



# Cisco ASDM Release Notes Version 5.2(1)

---

## August 2006

This document contains release information for Cisco ASDM Version 5.2(1) on Cisco PIX 500 series and Cisco ASA 5500 series security appliances Version 7.2(1). It includes the following sections:

- [Introduction, page 1](#)
- [New Device Manager Features, page 2](#)
- [New Security Appliance Features, page 3](#)
- [Client PC Operating System and Browser Requirements, page 5](#)
- [Caveats, page 23](#)
- [Upgrading ASDM, page 12](#)
- [Getting Started with ASDM, page 13](#)
- [ASDM Limitations, page 20](#)
- [ASDM and SSM Compatibility, page 12](#)
- [Caveats, page 23](#)
- [Related Documentation, page 25](#)
- [Obtaining Documentation, page 25](#)
- [Documentation Feedback, page 26](#)
- [Obtaining Technical Assistance, page 26](#)
- [Obtaining Additional Publications and Information, page 28](#)

## 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**

© 2006 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 7.2(1). Its secure, web-based design enables anytime, anywhere access to security appliances.

## New Device Manager Features

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

- Support for the ASA 5505 and ASA 5550.
- Supports IPS Version 6.0 and later.
- **Packet Tracer**—The new patent-pending Packet Tracer tool lets you easily trace the life span of a packet through the security appliance in an animated packet flow model to see if it is behaving as expected and simplify troubleshooting no matter how complex the network design. The tool provides the attributes of a packet such as source and destination IP addresses with a visual representation of the different phases of the packet and the relevant configuration, which is accessible with a single click. For each phase, it displays whether the packet is dropped or allowed.
- The traceroute tool lets you trace the route of a packet to its destination.
- **Enhanced ASDM rules table**—The ASDM rule tables have been redesigned to streamline policy creation. In addition to simplified rule creation that maps more closely with CLI, the rule tables support most configuration scenarios including super-netting and using an object group that is associated to more than interface. The use of ASDM location and ASDM group was removed to simplify the creation of rules. You now have the ability to:
  - Create objects, object-groups and rules from a single panel
  - Filter on interfaces, source, destination or services
  - Policy query in the rule table for advanced filtering using multiple conditions
  - Show logs for a particular access rule in the real time log viewer
  - Select a rule and packet trace with a single click which will populate with appropriate packet attributes
  - Easily organize and move up and down in the table to change the order of access list entries
  - Expand and display elements in an object group
  - See attributes of an object or members of a group via tooltips
- The High Availability and Scalability Wizard is used to simplify configuration of Active/Active, Active/Standby failover and VPN Load balancing. The wizard also intelligently configures the peer device.
- Enhancements to the syslog features include:
  - Syslog parsing to display source IP, destination IP, syslog ID, date and time into different columns
  - Integrated syslog references with explanations and recommended actions for each syslog with a single click
  - Syslog coloring based on severity level
  - A brief explanation of the syslogs as a tool tip in the log viewer
- The creation of NAT rules is simplified.
- There is now full ASDM support of network, service, protocol and ICMP-type object groups.

- The ability to create a name to be associated with an IP Address now exists.
- The new ASDM Assistant provides task-oriented guidance to configuring features such as AAA server, logging filters, SSL VPN Client, and others features. You can also upload new guides.
- Context management is improved, including context caching and better scalability.
- Enhancements to Application Inspection include the following:
  - Support for DNS, ESMTP, H.323, IM, SCCP (Skinny) and other protocols.
  - Predefined low, medium and high security settings simplify creation and management of inspection maps.
  - RADIUS Accounting inspection maps allow inspection of management traffic to the device.

## New Security Appliance Features

The following lists some of the new features supported by the security appliance.

- The Cisco ASA 5505 Easy VPN supports hardware client feature parity with the Cisco VPN 3002 and Cisco PIX501/506.
- The Cisco ASA 5505 has Power over Ethernet (PoE) switch ports that can be used for PoE devices, such as IP phones. However, these ports are not restricted to that use. They can also be used as Ethernet switch ports.
- The Cisco ASA 5505 includes the ability to detect and prevent the use of non-Cisco memory, SSM modules, SSC cards, or other modules in the security appliance. It also detect the presence of obsolete and prototype hardware. It authenticates all modules, starting with the host (itself). It disables or reboots any module that fails authentication.
- Enhanced Application Inspection and Control. Many enhancements for the Application Inspection and Control are supported in ASA Version 7.2(1). For a complete list, see the [Cisco ASA 5500 Series Release Notes Version 7.2\(1\)](#)
- Online Certificate Status Protocol (OCSP), which provides an alternative to CRL for obtaining the revocation status of X.509 digital certificates, is supported.
- The security appliance supports RIP Version 1 and RIP Version 2.
- Layer 2 Tunneling Protocol (L2TP) over IPSec is supported.
- The security appliance supports Network Access Control (NAC) with a configured ACS.
- You can establish a VPN using a handheld Nokia 92xx Communicator series cellular device for remote access.
- You can include the security appliance in a network that deploys the Zone Labs Integrity System for enforcement of security policies on remote VPN clients.
- You can configure hybrid authentication to enhance the IKE security between the security appliance and remote users.
- You can monitor additional IPSec fragmentation and reassembly statistics that are helpful in debugging IPSec-related fragmentation and reassembly issues.
- PPPoE clients are supported.
- You can create dynamic DNS (DDNS) update methods and configure them to update the Resource Records (RRs) on the DNS server at whatever frequency you need.

