Cisco ASDM Release Notes Version 6.0(3)

May 2008

This document contains release information for Cisco ASDM Version 6.0(3) on the Cisco ASA 5500 series adaptive security appliance. It includes the following sections:

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

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco ASA 5500 series adaptive security appliances through an intuitive, easy-to-use, web-based management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by Cisco ASA 5500 series adaptive security appliance software Version8.0(3). Its secure, web-based design enables anytime, anywhere access to security appliances.

New Features

Released: November 7, 2007

Table 1 lists the new features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3).

Table 1 New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3)

Feature	Description
VPN Features	
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.

Clientless SSL VPN Caching Static Content Enhancement	There are two changes to the clientless SSL VPN caching commands:
	The **cache-compressed** command is deprecated.
	The new **cache-static-content** command configures the security appliance to cache all static content, which means all cacheable Web objects that are not subject to SSL VPN rewriting. This includes content such as images and PDF files.
	The syntax of the command is **cache-static-content** {**enable** | **disable**}. By default, static content caching is disabled.
	Example:
	`hostname (config) # webvpn`
	`hostname (config-webvpn) # cache`
	`hostname (config-webvpn-cache) # cache-static-content enable`
	`hostname (config-webvpn-cache) #`
	In ASDM, see Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Content Cache.
	Also available in Version 7.2(3).

Table 1 New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Smart Card Removal Disconnect</td><td>This feature allows the central site administrator to configure remote client policy for deleting active tunnels when a Smart Card is removed. The Cisco VPN Remote Access Software clients (both IPSec and SSL) will, by default, tear down existing VPN tunnels when the user removes the Smart Card used for authentication. The following cli command disconnects existing VPN tunnels when a smart card is removed: <b>smartcard-removal-disconnect</b> {<b>enable</b> | <b>disable</b>}. This option is enabled by default.
In ASDM, see Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit Internal/External Group Policies > More Options.
<i>Also available in Version 7.2(3).</i></td></tr>
<tr><td>WebVPN load Balancing</td><td>The PIX Security Appliance now supports the use of FQDNs for load balancing. To perform WebVPN load balancing using FQDNs, you must enable the use of FQDNs for load balancing, enter the <b>redirect-fqdn enable</b> command. Then add an entry for each of your PIX Security Appliance outside interfaces into your DNS server if not already present. Each PIX Security Appliance outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for reverse lookup. Enable DNS lookups on your PIX Security Appliance with the <b>dns domain-lookup inside</b> command (or whichever interface has a route to your DNS server). Finally, you must define the ip address, of your DNS server on the PIX Security Appliance. Following is the new CLI associated with this enhancement: <b>redirect-fqdn</b> {<b>enable</b> | <b>disable</b>}.
In ASDM, see Configuration > VPN > Load Balancing.
<i>Also available in Version 7.2(3).</i></td></tr>
<tr><td colspan="2"><b>Application Inspection Features</b></td></tr>
<tr><td>WAAS and ASA Interoperability</td><td>The <b>inspect waas</b> command is added to enable WAAS inspection in the policy-map class configuration mode. This CLI is integrated into Modular Policy Framework for maximum flexibility in configuring the feature. The <b>[no] inspect waas</b> command can be configured under a default inspection class and under a custom class-map. This inspection service is not enabled by default.
The keyword option waas is added to the <b>show service-policy inspect</b> command to display WAAS statistics.
<code>show service-policy inspect waas</code>
A new system log message is generated when WAAS optimization is detected on a connection. All L7 inspection services including IPS are bypassed on WAAS optimized connections.
System Log Number and Format:
%ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.
A new connection flag "W" is added in the WAAS connection. The <b>show conn detail</b> command is updated to reflect the new flag.
In ASDM, see Configuration > Firewall > Service Policy Rules > Add/Edit Service Policy Rule > Rule Actions > Protocol Inspection.
<i>Also available in Version 7.2(3).</i></td></tr>
</table>

Table 1 New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)

Feature	Description
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. *Also available in Version 7.2(3).*

