



Cisco ASDM Release Notes Version 6.1(3)

August 2008

This document contains release information for Cisco ASDM Version 6.1(3) on Cisco ASA 5500 Adaptive Series Security Appliances. It includes the following sections:

- [Introduction, page 2](#)
- [New Device Manager Features, page 2](#)
- [New Platform Features, page 6](#)
- [Supported Platforms and Feature Licenses, page 7](#)
- [ASDM and SSM Compatibility, page 7](#)
- [Upgrading ASDM and ASA, page 7](#)
- [Getting Started with ASDM, page 8](#)
- [ASDM Limitations, page 14](#)
- [Caveats, page 16](#)
- [End-User License Agreement, page 19](#)
- [Related Documentation, page 20](#)
- [Obtaining Documentation and Submitting a Service Request, page 20](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

Introduction

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for Cisco ASA 5500 series adaptive security appliances through an intuitive, easy-to-use, web-based management interface. Bundled with supported security appliances, the device manager accelerates security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced security and networking features offered by Cisco ASA 5500 series adaptive security appliance software Version 8.1. Its secure, web-based design enables anytime, anywhere access to security appliances.

**Note**

ASDM 6.1 is compatible with Cisco ASA 5500 Adaptive Series Security Appliance versions 8.0 and 8.1, and Cisco PIX 500 Series Security Appliances version 8.0, but not earlier versions. The Cisco ASA 5580 Adaptive Series Security Appliance is only compatible with ASDM 6.1 and ASA version 8.1 software. For more information on platform support, see [Table 2 ASDM Version 6.1 Support by Platform, page 7](#).

New Device Manager Features

Version 6.1(3) contains the following enhancements that have been implemented since ASDM version 6.1(1):

ASDM Feature Type	Feature	Description
New Features	Cisco Phone Proxy	<p>ASDM now supports a newly designed Phone Proxy panel that enables you to configure the attributes of a phone proxy instance. The actual name of the phone proxy is then generated by ASDM.</p> <p>The Cisco Phone Proxy provides similar features to those of the Metreos Cisco Unified Phone Proxy with additional support for SIP inspection and enhanced security. The phone proxy has the following key features:</p> <ul style="list-style-type: none"> • Secures remote IP phones by forcing the phones to encrypt signaling and media • Performs certificate-based authentication with remote IP phones • Terminates TLS signaling from IP phones and initiates TCP and TLS to Cisco Unified Mobility Advantage (CUMA) servers • Terminates SRTP and initiates RTP/SRTP to the called party <p>To configure this feature, see Configuration > Firewall > Advanced > Encrypted Traffic Inspection > Enable Phone Proxy.</p>
	TLS Proxy for Cisco Unified Mobility	<p>Secure connectivity (mobility proxy) between Cisco Unified Mobility Advantage (CUMA) clients and servers is supported using a newly redesigned set of TLS Proxy panels to configure the attributes of TLS proxy instances.</p> <p>CUMA solutions include the Cisco Unified Mobile Communicator (CUMC), an easy-to-use software application for mobile handsets that extends enterprise communications applications and services to mobile phones and smart phones and the Cisco Unified Mobility Advantage (CUMA) server. The mobility solution streamlines the communication experience, enabling real-time collaboration across the enterprise.</p> <p>TLS proxy instances are used to encrypt SIP and SCCS signalling in secure and non-secure modes. ASDM provides three new panels for TLS Proxy configuration:</p> <ul style="list-style-type: none"> • TLS Proxy Instance • Server Configuration • Client Configuration <p>To configure this feature, see Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy.</p>

