit Monitor-only mode, use the CLI tool or access the security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.



**Note** You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to three by your system administrator, which allows Monitor-only mode. For more information, choose Configuration > Device Management > Users/AAA > User Accounts and Configuration > Device Management > Users/AAA > AAA Access.

## 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. From the ASDM Tools menu, click **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 and Resolved Caveats for Software Version 6.2

The following section lists the open and resolved caveats in ASDM software Version 6.2.

- [Open Caveats for Software Version 6.2, page 30](#)
- [Resolved Caveats for Software Version 6.2.3, page 32](#)
- [Resolved Caveats for Software Version 6.2.1, page 33](#)

### Open Caveats for Software Version 6.2

Table 11 lists the open caveats for Version 6.2.

**Table 11**      **Open Caveats in Version 6.2**

Caveat ID	Description
CSCso05236	Pasting of address bar fails in some applications.
CSCso46258	Cannot load ASDM with read-only user when DAP configured.
CSCsx17471	Public Server: ASDM should pop up error message for Network Address.
CSCsx20290	Deleting 'default' res class won't create default class with default value.
CSCsx74139	Multiple session ASDM/IDM do not get change notification.
CSCsx77133	SSC Startup Wizard does not update content from IPS.
CSCsy07567	Navigating to help cause exception: no such entry help/mappingfiles/csdm.
CSCsy11676	Config in IPS>Launch Startup Wizard does not sync with IPS>Setup screen.
CSCsy24230	Global MTA throws error if configured to a named network object.
CSCsy25029	ASDM should not allow deleting a TLS proxy that is used by phone proxy.
CSCsy26853	Mac OS: ASDM Interfaces Screen buttons display "..." not Add/Edit/Delete.
CSCsy28021	Mac OS: Time Ranges, Services, Addresses show as separate panes.
CSCsy41640	Deleting certificate cannot be cancelled if done from a Manage dialog.
CSCsy44699	Cannot delete ACL - Config>Rem Acces>Net (Client) Acc>Adv>ACL Manager.
CSCsy46207	PIM multicast boundary config edit show blank screen.
CSCsy46539	PIM multicast boundary config - Hit Cancel still deletes a rule.
CSCsy47247	After deletion of subint from system context, blank screen is displayed.
CSCsy47315	IPv6: Unable to edit more than one IPv6 address in Startup Wizard.
CSCsy47893	Reboot message not displayed for tls-proxy max sessions in trans modes.
CSCsy48032	When switching from single to multiple mode, get activation key error.
CSCsy48841	ASDM should exclude intf in contexts from redundant intf member list.
CSCsy49878	Event classes listed in ASDM and ASA in various modes don't match.
CSCsy52191	Multicast boundary config - Add/Delete/Add does not save rule
CSCsy55381	ASDM posts Password only prompt after failed Cert validation.
CSCsy55390	ASDM should allow users to correct connection parameters - password.
CSCsy59235	Management Access screens allows multiple entries for same telnet host.

