



CHAPTER 2

Welcome to ASDM

Cisco Adaptive Security Device Manager (ASDM) delivers world-class security management and monitoring services for security appliances through an intuitive, easy-to-use, 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 and Cisco PIX 500 series security appliances.



Note

If you change the color scheme of your operating system while ASDM is running, you should restart ASDM, because some ASDM windows might not display correctly.

This chapter includes the following sections:

- [ASDM Client Operating System and Browser Requirements, page 2-2](#)
- [Supported Platforms and SSMs, page 2-2](#)
- [Multiple ASDM Session Support, page 2-3](#)
- [Unsupported Commands, page 2-3](#)
- [Defining Preferences, page 2-5](#)

ASDM Client Operating System and Browser Requirements

Table 2-1 lists the supported and recommended client operating systems and Java for ASDM.

Table 2-1 Operating System and Browser Requirements

Operating System	Browser			Sun Java SE Plug-in ¹
	Internet Explorer	Firefox	Safari	
Microsoft Windows (English and Japanese): <ul style="list-style-type: none"> • 7 • Vista • 2003 Server • XP • 2000 (Service Pack 4 or higher) 	6.0 or above	1.5 or above	No support.	<ul style="list-style-type: none"> • 5.0 (1.5.0) • 6.0
Apple Macintosh OS X: <ul style="list-style-type: none"> • 10.6 • 10.5 • 10.4 	No support.	1.5 or above	2.0 or above	<ul style="list-style-type: none"> • 5.0 (1.5.0) • 6.0
Red Hat Enterprise Linux 5 (GNOME or KDE): <ul style="list-style-type: none"> • Desktop • WS 	N/A	1.5 or above	N/A	<ul style="list-style-type: none"> • 5.0 (1.5.0) • 6.0

1. Obtain Sun Java from java.sun.com.



Note

ASDM supports up to a maximum of a 512 KB configuration. If you exceed this amount, you may experience performance issues.

Supported Platforms and SSMs



Note

ASDM 6.2(1) and higher is not supported on the PIX platforms. The last release that ASDM is supported on is 6.1(5).

ASDM Version 6.2 supports the following platforms and releases:

- ASA 5505, software Version 8.2(2), 8.2(1), 8.0(2), 8.0(3), 8.0(4), and 8.0(5)
- ASA 5510, software Version 8.2(2), 8.2(1), 8.0(2), 8.0(3), 8.0(4), and 8.0(5)
- ASA 5520, software Version 8.2(2), 8.2(1), 8.0(2), 8.0(3), 8.0(4), and 8.0(5)
- ASA 5540, software Version 8.2(2), 8.2(1), 8.0(2), 8.0(3), 8.0(4), and 8.0(5)
- ASA 5550, software Version 8.2(2), 8.2(1), 8.0(2), 8.0(3), 8.0(4), and 8.0(5)

- ASA 5580, software Version 8.2(2), 8.2(1), 8.1(1) and 8.1(2)

ASDM Version 6.2 supports the following SSMs and releases:

- Advanced Inspection and Prevention (AIP) SSM, software Versions 5.0, 5.1, 6.0, 6.1, and 6.2
- Content Security and Control (CSC) SSM, software Versions 6.1, 6.2, and 6.3

See the “SSM and SSC Support Per Model” section on page 3-2 for more information.

Multiple ASDM Session Support

ASDM allows multiple PCs or workstations to each have one browser session open with the same security appliance software. A single security appliance can support up to five concurrent ASDM sessions in single, routed mode. Only one session per browser per PC or workstation is supported for a specified security appliance. In multiple context mode, five concurrent ASDM sessions are supported per context, up to a maximum of 32 total connections for each security appliance.

Unsupported Commands

ASDM supports almost all commands available for the adaptive security appliance, but ASDM ignores some commands in an existing configuration. Most of these commands can remain in your configuration; see Tools > Show Commands Ignored by ASDM on Device for more information.

This section includes the following topics:

- [Ignored and View-Only Commands, page 2-3](#)
- [Effects of Unsupported Commands, page 2-4](#)
- [Discontinuous Subnet Masks Not Supported, page 2-5](#)
- [Interactive User Commands Not Supported by the ASDM CLI Tool, page 2-5](#)

Ignored and View-Only Commands

Table 2-2 lists commands that ASDM supports in the configuration when added through 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 the command is view-only, then it appears in the GUI, but you cannot edit it.

Table 2-2 List of Unsupported Commands

Unsupported Commands	ASDM Behavior
<code>access-list</code>	Ignored if not used.
<code>capture</code>	Ignored.
<code>coredump</code>	Ignored. This can be configured only using the CLI.
<code>eject</code>	Unsupported.
<code>established</code>	Ignored.
<code>failover timeout</code>	Ignored.
<code>ipv6 nd prefix</code>	Unsupported.