ASDM Feature Type	Feature	Description
	Supports TLS Proxy for Cisco Unified Presence	<p>ASDM now supports secure connectivity (presence federation proxy) between Cisco Unified Presence servers and Cisco/Microsoft Presence servers with Mobile Multiplexing Protocol (MMP) in the Service Policy rules table.</p> <p>See Configuration > Service Policy Rules > Protocol Inspection or Configuration > Firewall > Advanced > Encrypted Traffic Inspection > TLS Proxy > Add > Client Configuration.</p>
	Show Active Directory Groups	<p>ASDM has the ability to list the Active Directory Server Groups on a Microsoft LDAP Active Directory Server so that you can configure the DAP. This feature is useful for the configuration of DAP, which requires the administrator to know the names of the groups on a Microsoft LDAP Active Directory. See Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies > Add/Edit DAP > Add/Edit AAA Attribute.</p>
	Entrust Certificate Provisioning	<p>ASDM now includes a link to the Entrust website to apply for temporary (test) or discounted permanent SSL identity certificates for your ASA. To use this feature, navigate to Configuration > Remote Access VPN > Certificate Management > Identity Certificates. Click Enroll ASA SSL VPN head-end with Entrust.</p>
	Extended Time for User Reauthentication on IKE Rekey	<p>ASDM now allows users more time to enter credentials before the tunnel drops. You can configure the security appliance to let remote users enter credentials at any time from the start of the reauthentication-on-rekey until the SA expires.</p> <p>See Configuration > Device Management > Certificate Management > Identity Certificates..</p>
	QoS Traffic Shaping	<p>ASDM allows you to manage networks with differing line speeds, by configuring the security appliance to transmit packets at a fixed slower rate.</p> <p>This is helpful if you have a device that transmits packets at a high speed, such as a security appliance with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped.</p> <p>See the Configuration > Security Policy > Service Policy Rules panel, and then add or edit a rule to access the QoS tab. Note that the only traffic class supported for traffic shaping is class-default, which matches all traffic.</p>

ASDM Feature Type	Feature	Description
	Support for Smart Tunnels on Mac OS	Support for Smart Tunnels on Mac OS X has been added to ASDM. See the Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels panel. This feature is introduced on the ASA 8.0.4 platform, but is not available in ASA 8.1.1.
	Support for Auto-Sign on with Smart Tunnels with Internet Explorer	Added functionality that allows an administrator to create an auto-sign server list for users. See the Firewall > Advanced > ACL Manager panel.
	Support for icmp unreachable command	Rate and burst limit sizes for ICMP messages can now be adjusted from the Configuration > Device Management > Management Access > ICMP panel.
	Timeout for SIP provisional media	You can now configure the timeout for SIP provisional media on the Configuration > Properties > Timeouts panel.
	TCP Normalizer	You can now configure TCP normalization actions for certain packet types. Previously, the default actions for these kinds of packets was to drop the packet. Now you can set the TCP normalizer to allow the packets. You can also set the TCP out-of-order packet buffer timeout. Previously, the timeout was 4 seconds. You can now set the timeout to another value. The default action for packets that exceed MSS has changed from drop to allow. See Configuration > Firewall > Objects > TCP Maps > Add/Edit .
	Simplify DNS Panel	The DNS Panel on the ASDM GUI has been modified for ease of use. See Configuration > Device Management > DNS .
	Redesign the File Transfer Dialog box	You can drag-and-drop files in the File Transfer dialog box. To access this dialog box, go to Tools > File Management , and then click File Transfer .
	Clear ACL Hit Counters	Added functionality enabling users to clear ACL hit counters. See the Firewall > Advanced > ACL Manager panel.
	Renaming ACLs	Added the ability to rename ACLs from ASDM. See the Firewall > Advanced > ACL Manager panel.

ASDM Feature Type	Feature	Description
	Combine ASDM/HTTPS, SSH, Telnet into One Panel	ASDM has combined the ASDM, HTTPS, SSH, Telnet into one panel. See the Monitoring > Properties > Device Access > ASDM/HTTPS/Telnet/SSH Sessions panel.
	Display all standard ACLs in ACL Manager	Added functionality enabling users to display all standard ACL in the ACL Manager. See the Firewall > Advanced > ACL Manager panel.

New Platform Features

ASDM supports the enhancements to services and features introduced in the Cisco ASA 5500 software release Version 8.0.4.