- The multicast routing enhancements let you define multicast boundaries so that domains with RPs that have the same IP address do not leak into each other, filter PIM neighbors to better control the PIM process, and filter PIM bidir neighbors to support mixed bidirectional and sparse-mode networks.
- You can assign a private MAC address (both active and standby for failover) for each interface. For multiple context mode, you can automatically generate unique MAC addresses for shared context interfaces, which makes classifying packets into contexts more reliable.
- Failover now responds to a failure in less than a second.
- This feature lets you configure a link standby ISP in case the link to your primary ISP fails. It uses static routing and object tracking to determine the availability of the primary route and to activate the secondary route when the primary fails.
- You can use DNS domain names, such as `www.example.com`, when configuring AAA servers and also with the ping and traceroute features.
- RTP and RTCP inspection monitors call signaling traffic and performs message validation for VoIP. It also NATs embedded IP addresses and opens pinholes for RTP and RTCP traffic.
- Generic input rate limiting is introduced to prevent Denial of Service attacks on a firewall or on certain inspection engines on a firewall.
- Long URL filtering, HTTPS filtering, and FTP filtering are enabled using both Websense (the current vendor) and N2H2 (a vendor that has been purchased by Secure Computing).
- The Auto Update feature now includes the ability to poll multiple Auto Update servers, and the ability to configure the security appliance to poll Auto Update servers on a single day, or any combination of days and times of day. You can also randomize the time of polling for any configured day, or combination of days.
- Dead Connection Detection (DCD) allows the adaptive security appliance to automatically detect and expire dead connections.
- You can now save all context configurations at once from the system execution space.
- You can now allow any traffic to enter and exit the same interface, and not just VPN traffic.
- You can now define a Layer 3/4 class map for to-the-security-appliance traffic, so you can perform special actions on management traffic. For this version, you can inspect RADIUS accounting traffic.
- The packet tracer tool lets you trace the life span of a packet through the security appliance to see if it is behaving as expected. The traceroute tool lets you trace the route of a packet to its destination.
- The Web Cache Communication Protocol (WCCP) feature lets you specify WCCP service groups and redirect web cache traffic.
- You can configure the security appliance to require that IPv6 addresses for directly connected hosts use the Modified-EUI format for the interface identifier portion of the address.
- Gatekeeper Routed Control Signaling (GKRCS), and Direct Call Signaling (DCS) control signaling methods are supported.
- SCCP version 4.1.2 messages and CCM 4.0.1 messages are supported.
- SIP IP address privacy is supported.
- Inspection, IPS, and Trend Micro for WebVPN traffic in clientless mode and port forwarding mode is supported.

For additional information see the online help for particular features. For improvements to the Cisco 5500 series ASA security appliance software, see the [Cisco ASA 5500 Series Release Notes Version 7.2\(1\)](#).

# Client PC Operating System and Browser Requirements

Table 1 lists the supported and recommended PC operating systems and browsers for Version 5.2(1).

**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 (English or Japanese versions) | Internet Explorer 6.0 with Sun Java <sup>2</sup> Plug-in 1.4.2 or 5.0 (1.5.0) -or-<br>Firefox 1.5 with Java Plug-in 1.4.2 or 5.0 (1.5.0)<br><br><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. | <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 Desktop, Red Hat Enterprise Linux WS version 3 running GNOME or KDE                  | Firefox 1.5 with Java Plug-in 1.4.2 or 5.0 (1.5.0) <sup>3</sup>  |  |

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)
3. On Windows and Linux, Firefox 1.5 replaces Mozilla 1.7.3, which was used in previous ASDM releases.

## 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 and Solaris](#)

### 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** Close all instances of Internet Explorer or Netscape.
  - 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 and Solaris

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

---

**Step 1** Close all instances of Netscape or Mozilla.

**Step 2** Bring up Java Plug-in Control Panel by launching the ControlPanel executable file.



**Note**

In the Java 2 SDK, this file is located in *SDK installation directory*/jre/bin/ControlPanel. For example if your 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

This software version supports the following platforms; see the associated tables for the feature support for each model:

- ASA 5505, [Table 2](#)
- ASA 5510, [Table 3](#)
- ASA 5520, [Table 4](#)
- ASA 5540, [Table 5](#)
- ASA 5550, [Table 6](#)

- PIX 515/515E, [Table 7](#)
- PIX 525, [Table 8](#)
- PIX 535, [Table 9](#)

**Note**

Items that are in italics are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 WebVPN license plus the GTP/GPRS license; or all four licenses together.

