



# Cisco ASDM Release Notes Version 5.1(1)

---

February 2006

## Contents

This document contains release information for Cisco ASDM Version 5.1(1) on Cisco PIX 500 series and Cisco ASA 5500 series security appliances Version 7.1(1). It includes the following sections:

- [Introduction, page 1](#)
- [System Requirements, page 2](#)
- [Usage Notes, page 3](#)
- [Platform Feature Licenses, page 14](#)
- [ASDM Demo Mode, page 17](#)
- [ASDM and IPS Compatibility, page 18](#)
- [Caveats, page 18](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation, page 20](#)
- [Documentation Feedback, page 21](#)
- [Obtaining Technical Assistance, page 21](#)
- [Obtaining Additional Publications and Information, page 22](#)

## Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco PIX 500 and ASA 5500 series 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,



---

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

© <year> Cisco Systems, Inc. All rights reserved.

and versatile monitoring services that complement the advanced security and networking features offered by Cisco PIX 500 and ASA 5500 series security appliance software Version 7.1(1). Its secure, web-based design enables anytime, anywhere access to security appliances.

## New Platform Features

The PIX 500 and ASA 5500 series security appliances Version 7.1(1) introduce significant enhancements to VPN services and management/monitoring features. ASDM supports these new platform features. In addition, ASDM adds support for the new Content Security and Control SSM in the ASA 5500 series security appliances.

This document contains release information about ASDM only. For detailed information on new platform features, see [Cisco ASA 5500 Series Release Notes Version 7.1\(1\)](#).

## New Device Manager Features

The following list highlights the new device manager features in this release:

- WebVPN sections of ASDM have been reorganized to simplify configuration tasks and to support the new WebVPN/SSL VPN features found in ASA Version 7.1(1).
- ASDM and WebVPN can now run on the same interface simultaneously.
- ASDM introduces support for syslog correlation to the access rule that triggered a system log message.
- Configuration, monitoring and management of the new Control Security and Control SSM
- Support for management of IPS 5.0 and 5.1 on AIP SSM modules.
- ASDM Demo Mode initial support.

For improvements to the Cisco 5500 series ASA security appliance software, see the [Cisco ASA 5500 Series Release Notes Version 7.1\(1\)](#).

## System Requirements

This section includes the following topics:

- [Hardware Requirements](#)
- [Client PC Operating System and Browser Requirements](#)

## Hardware Requirements

ASDM software runs on the following platforms:

- Cisco ASA 5510
- Cisco ASA 5520
- Cisco ASA 5540
- SSM 10
- SSM 20

- PIX 515/515E
- PIX 525
- PIX 535



**Note** ASDM is not currently supported on PIX 501, PIX 506/506E, or PIX 520 hardware.

For more information on minimum hardware requirements, see:

<http://www.cisco.com/en/US/docs/security/asa/asa70/asdm50/webhelp/sysreq.html>

Certain features, such as load balancing and QoS, require particular hardware platforms. Other features require licensing. For more information on feature support for each platform license, see:

[http://www.cisco.com/en/US/docs/security/asa/asa70/asdm50/webhelp/gen\\_info\\_licenses.html](http://www.cisco.com/en/US/docs/security/asa/asa70/asdm50/webhelp/gen_info_licenses.html)

## Client PC Operating System and Browser Requirements

Table 1 lists the supported and recommended PC operating systems and browsers for Version 5.0.

**Table 1** *Operating System and Browser Requirements*

	Operating System	Browser	Other Requirements
Windows <sup>1</sup>	Windows 2000 (Service Pack 4) or Windows XP operating systems	Internet Explorer 6.0 with Sun Java <sup>2</sup> Plug-in 1.4.2 or 1.5.0  <b>Note</b> <b>HTTP 1.1</b> —Settings for Internet Options > Advanced > HTTP 1.1 should use HTTP 1.1 for both proxy and non-proxy connections.  Netscape 7.1/7.2 with Sun Java Plug-in 1.4.2 or 1.5.0	<b>SSL Encryption Settings</b> —All available encryption options are enabled for SSL in the browser preferences.
Sun Solaris	Sun Solaris 8 or 9 running CDE window manager	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2 or 1.5.0	
Linux	Red Hat Linux 9.0 or Red Hat Linux WS, Version 3 running GNOME or KDE	Mozilla 1.7.3 with Sun Java Plug-in 1.4.2 or 1.5.0	