This document contains release information about ASDM only. For detailed information on new platform features, see the online help, or the Cisco ASA 5000 Series Release Notes.

ASDM Client PC Operating System and Browser Requirements

[Table 1](#) lists the supported and recommended PC operating systems and browsers for ASDM Version 6.1(3).

Table 1 Operating System and Browser Requirements

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

- ASDM is not supported on Windows 3.1, Windows 95, Windows 98, Windows ME, or Windows NT4.
- Obtain Sun Java from java.sun.com.

Supported Platforms and Feature Licenses

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

Table 2 ASDM Version 6.1 Support by Platform

Hardware Platform	ASA Software Version
ASA 5580 Series	ASA 8.1 ¹
ASA 5500 Series ²	ASA 8.0
PIX 500 ³ Series	PIX 8.0

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

For information on supported platforms and feature licenses, see:

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

ASDM and SSM Compatibility



Note

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

Upgrading ASDM and ASA

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

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

If you have a previous release of ASDM on your security appliance and want to upgrade to the latest release, you can do so from within ASDM. We recommend that you upgrade the ASDM image before the platform image. ASDM is backwards compatible, so you can upgrade the platform image using the new ASDM; you cannot use an old ASDM with a new platform image.



Note

ASDM 6.1 is compatible with Cisco ASA 5500 Adaptive Series Security Appliance versions 8.0 and 8.1, and Cisco PIX 500 Series Security Appliances version 8.0, but not earlier versions. The Cisco ASA 5580 Adaptive Series Security Appliance is only compatible with ASDM 6.1 and ASA version 8.1 software. For more information on platform support, see [Table 2 ASDM Version 6.1 Support by Platform, page 7](#).

To upgrade ASDM, perform the following steps:

-
- Step 1** Download the new ASDM image to your PC.
Optionally, you can download a new platform image to your PC if the installed image is earlier than 8.0.
- Step 2** Launch ASDM.

- Step 3** From the Tools menu:
- In ASDM 5.0 and 5.1, click **Tools > Upload Image from Local PC**.
 - In ASDM 5.2, click **Tools > Upgrade Software**.
 - In ASDM 6.0, click **Tools > Upload Software from Local Computer**.
- Step 4** With ASDM selected, click **Browse Local** to select the new ASDM image.
- Step 5** To specify the location in Flash memory where you want to install the new image, enter the directory path in the field or click **Browse Flash**.
- If your security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.
- If you have enough memory for both versions, you can specify a different name for the new version. If you need to revert to the old version, it is still in your Flash memory.
- Step 6** Click **Upload Image**.
- When ASDM is finished uploading, the following message appears:
- “ASDM Image is Uploaded to Flash Successfully.”
- Step 7** **For Version 5.x only:** If the new ASDM image has a different name than the old image, then you must configure the security appliance to load the new image. Use the **Configuration > Properties > Device Administration > Boot System/Configuration** panel.
- Step 8** If installing a new platform image, download the new platform image using the **Tools > Upgrade Software** tool with ASA or PIX selected.
- If your security appliance does not have enough memory to hold two ASDM images, overwrite the old image with the new one by specifying the same destination filename. You can rename the image after it was uploaded using the **Tools > File Management** tool.
- Step 9** If installing a new image, select ASA as the new image, and reload the security appliance using the **Tools > System Reload** tool.
- Make sure to choose "Save the running configuration at time of reload".
- Step 10** To run the new ASDM image, exit ASDM and reconnect.
-

Getting Started with ASDM

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

This section includes the following topics:

- [Before You Begin, page 9](#)
- [Downloading the ASDM Launcher, page 9](#)
- [Starting ASDM from the ASDM Launcher, page 10](#)
- [Using ASDM in Demo Mode, page 10](#)

- [Starting ASDM from a Web Browser, page 12](#)
- [Using the Startup Wizard, page 12](#)
- [Using the IPsec VPN Wizard, page 13](#)
- [Printing from ASDM, page 13](#)

Before You Begin

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

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

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

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



Note

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

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

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

Downloading the ASDM Launcher

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

To download the ASDM Launcher, perform the following steps:

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

https://interface_ip_address/admin

In transparent firewall mode, enter the management IP address.