**Table 2** *ASA 5505 Adaptive Security Appliance License Features*

| ASA 5505                               | Base License  |  | Security Plus                                       |  |
|--|---|--|---|--|
| Users, concurrent <sup>1</sup>         | 10  | <i>Optional Licenses:</i>                  | 10  | <i>Optional Licenses:</i>                  |
|  |   | 50 <i>Unlimited</i>                        |   | 50 <i>Unlimited</i>                        |
| Security Contexts                      | No support  |  | No support  |  |
| VPN Sessions <sup>2</sup>              | 10 combined IPSec and WebVPN  |  | 25 combined IPSec and WebVPN                        |  |
| Max. IPSec Sessions                    | 10  |  | 25  |  |
| Max. WebVPN Sessions                   | 2   | <i>Optional License: 10</i>                | 2   | <i>Optional License: 10</i>                |
| VPN Load Balancing                     | No support  |  | No support  |  |
| Failover                               | None  |  | Active/Standby (no stateful failover)               |  |
| GTP/GPRS                               | No support  |  | No support  |  |
| Maximum VLANs/Zones                    | 3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone) |  | 5 (3 zones, 1 failover link, and 1 backup ISP link) |  |
| Concurrent Firewall Conns <sup>3</sup> | 10 K  |  | 25 K  |  |
| Max. Physical Interfaces               | Unlimited, assigned to VLANs/zones  |  | Unlimited, assigned to VLANs/zones                  |  |
| Encryption                             | Base (DES)  | <i>Optional license: Strong (3DES/AES)</i> | Base (DES)  | <i>Optional license: Strong (3DES/AES)</i> |
| Minimum RAM                            | 128 MB  |  | 128 MB  |  |

1. In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit only when they communicate with the outside (Internet VLAN). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host command** to view the host limits.
2. 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.
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.

**Table 3** *ASA 5510 Adaptive Security Appliance License Features*

| ASA 5510          | Base License |  | Security Plus |                           |
|-------------------|--------------|--|---------------|---------------------------|
| Users, concurrent | Unlimited    |  | Unlimited     |                           |
| Security Contexts | No support   |  | 2             | <i>Optional Licenses:</i> |
|                   |              |  |               | 5                         |

**Table 3** ASA 5510 Adaptive Security Appliance License Features (continued)

| ASA 5510                               | Base License  |  |    |    |     | Security Plus                   |  |                           |    |    |     |     |
|--|---|--|----|----|-----|---------------------------------|--|---------------------------|----|----|-----|-----|
| VPN Sessions <sup>1</sup>              | 250 combined IPsec and WebVPN   |  |    |    |     | 250 combined IPsec and WebVPN   |  |                           |    |    |     |     |
| Max. IPsec Sessions                    | 250   |  |    |    |     | 250                             |  |                           |    |    |     |     |
| Max. WebVPN Sessions                   | 2   | <i>Optional Licenses:</i>                  |    |    |     |                                 | 2  | <i>Optional Licenses:</i> |    |    |     |     |
|  |   | 10   | 25 | 50 | 100 | 250                             |  | 10                        | 25 | 50 | 100 | 250 |
| VPN Load Balancing                     | No support  |  |    |    |     | No support                      |  |                           |    |    |     |     |
| Failover                               | None  |  |    |    |     | Active/Standby or Active/Active |  |                           |    |    |     |     |
| GTP/GPRS                               | No support  |  |    |    |     | No support                      |  |                           |    |    |     |     |
| Max. VLANs                             | 10  |  |    |    |     | 25                              |  |                           |    |    |     |     |
| Concurrent Firewall Conns <sup>2</sup> | 50 K  |  |    |    |     | 130 K                           |  |                           |    |    |     |     |
| Max. Physical Interfaces               | 3 at 10/100 plus the Management interface for management traffic only |  |    |    |     | Unlimited                       |  |                           |    |    |     |     |
| Encryption                             | Base (DES)  | <i>Optional license: Strong (3DES/AES)</i> |    |    |     | Base (DES)                      | <i>Optional license: Strong (3DES/AES)</i> |                           |    |    |     |     |
| Min. RAM                               | 256 MB  |  |    |    |     | 256 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 1 host and 1 dynamic translation for every 4 connections.