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

2. Get Sun Java from [java.sun.com](http://java.sun.com)

## Usage Notes

This section includes the following topics:

- [Upgrading to a New Software Release](#)
- [Getting Started with ASDM](#)
- [Unsupported Characters](#)
- [ASDM CLI Does Not Support Interactive User Commands](#)

- [Printing from ASDM](#)
- [Unsupported Commands](#)
- [Securing the Failover Key](#)

## Upgrading to a New Software Release

If you have a Cisco Connection Online (CCO) login, you can obtain software from the following website:

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

See the *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0* for more information.



### Note

Before you upgrade your device manager, upgrade your platform software to Cisco PIX software Version 7.1.

### Upgrading from PIX Device Manager to ASDM.

To upgrade from PIX Device Manager to ASDM, perform the following steps:

- 
- Step 1** Copy the ASDM binary file (asdm-511.bin) to a TFTP or FTP server on your network.
  - Step 2** Log in to your security appliance using the console (or other appropriate method that you have configured).
  - Step 3** Ensure that you have connectivity from your security appliance to your TFTP/FTP server.
  - Step 4** If you have an existing copy of the PIX Device Manager, delete it:
 

```
delete flash:/pdm
```
  - Step 5** Copy the ASDM binary onto your security appliance using the appropriate command:
    - For TFTP: `copy tftp://your-server-IP/pathtofile flash:/asdm-511.bin`
    - For FTP: `copy ftp://your-server-IP/pathtofile flash:/asdm-511.bin`



### Note

For more information on the `copy` command and its options, see the *Cisco Security Appliance Command Reference*.

- 
- Step 6** If you have more than one ASDM image, enter the following command to configure the location of the ASDM image:
 

```
asdm image flash:/asdm511.bin
```
  - Step 7** Enter the following command to enable the HTTPS server on the device:
 

```
http server enable
```
  - Step 8** Identify the systems or networks that are allowed to access ASDM by specifying one or more hosts/networks, using the following command:
 

```
http 10.1.1.1 255.255.255.255 inside
```

where IP address 10.1.1.1 is a host that can access ASDM and which is connected via the inside interface. See the *Cisco Security Appliance Command Reference* for more information on the options to the **http** command.

- Step 9** Verify that ASDM is installed correctly by connecting from the client system (10.1.1.1 in the preceding example) to the security appliance, using a supported browser. For example:

```
https://10.1.1.254/admin/
```

where 10.1.1.254 is the IP address of the inside interface of the device in Step 8.



**Note**

ASDM requires Java Plug-in software. After you install ASDM, download the latest Java Plug-in from the following site: <http://www.cisco.com/cgi-bin/tablebuild.pl/java2>.

## Upgrading to ASDM 5.1(1) from 5.0(1) or Higher

To upgrade to ASDM 5.1(1) from Version 5.0(1) or higher, perform the following the steps:

- 
- Step 1** Copy the ASDM binary file (asdm-511.bin) and the ASA software to a TFTP or FTP server on your network.
- Step 2** Delete existing ASDM 5.0(1) and ASA/PIX 7.0(1) binary images from flash using **Tools > File Management** feature.
- Step 3** Upload the ASA or PIX Version 7.1(1) image from your local PC to the device flash using **Tools > Software Upgrade**.
- Step 4** Upload the ASDM 5.1(1) image from your local PC to the device Flash using **Tools > Software Upgrade**. During upload a warning will appear that this is not a valid ASDM image file. You can safely ignore this warning.
- Step 5** Using **Configuration -> Device Admin > Boot Config/Image**, set the boot image for ASA/PIX and ASDM image to the correct images loaded into Flash. A warning will appear that the ASDM image is not a valid image file when applying configuration, but you can safely ignore this warning and submit the configuration.
- Step 6** Save the configuration clicking **Save**.
- Step 7** Reboot the device using **Tools > System Reload**. After the device boots up, the ASA or PIX version will be Version 7.1(1) and ASDM version will be Version 5.1(1).