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

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

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM in a browser**

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

The installer downloads to your PC.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

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

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

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

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

Using ASDM in Demo Mode

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

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

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

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI but are not applied to the configuration file. That is, when you click the **Refresh** button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File/Disk operations are not supported.

- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot log in as a monitor-only or read-only user.
- Demo Mode does not support the following features:
 - File menu:
 - Reset Device to the Factory Default Configuration
 - Save Running Configuration to Flash
 - Save Running Configuration to TFTP Server
 - Save Running Configuration to Standby Unit
 - Save Internal Log Buffer to Flash
 - Clear Internal Log Buffer
 - Tools menu:
 - Command Line Interface
 - Ping
 - Traceroute
 - File Management
 - Upgrade Software from Local Computer
 - Upgrade Software from Cisco.com
 - Backup Configurations
 - Restore Configurations
 - System Reload
 - Administrator's Alert to Clientless SSL VPN Users
 - Toolbar/Status bar > Save
 - Configuration > Interface > Edit Interface > Renew DHCP Lease
 - Failover—Configuring a standby device
- These operations cause a reread of the configuration and therefore will revert the configuration back to the original settings.
 - Switching contexts
 - Making changes in the Interface panel
 - NAT panel changes
 - Clock panel changes

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

-
- Step 1** If you have not yet installed the Demo Mode application, perform the following steps:
- a. Download the ASDM Demo Mode installer from the following website:
<http://www.cisco.com/public/sw-center/index.shtml>
 The filename is asdm-demo-611.msi.
 - b. Double-click the installer to install the software.
- Step 2** Double-click the **Cisco ASDM Launcher** shortcut on your desktop, or start it from the **Start** menu.

- Step 3** Check **Run in Demo Mode**.
- Step 4** To set the platform, context and firewall modes, and ASDM Version, click **Demo** and make your selections from the Demo Mode area.
- Step 5** To use new ASDM images as they come out, you can either download the latest installer, or you can download the normal ASDM images and install them for Demo Mode:
- a. Download the image from the download page (see Step 1).
The filename is `asdm-version.bin`.
 - b. In the Demo Mode area, click **Install ASDM Image**.
A file browser appears. Find the ASDM image file in the browser.
- Step 6** Click **OK** to launch ASDM Demo Mode.
You see a Demo Mode label in the title bar of the window.
-

Starting ASDM from a Web Browser

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

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

`https://interface_ip_address/admin`

In transparent firewall mode, enter the management IP address.



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

- Step 2** Click **OK** or **Yes** to all browser prompts, including the name and password prompt. By default, leave the name and password blank.
A page displays with the following buttons:
- **Install ASDM Launcher and Run ASDM**
- Step 3** Click **Run ASDM**.
- Step 4** Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, leave the name and password blank.
-

Using the Startup Wizard

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

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

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

- In single context mode, click **Wizards > Startup Wizard**.
 - In multiple context mode, for each new context, perform the following steps:
 - a. Create a new context using the **System > Configuration > Security Context** pane.
 - b. Be sure to allocate interfaces to the context.
 - c. When you apply the changes, ASDM prompts you to use the Startup Wizard.
 - d. Click the **System/Contexts** icon on the toolbar, and choose the context name.
 - e. Click **Wizards > Startup Wizard**.
- Step 2** Click **Next** as you proceed through the Startup Wizard screens, filling in the appropriate information in each screen, such as device name, domain name, passwords, interface names, IP addresses, basic server configuration, and access permissions.
- Step 3** Click **Finish** on the last pane to transmit the configuration to the security appliance. Reconnect to ASDM using the new IP address, if the IP address of the connection changes.
- Step 4** Enter other configuration details on the **Configuration** panes.
-

Using the IPsec VPN Wizard

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

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

-
- Step 1** Click **Wizards > VPN Wizard**.
- Step 2** Supply information on each wizard pane. Click **Next** to move through the VPN Wizard panes. You may use the default IPsec and IKE policies. Click **Help** for more information about each field.
- Step 3** After you complete the VPN Wizard information, click **Finish** on the last pane to transmit the configuration to the security appliance.
-

Printing from ASDM



Note

Printing is supported only for Microsoft Windows 2000 or XP in this release.