**Table 4** ASA 5520 Adaptive Security Appliance License Features

| ASA 5520                               | Base License                    |  |    |    |     |     |     |           |
|--|---------------------------------|--|----|----|-----|-----|-----|-----------|
| Users, concurrent                      | Unlimited                       |  |    |    |     |     |     | Unlimited |
| Security Contexts                      | 2                               | <i>Optional Licenses:</i>                  |    |    |     |     |     |           |
|  |                                 | 5  | 10 | 20 |     |     |     |           |
| VPN Sessions <sup>1</sup>              | 750 combined IPsec and WebVPN   |  |    |    |     |     |     |           |
| Max. IPsec Sessions                    | 750                             |  |    |    |     |     |     |           |
| Max. WebVPN Sessions                   | 2                               | <i>Optional Licenses:</i>                  |    |    |     |     |     |           |
|  |                                 | 10   | 25 | 50 | 100 | 250 | 500 | 750       |
| VPN Load Balancing                     | Supported                       |  |    |    |     |     |     |           |
| Failover                               | Active/Standby or Active/Active |  |    |    |     |     |     |           |
| GTP/GPRS                               | None                            | <i>Optional license: Enabled</i>           |    |    |     |     |     |           |
| Max. VLANs                             | 100                             |  |    |    |     |     |     |           |
| Concurrent Firewall Conns <sup>2</sup> | 280 K                           |  |    |    |     |     |     |           |
| Max. Physical Interfaces               | Unlimited                       |  |    |    |     |     |     |           |
| Encryption                             | Base (DES)                      | <i>Optional license: Strong (3DES/AES)</i> |    |    |     |     |     |           |
| Min. RAM                               | 512 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 1 host and 1 dynamic translation for every 4 connections.

**Table 5 ASA 5540 Adaptive Security Appliance License Features**

| ASA 5540                               | Base License                    |                                     |    |    |     |           |     |     |      |      |
|--|---------------------------------|-------------------------------------|----|----|-----|-----------|-----|-----|------|------|
| Users, concurrent                      | Unlimited                       |                                     |    |    |     | Unlimited |     |     |      |      |
| Security Contexts                      | 2                               | Optional licenses:                  |    |    |     |           |     |     |      |      |
|  |                                 | 5                                   | 10 | 20 | 50  |           |     |     |      |      |
| VPN Sessions <sup>1</sup>              | 5000 combined IPsec and WebVPN  |                                     |    |    |     |           |     |     |      |      |
| Max. IPsec Sessions                    | 5000                            |                                     |    |    |     |           |     |     |      |      |
| Max. WebVPN Sessions                   | 2                               | Optional Licenses:                  |    |    |     |           |     |     |      |      |
|  |                                 | 10                                  | 25 | 50 | 100 | 250       | 500 | 750 | 1000 | 2500 |
| VPN Load Balancing                     | Supported                       |                                     |    |    |     |           |     |     |      |      |
| Failover                               | Active/Standby or Active/Active |                                     |    |    |     |           |     |     |      |      |
| GTP/GPRS                               | None                            | Optional license: Enabled           |    |    |     |           |     |     |      |      |
| Max. VLANs                             | 200                             |                                     |    |    |     |           |     |     |      |      |
| Concurrent Firewall Conns <sup>2</sup> | 400 K                           |                                     |    |    |     |           |     |     |      |      |
| Max. Physical Interfaces               | Unlimited                       |                                     |    |    |     |           |     |     |      |      |
| Encryption                             | Base (DES)                      | Optional license: Strong (3DES/AES) |    |    |     |           |     |     |      |      |
| Min. RAM                               | 1 GB                            |                                     |    |    |     |           |     |     |      |      |

- 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.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

**Table 6 ASA 5550 Adaptive Security Appliance License Features**

| ASA 5550                               | Base License                    |                                     |    |    |     |     |     |     |      |      |      |
|--|---------------------------------|-------------------------------------|----|----|-----|-----|-----|-----|------|------|------|
| Users, concurrent                      | Unlimited                       |                                     |    |    |     |     |     |     |      |      |      |
| Security Contexts                      | 2                               | Optional licenses:                  |    |    |     |     |     |     |      |      |      |
|  |                                 | 5                                   | 10 | 20 | 50  |     |     |     |      |      |      |
| VPN Sessions <sup>1</sup>              | 5000 combined IPsec and WebVPN  |                                     |    |    |     |     |     |     |      |      |      |
| Max. IPsec Sessions                    | 5000                            |                                     |    |    |     |     |     |     |      |      |      |
| Max. WebVPN Sessions                   | 2                               | Optional Licenses:                  |    |    |     |     |     |     |      |      |      |
|  |                                 | 10                                  | 25 | 50 | 100 | 250 | 500 | 750 | 1000 | 2500 | 5000 |
| VPN Load Balancing                     | Supported                       |                                     |    |    |     |     |     |     |      |      |      |
| Failover                               | Active/Standby or Active/Active |                                     |    |    |     |     |     |     |      |      |      |
| GTP/GPRS                               | None                            | Optional license: Enabled           |    |    |     |     |     |     |      |      |      |
| Max. VLANs                             | 200                             |                                     |    |    |     |     |     |     |      |      |      |
| Concurrent Firewall Conns <sup>2</sup> | 650 K                           |                                     |    |    |     |     |     |     |      |      |      |
| Max. Physical Interfaces               | Unlimited                       |                                     |    |    |     |     |     |     |      |      |      |
| Encryption                             | Base (DES)                      | Optional license: Strong (3DES/AES) |    |    |     |     |     |     |      |      |      |
| Min. RAM                               | 4 GB                            |                                     |    |    |     |     |     |     |      |      |      |