Support for ESMTP over TLS	This enhancement adds the configuration parameter **allow-tls** [**action log**] in the esmtp policy map. By default, this parameter is not enabled. When it is enabled, ESMTP inspection would not mask the 250-STARTTLS echo reply from the server nor the **STARTTLS** command from the client. After the server replies with the 220 reply code, the ESMTP inspection turns off by itself; the ESMTP traffic on that session is no longer inspected. If the **allow-tls action log** parameter is configured, the syslog message ASA-6-108007 is generated when TLS is started on an ESMTP session.
	`policy-map type inspect esmtp esmtp_map`
	`parameters`
	`allow-tls [action log]`
	A new line for displaying counters associated with the **allow-tls** parameter is added to the **show service-policy inspect esmtp** command. It is only present if **allow-tls** is configured in the policy map. By default, this parameter is not enabled.
	`show service-policy inspect esmtp`
	`allow-tls, count 0, log 0`
	This enhancement adds a new system log message for the **allow-tls** parameter. It indicates on an esmtp session the server has responded with a 220 reply code to the client **STARTTLS** command. The ESMTP inspection engine will no longer inspect the traffic on this connection.
	System log Number and Format:
	%ASA-6-108007: TLS started on ESMTP session between client <*client-side interface-name*>:<*client IP address*>/<*client port*> and server <*server-side interface-name*>:<*server IP address*>/<*server port*>
	In ASDM, see Configuration > Firewall > Objects > Inspect Map > ESMTP.
	Also available in Version 7.2(3).

High Availability Features	
Added Dataplane Keepalive Mechanism	You can now configure the security appliance so that a failover will not occur if the AIP SSM is upgraded. In previous releases when two security appliances with AIP SSMs are configured in failover and the AIP SSM software is updated, the security appliance triggers a failover, because the AIP SSM needs to reboot or restart for the software update to take effect. *Also available in Version 7.0(7) and 7.2(3)*
Fully Qualified Domain Name Support Enhancement	Added option in the **redirect-fqdn** 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.
DHCP Features	

Table 1 New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)

Feature	Description
DHCP client ID enhancement	If you enable the DHCP client for an interface using the **ip address dhcp** command, some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. Use this new command to include the interface MAC address for option 61. If you do not configure this command, the client ID is as follows: cisco-<MAC>-<interface>-<hostname>. We introduced the following command: **dhcp-client client-id interface** *interface_name* We modified the following screen: Configuration > Device Management > DHCP > DHCP Server; then click **Advanced**. *Also available in Version 7.2(3).*
DHCP client broadcast flag	If you enable the DHCP client for an interface using the **ip address dhcp** command, then you can use this command to set the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1. If you enter the **no dhcp-client broadcast-flag** command, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address. The DHCP client can receive both broadcast and unicast offers from the DHCP server. We introduced the following command: **dhcp-client broadcast-flag** We modified the following screen: Configuration > Device Management > DHCP > DHCP Server; then click **Advanced**.
Platform Features	
ASA 5510 Security Plus License Allows Gigabit Ethernet for Port 0 and 1	The ASA 5510 security appliance now has the security plus license to enable GE (Gigabit Ethernet) for port 0 and 1. If you upgrade the license from base to security plus, the capacity of the external port Ethernet0/0 and Ethernet0/1 increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface. *Also available in Version 7.2(3).*
ASA 5505 Increased VLAN range	The ASA 5505 security appliance now supports VLAN IDs between 1 and 4090. Originally, only VLAN IDs between 1 and 1001 were supported. *Also available in Version 7.2(3).*
Troubleshooting Features	
capture Command Enhancement	The enhancement to the **capture** command allows the user to capture traffic and display it in real time. It also allows the user to specify command line options to filter traffic without having to configure a separate access list. This enhancement adds the **real-time** and five-tupple **match** options. **capture** *cap_name* [**real-time**] [**dump**] [**detail** [**trace**] [**match** *prot* {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*] {**host** *ip* | *ip mask* | **any**} [{**eq** | **lt** | **gt**} *port*]] *Also available in Version 7.2(3).*
ASDM Features	

Table 1 New Features for ASA and PIX Version 8.0(3)/ASDM Version 6.0(3) (continued)