ASDM supports printing for the following features:

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

ASDM Limitations

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

- [Unsupported Commands](#), page 14
- [Interactive User Commands Not Supported in ASDM CLI Tool](#), page 15
- [Miscellaneous Limitations](#), page 16

Unsupported Commands

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

Effects of Unsupported Commands

- If ASDM loads an existing running configuration and finds IPv6-related commands, ASDM displays a dialog box informing you that it does not support IPv6. You cannot configure any IPv6 commands in ASDM, but all other configuration is available.
- If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, choose **Tools > Show Commands Ignored by ASDM on Device**.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

Monitor-only mode allows access to the following functions:

- The **Monitoring** area
- The CLI tool (**Tools > Command Line Interface**), which lets you use the CLI commands

To exit Monitor-only mode, use the CLI tool or access the security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco Security Appliance Command Reference* for more information.



Note

You might also be in Monitor-only mode because your user account privilege level, indicated in the status bar at the bottom of the main ASDM window, was set up as less than or equal to three by your system administrator, which allows Monitor-only mode. For more information, choose **Configuration >> Device Management > Users/AAA > User Accounts and Configuration > Device Management > Users/AAA > AAA Access**.

Ignored and View-Only Commands

The following table lists commands that ASDM supports in the configuration when you add them through the CLI, but that you cannot add or edit in ASDM. If ASDM ignores the command, it does not appear in the ASDM GUI at all. If the command is view-only, then it appears in the GUI, but you cannot edit it.

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used, except for use in VPN group policy screens
established	Ignored
failover timeout	Ignored
ipv6 , any IPv6 addresses	Ignored
pager	Ignored
pim accept-register route-map	Ignored. You can only configure the list option using ASDM.
prefix-list	Ignored if not used in an OSPF area
route-map	Ignored
service-policy global	Ignored if it uses a match access-list class. For example: <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>
sysopt nodnsalias	Ignored
sysopt uauth allow-http-cache	Ignored
terminal	Ignored
threat-detection statistics tcp-intercept	Ignored
threat-detection scanning-threat shun duration	Ignored
switchport trunk native vlan	Ignored

Discontinuous Subnet Masks Not Supported

ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, you cannot use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Interactive User Commands Not Supported in ASDM CLI Tool

The ASDM CLI tool does not support interactive user commands. If you enter a CLI command that requires interactive confirmation, ASDM prompts you to enter “[yes/no]” but does not recognize your input. ASDM then times out waiting for your response.

For example:

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

ASDM generates the default 1024-bit RSA key.

3. Enter the command again: **crypto key generate rsa**

Instead of regenerating the RSA keys by overwriting the previous one, ASDM displays the following error:

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
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 panes.
- For CLI commands that have a **noconfirm** option, use this option when entering the CLI command. For example:

```
crypto key generate rsa noconfirm
```

Miscellaneous Limitations

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

Caveats

The following sections describes the open and resolved caveats for Version 6.1(3).