## Deleting Your Old Cache

In early beta releases of ASDM and in previous releases of PDM (Versions 4.1 and earlier), the device manager stored its cache in: <userdir>\pdmcache. For example, D:\Documents and Settings\jones\pdmcache.

Now, the cache directory for ASDM is located in: <user dir>\.asdm\cache.

The File > Clear ASDM Cache option in ASDM clears this new cache directory. It does not clear the old one. To free up space on your system, if you are no longer using your older versions of PDM or ASDM, delete your pdmcache directory manually.

## Getting Started with ASDM

If you are using ASDM for the first time on a new security appliance, follow the instructions in this section to get started using ASDM. If you are upgrading an existing device, see [Upgrading to a New Software Release, page 4](#).

Because ASDM uses a GUI interface, it requires that you access it from a PC using a supported web browser. For the supported browsers, see the “[Client PC Operating System and Browser Requirements](#)” section on page 3.

### Before You Begin




---

**Note** The following uses a PIX security appliance in single mode. If you are using an ASA security appliance, use the `Management0/0` interface in place of `Ethernet1`.

---

The following list shows the steps to take before using ASDM for the first time:

- 
- Step 1** Set up your security appliance.
  - Step 2** Connect your PC directly to the security appliance via the port Ethernet 1.
  - Step 3** Do one of the following:
    - Either configure your PC for DHCP, or
    - Make sure your PC is on the same subnet as the security appliance. (The default IP address for the security appliance is: 192.168.1.1. The default subnet mask is 255.255.255.0.)
    - If you want to configure transparent firewall mode on your security appliance, enter the CLI **setup** command. See the [Cisco Security Appliance Command Line Configuration Guide](#) for more information.
- 

### Starting ASDM




---

**Note** If you have a pop-up blocker, remember to disable it before starting ASDM.

---

The following list shows the steps to take to start ASDM for the first time:

- 
- Step 1** Start ASDM from a supported web browser connected to the security appliance by entering the URL:  
`https://192.168.1.1/admin/`  
where 192.168.1.1 is the IP address of the security appliance.




---

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

---

- Step 2** Click **OK** or **Yes** to all prompts, including the name and password prompt. No name or password is required for a new device.

If ASDM does not start, check the device configuration. Your security appliance should be configured to accept ASDM configuration on its inside interface. (A new security appliance is configured this way by default.) If you need to modify the configuration to reestablish this default setting, use the CLI. Include configuration information similar to the following.



**Note** The following uses a PIX security appliance in single mode. If you are using an ASA security appliance, use the `Management0/0` interface in place of `Ethernet1`.

```
interface Ethernet1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
http server enable
http 0.0.0.0 0.0.0.0 inside
```

where the IP address 192.168.1.1 is on the same subnet as your security appliance and `inside` is the default name of the interface. (You might give your interface a different name, such as “management.”)

The **http server enable** command with the `inside` argument enables the HTTP(S) server on the security appliance interface named `inside`. The **http** command with the `0.0.0.0 0.0.0.0` arguments allows HTTP traffic from any and all IP addresses and subnet masks to the HTTP server through the interface named `inside`. For more information, see the **http** and **http server enable** commands in the [Cisco Security Appliance Command Reference](#).



**Note** See the **configure factory defaults** or **setup** command in the [Cisco Security Appliance Command Line Configuration Guide](#) for more information on using the CLI to reestablish factory default settings.

## Using the Startup Wizard

The Startup Wizard helps you easily configure a single mode device or a context of a multiple mode device.

The following list shows the steps to use the Startup Wizard to configure the basic set-up of your security appliance:

- Step 1** If your security appliance is in multi mode, for each new context, do the following:
- a. Create a new context using the **System > Configuration > Features > Security Context** panel.
  - 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 **Context** icon on the upper header bar and select the context name from the Context menu on the lower header bar.
  - e. Click **Context > Configuration > Wizards > Startup**.
  - f. Click **Launch Startup Wizard**.

