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

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, 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.

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

New Features

Released: February 6, 2006

Table 1 lists the new features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1).

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1)

Feature	Description
Platform Features	
Support for the Content Security and Control (CSC) SSM	The CSC SSM, an integral part of Cisco's Anti-X solution, delivers industry-leading threat protection and content control at the Internet edge providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phising, URL blocking and filtering, and content filtering services. The CSC SSM services module helps businesses more effectively protect their networks, increase network availability, and increase employee productivity through the following key elements: • Antivirus—Market leading antivirus, from Trend Micro, shields your internal network resources from both known and unknown virus attacks, at the most effective point in your infrastructure, the Internet gateway. By cleaning your email and web traffic at the perimeter, it eliminates the need for resource intensive malware infection clean-ups and ensures business continuity. • Anti-Spyware—Blocks spyware from entering your network through web traffic (HTTP & FTP) and email traffic. Frees-up IT support resources from costly spyware removal procedures and improves employee productivity by blocking spyware at the gateway. • Anti-Spam—Effective blocking of spam with very low false positives helps to restore the effectiveness of your email communications, so contact with customers, vendors, and partners continues uninterrupted. • Anti-Phishing—Identity theft protection guards against phishing attacks thereby preventing employees inadvertently disclosing company or personal details which could lead to financial loss. • Automatic Updates from TrendLabs—The solution is backed and supported by one of the largest teams of virus, spyware and spam experts in the industry working 24x7 to ensure that your solution is providing the most up to date protection – automatically. • Central Administration—Easy, set-and-forget administration through a remotely accessible web-console and automated updates reduces IT support costs. • Real-time protection for Web access, Mail (SMTP & POP3) and FTP (file transfer)—Even if the company mail is already protected, many employees will access their own private web-mail from their company PCs or laptops introducing yet another entry point for internet borne threats. Similarly, employees may directly download programs of files which may be similarly contaminated. Real-time protection of all web traffic at the internet gateway greatly reduces this often over-looked point of vulnerability. • Full URL filtering capability with categories, scheduling and cache—URL filtering can be used to control employee internet usage by blocking access to inappropriate or non-work related websites improving employee productivity and limiting the risk of legal action being taken by employees exposed to offensive web content. • Email Content Filtering—Email filtering minimizes legal liability for offensive material transferred by email and enforces regulatory compliance, helping organizations meet the requirements of legislation such as GLB and the Data Protection Act.

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)

Feature	Description
General VPN Features	
Cisco Secure Desktop	Cisco Secure Desktop (CSD) is an optional Windows software package you can install on the security appliance to validate the security of client computers requesting access to your SSL VPN, ensure they remain secure while they are connected, and remove all traces of the session after they disconnect. After a remote PC running Microsoft Windows connects to the security appliance, CSD installs itself and uses the IP address and presence of specific files, registry keys, and certificates to identify the type of location from which the PC is connecting. Following user authentication, CSD uses optional criteria as conditions for granting access rights. These criteria include the operating system, antivirus software, antispyware, and personal firewall running on the PC. To ensure security while a PC is connected to your network, the Secure Desktop, a CSD application that runs on Microsoft Windows XP and Windows 2000 clients, limits the operations available to the user during the session. For remote users with administrator privileges, Secure Desktop uses the 168-bit Triple Data Encryption Standard (3DES) to encrypt the data and files associated with or downloaded during an SSL VPN session. For remote users with lesser privileges, it uses the Rivest Cipher 4 (RC4) encryption algorithm. When the session closes, Secure Desktop overwrites and removes all data from the remote PC using the U.S. Department of Defense (DoD) security standard for securely deleting files. This cleanup ensures that cookies, browser history, temporary files, and downloaded content do not remain after a remote user logs out or an SSL VPN session times out. CSD also uninstalls itself from the client PC. Cache Cleaner, which wipes out the client cache when the session ends, supports Windows XP, Windows 2000, Windows 9x, Linux, and Apple Macintosh OS X clients.
Customized Access Control Based on CSD Host Checking	Adaptive security appliances with Cisco Secure Desktop installed can specify an alternative group policy. The security appliance uses this attribute to limit access rights to remote CSD clients as follows: • Always use it if you set the VPN feature policy to "Use Failure Group-Policy." • Use it if you set the VPN feature policy to "Use Success Group-Policy, if criteria match" and the criteria then fail to match. This attribute specifies the name of the alternative group policy to apply. Choose a group policy to differentiate access rights from those associated with the default group policy. The default value is DfltGrpPolicy. **Note** The security appliance does not use this attribute if you set the VPN feature policy to "Always use Success Group-Policy."