Feature	Description
ASDM banner enhancement	The PIX Security Appliance software supports an ASDM banner. If configured, when you start ASDM, this banner text will appear in a dialog box with the option to continue or disconnect. The Continue option dismisses the banner and completes login as usual whereas, the Disconnect option dismisses the banner and terminates the connection. This enhancement requires the customer to accept the terms of a written policy before connecting. Following is the new CLI associated with this enhancement: **banner** {**exec** | **login** | **motd** | **asdm**} *text* **show banner** [**exec** | **login** | **motd** | **asdm**] **clear banner** In ASDM, see Configuration > Properties > Device Administration > Banner. *Also available in Version 7.2(3).*
Localization Enhancement in ASDM	ASDM is now enhanced to supports AnyConnect Localization. See **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization,** or on the **Configuration > RemoteAccess > Network Access > AnyConnect Customization and Configuration > RemoteAccess > Language Localization > MST Translation panel**.
Time-based License Enhancement	On the Home page, the License tab of the Device Dashboard tab now includes the number of days until a time-based license expires (if applicable).
Network Objects	You can now add true network objects that you can use in firewall rules. Objects can be named, and when you edit an object, the change is inherited wherever the object is used. Also, when you create a rule, the networks that you specify in the rule are automatically added to the network object list so you can reuse them elsewhere. You can name and edit these automatic entries as well. See **Configuration > Firewall > Objects > Network Objects/Groups**.
Client Software Location Enhancement	Added support in Client Software Location list to allow client updates from Linux or Mac systems. See **Configure > Remote Access VPN > Language Localization**. *Also available in Version 7.2(3).*
CSC Event and Statistic Reporting Enhancement	With the Cisco Content Security and Control (CSC) 6.2 software, ASDM provides events and statistics for the new Damage Cleanup Services (DCS) feature. DCS removes malware from clients and servers and repairs system registries and memory.

Important Notes

If you download the ASDM Version 6.0(3) image from Cisco.com, you must download the images to your local machine and continue the upgrade from there.

New Platform Features

ASDM supports the enhancements to services and features introduced in the ASA 5500 software release Version 8.0(3).

This document contains release information about ASDM only. For detailed information on new platform features, see the online help, or the Cisco ASA 5500 Series Release Notes.

ASDM Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for ASDM Version 6.0(3).

Table 2 Operating System and Browser Requirements

Operating System	Version	Browser	Other Requirements
Microsoft Windows[1]	Windows Vista Windows 2003 Server Windows XP Windows 2000 (Service Pack 4 or higher)	Internet Explorer 6.0 or higher with Sun Java SE[2] Plug-in 1.4.2, 5.0 (1.5.0), or 6.0 Firefox 1.5 or higher with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0 (1.6.0)	**SSL Encryption Settings**—All available encryption options are enabled for SSL in the browser preferences.
Note We support both the English and Japanese versions of Windows.		**Note** **HTTP 1.1**—Settings for **Internet Options > Advanced > HTTP 1.1** should use HTTP 1.1 for both proxy and non-proxy connections.	
Apple MacIntosh	Apple MacIntosh OS X	Firefox 1.5 or higher or Safari 2.0 or higher with Java SE Plug-in 5.0 (1.5.0), or 6.0(1.6.0)	
Linux	Red Hat Desktop, Red Hat Enterprise Linux WS version 4 running GNOME or KDE	Firefox 1.5 or higher with Java SE Plug-in 1.4.2, 5.0 (1.5.0), or 6.0(1.6.0)	

[1] ASDM is not supported on Windows 3.1, Windows 95, Windows 98, Windows ME, or Windows NT4.

[2] Obtain Sun Java from http://www.java.com/en/download/manual.jsp.

Memory Errors in Firefox

Firefox may stop responding or give an out of memory error message Linux and Windows if multiple instances of ASDM are running. You can use the following steps to increase the Java memory and work around the behavior.

This section describes how to increase the memory for Java on the following platforms:

- Java Plug-In for Windows
- Java Plug-In on Linux

Java Plug-In for Windows

To change the memory settings of the Java Plug-in on Windows for Java Plug-in versions 1.4.2 and 1.5, perform the following steps:

Step 1 Exit all browsers.

Step 2 Click **Start > Settings > Control Panel**.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click **Java Plug-in**. The Java Plug-in Control Panel appears.

b. Click the **Advanced** tab.

c. Type **-Xmx256m** in the Java RunTime Parameters field.

d. Click **Apply** and exit the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click **Java**. The Java Control Panel appears.

b. Click the **Java** tab.

c. Click **View** under Java Applet Runtime Settings. The Java Runtime Settings Panel appears.

d. Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.

e. Click **OK** and exit the Java Control Panel.