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 1 host and 1 dynamic translation for every 4 connections.

**Table 7** PIX 515/515E Security Appliance License Features

| PIX 515/515E                           | R (Restricted) |                              | UR (Unrestricted)               |                              | FO (Failover) <sup>1</sup> |                              | FO-AA (Failover Active/Active) <sup>1</sup> |                              |                   |
|--|----------------|------------------------------|---------------------------------|------------------------------|----------------------------|------------------------------|---|------------------------------|-------------------|
| Users, concurrent                      | Unlimited      |                              | Unlimited                       |                              | Unlimited                  |                              | Unlimited                                   |                              |                   |
| Security Contexts                      | No support     |                              | 2                               | Optional license: 5          | 2                          | Optional license: 5          | 2   | Optional license: 5          |                   |
| IPSec Sessions                         | 2000           |                              | 2000                            |                              | 2000                       |                              | 2000  |                              |                   |
| WebVPN Sessions                        | No support     |                              | No support                      |                              | No support                 |                              | No support                                  |                              |                   |
| VPN Load Balancing                     | No support     |                              | No support                      |                              | No support                 |                              | No support                                  |                              |                   |
| Failover                               | No support     |                              | Active/Standby<br>Active/Active |                              | Active/Standby             |                              | Active/Standby<br>Active/Active             |                              |                   |
| GTP/GPRS                               | None           | Optional license:<br>Enabled | None                            | Optional license:<br>Enabled | None                       | Optional license:<br>Enabled | None  | Optional license:<br>Enabled |                   |
| Max. VLANs                             | 10             |                              | 25                              |                              | 25                         |                              | 25  |                              |                   |
| Concurrent Firewall Conns <sup>2</sup> | 48 K           |                              | 130 K                           |                              | 130 K                      |                              | 130 K                                       |                              |                   |
| Max. Physical Interfaces               | 3              |                              | 6                               |                              | 6                          |                              | 6   |                              |                   |
| Encryption                             | None           | Optional licenses:           |                                 | None                         | Optional licenses:         |                              | None  | Optional licenses:           |                   |
|  |                | Base (DES)                   | Strong (3DES/AES)               |                              | Base (DES)                 | Strong (3DES/AES)            |   | Base (DES)                   | Strong (3DES/AES) |
| Min. RAM                               | 64 MB          |                              | 128 MB                          |                              | 128 MB                     |                              | 128 MB                                      |                              |                   |

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

**Table 8** PIX 525 Security Appliance License Features

| PIX 525           | R (Restricted) |  | UR (Unrestricted)                |                                  |                                  |                                  | FO (Failover) <sup>1</sup>       |                                  |                                  |                                  | FO-AA (Failover Active/Active) <sup>1</sup> |  |  |  |
|-------------------|----------------|--|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|---|--|--|--|
| Users, concurrent | Unlimited      |  | Unlimited                        |                                  |                                  |                                  | Unlimited                        |                                  |                                  |                                  | Unlimited                                   |  |  |  |
| Security Contexts | No support     |  | 2                                |                                  |                                  |                                  | 2                                |                                  |                                  |                                  | 2   |  |  |  |
|                   |                |  | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 | Optional licenses:<br>5 10 20 50 |   |  |  |  |
| IPSec Sessions    | 2000           |  | 2000                             |                                  |                                  |                                  | 2000                             |                                  |                                  |                                  | 2000  |  |  |  |