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)

Feature	Description
SSL VPN Client	SSL VPN client is a VPN tunneling technology that gives remote users the connectivity benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance. To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as *requiring* the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies the user as having the *option* to use the SVC, the security appliance downloads the SVC to the remote computer while presenting a link on the user screen to skip the SVC installation. After downloading, the SVC installs and configures itself, When the connection terminates, SVC either remains or uninstalls itself (depending on the configuration) from the remote computer.
WebVPN Functions and Performance Optimizations	This version enhances WebVPN performance and functions through the following components: • Flexible content transformation/rewriting that includes complex JavaScript, VBScript, and Java • Server-side and browser caching • Compression • Proxy bypass • Application Profile Customization Framework support • Application keep-alive and timeout handling • Support for logical (VLAN) interfaces
Citrix Support for WebVPN	WebVPN users can now use a connection to the security appliance to access Citrix MetaFrame services. In this configuration, the security appliance functions as the Citrix secure gateway. Therefore you must configure your Citrix Web Interface software to operate in a mode that does not use the Citrix secure gateway. Install an SSL certificate onto the security appliance interface to which remote users use a fully qualified domain name (FQDN) to connect; this function does not work if you specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the security appliance. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN. Finally, use the **functions** command to enable Citrix.
PDA Support for WebVPN	You can access WebVPN from your Pocket PC 2003 or Windows Mobile X. If you are a PDA user, this makes accessing your private network more convenient. This feature requires no configuration.

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)

Feature	Description
WebVPN Support of Character Encoding for CIFS Files	WebVPN now supports optional character encoding of portal pages to ensure proper rendering of Common Internet File System files in the intended language. The character encoding supports the character sets identified on the following Web page, including Japanese Shift-JIS characters: http://www.iana.org/assignments/character-sets Use the **character-encoding** command to specify the character set to encode in WebVPN portal pages to be delivered to remote users. By default, the encoding type set on the remote browser determines the character set for WebVPN portal pages. The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, you can use the **file-encoding** command to specify the encoding for WebVPN portal pages from specific CIFS servers. Thus, you can use different file-encoding values for CIFS servers that require different character encodings. The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue. **Tip:** The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, or enter the **no page style** command in webvpn customization command mode to remove the font family.
Compression for WebVPN and SSL VPN Client Connections	Compression can reduce the size of the transferring packets and increase the communication performance, especially for connections with bandwidth limitations, such as with dialup modems and handheld devices used for remote access. Compression is enabled by default, for both WebVPN and SVC connections. You can configure compression using ASDM or CLI commands. You can disable compression for all WebVPN or SVC connections with the **compression** command from global configuration mode. You can disable compression for a specific group or user for WebVPN connections with the **http-comp** command, or for SVC connections with the **svc compression** command, in the group policy or username webvpn modes.
Active/Standby Stateful Failover for WebVPN and SVC Connections	During a failover, WebVPN and SVC connections, as well as IPSec connections, are reestablished with the secondary, standby security appliance for uninterrupted service. Active/standby failover requires a one-to-one active/standby match for each connection. A security appliance configured for failover shares authentication information about WebVPN users with the standby security appliance. Therefore, after a failover, WebVPN users do not need to reauthenticate. For SVC connections, after a failover, the SVC reconnects automatically with the standby security appliance.

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)

Feature	Description
WebVPN Customization	You can customize the WebVPN page that users see when they connect to the security appliance, and you can customize the WebVPN home page on a per-user, per-group, or per-tunnel group basis. Users or groups see the custom WebVPN home page after the security appliance authenticates them. You can use Cascading Style Sheet (CSS) parameters. To easily customize, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.
Auto Applet Download	To run a remote application over WebVPN, a user clicks Start Application Access on the WebVPN homepage to download and start a port-forwarding Java applet. To simplify application access and shorten start time, you can now configure WebVPN to automatically download this port-forwarding applet when the user first logs in to WebVPN.
Authentication and Authorization VPN Features	
Override Account Disabled	You can configure the security appliance to override an account-disabled indication from a AAA server and allow the user to log on anyway. We introduced the following command: **override account disabled.**
LDAP Support	You can configure the security appliance to authenticate and authorize IPSec VPN users, SSL VPN clients, and WebVPN users to an LDAP directory server. During authentication, the security appliance acts as a client proxy to the LDAP server for the VPN user, and authenticates to the LDAP server in either plain text or using the Simple Authentication and Security Layer (SASL) protocol. The security appliance supports any LDAP V3 or V2 compliant directory server. It supports password management features only on the Sun Microsystems Java System Directory Server and the Microsoft Active Directory server.
Password Management	You can configure the security appliance to warn end users when their passwords are about to expire. When you configure this feature, the security appliance notifies the remote user at login that the current password is about to expire or has expired. The security appliance then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in using that password. This command is valid for AAA servers that support such notification; that is, RADIUS, RADIUS with an NT server, and LDAP servers. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured. Note that this command does not change the number of days before the password expires, but rather specifies the number of days before expiration that the security appliance starts warning the user that the password is about to expire. The default value is 14 days. For LDAP server authentication only, you can specify a specific number of days before expiration to begin warning the user about the pending expiration. We introduced the following command: **password management**.