*If your security appliance is in single mode:*

- a. Click **Configuration > Wizards > Startup**.
- b. Click **Launch Startup Wizard**.

- Step 2** Click **Next** as you proceed through the Startup Wizard panels, filling in the appropriate information in each panel, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.
- Step 3** Click **Finish** on the last panel to transmit your configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of your connection changes.
- 

(Optional.) You can now enter other configuration details on the **Configuration > Features** panels.

## VPN Wizard

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

The following list shows the steps to start the VPN Wizard:

- 
- Step 1** Start ASDM.
- Step 2** Click **Configuration > Wizards > VPN**. Click **Launch VPN Wizard**.
- Step 3** Supply information on each wizard panel. Click **Next** to move through the VPN Wizard panels. You may use the default IPsec and IKE policies. Click the **Help** button for more information on each field.
- Step 4** After you complete entering the VPN Wizard information, click **Finish** on the last panel to transmit your configuration to the security appliance.

You can now test the configuration.

---

## Bootstrapping LAN Failover

This section describes how to implement failover on security appliances connected via a LAN.

If you are connecting two ASA security appliances for failover, you must connect them via a LAN. If you are connecting two PIX security appliances, you can connect them using either a LAN or a serial cable.



**Tip** If your PIX security appliances are located near each other, you might prefer connecting them with a serial cable to connecting them via the LAN. Although the serial cable is slower than a LAN connection, using a cable prevents having to use an interface or having LAN and state failover share an interface, which could affect performance. Also, using a cable enables the detection of power failure on the peer device.

---

As specified in the *Cisco Security Appliance Command Line Configuration Guide*, both devices must have appropriate licenses and have the same hardware configuration.

Before you begin, decide on active and standby IP addresses for the interfaces ASDM connects through on the primary and secondary devices. These IP addresses must be assigned to device interfaces with HTTPS access.

To configure LAN failover on your security appliance, perform the following steps:

**Step 1** Configure the secondary device for HTTPS IP connectivity. Use the **configure factory defaults** or the **setup** CLI command to assign the standby IP address to the ASDM interface on the secondary device.

**Step 2** After configuration, the secondary device, has a configuration such as the following. (If you are using an ASA security device, replace the interface `Ethernet1` with `Management0/0`.)

```
interface Ethernet1
  nameif inside
  security-level 100
  ip address 192.168.1.2 255.255.255.0
http server enable
http 0.0.0.0 0.0.0.0 inside
```

where in this example IP address 192.168.1.2 is the standby IP address of the ASDM interface on the secondary device.

**Step 3** Configure the primary device for HTTPS IP connectivity using the active IP address for the ASDM interface.

**Step 4** Connect the pair of devices together and to their networks in their failover LAN cable configuration.

**Step 5** Start ASDM from the primary device through a supported web browser. (See the section [Starting ASDM](#), page 6.)

**Step 6** Perform one of the following steps, depending on your security context mode:

- a. If your device is in multiple security context mode, click **Context**. Choose the **admin** context from the **Context** drop-down menu, and click **Configuration > Features > Properties > Failover**.
- b. If your device is in single mode, click **Configuration > Features > Properties > Failover**. Click the **Interfaces** tab.

**Step 7** Perform one of the following steps, depending on your firewall mode:

- a. If your device is in routed mode: configure standby addresses for all routed mode interfaces.
- b. If your device is in transparent mode: configure a standby management IP address.



**Note** Interfaces used for failover connectivity should not have names (in single mode) or be allocated to security contexts (in multiple security context mode). In multiple context mode, other security contexts may also have standby IP addresses configured.

**Step 8** Perform one of the following steps, depending on your security context mode:

- a. If your device is in multiple security context mode: click **System > Configuration > Features > Failover**.
- b. If your device is in single mode: click **Configuration > Features > Properties > Failover**.

**Step 9** On the **Setup** tab of the **Failover** panel under **LAN Failover**, select the interface that is cabled for LAN failover.

**Step 10** Configure the remaining **LAN Failover** fields.

**Step 11** (Optional) Provide information for other fields in all of the failover tabs. If you are configuring Active/Active failover, you must configure failover groups in multiple security context mode. If more than one failover pair of devices coexist on a LAN in Active/Active failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.