**Table 8 PIX 525 Security Appliance License Features (continued)**

| PIX 525                                | R (Restricted) |                                      | UR (Unrestricted)               |                                      | FO (Failover) <sup>1</sup> |                                      | FO-AA (Failover Active/Active) <sup>1</sup> |                                      |                          |
|--|----------------|--------------------------------------|---------------------------------|--------------------------------------|----------------------------|--------------------------------------|---|--------------------------------------|--------------------------|
| WebVPN Sessions                        | No support     |                                      | No support                      |                                      | No support                 |                                      | No support                                  |                                      |                          |
| VPN Load Balancing                     | No support     |                                      | No support                      |                                      | No support                 |                                      | No support                                  |                                      |                          |
| Failover                               | No support     |                                      | Active/Standby<br>Active/Active |                                      | Active/Standby             |                                      | Active/Standby<br>Active/Active             |                                      |                          |
| GTP/GPRS                               | None           | <i>Optional license:<br/>Enabled</i> | None                            | <i>Optional license:<br/>Enabled</i> | None                       | <i>Optional license:<br/>Enabled</i> | None  | <i>Optional license:<br/>Enabled</i> |                          |
| Max. VLANs                             | 25             |                                      | 100                             |                                      | 100                        |                                      | 100   |                                      |                          |
| Concurrent Firewall Conns <sup>2</sup> | 140 K          |                                      | 280 K                           |                                      | 280 K                      |                                      | 280 K                                       |                                      |                          |
| Max. Physical Interfaces               | 6              |                                      | 10                              |                                      | 10                         |                                      | 10  |                                      |                          |
| Encryption                             | None           | <i>Optional licenses:</i>            |                                 | None                                 | <i>Optional licenses:</i>  |                                      | None  | <i>Optional licenses:</i>            |                          |
|  |                | <i>Base (DES)</i>                    | <i>Strong (3DES/AES)</i>        |                                      | <i>Base (DES)</i>          | <i>Strong (3DES/AES)</i>             |   | <i>Base (DES)</i>                    | <i>Strong (3DES/AES)</i> |
| Min. RAM                               | 128 MB         |                                      | 256 MB                          |                                      | 256 MB                     |                                      | 256 MB                                      |                                      |                          |

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

**Table 9 PIX 535 Security Appliance License Features**

| PIX 535            | R (Restricted) |                                      | UR (Unrestricted)               |                                      | FO (Failover) <sup>1</sup> |                                      | FO-AA (Failover Active/Active) <sup>1</sup> |                                      |
|--------------------|----------------|--------------------------------------|---------------------------------|--------------------------------------|----------------------------|--------------------------------------|---|--------------------------------------|
| Users, concurrent  | Unlimited      |                                      | Unlimited                       |                                      | Unlimited                  |                                      | Unlimited                                   |                                      |
| Security Contexts  | No support     |                                      | 2                               | <i>Optional licenses:</i>            |                            | 2                                    | <i>Optional licenses:</i>                   |                                      |
|                    |                |                                      |                                 | 5                                    | 10                         |                                      | 20  | 50                                   |
| IPSec Sessions     | 2000           |                                      | 2000                            |                                      | 2000                       |                                      | 2000  |                                      |
| WebVPN Sessions    | No support     |                                      | No support                      |                                      | No support                 |                                      | No support                                  |                                      |
| VPN Load Balancing | No support     |                                      | No support                      |                                      | No support                 |                                      | No support                                  |                                      |
| Failover           | No support     |                                      | Active/Standby<br>Active/Active |                                      | Active/Standby             |                                      | Active/Standby<br>Active/Active             |                                      |
| GTP/GPRS           | None           | <i>Optional license:<br/>Enabled</i> | None                            | <i>Optional license:<br/>Enabled</i> | None                       | <i>Optional license:<br/>Enabled</i> | None  | <i>Optional license:<br/>Enabled</i> |
| Max. VLANs         | 50             |                                      | 150                             |                                      | 150                        |                                      | 150   |                                      |

**Table 9** PIX 535 Security Appliance License Features (continued)

| PIX 535                                | R (Restricted) |                    | UR (Unrestricted) |      | FO (Failover) <sup>1</sup> |                   | FO-AA (Failover Active/Active) <sup>1</sup> |                    |                   |
|--|----------------|--------------------|-------------------|------|----------------------------|-------------------|---|--------------------|-------------------|
| Concurrent Firewall Conns <sup>2</sup> | 250 K          |                    | 500 K             |      | 500 K                      |                   | 500 K                                       |                    |                   |
| Max. Physical Interfaces               | 8              |                    | 14                |      | 14                         |                   | 14  |                    |                   |
| Encryption                             | None           | Optional licenses: |                   | None | Optional licenses:         |                   | None  | Optional licenses: |                   |
|  |                | Base (DES)         | Strong (3DES/AES) |      | Base (DES)                 | Strong (3DES/AES) |   | Base (DES)         | Strong (3DES/AES) |
| Min. RAM                               | 512 MB         |                    | 1024 MB           |      | 1024 MB                    |                   | 1024 MB                                     |                    |                   |

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

## ASDM and SSM Compatibility

For a table showing ASDM compatibility with SSMs, see:

<http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrix.html>

## 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 the following website:

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



### Note

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

If you have a previous release of ASDM on your security appliance and want to upgrade to the latest release, you can do so from within ASDM. We recommend that you upgrade the ASDM image before the platform image. ASDM is 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:
    - In ASDM 5.0 and 5.1, click **Upload Image from Local PC**.
    - In ASDM 5.2, click **Upgrade Software**.
  - Step 4** With ASDM selected, click the **Browse Local** button 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 the **Browse Flash** button.
- 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, you see the following message:
- “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 quit out of 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, page 14](#)
- [Downloading the ASDM Launcher, page 14](#)
- [Starting ASDM from the ASDM Launcher, page 15](#)
- [Using ASDM in Demo Mode, page 15](#)
- [Starting ASDM from a Web Browser, page 17](#)
- [Using the Startup Wizard, page 17](#)
- [Using the VPN Wizard, page 18](#)
- [Configuring Stateful Failover, page 18](#)
- [Printing from ASDM, page 20](#)

## 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. For the PIX 500 series security appliance, the interface to which you connect with ASDM is Ethernet 1. To restore the default configuration, enter the **configure factory-default** command at the security appliance CLI.

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. The **setup** command prompts you for a minimal configuration to connect to the security appliance using ASDM.



### Note

You must have an inside interface already configured to use the **setup** command. The Cisco PIX security appliance default configuration includes an inside interface, but the Cisco ASA adaptive security appliance default configuration does not. 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 Cisco PIX 500 series and the ASA 5510 adaptive security appliance have an Ethernet-type interface.

## 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
```

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 SSM (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 login 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 it back to the original configuration.
  - 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:  
<http://www.cisco.com/public/sw-center/index.shtml>  
 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** Click the **Run in Demo Mode** check box.
- Step 4** To set the platform, context and firewall modes, and ASDM Version, click the **Demo** button and make your selections from the Demo Mode area.
- Step 5** If you want 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`

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, 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 your security appliance:

**Step 1** Launch the wizard according to the steps for your 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 your configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of your connection changes.

- Step 4** You can now 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:

- 
- 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 the **Help** button for more information on each field.
- Step 3** After you complete the VPN Wizard information, click **Finish** on the last pane to transmit your configuration to the security appliance.
- 

## Configuring Stateful Failover

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

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



**Tip** If your 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 the LAN and Stateful 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 Stateful Failover on your security appliance, perform the following steps:

- 
- Step 1** Configure the secondary device for HTTPS IP connectivity. See the [Before You Begin, page 14](#), and use a different IP address on the same network as the primary device.
- Step 2** Connect the pair of devices together and to their networks in their Stateful Failover LAN cable configuration.
- Step 3** Start ASDM from the primary device through a supported web browser. (See the section [Downloading the ASDM Launcher, page 14](#).)

- Step 4** Perform one of the following steps, depending on your context mode:
- If your device is in multiple context mode, click **Context**. Choose the **admin** context from the **Context** drop-down menu, and click **Configuration > Properties > Failover**.
  - If your device is in single mode, click **Configuration > Properties > Failover**. Click the **Interfaces** tab.
- Step 5** Perform one of the following steps, depending on your firewall mode:
- If your device is in routed mode, configure standby addresses for all routed mode interfaces.
  - 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 6** Perform one of the following steps, depending on your security context mode:
- If your device is in multiple security context mode: click **System > Configuration > Failover**.
  - If your device is in single mode: click **Configuration > Properties > Failover**.
- Step 7** On the **Setup** tab of the **Failover** pane under **LAN Failover**, select the interface that is cabled for LAN Stateful Failover.
- Step 8** Configure the remaining **LAN Failover** fields.
- Step 9** (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 Stateful Failover, provide failover-group MAC addresses for any interfaces on shared LAN networks.
- Step 10** On the **Setup** tab, check the **Enable Failover** check box. If you are using the PIX 500 series security appliance, check the **Enable LAN rather than serial cable failover** check box.
- Step 11** Click **Apply**, read the warning dialog that appears, and click **OK**. A dialog box about configuring the peer appears.
- Step 12** 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 13** 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.

## 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 Stateful Failover is reenables, the failover communication is encrypted with the key.

To secure the failover key, follow this procedure on the active device:

- 
- Step 1** Perform one of the following steps, depending on your security context mode:
- a. If your device is in single mode, navigate to **Configuration > Properties > Failover > Setup**.
  - b. If your device is in multiple mode, navigate to **System > Configuration > Failover > Setup**.
- Step 2** Turn off failover. (The standby should switch to pseudo-standby mode.)
- a. Uncheck the **Enable failover** check box.
  - b. Click **Apply**. (Click **OK** if CLI preview is enabled.)
- Step 3** Enter the failover key in the **Shared Key** box.
- Step 4** Reenable failover.
- a. Check the **Enable failover** check box.
  - b. 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.
- 

## 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 which 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 sections:

- [Unsupported Commands](#), page 21
- [Interactive User Commands Not Supported in ASDM CLI Tool](#), page 22
- [Unsupported Characters](#), page 23

## 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.

## One-Time Password Not Supported

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

## 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 > Properties > Device Administration > User Accounts** and **Configuration > Properties > 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   |

| Unsupported Commands                 | ASDM Behavior   |
|--------------------------------------|---|
| <b>ipv6</b> , any IPv6 addresses     | Ignored   |
| <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:<br><br><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   |
| <b>terminal</b>                      | Ignored   |
| <b>virtual</b>                       | Ignored   |

## 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
```

## 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:

- From the ASDM Tools menu, click **Command Line Interface**.
- Enter the command: **crypto key generate rsa**

ASDM generates the default 1024-bit RSA key.