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)

Feature	Description
Single sign-on (SSO)	Single sign-on (SSO) support lets WebVPN users enter a username and password only once to access multiple protected services and web servers. You can choose among the following methods to configure SSO: • Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder)—You typically would choose to implement SSO with SiteMinder if your Web site security infrastructure already incorporates SiteMinder. • HTTP Forms—A common and standard approach to SSO authentication that can also qualify as a AAA method. You can use it with other AAA servers such as RADIUS or LDAP servers. • SSO with Basic HTTP and NTLM Authentication—The simplest of the three SSO methods passes WebVPN login credentials for authentication through to internal servers using basic HTTP or NTLM authentication. This method does not require an external SSO server.
Tunnel Group and Group Policy VPN Features	
WebVPN Tunnel Group Type	This version adds a WebVPN tunnel group, which lets you configure a tunnel group with WebVPN-specific attributes, including the authentication method to use, the WebVPN customization to apply to the user GUI, the DNS group to use, alternative group names (aliases), group URLs, the NBNS server to use for CIFS name resolution, and an alternative group policy to apply to CSD users to limit access rights to remote CSD clients.
Group-Based DNS Configuration for WebVPN	You can define a list of DNS servers under a group. The list of DNS servers available to a user depends on the group that the user is assigned to. You can specify the DNS server to use for a WebVPN tunnel group. The default value is DefaultDNS.
New Login Page Option for WebVPN Users	You can optionally configure WebVPN to display a user login page that offers the user the opportunity to select the tunnel group to use for login. If you configure this option, the login page displays an additional field offering a drop-down menu of groups from which to select. The user is authenticated against the selected group.
Group Alias and Group URL	You can create one or more alternate names by which the user can refer to a tunnel group by specifying one or more group aliases. The group aliases that you specify here appear in the drop-down list on the user login page. Each group can have multiple aliases or no alias. If you want the actual name of the tunnel group to appear on this list, specify it as an alias. This feature is useful when the same group is known by several common names, such as “Devtest” and “QA”. Specifying a group URL eliminates the need for the user to select a group at login. When a user logs in, the security appliance looks for the user incoming URL in the tunnel-group-policy table. If it finds the URL and if this feature is enabled, then the security appliance automatically selects the appropriate server and presents the user with only the username and password fields in the login window. If the URL is disabled, the dropdown list of groups also appears, and the user must make the selection. You can configure multiple URLs (or no URLs) for a group. You can enable or disable each URL individually. You must use a separate specification (**group-url** command) for each URL. You must specify the entire URL, which can use either the HTTP or HTTPS protocol. You cannot associate the same URL with multiple groups. The security appliance verifies the uniqueness of the URL before accepting the URL for a tunnel group.
ASDM Features	

Table 1 New Features for ASA and PIX Version 7.1(1)/ASDM Version 5.1(1) (continued)