**Step 12** On the **Setup** tab, check the **Enable Failover** check box. If you are using the PIX 500 series security appliance, select the **Enable LAN rather than serial cable failover** check box.

- Step 13** Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.
- Step 14** Enter the IP address of the secondary device, which you configured as the standby IP address of the ASDM interface. Wait about 60 seconds. The standby peer still could become temporarily inaccessible.
- Step 15** Click **OK**. Wait for configuration to be synchronized to the standby device over the failover LAN connection.

The secondary device should now enter standby failover state using the standby IP addresses. Any further configuration of the active device or an active context is replicated to the standby device or the corresponding standby context.

## ASA Interface Supports Either WebVPN or ASDM Admin Session

The security appliance supports either WebVPN or an ASDM administrative session on an interface, but not both simultaneously. To use ASDM and WebVPN at the same time, configure them on different interfaces.

## 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 language other than English, be careful not to enter non-English characters accidentally.

*Workaround:*

For workarounds, see CSCeh39437 under [Caveats, page 18](#).

## ASDM CLI Does Not Support Interactive User Commands

ASDM provides a CLI tool (click **Tools > Command Line Interface**) that allows you to enter certain CLI commands from ASDM. For a list of specific commands that are not supported, see [Unsupported Commands, page 11](#).

The ASDM CLI feature also 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
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 panels.
- For CLI commands that have a noconfirm option, use the noconfirm option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

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

## 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. In the case of the **alias** command, ASDM enters Monitor-only mode until you remove the command from 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, see **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 3 by your system administrator, which allows Monitor-only mode. For more information, see **Configuration > Device Administration > User Accounts** and **Configuration > Device Administration > AAA Access**.

## Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when added by 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 it is view-only, then the command appears in the GUI, but you cannot edit it.

Unsupported Commands	ASDM Behavior
<b>access-list</b>	Ignored if not used, except for use in VPN group policy screens
<b>capture</b>	Ignored
<b>established</b>	Ignored
<b>failover timeout</b>	Ignored
<b>ipv6</b> , any IPv6 addresses	Ignored
<b>object-group icmp-type</b>	View-only
<b>object-group network</b>	Nested group is view-only
<b>object-group protocol</b>	View-only
<b>object-group service</b>	Nested group cannot be added
<b>pager</b>	Ignored
<b>pim accept-register route-map</b>	Ignored. Only the <b>list</b> option can be configured using ASDM
<b>prefix-list</b>	Ignored if not used in an OSPF area
<b>route-map</b>	Ignored
<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>sysopt nodnsalias</b>	Ignored
<b>sysopt uauth allow-http-cache</b>	Ignored

Unsupported Commands	ASDM Behavior
terminal	Ignored
virtual	Ignored

## ASDM Limitations

ASDM does not support the one-time password (OTP) authentication mechanism.