- [Open Caveats - Version 6.1\(3\), page 16](#)
- [Resolved Caveats - Version 6.1\(3\), page 17](#)



Note

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

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

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

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

Open Caveats - Version 6.1(3)

The following list shows caveats that are opened for Version 6.1(3):

Table 3 Open ASDM Caveats

ID Number	Software Version 6.1(3)	
	Corrected	Caveat Title
CSCs150642	No	Add/Del Interface through CLI not shown in ASDM home page.
CSCsm58048	No	GUI does not show privilege level change until it is applied
CSCsm85034	No	ASDM refresh errors after failover - no response for 60 secs warning
CSCsm85510	No	NTP/clock: clock set cmd sent with ntp cmds if clock changed
CSCsm86157	No	NTP: In multi-mode, ntp config changes are not recognized.
CSCsm91240	No	Boot image config empty after switch from multiple to single context mod
CSCso05236	No	Pasting of address bar fails in some applications
CSCso46258	No	Cannot view DAP for Read-only admins
CSCsr11493	No	ASDM - read-only users receive "enter network password" popup
CSCsr23498	No	Secure Desktop General panel, missing Help for "Launch the ...App"
CSCsr41717	No	ASDM: sends a [no] upon modifying a ST auto signon list
CSCsr52067	No	Connection issues with 8.1 ASA 5580 devices
CSCsr58575	No	Read-only user denied access to config screens in non-admin context
CSCsr65521	No	ASDM: User link in Smart Tunnels is broken
CSCsr66398	No	"CSC setup wizard" changed access-list setting
CSCsr71032	No	ASDM is unable to modify an address pool without removing it first
CSCsr73904	No	ASDM warning displays incorrect trustpoint info when deleting cert
CSCsr74830	No	ASDM generated cert request contains invalid character

Resolved Caveats - Version 6.1(3)

The following list shows caveats that are resolved for Version 6.1(3):

Table 4 Resolved ASDM Caveats

ID Number	Software Version 6.1(3)	
	Corrected	Caveat Title
CSCsc63204	Yes	ASDM to honor New Zealand Daylight Savings time (NZDT)
CSCs115055	Yes	ASDM may show no ACL hitcounts for active access-lists
CSCs139376	Yes	ASDM DAP incorrect condition on AAA attributes
CSCs182825	Yes	Traversing Advanced>SSL Setting cause ASDM to send ssl commands.
CSCsm05271	Yes	ASDM support needed for IDM Startup Wizard animation
CSCsm25784	Yes	TCP Service Group named "http-https" acts as range
CSCsm66235	Yes	ACL manager in ASDM 6.0(3) does not display standard ACLs
CSCsm76473	Yes	Name entries in ASA not showing as Network Objects in ASDM
CSCsm83131	Yes	Capture wizard, ethereal.exe not found error

Table 4 Resolved ASDM Caveats (continued)

ID Number	Software Version 6.1(3)	
	Corrected	Caveat Title
CSCsm85017	Yes	Browse Language Code window does not display all languages.
CSCsm85594	Yes	NTP: Add server without interface, then edit, shows first interface
CSCsm91575	Yes	EDIT button is not functioning properly in ICMP panel.
CSCsm92154	Yes	ASDM: Java Exception when non-numerical entered into CRL port field
CSCsm93373	Yes	ASDM freezes at 77% during loading
CSCsm95257	Yes	ASDM: ACL with trailing remark causes ASDM to add bogus remarks to ACL
CSCsm95423	Yes	VPN Statistics-Sessions, rename Remote Access and Site-to-Site with IPsec
CSCsm99833	Yes	Rule table buttons are truncated
CSCso02264	Yes	WebVPN: GUI Customization for a bookmark - Wrong error message
CSCso03780	Yes	Error message when AAA--> DAP selected
CSCso04692	Yes	CCO download wizard does not complete in multiple mode
CSCso04935	Yes	ASDM: Process "Path" is not reported from a Vista PC
CSCso05192	Yes	HAS Wizard does not run in demo mode
CSCso08240	Yes	sip-provisional-media limits don't match platform
CSCso11752	Yes	ASDM: disable ST for any bookmark not starting with http, https, and ftp
CSCso20071	Yes	ASDM Home Page, VPN Tunnel stats inaccurate
CSCso22740	Yes	Associated trustpoint is different from original config after restored
CSCso23392	Yes	Restoring All via ASDM makes gif file restoration incomplete
CSCso28426	Yes	ASDM when viewing ASA license with ASDM AnyConnect Mobile issue
CSCso30504	Yes	ASDM: Smart Tunnel usability
CSCso30795	Yes	ASDM: Apply Button remains grayed after editing Device Endpt Attribute
CSCso31335	Yes	DAP: Endpt Attrib fail to match - DAP record isn't selected
CSCso33359	Yes	In the network object group, IP address column displays name.
CSCso35177	Yes	Auto created CSD & DAP - for Mac/Linux Default Policy contain spaces
CSCso43915	Yes	Monitoring>ARP Table doesn't show all the arp entries
CSCso43946	Yes	Log Viewer does not display source/dest IP for some syslog 302020
CSCso45991	Yes	Changing address of network object removes it from the object group
CSCso49954	Yes	Gives error "brs" when filtering for object-group
CSCso55100	Yes	ASDM rejects to enter non-English characters while creating bookmark
CSCso58713	Yes	Wrong names and password field for HTTP Form-based authentication
CSCso72416	Yes	ASDM Backup All doesn't backup csd image
CSCso75243	Yes	ASDM Memory Usage report shows incorrect numbers
CSCso76109	Yes	Add Dynamic NAT Rule is not responding and hanging ASDM
CSCso79510	Yes	A syslog containing the ' ' character will be truncated
CSCso81026	Yes	ASDM: backup doesn't allow a dot in the path name