Feature	Description
Management and Monitoring Support for the CSC SSM	ASDM Version 5.1 delivers an industry-first solution that blends the simplicity of Trend Micro's HTML-based configuration panels with the ingenuity of ASDM. This helps ensure consistent policy enforcement, and simplifies the complete provisioning, configuration, and monitoring processes for the rich unified threat management functions offered by the CSC SSM. ASDM provides a complementing monitoring solution with a new CSC SSM homepage and new monitoring panels. Once a CSC SSM is installed, the main ASDM homepage is automatically updated to display a new CSC SSM panel, which provides a historic view into threats, e-mail viruses, live events, and vital module statistics such as last installed software/signature updates, system resources, and more. Within the monitoring section of ASDM, a rich set of analysis tools provide detailed visibility into threats, software updates, resource graphs, and more. The Live Security Event Monitor is a new troubleshooting and monitoring tool that provides real-time updates regarding scanned or blocked e-mail messages, identified viruses/worms, detected attacks, and more. It gives administrators the option to filter messages using regular-expression string matching, so specific attack types and messages can be focused on and analyzed in detail.
Syslog to Access Rule Correlation	This ASDM release introduces a new Syslog to Access Rule Correlation tool that greatly enhances day-to-day security management and troubleshooting activities. With this dynamic tool, security administrators can quickly resolve common configuration issues, along with most user and network connectivity problems. Users can select a syslog message within the Real-Time Syslog Viewer panel, and by simply clicking the Create button at the top of the panel, can invoke the access-control options for that specific syslog. Intelligent defaults help ensure that the configuration process is simple, which helps improve operational efficiency and response times for business-critical functions. The Syslog to Access Rule Correlation tool also offers an intuitive view into syslog messages invoked by user-configured access rules.
Customized Syslog Coloring	ASDM allows for rapid critical system message identification and convenient syslog monitoring by allowing the colored grouping of syslog messages according to syslog level. Users can select the default coloring options, or create their own unique colored syslog profiles for ease of identification.
ASDM and WebVPN interface	ASDM and WebVPN can now run on the same interface simultaneously.
ASDM Demo Mode	ASDM Demo Mode initial support.

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

Client PC Operating System and Browser Requirements

Table 2 lists the supported and recommended PC operating systems and browsers for Version 5.0.

Table 2 Operating System and Browser Requirements

	Operating System	Browser	Other Requirements
Windows[1]	Windows 2000 (Service Pack 4) or Windows XP operating systems	Internet Explorer 6.0 with Sun Java[2] Plug-in 1.4.2 or 1.5.0 **Note** **HTTP 1.1**—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	**SSL Encryption Settings**—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 the Java website.

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/cisco/software/navigator.html

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/cisco/software/navigator.html.

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 10.

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 9.

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 applicance, 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 12.)

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 24.

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 support, see Unsupported Commands, page 17.

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
ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

Workaround:

- You can configure most commands that require user interaction by means of the ASDM 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
access-list	Ignored if not used, except for use in VPN group policy screens
capture	Ignored
established	Ignored
failover timeout	Ignored
ipv6, any IPv6 addresses	Ignored
object-group icmp-type	View-only
object-group network	Nested group is view-only
object-group protocol	View-only
object-group service	Nested group cannot be added
pager	Ignored
pim accept-register route-map	Ignored. Only the **list** option can be configured using ASDM
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored

Unsupported Commands	ASDM Behavior

service-policy global	Ignored if it uses a **match access-list** class. For example:
	`access-list myacl line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`policy-map mypm`
	`class mycm`
	`inspect ftp`
	`service-policy mypm global`

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

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 reenable failover. When failover is reenabled, 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:

a. If your device is in single mode, navigate to **Configuration > Features > Properties > Failover > Setup**.

b. If you 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.)

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.

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 0-3 ASA 5500 Series Adaptive Security Appliance License Features

<table>
<tr><th>Platforms and Features</th><th colspan="12">Licenses</th></tr>
<tr><td>ASA 5510</td><td colspan="6">Base License</td><td colspan="6">Security Plus</td></tr>
<tr><td>Security Contexts</td><td colspan="6">No support</td><td colspan="6">No support</td></tr>
<tr><td>VPN Sessions[1]</td><td colspan="6">250 combined IPSec and WebVPN</td><td colspan="6">250 combined IPSec and WebVPN</td></tr>
<tr><td>Max. IPSec Sessions</td><td colspan="6">250</td><td colspan="6">250</td></tr>
<tr><td rowspan="2">Max. WebVPN Sessions</td><td rowspan="2">2</td><td colspan="5">Add-on Licenses:</td><td rowspan="2">2</td><td colspan="5">Add-on Licenses:</td></tr>
<tr><td>10</td><td>25</td><td>50</td><td>100</td><td>250</td><td>10</td><td>25</td><td>50</td><td>100</td><td>250</td></tr>
<tr><td>VPN Load Balancing</td><td colspan="6">No support</td><td colspan="6">No support</td></tr>
<tr><td>Failover</td><td colspan="6">None</td><td colspan="6">Active/Standby</td></tr>
<tr><td>GTP/GPRS</td><td colspan="6">Not supported</td><td colspan="6">Not supported</td></tr>
<tr><td>Maximum VLANs</td><td colspan="6">10</td><td colspan="6">25</td></tr>
<tr><td>Concurrent Firewall Connections[2]</td><td colspan="6">50 K</td><td colspan="6">130 K</td></tr>
<tr><td>Max. Physical Interfaces</td><td colspan="6">3 at 10/100 plus the Management interface for management traffic only (to-the-security-appliance)</td><td colspan="6">Unlimited</td></tr>
<tr><td>Encryption</td><td colspan="2">Base (DES)</td><td colspan="4">Add-on license:
Strong (3DES/AES)</td><td colspan="2">Base (DES)</td><td colspan="4">Add-on license:
Strong (3DES/AES)</td></tr>
<tr><td>Minimum RAM</td><td colspan="6">256 MB</td><td colspan="6">256 MB</td></tr>
<tr><td>ASA 5520</td><td colspan="12">Base License</td></tr>
<tr><td rowspan="2">Security Contexts</td><td rowspan="2">2</td><td colspan="11">Add-on Licenses:</td></tr>
<tr><td>5</td><td>10</td><td colspan="9">20</td></tr>
</table>