Java Plug-In on Linux

To change the settings of Java Plug-in version 1.4.2 or 1.5 on Linux, perform the following steps:

Step 1 Exit all browsers.

Step 2 Open the Java Plug-in Control Panel by launching the Control Panel executable file.

Note In the Java 2 SDK, this file is located in SDK installation directory/jre/bin/ControlPanel. For example: if the Java 2 SDK is installed at /usr/j2se, the full path is /usr/j2se/jre/bin/ControlPanel. In a Java 2 Runtime Environment installation, the file is located at JRE installation directory/bin/ControlPanel.

Step 3 If you have Java Plug-in 1.4.2 installed:

a. Click the **Advanced** tab.

b. Type **-Xmx256m** in the Java RunTime Parameters field.

c. Click **Apply** and close the Java Control Panel.

Step 4 If you have Java Plug-in 1.5 installed:

a. Click the **Java** tab.

b. Click **View** under Java Applet Runtime Settings.

c. Type **-Xmx256m** in the Java Runtime Parameters field and then click **OK**.

d. Click **OK** and exit the Java Control Panel.

Supported Platforms and Feature Licenses

For information on supported platforms and feature licenses, see:

http://www.cisco.com/en/US/docs/security/asa/asa80/license/license80.html

ASDM and SSM Compatibility

ASDM Version 6.0(3) supports the following SSMs and releases:

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

Upgrading ASDM

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

http://www.cisco.com/cisco/software/navigator.html

Note ASDM 6.0(3) is not backward compatible. If you have an earlier version of ASDM 6.0, or platform version earlier than 8.0, ASDM and the platform image should be upgraded at the same time before reloading or restarting ASDM.

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 backwards compatible, so you can upgrade the platform image using the new ASDM; you cannot use an old ASDM with a new platform image.

To upgrade ASDM, perform the following steps:

Step 1 Download the new ASDM image to your PC.

Step 2 Launch ASDM.

Step 3 From the Tools menu:

a. In ASDM 5.0 and 5.1, click **Upload Image from Local PC**.

b. In ASDM 5.2, click **Upgrade Software**.

Note When downloading the image from Cisco.com, you must download the images to your local machine and continue the upgrade from there.

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 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 in the **Configuration > Properties > Device Administration > Boot System/Configuration** pane.

Step 8 To run the new ASDM image, you must exit ASDM and reconnect.

Step 9 Download the new platform image using the **Tools > Upgrade Software** tool.

To reload the new image, reload the security appliance using the **Tools > System Reload** tool.

Getting Started with ASDM

This section describes how to connect to ASDM and start your configuration. If you are using the security appliance for the first time, your security appliance might include a default configuration. You can connect to a default IP address with ASDM so that you can immediately start to configure the security appliance from ASDM. If your platform does not support a default configuration, you can log in to the CLI and run the **setup** command to establish connectivity. See Before You Begin for more detailed information about networking.

This section includes the following topics:

Before You Begin

If your security appliance includes a factory default configuration, you can connect to the default management address of 192.168.1.1 with ASDM. On the ASA 5500 series adaptive security appliance, the interface to which you connect with ASDM is Management 0/0. To restore the default configuration, enter the **configure factory-default** command at the security appliance CLI.

It is also recommended that you install the recommended version of Java before you being the installation.

Make sure the PC is on the same network as the security appliance. You can use DHCP on the client to obtain an IP address from the security appliance, or you can set the IP address to a 192.168.1.0/24 network address.

If your platform does not support the factory default configuration, or you want to add to an existing configuration to make it accessible for ASDM, access the security appliance CLI according to the *Cisco Security Appliance Command Line Configuration Guide*, and enter the **setup** command.

Note Running the `setup` command may remove any existing configuration. If a platform does not support the factory default configuration, then the setup command won't be supported

You must have an inside interface already configured to use the **setup** command. Before using the **setup** command, enter the **interface gigabitethernet** *slot*/*port* command, and then the **nameif inside** command. The *slot* for interfaces that are built in to the chassis is **0**. For example, enter **interface gigabitethernet 0/1.**

The ASA 5510 adaptive security appliance has an Ethernet-type interface. When using the using the **setup** command, remember that the interface ID is dependent upon the platform. For example, on PIX 500 series, enter the **interface ethernet** *slot*/*port*. On ASA, enter **interface gigabitethernet** *slot*/*port* command.

Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM in a Java Applet. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches faster, and caches previously-entered IP addresses and usernames.

To download the ASDM Launcher, perform the following steps:

Step 1 From a supported web browser on the security appliance network, enter the following URL:

```
https://interface_ip_address/admin
```

In transparent firewall mode, enter the management IP address.

Note Be sure to enter **https**, not **http**.

Step 2 Click **OK** or **Yes** to all prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

Step 3 Click **Download ASDM Launcher and Start ASDM**.

The installer downloads to your PC.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

To start ASDM from the ASDM Launcher, perform the following steps:

Step 1 Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

Step 2 Enter the security appliance IP address or hostname, your username, and your password, and then click **OK**.

If there is a new version of ASDM on the security appliance, the ASDM Launcher automatically downloads it before starting ASDM.

Using ASDM in Demo Mode

ASDM Demo Mode is available as a separately installed application running under Windows. It makes use of the ASDM Launcher and pre-packaged configuration files to let you run ASDM without having a live device available. ASDM Demo Mode lets you:

- Perform configuration and select monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and monitoring tasks with the Content Security and Control (CSC) SSM.

ASDM Demo Mode provides simulated monitoring data, including real-time system log messages. The data shown is randomly generated, but the experience is identical to what you would see when connecting to a real device.

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI but are not applied to the configuration file. That is, when you click the **Refresh** button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File/Disk operations are not supported.
- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot log in as a monitor-only or read-only user.
- Demo Mode does not support the following features:
  - File menu:

    Save Running Configuration to Flash

    Save Running Configuration to TFTP Server

    Save Running Configuration to Standby Unit

    Save Internal Log Buffer to Flash

    Clear Internal Log Buffer
  - Tools menu:

    Command Line Interface

    Ping

File Management

Update Image

File Transfer

Upload image from Local PC

System Reload

  - Toolbar/Status bar > Save
  - Configuration > Interface > Edit Interface > Renew DHCP Lease
  - Failover—Configuring a standby device

- These operations cause a reread of the configuration and therefore will revert the configuration back to the original settings.
  - Switching contexts
  - Making changes in the Interface panel
  - NAT panel changes
  - Clock panel changes

To run ASDM in Demo Mode, perform the following steps:

Step 1 If you have not yet installed the Demo Mode application, perform the following steps:

a. Download the ASDM Demo Mode installer from the following website:

http://www.cisco.com/cisco/software/navigator.html

The filename is asdm-demo-*version*.msi.

b. Double-click the installer to install the software.

Step 2 Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

Step 3 Check **Run in Demo Mode**.

Step 4 To set the platform, context and firewall modes, and ASDM Version, click **Demo** and make your selections from the Demo Mode area.

Step 5 To use new ASDM images as they come out, you can either download the latest installer, or you can download the normal ASDM images and install them for Demo Mode:

a. Download the image from the download page (see Step 1).

The filename is asdm-*version*.bin.

b. In the Demo Mode area, click **Install ASDM Image**.

A file browser appears. Find the ASDM image file in the browser.

Step 6 Click **OK** to launch ASDM Demo Mode.

You see a Demo Mode label in the title bar of the window.

Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

Step 1 From a supported web browser on the security appliance network, enter the following URL:

https://*interface_ip_address/admin*

In transparent firewall mode, enter the management IP address.

Note Be sure to enter **https**, not **http**.

Step 2 Click **OK** or **Yes** to all browser prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

Step 3 Click **Run ASDM as a Java Applet**.

Step 4 Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, the name and password fields are left blank.

Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode security appliance or a context in multiple context mode.

To use the Startup Wizard to configure the basic setup of the security appliance, perform the following steps:

Step 1 Launch the wizard according to the steps for the correct security context mode.

- In single context mode, click **Wizards > Startup Wizard**.
- In multiple context mode, for each new context, perform the following steps:
  - **a.** Create a new context using the **System > Configuration > Security Context** pane.
  - **b.** Be sure to allocate interfaces to the context.
  - **c.** When you apply the changes, ASDM prompts you to use the Startup Wizard.
  - **d.** Click the **System/Contexts** icon on the toolbar, and choose the context name.
  - **e.** Click **Wizards > Startup Wizard**.