**Table 11** *Open Caveats in Version 6.2 (continued)*

<b>Caveat ID</b>	<b>Description</b>
CSCsy60282	ASDM 6.2: Warning is displayed while navigating away from PP screen.
CSCsy60567	SNMPv3 users is able to be deleted when trap host is configured.
CSCsy60576	ASDM errors when initially connecting to the IPS.
CSCsy61040	Link to monitoring track in search results lead to no page found.
CSCsy64189	System resource homepage: Core usage tab does not show CPU info.
CSCsy66490	PS: Changing public server entry might affect other entries.
CSCsy72304	ASDM: Force Immediate Reload is always grayed out.
CSCsz34731	Configuration > Firewall > Advanced > Fragment config cannot be changed.
CSCsz37172	Device setup panel was not updating when switching from 5520 to 5505.
CSCsz53036	CCO upgrade tool needs to select image by platform.
CSCsz67338	CSD: Prelogin Screen is jumpy & difficult to configure.
CSCsz83538	ASDM unable to connect to SSC when max password attempts are set.
CSCta28735	Usability - ASDM not capable of configuring "no client-types" CLI.
CSCta28784	ASDM: logging locks up when connecting with IPsec client.
CSCta28792	ASDM: Hangs up with requesting cert access.
CSCta35861	Challenge/response (CRACK) needs to be removed from site-to-site wizard.
CSCta42826	ASDM: CSD upload fails on a 5505.
CSCta59192	Phone Proxy: changing TFTP servers can lead to a CLI error.
CSCtb25499	ASDM fails to show IPsec connections page.
CSCtb39103	Logging > E-mail Setup: Adding an entry for Warning causes a CLI warning.
CSCtb70819	ASDM: Group Policy Help missing info on Tunnel Group Lock
CSCtb83506	Not showing the URL to get crypto access when upgrading ASA/ASDM.
CSCtc17246	ASDM Home, VPN Sessions panel has SSL counts discrepancy.
CSCtc23480	ASDM still uses aaa.cisco.class attribute with 8.0.4.x.
CSCtc33135	ASDM: Ping and Traceroute buttons are not visible for priv 5 users.
CSCtc36640	Language translation table edit doesn't work properly.
CSCtc38749	ACL name with ISO-8859-1 char set not shown properly in ASDM.
CSCtc41192	Auto-signon password variable/macros should be shown, and not dots.
CSCtc53304	With a large config, ASDM takes a long time to change config windows.
CSCtc54761	ASDM: SSL VPN Client Profile - need the ability to re-submit the command.
CSCtc55238	URL Blocked value in threats monitoring is incorrect.
CSCtc55873	Error when setting storage-objects cookies,credentials in group-policy.
CSCtc59297	ASDM: Update text in clientless bookmarks for password macro caveats.
CSCtc68152	Need an ERROR msg when overlap IPv6 address assigned to an intf.
CSCtc68258	No ERROR msg when multicast IPv6 assigns info.
CSCtc68845	Losing Web links in Trend Micro Content Security.

**Table 11** Open Caveats in Version 6.2 (continued)

Caveat ID	Description
CSCtc76298	NAT: Error message on Global pool configuration in Transparent mode.
CSCtc81893	ASDM 6.2 will not allow interface as source or destination on ACL line.
CSCtc83664	ASDM: Last Updated time on screens does not account for time zone.
CSCtc85528	Packet Capture Wizard missing buttons.

## Resolved Caveats for Software Version 6.2.3

Table 12 lists the resolved caveats for Version 6.2.3

**Table 12** Resolved Caveats in Version 6.2.3

Caveat ID	Description
CSCsk42250	ASDM does not support 1000 mbit/s ports on ASA5510
CSCso60199	Packet Tracer Tool not available with ASDM Read-Only profile.
CSCsq10143	Edit Static NAT Rule dialog is overlapping other text.
CSCsw78887	ASDM does not build Protocol 50 based reverse access-lists.
CSCsy13589	Remove http idle-timeout check box.
CSCsy41336	ASDM: Ascertain parity with warning messages for ACE / CSD.
CSCsy43548	IPv6: ASDM Static Route Panel support not allow hop count to be less than 255.
CSCsy48416	NAT: ASDM displays overlap error message for valid static NAT entry.
CSCsy55679	ASDM sometimes deletes the wrong Global Pool entry.
CSCsy62866	SSLVPN: Can't edit DAP record name that contains spaces.
CSCsy70075	Restore Configs use backward slash on Mac OS X.
CSCsy73695	IPv6: Edit IPv6 address in object group fails when group had IPv4 address.
CSCsy73787	IPv6: cut / paste fails on ACL Manager.
CSCsy80386	ASDM: Disabling 1 L2L ipsec connection profile may also disable others.
CSCsy81499	High Availability Wizard doesn't send join-failover-group.
CSCsy90560	ASDM windows sometimes lack access to some options.
CSCsy93539	Can't edit a language translation table.
CSCsy98518	ASDM: RDPv2 needs to be added as an import option.
CSCsz09478	IPv6 standby error in HAS wizard.
CSCsz24613	AnyConnect Conn Profile shouldn't list Portal Page Customization option.
CSCsz32744	Display incorrect default value from "Enable TTL evasion protection".
CSCsz35267	Unable to upgrade ASDM Launcher. Upgrading the ASDM demo also fails..
CSCsz35773	Apply button inactive for DNS added static NAT.
CSCsz37223	ASDM: New proposal for translation domain presentation and text.
CSCsz50664	TNXXXX Plugins should not be shown in ASDM until we officially support.