- 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
```

## 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 23](#).

## Caveats

The following sections describe caveats for the 5.2(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 5.2(1)

**Table 10** Open Caveats

| ID Number  | Software Release 5.2(1) |  |
|------------|-------------------------|--|
|            | Corrected               | Caveat Title   |
| CSCse15764 | No                      | ASDM: File > Print very slow to execute                                  |
| CSCse27211 | No                      | When you modify an ACE for remark or logging, ASDM issues clear xlate    |
| CSCse27112 | No                      | QoS Help: SgzApplet-0: Httpd: no such entry help/mappingfiles/csdm_hlp.j |
| CSCse27696 | No                      | Negating a regex range [] give a false warning message                   |

**Table 10** *Open Caveats (continued)*

| ID Number  | Software Release 5.2(1) |  |
|------------|-------------------------|--|
|            | Corrected               | Caveat Title   |
| CSCse30178 | No                      | interface cost does not sort correctly                                   |
| CSCse07045 | No                      | Service policy classes not listed in same order as the CLI               |
| CSCsd75599 | No                      | Modifying a shared extended ACL should warn user of sharing implications |
| CSCse12224 | No                      | MGCP: all panels help not present, or not correct or shows wrong window  |
| CSCse25002 | No                      | HAS wizard doesn't catch same active/standby IP for fail and state links |
| CSCse02013 | No                      | Cannot delete failover group 2 if it is in the first row of the table    |
| CSCse23663 | No                      | Status window and command preview window pop up at same time on Linux    |
| CSCsd93317 | No                      | Some multicast commands are not supported by ASDM                        |
| CSCse27211 | No                      | When you modify an ACE for remark or logging, ASDM issues "clear xlate"  |
| CSCse27696 | No                      | Negating a regex range [] give a false warning message                   |
| CSCse32907 | No                      | ASDM: 'Delete All APCF Profiles' cannot be executed- Apply grayed        |
| CSCse33050 | No                      | Unnamed interfaces not listed in backup interface drop down              |
| CSCse33796 | No                      | VPN Monitoring Sessions:Peer IP not filled in when using VPN Server      |
| CSCse33814 | No                      | SIP map: if log only action configured, won't show for some field cm     |
| CSCse33948 | No                      | Startup Wizard does not recognize or save PPPoE IP address setting       |
| CSCse34030 | No                      | ASDM incorrectly allows configuring ASA 5505 to boot from a TFTP server  |
| CSCse34044 | No                      | Startup Wizard cannot configure or read static route monitoring option   |
| CSCse35076 | No                      | "WebVPN Auto Signon" tab in user/Group should be grayed out              |
| CSCse35606 | No                      | Log viewer Show Rule doesn't return to Access Rules table                |
| CSCse38580 | No                      | IPSec Rules: PFS configuration problems                                  |
| CSCse38624 | No                      | The Home Page display is not completely shown in some situations         |

## Resolved Caveats - Release 5.2(1)

The following list shows caveats that are resolved for Version 5.2(1):

**Table 11** *Resolved Caveats*

| ID Number  | Software Release 5.2(1) |  |
|------------|-------------------------|--|
|            | Corrected               | Caveat Title   |
| CSCsd26144 | Yes                     | Trustpoint enrollment URL field - missing validation                     |
| CSCsd26151 | Yes                     | Generating default key-pair gives an error                               |
| CSCsd26163 | Yes                     | CLI tool: not clear that the command drop-down is editable               |
| CSCsd26165 | Yes                     | VPN Wizard, Site-to-Site: remote peer tunnel group name can't be changed |
| CSCsd82585 | Yes                     | Making change to AAA server results in no-change                         |
| CSCsd96769 | Yes                     | Edit Rule Query does not show Field value                                |

## 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*
- *Installing and Using Cisco Intrusion Prevention System Device Manager 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>

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/partner/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/techsupport>

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/techsupport/servicerequest>

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/techsupport/contacts>

## 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/go/marketplace/>

- 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://cisco.com/univercd/cc/td/doc/pcat/>

- *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 the “[Obtaining Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0711R)

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

© 2006 Cisco Systems, Inc. All rights reserved.