## Other CLI Limitations

- 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
```

## Securing the Failover Key

To prevent the failover key from being replicated to the peer unit in clear text for an existing failover configuration, disable failover on the active unit (or in the system execution space on the unit that has failover group 1 in the active state), enter the failover key on both units, and then reenables failover. When failover is reenables, the failover communication is encrypted with the key.

Follow this procedure on the active device:

- 
- Step 1** Perform one of the following steps, depending on your security context mode:
- If your device is in single mode, navigate to **Configuration > Features > Properties > Failover > Setup**.
  - If your device is in multiple mode, navigate to **System > Configuration > Features > Failover > Setup**.
- Step 2** Turn off failover. (The standby should switch to pseudo-standby mode.)
- Uncheck the **Enable failover** check box.
  - Click **Apply**. (Click **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** box.
- Step 4** Reenable failover.
- Check the **Enable failover** check box.
  - Click **Apply**. (Click **OK** if CLI preview is enabled.) A dialog box about configuring the peer appears.
- Step 5** Enter the IP address of the peer. Wait about 60 seconds. Even though the standby peer does not have the shared failover key, the standby peer still could become inaccessible.
- Step 6** Click **OK**. (Click **OK** if CLI preview is enabled.) Wait for configuration to be synchronized to the standby device over the encrypted failover LAN connection.

# Platform Feature Licenses

The following tables list the feature support for each platform license.


**Note**

Items that are in italics are separate, optional licenses that you can add on to a base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the VPN Plus license plus the GTP/GPRS license; or all four licenses together.

**Table 0-2 ASA 5500 Series Adaptive Security Appliance License Features**

Platforms and Features	Licenses	
<b>ASA 5510</b>	<b>Base License</b>	<b>Security Plus</b>
Security Contexts	No support	No support
VPN Sessions <sup>1</sup>	250 combined IPSec and WebVPN	250 combined IPSec and WebVPN
Max. IPSec Sessions	250	250
Max. WebVPN Sessions	2	2
	<i>Add-on Licenses:</i>	<i>Add-on Licenses:</i>
	10 25 50 100 250	10 25 50 100 250
VPN Load Balancing	No support	No support
Failover	None	Active/Standby
GTP/GPRS	Not supported	Not supported
Maximum VLANs	10	25
Concurrent Firewall Connections <sup>2</sup>	50 K	130 K
Max. Physical Interfaces	3 at 10/100 plus the Management interface for management traffic only (to-the-security-appliance)	Unlimited
Encryption	Base (DES) <i>Add-on license: Strong (3DES/AES)</i>	Base (DES) <i>Add-on license: Strong (3DES/AES)</i>
Minimum RAM	256 MB	256 MB
<b>ASA 5520</b>	<b>Base License</b>	
Security Contexts	2	<i>Add-on Licenses:</i>
	5 10 20	
VPN Sessions <sup>1</sup>	750 combined IPSec and WebVPN	
Max. IPSec Sessions	750	
Max. WebVPN Sessions	2	<i>Add-on Licenses:</i>
	10 25 50 100 250 500 750	
VPN Load Balancing	Supported	
Failover	Active/Standby Active/Active	
GTP/GPRS	None	<i>Add-on license: Enabled</i>
Maximum VLANs	100	

**Table 0-2 ASA 5500 Series Adaptive Security Appliance License Features (continued)**

Platforms and Features	Licenses									
Concurrent Firewall Connections <sup>2</sup>	280 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		<i>Add-on license: Strong (3DES/AES)</i>							
Minimum RAM	512 MB									
<b>ASA 5540</b>	<b>Base License</b>									
Security Contexts	2		<i>Add-on licenses:</i>							
			5	10	20	50				
VPN Sessions <sup>1</sup>	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2		<i>Add-on Licenses:</i>							
			10	25	50	100	250	500	750	1000
VPN Load Balancing	Supported									
Failover	Active/Standby Active/Active									
GTP/GPRS	None		<i>Add-on license: Enabled</i>							
Maximum VLANs	200									
Concurrent Firewall Connections <sup>2</sup>	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		<i>Add-on license: Strong (3DES/AES)</i>							
Minimum RAM	1024 MB									

1. Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

**Table 0-3 PIX 500 Series Security Appliance License Features**

Platforms and Features	Licenses										
PIX 515/515E <sup>1</sup>	R (Restricted)		UR (Unrestricted)			FO (Failover) <sup>2</sup>		FO-AA (Failover Active/Active) <sup>2</sup>			
Security Contexts	No support		2	<i>Add-on license:</i>		2	<i>Add-on license:</i>		2	<i>Add-on license:</i>	
