# Cisco ASDM Release Notes Version 6.1

**March 2008**

This document contains release information for Cisco ASDM Version 6.1 on Cisco ASA 5500 Adaptive Series Security Appliances. 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 Version8.1. Its secure, web-based design enables anytime, anywhere access to security appliances.

**Note** ASDM 6.1 is compatible with Cisco ASA 5500 Adaptive Series Security Appliance versions 8.0 and 8.1, and Cisco PIX 500 Series Security Appliances version 8.0, but not earlier versions. The Cisco ASA 5580 Adaptive Series Security Appliance is only compatible with ASDM 6.1 and ASA version 8.1 software. For more information on platform support, see Table 3ASDM Version 6.1 Support by Platform, page 5.

# New Features

**Released: March 1, 2008**

Table 1 lists the new features for ASA Version 8.1(1)/ASDM Version 6.1(1). This ASA software version is only supported on the ASA 5580.

***Table 1 New Features for ASA Version 8.1(1)/ASDM Version 6.1(1)***

| Feature | Description |
|---|---|
| Introduction of the Cisco ASA 5580 | The Cisco ASA 5580 comes in two models:<br>• 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.<br>• 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.<br>In ASDM, see **Home > System Resource Status and Home > Device Information > Environment Status**. |
| NetFlow | The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. For detailed information about this feature and the new CLI commands, see the *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide*.<br>In ASDM, see **Configuration > Device Management > Logging > Netflow**. |

*Table 1 New Features for ASA Version 8.1(1)/ASDM Version 6.1(1) (continued)*

| Feature | Description |
|---|---|
| Jumbo frame support | The Cisco ASA 5580 supports jumbo frames when you enter the **jumbo-frame reservation** command. A jumbo frame is an Ethernet packet larger than the standard maximun of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the the maximum use of other features, such as access lists.<br><br>In ASDM, see **Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced**. |
| Timeout for SIP Provisional Media | You can now configure the timeout for SIP provisional media using the **timeout sip-provisional-media** command.<br><br>In ASDM, see **Configuration > Firewall > Advanced > Global Timeouts**. |
| Details about the activation key | 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 **show activation key detail** command.<br><br>In ASDM in single context mode, see **Configuration > Device Management > System Image/Configuration > Activation Key**. In ASDM in multiple context mode, see **System > Configuration > Device Management > Activation Key**. |
| New ASDM online help engine | ASDM now supports a new look for the online help. The online help now maintains the topic-based selection of the user from the left bookmark pane while browsing through the right pane subject matter. |
| ASDM CPU Core Usage Graph | In single or multiple mode, the CPU core usage graph allows you to display the core CPU utilization status from the ASDM Home page. |
| Intelligent platform management interface (IPMI) for ASDM | Added support for intelligent platform management interface (IPMI), which provides the user with information on the status of the power supply, cooling fans, and temperature of the processors and chassis from the ASDM Home page. |
| ASDM Assistant | The ASDM Assistant is now available from **View** Menu, instead of the **Tools** Menu. The GUI has been changed to simplify the **Search** mechanism. |
| ASDM Backup and Restore Enhancement | The backup and restore enhancement allows you to back up configurations to the local machine and then restore them back on the server as necessary. Additionally, this feature backs up SSL VPN-related files. This feature is found in **Tools > Backup Configuration**, and **Tools > Restore Configuration**.<br><br>*Also supported for Version 8.0.* |
| ASDM Log Viewer | The Log viewer enhancement displays the source and destination port information parsed from the syslog messages. This information is displayed on the **Monitoring > Logging > Real-Time Log Viewer,** and **Log Buffer** page.<br><br>*Also supported for Version 8.0.* |
| Enhanced VPN Search in ASDM | Added a CLI command-based Search facility that offers intelligent hints while you are typing in keywords or a command. This search enhancement only exists on User Accounts, Connection Profiles, and Group Policies pages.<br><br>*Also supported for Version 8.0.* |

# ASDM Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for ASDM Version 6.1.

***Table 2 Operating System and Browser Requirements***

| Operating System | Version | Browser |
|---|---|---|
| Microsoft Windows[1] | Windows Vista<br>Windows 2003 Server<br>Windows XP<br>Windows 2000 (Service Pack 4 or higher) | Internet Explorer 6.0 or higher with Sun Java (JRE)[2] 1.4.2, 5.0 (1.5), or 6.0<br>Firefox 1.5 or higher with Sun Java (JRE) 1.4.2, 5.0 (1.5), or 6.0 |
| Apple Macintosh® | Apple Macintosh OS X | Firefox 1.5 or higher or Safari 2.0 or higher withSun Java (JRE) 5.0 (1.5). |
| Linux | Red Hat Linux, Red Hat Enterprise Linux WS version 4 running GNOME or KDE | Firefox 1.5 or higher with Sun Java (JRE) 1.4.2, 5.0 (1.5), or 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 java.sun.com.