Step 2 Click **Next** as you proceed through the Startup Wizard screens, filling in the appropriate information in each screen, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.

Step 3 Click **Finish** on the last pane to transmit the configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of the connection changes.

Step 4 Enter other configuration details on the **Configuration** panes.

Using the VPN Wizard

The VPN Wizard configures basic VPN access for LAN-to-LAN or remote client access. The VPN Wizard is available only for security appliances running in single context mode and routed (not transparent) firewall mode.

To use the VPN Wizard to configure VPN, perform the following steps:

Step 1 Click **Wizards > VPN Wizard**.

Step 2 Supply information on each wizard pane. Click **Next** to move through the VPN Wizard panes. You may use the default IPSec and IKE policies. Click **Help** for more information about each field.

Step 3 After you complete the VPN Wizard information, click **Finish** on the last pane to transmit the configuration to the security appliance.

Printing from ASDM

Note Printing is supported only for Microsoft Windows 2000 or XP in this release. There is a known caveat (CSCse15764) for printing from Windows XP that causes printing to be extremely slow.

ASDM supports printing for the following features:

- The Configuration > Interfaces table
- All Configuration > Security Policy tables
- All Configuration > NAT tables
- The Configuration > VPN > IPSec > IPSec Rules table
- Monitoring > Connection Graphs and its related table

ASDM Limitations

This section describes ASDM limitations, and includes the following topics:

- Unsupported Commands, page 17
- Interactive User Commands Not Supported in ASDM CLI Tool, page 18
- Unsupported Characters, page 19

Unsupported Commands

ASDM does not support the complete command set of the CLI. In most cases, ASDM ignores unsupported commands, and they can remain in your configuration.

Effects of Unsupported Commands

- If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but all other configuration is available.
- If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, choose **Options > 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, see the following URL:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/devadmin.html.

Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when you add them through the CLI, but that you cannot add or edit 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.

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens
capture	Ignored
established	Ignored
failover timeout	Ignored
icmp unreachable rate-limit	Ignored
ipv6, **any IPv6 addresses**	Ignored
pager	Ignored

Unsupported Commands	ASDM Behavior
pim accept-register route-map	Ignored. You can only configure the **list** option using ASDM.
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`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`

sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
terminal	Ignored
virtual	Ignored

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 in 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 command: **`crypto key generate rsa`**

   ASDM generates the default 1024-bit RSA key.
3. Delete the key with the following command: **`crypto key zeroize rsa`**