**Table 12** *Resolved Caveats in Version 6.2.3 (continued)*

<b>Caveat ID</b>	<b>Description</b>
CSCsz53047	"Clear content" on ASDM Syslog messages window doesn't work.
CSCsz57819	ASDM displaying message of unsupported characters when adding bookmarks.
CSCsz61110	ASDM login failure with a trailing space in password.
CSCsz66274	Unable to add aaa-server from ASDM.
CSCsz66527	Editing AAA rules to include multiple services throws exception.
CSCsz68231	ASDM warns before shutting down a subinterface incorrectly.
CSCsz74906	ASDM: Support for the new username & password for auto-signon.
CSCsz83205	ASDM: Unable to logoff VPN users without command authorization.
CSCta05224	ASDM always removing track and sla along with tracked static route.
CSCta09436	In ASDM 6.2 unable to set Radius-SDI-Xauth under Tunnel-Group.
CSCta14142	Strip-Realm for SSL VPN Connection Profiles needs to be added to ASDM.
CSCta42388	Source and Destination not correct in Real-Time Log Viewer.
CSCta43123	VPN loadbalancing cluster load page stuck at 72%.
CSCta49499	DAP: ldap memberof attribute match should not be case sensitive.
CSCta54516	ACL and NAT diagram hides config choices at bottom of screen.
CSCta59407	Launcher v. 1.5(43) doesn't work with ASA 8.2/ASDM 6.2.
CSCta73805	Space character not allowed in DAP not for older ASA images.
CSCta94242	Cut/paste of ACL with object-group does not work.
CSCtb17517	ASDM:Filter not working in 'Crypto Map > Find'.
CSCtb53837	Phone Proxy: CLI error because of incorrect http-proxy config.
CSCtb73849	ASDM does not work with MAC OS 10.6 (Snow Leopard).
CSCtb81523	ASDM RA-VPN wizard will not complete configuration.
CSCtc49841	Cannot perform ASDM backup with some CSD configs.
CSCtc53541	JideSplitButton text clipped in toolbars with JIDE 2.7.3.
CSCtc54002	Java console logs on Packet-tracer.
CSCtc55401	Configuration > Firewall has unexpected panel behavior.
CSCtc57536	Adding and immediately deleting an access rule causes null pointer exception.
CSCtc58631	Exception thrown while taking the backup.
CSCtc59963	Filter fields in Services and Addresses panes have translucent backgrounds.
CSCtc60020	ASDM:CSD panels missing from 6.3.0.88 and above, and 6.2.2.51.
CSCtc62500	ASDM: Edit Context Interface list not populated.
CSCtc65947	Addresses panel reappears when switching between Firewall tree nodes

## Resolved Caveats for Software Version 6.2.1

Table 13 lists the resolved caveats for Version 6.2.1

**Table 13** *Resolved Caveats in Version 6.2.1*

<b>Caveat ID</b>	<b>Description</b>
CSCse00007	VPN session monitoring: data is not loaded when filter is changed.
CSCsf19215	ASDM hard timeout for device i/o causes disconnect with large ACL.
CSCso63191	ASDM users with Privilege Level 0,1 Shouldn't Gain ASDM Access.
CSCsr29312	Unable to bring up Spyware Blocked Graph in Monitoring Module.
CSCsr56857	Click on configuration>content security hangs ASDM.
CSCsr59735	ASDM: SSL Server/Client Settings.
CSCsu00498	ASDM fails to add ACLs when access rules are filtered.
CSCsu22860	Time-range object for periodic/recurring time always displays Sunday.
CSCsu36051	The panel for File Transfer between Remote Server and Flash is hidden.
CSCsu43237	Global VPN parameters being set from tunnel-group screen.
CSCsu74661	ASDM monitoring stats are being cached between devices.
CSCsu78452	Can't enter domain name with multiple DNS server groups option.
CSCsu78499	Deleting group-policy Stop msg still used by Connection Profile
CSCsu79785	ASDM did not stop user to config vlan over system limit.
CSCsv02654	Number-of-rate option has wrong default for threat-detection config.
CSCsv12681	Error while loading ASDM: "Unconnected sockets not implemented".
CSCsv21391	ASDM Privacy Protection panel...Secure Desktop (Vault) clarification.
CSCsv21411	ClassNotFoundException on switching between devices.
CSCsv22348	CSC: CPU and memory graphs not displayed correctly.
CSCsv31292	ASDM:Group Policies panel description mods & link to LDAPAttribute Map.
CSCsv31821	ASDM panels need to state where parameter can be enforced.
CSCsv34865	Help > Release Notes is pointing to the wrong Release Notes.
CSCsv40389	ASDM :Privacy Protection in endpoint attributes "None".
CSCsv46652	ASDM: Include a link in Webtype ACL's to group policy and user.
CSCsv48386	ASDM handling of group-policies with special chars.
CSCsv48531	Logging : event classes listed in ASDM and ASA don't match.
CSCsv52632	User preferences: log color chooser dialog not modal.
CSCsv58991	ASDM: Description field in "Add Network Object" depends on Name field.
CSCsv60678	ASDM with CSC blank panels and left navigation only.
CSCsv65908	Unable to enroll user using local CA on with ASDM 6.1.5.
CSCsv66686	Add information text when enabling Smart Tunnel on a Bookmark.
CSCsv66700	ASDM: "only originate-only" error when configuring multi VPN peers.
CSCsv66778	Add a Bookmark Entry, Enable Smart Tunnel option modify Help.
CSCsv80695	ASDM is not able to configure webvpn http-proxy.
CSCsv83883	Network object group changes are not reflected in the GUI.
CSCsv90515	Addresses window moves back to the top when opening a nw object group.