				5			5			5	
IPSec Sessions	2000		2000			2000		2000			
Failover	No support		Active/Standby Active/Active			Active/Standby		Active/Standby Active/Active			

Table 0-3 PIX 500 Series Security Appliance License Features (continued)

Platforms and Features	Licenses																	
GTP/GPRS	None	<i>Add-on license: Enabled</i>		None	<i>Add-on license: Enabled</i>		None	<i>Add-on license: Enabled</i>		None	<i>Add-on license: Enabled</i>							
Maximum VLANs	10			25			25			25								
Concurrent Firewall Connections <sup>3</sup>	48 K			130 K			130 K			130 K								
Max. Physical Interfaces	3			6			6			6								
Encryption	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>						
Minimum RAM	64 MB			128 MB			128 MB			128 MB								
<b>PIX 525<sup>1</sup></b>	<b>R (Restricted)</b>			<b>UR (Unrestricted)</b>			<b>FO (Failover)<sup>2</sup></b>			<b>FO-AA (Failover Active/Active)<sup>2</sup></b>								
Security Contexts	No support			2	<i>Add-on licenses:</i>				2	<i>Add-on licenses:</i>				2	<i>Add-on licenses:</i>			
					5	10	20	50		5	10	20	50		5	10	20	50
IPSec Sessions	2000			2000			2000			2000								
Failover	No support			Active/Standby Active/Active			Active/Standby			Active/Standby Active/Active								
GTP/GPRS	None	<i>Add-on license: Enabled</i>		None	<i>Add-on license: Enabled</i>		None	<i>Add-on license: Enabled</i>		None	<i>Add-on license: Enabled</i>							
Maximum VLANs	25			100			100			100								
Concurrent Firewall Connections <sup>3</sup>	140 K			280 K			280 K			280 K								
Max. Physical Interfaces	6			10			10			10								
Encryption	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>	None	<i>Add-on license: Base (DES)</i>	<i>Add-on license: Strong (3DES/AES)</i>						
Minimum RAM	128 MB			256 MB			256 MB			256 MB								
<b>PIX 535<sup>1</sup></b>	<b>R (Restricted)</b>			<b>UR (Unrestricted)</b>			<b>FO (Failover)<sup>2</sup></b>			<b>FO-AA (Failover Active/Active)<sup>2</sup></b>								

**Table 0-3 PIX 500 Series Security Appliance License Features (continued)**

Platforms and Features	Licenses											
	No support			2			2			2		
Security Contexts	No support			Add-on licenses:			Add-on licenses:			Add-on licenses:		
	5	10	20	50	5	10	20	50	5	10	20	50
IPSec Sessions	2000			2000			2000			2000		
Failover	No support			Active/Standby Active/Active			Active/Standby			Active/Standby Active/Active		
GTP/GPRS	None	Add-on license: Enabled		None	Add-on license: Enabled		None	Add-on license: Enabled		None	Add-on license: Enabled	
Max. VLANs	50			150			150			150		
Concurrent Firewall Connections <sup>3</sup>	250 K			500 K			500 K			500 K		
Max. Physical Interfaces	8			14			14			14		
Encryption	None	Add-on license: Base (DES)	Add-on license: Strong (3DES/ AES)	None	Add-on license: Base (DES)	Add-on license: Strong (3DES/ AES)	None	Add-on license: Base (DES)	Add-on license: Strong (3DES/ AES)	None	Add-on license: Base (DES)	Add-on license: Strong (3DES/ AES)
Minimum RAM	512 MB			1024 MB			1024 MB			1024 MB		

1. The PIX 500 series security appliance does not support WebVPN or VPN load balancing.
2. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
3. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

## ASDM Demo Mode

ASDM Demo Mode is available as a separately installed application running under Windows 2000 and Windows XP. 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 PIX/ASA features using the ASDM interface.
- Perform configuration and monitoring tasks with the Content Security and Control SSM (CSC SSM).

You can choose to connect to a real device or utilize ASDM Demo Mode from the ASDM Launcher main window. By checking the **Run in Demo Mode** check box, you will be presented with a list of device types and configurations which are available. Select the device type, mode (routed/transparent) and configuration and ASDM will start up using that configuration and device type. You will see a **Demo Mode** label in the title bar of the window.

ASDM Demo Mode will provide simulated monitoring data, including real-time syslogs and security events from the CSC SSM. The data shown is randomly generated, but the experience is identical to what you would see when connecting to a real device.

The ASDM Demo Mode application will be made available to customers on CCO shortly after the release of ASDM 5.1(1). Until then, the **Run in Demo Mode** checkbox seen in the ASDM Launcher will not allow you to run in Demo Mode.

## ASDM and IPS Compatibility

Table 4 lists ASDM versions and their compatibility with versions of IPS.

**Table 4 ASDM and IPS Compatibility**

	IPS Version 5.0(1)	IPS Version 5.1(1)