# Supported Platforms and Feature Licenses

The following table lists the supported platforms specifically for ASDM 6.1:

*Table 3 ASDM Version 6.1 Support by Platform*

| Hardware Platform | ASA Software Version |
|---|---|
| ASA 5580 Series | ASA 8.1[1] |
| ASA 5500 Series[2] | ASA 8.1<br>ASA 8.0 |
| PIX 500[3] Series | PIX 8.0 |

1. ASA 8.1 does not support PIX, however, ASDM 6.1 will work with PIX 8.0.
2. Cisco ASA 5500 series excludes the 5580 platform.
3. PIX 500 Series excludes the PIX 501 and PIX 506/506E platforms which are only supported up to version 6.3.

For information on supported platforms and feature licenses, see:

http://www.cisco.com/en/US/docs/security/asa/asa81/release/notes/asarn81.html

# ASDM and SSM Compatibility

**Note** SSMs are not supported on the ASA 5580 Adaptive Series Security Appliance.

# Upgrading ASDM and ASA

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

http://www.cisco.com/public/sw-center/index.shtml

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.

**Note** ASDM 6.1 is compatible with Cisco ASA 5500 Adaptive Series Security Appliance versions 8.0 and 8.1, and Cisco PIX 500 Series Security Appliances version 8.0, but not earlier versions. The Cisco ASA 5580 Adaptive Series Security Appliance is only compatible with ASDM 6.1 and ASA version 8.1 software. For more information on platform support, see Table 3ASDM Version 6.1 Support by Platform, page 5.

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, click **Tools > Upload Image from Local PC**.

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

c. In ASDM 6.0, click **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** panel.

**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.

# 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 begin 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** If your platform does not support the factory default configuration, running the **setup** command may remove any existing configuration.

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 browser. 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 in a browser**

**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:

- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and select monitoring tasks via ASDM as though you were interacting with a real device.

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:

    Reset Device to the Factory Default Configuration

    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

    Traceroute

    File Management

    Upgrade Software from Local Computer

    Upgrade Software from Cisco.com

    Backup Configurations

    Restore Configurations

    System Reload

    Administrator's Alert to Clientless SSL VPN Users
  - 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-611.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:

- **Install ASDM Launcher and Run ASDM**

**Step 3** Click **Run ASDM**.

**Step 4** Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, leave the name and password 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 IPsec VPN Wizard

The IPsec 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.

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

ASDM does not support the complete command set of the CLI. For any CLI configuration that ASDM does not support, the commands remain unchanged in the 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 **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.**

### 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 |
| **established** | Ignored |
| **failover timeout** | Ignored |
| **icmp unreachable rate-limit** | Ignored |
| **ignore-ipsec-keyusage** | Ignored; under the "crypto ca trustpoint <tp-name>" mode. |
| **ignore-ssl-keyusage** | Ignored; under the "crypto ca trustpoint <tp-name>" mode. |
| **ipv6**, any IPv6 addresses | Ignored |
| **pager** | Ignored |
| **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:<br>`access-list myacl line 1 extended permit ip any any`<br>`class-map mycm`<br>`match access-list mycl`<br>`policy-map mypm`<br>`class mycm`<br>`inspect ftp`<br>`service-policy mypm global` |
| **sysopt nodnsalias** | Ignored |
| **sysopt uauth allow-http-cache** | Ignored |
| **system internal** and all subcommands | Ignored |
| **terminal** | 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. Enter the command again: **crypto key generate 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 generate rsa noconfirm**

# Miscellaneous Limitations

- Configuration > Remote Access VPN > Secure Desktop Manager is not supported.
- Dynamic Access Policies, located in **Configuration > Remote Access VPN > Network (Client) Access and Configuration > Remote Access VPN > Clientless SSL VPN Access**, have limited support because it depends on Secure Desktop Manager which is not supported.

# Caveats

The following sections describes the open caveats for Version 6.1(1).

**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 6.1(1)

The following list shows caveats that are opened for Version 6.1(1):

*Table 4 Open ASDM Caveats*

| | Software Version 6.1(1) | |
|---|---|---|
| **ID Number** | **Corrected** | **Caveat Title** |
| CSCsk41460 | | Need to validate different GE/10GE interfaces to one redundant interface. |
| CSCsk49384 | | Deleted interfaces still shows in user context. |
| CSCsl50642 | | Add/Del Interface through CLI not shown in ASDM home page. |
| CSCsm66235 | | ACL manager in ASDM 6.0(3) does not display standard ACLs. |
| CSCsm85034 | | ASDM refresh errors after failover - no response for 60 secs warning. |
| CSCsm85594 | | ntp: add server without interface, then edit, shows first interface. |
| CSCsm91240 | | Boot image config empty after switch from multiple to single context mode. |
| CSCsm92154 | | ASDM: Java Exception when non-numerical entered into CRL port field. |
| CSCsm92524 | | HT:Exception generated when accessing Real-time Log Viewer in context. |
| CSCsm95257 | | ASDM: ACL with trailing remark causes ASDM to add bogus remarks to ACL. |

# End-User License Agreement

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

http://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*
- *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.