**Table 13** *Resolved Caveats in Version 6.2.1 (continued)*

<b>Caveat ID</b>	<b>Description</b>
CSCsv90530	The left or right-hand ASDM pane is reduced in width.
CSCsw15502	DAP screen text changes for better usability.
CSCsw18031	ASDM: Present drop-down-list of URL variables/macros in Bookmarks panels.
CSCsw35562	ASDM: POST options need to be grayed in bookmark if ST is enabled.
CSCsw36338	DAP: DfltAccessPolicy misspelled as DflAccessPolicy on a couple of places.
CSCsw37361	ASDM: Usability for wildcarding with Webtype ACL's.
CSCsw37812	ASDM: Apply button is not always available upon deleting a smart tunnel window.
CSCsw41993	Clientless group-alias & group-url config needs Edit capability.
CSCsw43601	DAP DfltAccessPolicy Info bubble message corrections.
CSCsw43603	ASDM not recognizing pre-shared keys with "(" or ")".
CSCsw44286	Clicking refresh results in "saving the configuration to flash" message.
CSCsw45755	ASDM: Usability Improvement for Auto Signon with Smart Tunnels.
CSCsw49253	ASDM: Informative icon for fmatch with ASO Smart Tunnels host name.
CSCsw63632	Group Filter field only lists the extended access-lists.
CSCsw67961	Support ASA CLI: merge-dacl.
CSCsw69606	SSL wizard: selecting "Group Alias/URL" clears the selected Certificate.
CSCsw75528	Can't apply change to LDAP server scope.
CSCsw76614	ASDM: VPN graphs WebVPN/SVC Active Sessions - Terminology change needed.
CSCsw77282	Connection Profile - address pool appears as blank line in advanced view.
CSCsw81248	ASDM: webvpn auto-signon shows CIFS incorrectly as auth type with FTP.
CSCsw85477	ASDM: Smart Tunnels auto signon informative ballon is cut off by window.
CSCsx03483	ASDM should not set a number-of-rate value for TD host statistics.
CSCsx04911	ASDM: "group-url" can't be disabled from ASDM.
CSCsx07674	ASDM - network object group changes with filter causes errored entries.
CSCsx24433	ASDM fails to start with java.lang.StringIndexOutOfBoundsException error.
CSCsx27956	ASDM should use 'user-alert cancel' instead of 'no user-alert'.
CSCsx42814	Remove ASDM restriction in order to support ISO-8859-1.
CSCsx48813	ASDM Support for DAP record name with spaces.
CSCsx50131	CSC graphs show wrong time for timezones other than UTC.
CSCsx59463	ASDM: DHCP server panel help missing Allow VPN over-ride option.
CSCsx97142	TCP Map: creating a map on ASA 8.0 fails.
CSCsy27439	ASDM: Check for L2TP/IPSec PPP auth and AAA server combos.
CSCsy58573	ASDM: Disabling 1 connection profile entry may also disable others.
CSCsy60266	Botnet monitoring not available for read-only/ monitor-only user.

# End-User License Agreement

For information on the end-user license agreement, go to:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/eu1jen\\_\\_.pdf](http://www.cisco.com/univercd/cc/td/doc/es_inpk/eu1jen__.pdf)

## Related Documentation

For additional information on ASDM or its platforms, see *Navigating the Cisco ASA 5500 Series Documentation*:

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

## Obtaining 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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

---

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

©2009 Cisco Systems, Inc. All rights reserved.