Table 4 Resolved ASDM Caveats (continued)

ID Number	Software Version 6.1(3)	
	Corrected	Caveat Title
CSCso83893	Yes	Disable IPSec L2L tunnel in ASDM 6.1 fails
CSCso92813	Yes	ASDM stops displaying syslog messages after some time
CSCsq04345	Yes	ssh sessions cannot be disconnected using the disconnect feature
CSCsq07023	Yes	Group-Lock feature - change to general option from ipsec client options
CSCsq07318	Yes	ASDM - Modifying NAT rules may clear all xlates for the interface
CSCsq10143	Yes	Edit Static NAT Rule dialog is overlapping other text.
CSCsq14432	Yes	DAP expression generated by ASDM allows room to bypass the record
CSCsq22531	Yes	ASDM: Check for /path in Smart Tunnel Webtype ACLs
CSCsq23816	Yes	ASA/PIX: ASDM may prompt to save changes while logged in as Read Only
CSCsq32331	Yes	Proxy Server config in Phone Proxy configured in CLI shows as ignored
CSCsq48487	Yes	ASDM no longer has search functionality for tunnel session via name/IP
CSCsq71790	Yes	ASDM: Subsequent bookmarks default to ST enabled
CSCsq71857	Yes	ASDM will may freeze for 3 to 4 minutes after an ACL is edited
CSCsq72829	Yes	Cannot add a named Interface
CSCsq76138	Yes	CSC-SSM demo version is older and need 6.2.x version
CSCsq81029	Yes	CSD: Image Invalid message after resetting
CSCsq85965	Yes	ASDM "where used" on network objects shows duplicated results
CSCsq94285	Yes	ASDM not defining inline service groups properly
CSCsq96953	Yes	Unable to apply hash value to a smart tunnel using the ASDM 6.1.1
CSCsq99243	Yes	ASDM-DAP: Selecting Device should provide error mgs when CSD is disabled
CSCsr18432	Yes	Real-time log viewer flickering
CSCsr28762	Yes	HAS Wizard complains 4GE card incompatibility incorrectly
CSCsr50905	Yes	ASDM: radius-sdi-xauth CLI is not supported in IPSec Connection Profiles
CSCsr51673	Yes	ASDM: DAP doesn't match on endpoint.os.servicepack,"EQ","10.4.11" value

End-User License Agreement

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

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

Related Documentation

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

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

Obtaining Documentation and Submitting a Service Request

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

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

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

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

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0807R)

© 2008 Cisco Systems, Inc.

All rights reserved.