   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
   ke0000000000000$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 zeroize rsa noconfirm
  ```

Unsupported Characters

ASDM does not support any non-English characters or any other special characters. If you enter non-English characters in any text entry field, they become unrecognizable when you submit the entry, and you cannot delete or edit them.

If you are using a non-English keyboard or usually type in a language other than English, be careful not to enter non-English characters accidentally.

Workaround:

For workarounds, see CSCeh39437 under Caveats, page 19.

Caveats

The following sections describes the open and resolved caveats for Version 6.0(3).

Note If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

http://tools.cisco.com/Support/BugToolKit/

To become a registered cisco.com user, go to the following website:

http://tools.cisco.com/RPF/register/register.do

Open Caveats - Version 6.0(3)

The following list shows caveats that are open for Version 6.0(3):

Table 3 Open ASDM Caveats

	Software Version 6.0(3)	
ID Number	**Open**	**Caveat Title**
CSCsi24281	Yes	ASDM: Using the path Client cert auth -> Multiple client certs popup may lockup the system.
CSCsi39246	Yes	Refresh arrows turn pink on accessing or leaving various screens
CSCsi93348	Yes	ASDM: Add DAP endpoint selection attribute endpoint.hostname.
CSCsj00059	Yes	ASDM: When searching for VPN-Session details, ACL hits are not updated even after a Refresh.
CSCsj07705	Yes	ASDM: Exception after Deleting Local CA and clicking Reset.
CSCsj16580	Yes	Cannot configure TLS Maximum Sessions in multiple mode.
CSCsj22650	Yes	ASDM will not allow customer to choose VLAN on an ASA 5505 platform.
CSCsj40412	Yes	Cannot delete tunnel-group or group-policy with ASDM.
CSCsk21876	Yes	ASDM hangs 100% and throws java null pointer.
CSCsk59189	Yes	ASDM 6.0.2 shows n/a - config out of sync
CSCsk71656	Yes	ASDM: ACL hit count being not shown for some ACEs
CSCsk91131	Yes	ASDM-device dashboard int status shows inside int in a dwn/dwn state incorrectly.
CSCsk97052	Yes	Time screen is stuck in ASDM demo mode.
CSCsl09153	Yes	ASDM comes up in demo mode when demo mode is not checked.
CSCsl09313	Yes	ssh: change config thru ASDM, apply, then change from ASA, not refreshed.
CSCsl10066	Yes	ASDM states ASDM is temporarily unable to contact the firewall.
CSCsl12327	Yes	Upgrade software shows older versions.
CSCsl15710	Yes	Packet tracer will fail if Special character like & in interface name.
CSCsl15782	Yes	ASDM graphs dont update when you change the ASA clock backward.

Resolved Caveats - Version 6.0(3)

The following list shows caveats that are resolved for Version 6.0(3):

Table 4 Resolved ASDM Caveats

	Software Version 6.0(3)	
ID Number	**Resolved**	**Caveat Title**
CSCeg54076	Yes	Failover-enabled popup is incorrect or misleading.
CSCsd83057	Yes	Cannot add failover interface in ASDM.
CSCsg29740	Yes	ASDM should not allow non-ascii chars to be entered into description.

Table 4 Resolved ASDM Caveats (continued)

ID Number	Software Version 6.0(3)	
	Resolved	Caveat Title
CSCsg68633	Yes	High Availability and Scalability (HAS) wizard is confusing introduction message on standby IP page.
CSCsh60343	Yes	System Home page resource graphs shows truncated system time.
CSCsi39528	Yes	DAP: Endpoint Attr Type=Policy did not show configured Locations in the Cisco Secure Desktop(CSD).
CSCsj02733	Yes	DAP: Vendor ID choicelist should be alphabetized.
CSCsj15140	Yes	Identity certificate status does not refresh ASDM.
CSCsj16920	Yes	Local CA: Leaving or returning while disabled enables blocked fields.
CSCsj18902	Yes	ASDM feature to support import and export of ASA config archive.
CSCsj20946	Yes	Default VLAN is out of range.
CSCsj22326	Yes	ASDM: Local CA passphrase field should be obscured; not out in clear view.
CSCsj22419	Yes	Local CA - Enable should be grayed out after Disabling CA.
CSCsj22691	Yes	Need to provide an option to select an interface in SLA monitoring
CSCsj22717	Yes	CSC Home Page graphs time is out of sync with the ASA time by one hour.
CSCsj22798	Yes	Graph table is automatically resized.
CSCsj26284	Yes	TFW NAT: Selecting IP address browse button twice will freeze panel
CSCsj26304	Yes	SSL VPN: smart-tunnel changes all entries.
CSCsj27201	Yes	Filtering should search within CSM_INLINE. Should not display CSM_INLINE.
CSCsj27897	Yes	System home resource graphs show all graphs, even though only 10 are selected.
CSCsj29060	Yes	Erroneous NAT-T command sent when configuring TCP in IKE Parameters.
CSCsj32088	Yes	ASDM: CCO upgrade failures -> error writing to server.
CSCsj37138	Yes	Log view tables become blank when moving columns around.
CSCsj40690	Yes	ASDM NAT-control Option Window Behavior.