Table 2-2 List of Unsupported Commands (continued)

Unsupported Commands	ASDM Behavior
match-metric	Ignored. This is a subcommand of route-map.
match-interface	Ignored. This is a subcommand of route-map.
match route-type	Ignored. This is a subcommand of route-map.
pager	Ignored.
pim accept-register route-map	Ignored. You can configure only the list option using ASDM.
prefix-list	Ignored if not used in an OSPF area.
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>
set metric	Ignored.
sysopt nodnsalias	Ignored.
sysopt uauth allow-http-cache	Ignored.
terminal	Ignored.
tunnel-group name general-attributes dhcp-server	The dhcp-server subcommand is unsupported. ASDM only allows one setting for all DHCP servers.

Effects of Unsupported Commands

- 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 ASA 5500 Series 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**.

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 by the 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 **crypto key generate rsa** command.

ASDM generates the default 1024-bit RSA key.

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

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
```

Defining Preferences

This feature lets you change the behavior of some ASDM functions between sessions.

To change various settings in ASDM, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Preferences**.
- The Preferences dialog box appears, with three tabs: General, Rules Table, and Syslog.
- Step 2** To define your settings, click one of these tabs: the **General** tab to specify general preferences; the **Rules Tables** tab to specify preferences for the Rules table; and the **Syslog** tab to specify the appearance of syslog messages displayed in the Home pane and to enable the display of a warning message for NetFlow-related syslog messages.
- Step 3** On the General tab, specify the following:
- a. Check the **Warn that configuration in ASDM is out of sync with the configuration in ASA** check box to be notified when the startup configuration and the running configuration are no longer in sync with each other.
 - b. Check the **Show configuration restriction message to read-only user** check box to display the following message to a read-only user at startup. This option is checked by default.

"You are not allowed to modify the ASA configuration, because you do not have sufficient privileges."
 - c. Check the **Confirm before exiting ASDM** check box to display a prompt when you try to close ASDM to confirm that you want to exit. This option is checked by default.
 - d. Check the **Enable screen reader support (requires ASDM restart)** check box to enable screen readers to work. You must restart ASDM to enable this option.
 - e. Check the **Preview commands before sending them to the device** check box to view CLI commands generated by ASDM.
 - f. Check the **Enable cumulative (batch) CLI delivery** check box to send multiple commands in a single group to the security appliance.
 - g. Enter the minimum amount of time in seconds for a configuration to send a timeout message. The default is 60 seconds.
 - h. To allow the Packet Capture Wizard to display captured packets, enter the name of the network sniffer application or click **Browse** to find it in the file system.
- Step 4** On the Rules Tables tab, specify the following:
- a. Display settings let you change the way rules appear in the Rules table.
 - Check the **Auto-expand network and service object groups with specified prefix** check box to display the network and service object groups automatically expanded based on the Auto-Expand Prefix setting.
 - In the Auto-Expand Prefix field, enter the prefix of the network and service object groups to expand automatically when displayed.
 - Check the **Show members of network and service object groups** check box to display members of network and service object groups and the group name in the Rules table. If the check box is not checked, only the group name is displayed.
 - In the Limit Members To field, enter the number of network and service object groups to display. When the object group members are displayed, then only the first *n* members are displayed.
 - Check the **Show all actions for service policy rules** check box to display all actions in the Rules table. When unchecked, a summary appears.

- b. Deployment settings let you configure the behavior of the security appliance when deploying changes to the Rules table.
 - Check the **Issue “clear xlate” command when deploying access lists** check box to clear the NAT table when deploying new access lists. This setting ensures the access lists that are configured on the security appliance are applied to all translated addresses.
- c. Access Rule Hit Count Settings let you configure the frequency for which the hit counts are updated in the Access Rules table. Hit counts are applicable for explicit rules only. No hit count will be displayed for implicit rules in the Access Rules table.
 - Check the **Update access rule hit counts automatically** check box to have the hit counts automatically updated in the Access Rules table.
 - In the Update Frequency field, specify the frequency in seconds in which the hit count column is updated in the Access Rules table. Valid values are 10 - 86400 seconds.

Step 5 On the Syslog tab, specify the following:

- In the Syslog Colors area, you can customize the message display by configuring background or foreground colors for messages at each severity level. The Severity column lists each severity level by name and number. To change the background color or foreground color for messages at a specified severity level, click the corresponding column. The Pick a Color dialog box appears. Click one of the following tabs:
 - On the Swatches tab, choose a color from the palette, and click **OK**.
 - On the HSB tab, specify the H, S, and B settings, and click **OK**.
 - On the RGB tab, specify the Red, Green, and Blue settings, and click **OK**.
- In the NetFlow area, to enable the display of a warning message to disable redundant syslog messages, check the **Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule** check box.

Step 6 After you have specified settings on these three tabs, click **OK** to save your settings and close the Preferences dialog box.



Note

Each time that you check or uncheck a preferences setting, the change is saved to the .conf file and becomes available to all the other ASDM sessions running on the workstation at the time. You must restart ASDM for all changes to take effect.