ASDM Version 5.1(1)	Yes	Yes

## Caveats

The following sections describe caveats for the 5.1(1) release.



### Note

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

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

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

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

## Open Caveats - Release 5.1(1)

**Table 5 Open Caveats**

ID Number	Software Release 5.1(1)	
	Corrected	Caveat Title
CSCeg14905	No	Applying service group change causes no ACL CLI to be generated.
CSCeg69476	No	ASDM can not take any input from keyboard from SunOS 5.8 / Mozilla.
CSCeh06459	No	ASDM can not create appropriate ACL for QoS on outbound interface.
CSCeh20409	No	Startup Wizard allows not naming any interface.

**Table 5** Open Caveats (continued)

Software Release 5.1(1)		
ID Number	Corrected	Caveat Title
CSCeh53158	No	Wrong cmds sent when objgp w/Policy NAT is edited to add net-obj with NAT.
CSCsb61151	No	Disable/Enable of class in a service policy sends wrong commands
CSCsb92243	No	ASDM IPSec Rules display incorrectly when static policy NAT is used
CSCsc11004	No	CLI warning is not anticipated when creating a tunnel group
CSCsc60062	No	ASDM hangs and loops at 52% when processing ACLs with object-groups
CSCsc67049	No	IP Audit Policy configuration, interface tables combo box arrows missing
CSCsd02755	No	Source or Dest Interface Interface drop down should be greyed-out
CSCsd03819	No	ASDM location not created when adding a new host to an existing group
CSCsd06006	No	Syslog: Create Rule feature may not pre-assign the correct direction
CSCsd22635	No	<p>IPS tree occupies the whole screen the first time IPS button is clicked</p> <p><b>Conditions:</b> For ASA systems with an AIP SSM installed only. The first time a user visits the IPS portion of ASDM, the content area of the IPS window will be missing, with only the navigation tree visible.</p> <p><b>Workaround:</b> Navigate away from the IPS area (for instance to Interfaces, Security Policy, and so on) and then return to the IPS area. The content area will now be visible. Another workaround is to resize the ASDM window when the problem is encountered. The content area will then be shown correctly.</p>

## Resolved Caveats - Release 5.1(1)

The following list shows caveats that are resolved for Version 5.1(1):

**Table 6** Resolved Caveats

Software Release 5.1(1)		
ID Number	Corrected	Caveat Title
CSCsc10806	Yes	ASDM: VPN wizard should not create crypto ACL for remote access
CSCei16647	Yes	Cannot read iplog file downloaded from IDM/ASDM
CSCei17771	Yes	Lost connection during sensor sigupdate
CSCsc00847	Yes	Show Promiscuous as detail in SSM platform is misleading
CSCsc48264	Yes	Search by Field on Action field in rules table does not work properly
CSCsc48900	Yes	Notification email is not accepting dot characters
CSCsc63204	Yes	ASDM does not honour New Zealand Daylight Savings time (NZDT)
CSCsc99674	Yes	Access rule is incomplete for network groups
CSCsc08343	Yes	CSC Hostname configuration validation message is incorrect
CSCsc03070	Yes	ASDM should generate Warning if kerberos-realm is not in all uppercase
CSCeh64793	Yes	The date/time in IPS Time panel is not clear
CSCeh72088	Yes	Need to have the sig Type category in Signature Configuration panel

## 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 Quick Start 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*
- *Cisco PIX Security Appliance Release Notes*
- *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*

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/en/US/docs/general/illus\\_process/PDI/pdi.htm](http://www.cisco.com/en/US/docs/general/illus_process/PDI/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

<http://www.cisco.com/en/US/ordering/index.shtml>

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/en/US/support/index.html>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



### Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/en/US/support/index.html>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/en/US/support/index.html>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/cgi-bin/marketplace/welcome.pl>

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://www.cisco.com/en/US/products/index.html>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

---

This document is to be used in conjunction with the documents listed in “[Related Documentation](#)” section.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0601R)

© 2006 Cisco Systems, Inc.  
All rights reserved.