CSCsj42435	Yes	The online Help > Feature Matrix points to 5.2(1) release notes instead of 6.0.
CSCsj47403	Yes	CSD Alternate Group Policy needs to be removed.
CSCsj51135	Yes	Support ESMTP over TLS in ASDM.
CSCsj51143	Yes	Add WAAS inspection support in ASDM.
CSCsj52635	Yes	CSC ASDM not reporting Damage Cleanup Services events and statistics.
CSCsj57076	Yes	CSD: Fix choices for Norton AntiVirus (MAC).
CSCsj57083	Yes	Authentication test fails when using ASDM and FQDN is configured.
CSCsj57390	Yes	ASDM: Cache file system (FS) limit is incorrect.
CSCsj58456	Yes	Interface Rx and Tx Utilization values shown wrong in ASDM.
CSCsj60230	Yes	ASDM does not respect the order of service policy rules.
CSCsj62045	Yes	ASDM supports the DNS Guard function.
CSCsj64642	Yes	ASDM 6.0 can't handle group-alias string containing spaces.
CSCsj66280	Yes	New CLI for smartcard-removal-disconnect not configurable in ASDM.

Table 4 Resolved ASDM Caveats (continued)

ID Number	Software Version 6.0(3)	
	Resolved	**Caveat Title**
CSCsj67417	Yes	ASDM Monitor mode displays failover interface in Interface Status
CSCsj68425	Yes	Confusing message when enabling HTTP replication using ASDM version 6.0.
CSCsj89744	Yes	ASDM listing object-group by IP selects wrong objects to be added.
CSCsj94089	Yes	ASDM: Search does not return the expected results.
CSCsk02011	Yes	Usability issue: Saving configuration.
CSCsk03955	Yes	ASDM **show version** command does not display Advanced Endpoint Assessment.
CSCsk07494	Yes	ASDM 6.0 VPN session does not show client version.
CSCsk08332	Yes	ASDM: Cannot sort on a VPN statistics table using Linux operating system.
CSCsk09308	Yes	Missing host/network concept in ASDM version 5.2 and higher.
CSCsk14359	Yes	CSD:MAC OS check fails to match DAP record.
CSCsk23886	Yes	The keywords **allocate-interface** is being sent before the **interface** command.
CSCsk24261	Yes	Implement IP Address reuse delay functionality.
CSCsk40718	Yes	Support for AnyConnect Localization Enhancements.
CSCsk41450	Yes	ASDM Issues 'Clear Xlate' For All Statics When a Static is Inserted.
CSCsk41716	Yes	Misleading error message when running ASDM on a non-default port.
CSCsk41856	Yes	ASDM freezes when bringing up the buffered Log Viewer.
CSCsk48790	Yes	ASDM demo mode is stuck when visited CSD screen.
CSCsk54346	Yes	ASDM: Logout a VPN Client in ASDM, status does not change on screen.
CSCsk55024	Yes	Cannot switch device to ASA/PIX if unit does not have an ASDM image.
CSCsk59058	Yes	Period time range for day Saturday reverts incorrectly set to Weekend.
CSCsk62984	Yes	ASDM doesn't recognize the Network File System (NFS) service in an access list.
CSCsk73420	Yes	WebVPN ASDM will not display svc image with regex.
CSCsk75320	Yes	CSDM’s Web link does not work.
CSCsk76753	Yes	ASDM does not have support for Radius SDI (tunnel-group & aaa-server)
CSCsk81917	Yes	Switching from IPS panels to ASDM tabs without selecting Apply to set changes, throws an exception.
CSCsk85478	Yes	E-mail Proxy setup not working on ASDM 6.0 with an ASA5505 platform.
CSCsk87169	Yes	Unable to add IP Names in the ASDM Objects -> IP Names window.
CSCsk88458	Yes	PIX hostname not getting updated.
CSCsk91189	Yes	Changing multiline Access Control List (ACL) or policy NAT description results in an error.
CSCsk91589	Yes	HAS wizard failover lan intf command not sent to FT.
CSCsk92537	Yes	Disable Backup configuration in multiple mode.
CSCsk93502	Yes	Network object is not hooked up yet.
CSCsk99572	Yes	Sort functionality not working for Top Usage Tables in FW Dashboard.
CSCsl00705	Yes	Remove IP Names category.

Table 4 Resolved ASDM Caveats (continued)

	Software Version 6.0(3)	
ID Number	**Resolved**	**Caveat Title**
CSCsl01422	Yes	Monitor mode: ASDM Assistant exposes Configuration panels.
CSCsl06404	Yes	ASDM: Can not configure NAT rule, java exception.
CSCsl06719	Yes	Cannot send commands to context in failover group 2.
CSCsl06751	Yes	ASDM: error when editing service-grp used in NAT.

End-User License Agreement

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

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

Related Documentation

For additional information on ASDM or its platforms, see the ASDM online Help or the following documentation found on Cisco.com:

- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Getting Started Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Migrating to ASA for VPN 3000 Series Concentrator Administrators*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Release Notes for Cisco Intrusion Prevention System 5.0*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.0*
- *Release Notes for Cisco Intrusion Prevention System 5.1*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 5.1*

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.