Table 0-3 ASA 5500 Series Adaptive Security Appliance License Features (continued)

Platforms and Features	Licenses									
VPN Sessions[1]	750 combined IPSec and WebVPN									
Max. IPSec Sessions	750									
Max. WebVPN Sessions	2	*Add-on Licenses:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*		
VPN Load Balancing	Supported									
Failover	Active/Standby Active/Active									
GTP/GPRS	None	*Add-on license: Enabled*								
Maximum VLANs	100									
Concurrent Firewall Connections[2]	280 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	*Add-on license:* *Strong (3DES/AES)*								
Minimum RAM	512 MB									
ASA 5540	**Base License**									
Security Contexts	2	*Add-on licenses:*								
		5	*10*	*20*	*50*					
VPN Sessions[1]	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	*Add-on Licenses:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
VPN Load Balancing	Supported									
Failover	Active/Standby Active/Active									
GTP/GPRS	None	*Add-on license: Enabled*								
Maximum VLANs	200									
Concurrent Firewall Connections[2]	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	*Add-on license:* *Strong (3DES/AES)*								
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 0-4 PIX 500 Series Security Appliance License Features

Platforms and Features	Licenses			
PIX 515/515E[1]	**R (Restricted)**	**UR (Unrestricted)**	**FO (Failover)[2]**	**FO-AA (Failover Active/Active)[2]**
Security Contexts	No support	2 · *Add-on license:* *5*	2 · *Add-on license:* *5*	2 · *Add-on license:* *5*
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*
Maximum VLANs	10	25	25	25
Concurrent FirewallConnections[3]	48 K	130 K	130 K	130 K
Max. Physical Interfaces	3	6	6	6
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	64 MB	128 MB	128 MB	128 MB
PIX 525[1]	**R (Restricted)**	**UR (Unrestricted)**	**FO (Failover)[2]**	**FO-AA (Failover Active/Active)[2]**
Security Contexts	No support	2 · *Add-on licenses:* *5* · *10* · *20* · *50*	2 · *Add-on licenses:* *5* · *10* · *20* · *50*	2 · *Add-on licenses:* *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*
Maximum VLANs	25	100	100	100
Concurrent FirewallConnections[3]	140 K	280 K	280 K	280 K
Max. Physical Interfaces	6	10	10	10

Table 0-4 PIX 500 Series Security Appliance License Features (continued)

Platforms and Features	**Licenses**																			
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	128 MB					256 MB					256 MB					256 MB				
PIX 535[1]	**R (Restricted)**					**UR (Unrestricted)**					**FO (Failover)[2]**					**FO-AA (Failover Active/Active)[2]**				
Security Contexts	No support					2	*Add-on licenses: 5*	*10*	*20*	*50*	2	*Add-on licenses: 5*	*10*	*20*	*50*	2	*Add-on licenses: 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[3]	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 5 lists ASDM versions and their compatibility with versions of IPS.

Table 5 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://tools.cisco.com/Support/BugToolKit/

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

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

Open Caveats - Release 5.1(1)

Table 6 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.
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	IPS tree occupies the whole screen the first time IPS button is clicked **Conditions:** 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. **Workaround:** 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.

Resolved Caveats - Release 5.1(1)

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

Table 7 Resolved Caveats

ID Number	Software Release 5.1(1) 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

Table 7 Resolved Caveats (continued)

ID Number	Software Release 5.1(1) Corrected	Caveat Title
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-relm 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 and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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