



CHAPTER 1

Welcome to ASDM

Welcome to ASDM, a browser-based, Java applet that you use to configure and monitor the software on security appliances. ASDM is loaded by the adaptive security appliance, and enables you to configure, monitor, and manage the device.



Note

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

This section includes the following topics:

- [New in This Release, page 1-1](#)
- [Multiple ASDM Session Support, page 1-1](#)
- [Caveats, page 1-2](#)
- [Unsupported Commands, page 1-2](#)
- [About the ASDM Interface, page 1-3](#)
- [About the Help Window, page 1-13](#)
- [Home Pane, page 1-14](#)
- [System Home Pane, page 1-22](#)

New in This Release

This release of ASDM requires Version 8.0(2) and does not run with earlier adaptive security appliance releases. For a complete list of new platform and ASDM features, see the *Cisco ASDM Release Notes* on Cisco.com.

Multiple ASDM Session Support

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

Caveats

Use the Bug Toolkit on Cisco.com to view current caveat information. You can access the Bug Toolkit at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

Unsupported Commands

This section includes the following topics:

- [Ignored and View-Only Commands, page 1-2](#)
- [Effects of Unsupported Commands, page 1-3](#)

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 [Show Commands Ignored by ASDM on Device](#) for more information.

In addition, ASDM does not support discontinuous subnet masks such as 255.255.0.255. For example, do not use the following:

```
ip address inside 192.168.2.1 255.255.0.255
```

Ignored and View-Only Commands

[Table 1-1](#) 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 1-1 List of Unsupported Commands

Unsupported Commands	ASDM Behavior
access-list	Ignored if not used
capture	Ignored
dns-guard	Ignored
eject	Unsupported
established	Ignored.
failover timeout	Ignored
icmp-unreachable rate-limit	Ignored
ipv6, any IPv6 addresses	Ignored
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
route-map	Ignored

Table 1-1 List of Unsupported Commands (continued)

Unsupported Commands	ASDM Behavior
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

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 other configurations are available.

If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the list of unsupported commands, choose **Tools > Show Commands Ignored by ASDM on Device**.

If you load an existing running configuration that includes the **alias** command, ASDM enters Monitor-only mode. This mode allows you to access the following functions:

- The Monitoring area
- The CLI tool. To access the CLI tool, choose **Tools > Command Line Interface**.

To exit Monitor-only mode, use the CLI tool or access the adaptive 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 as less than or equal to three by your system administrator. For more information, choose **Configuration > Properties > Device Administration > User Accounts** and **Configuration > Device Access > AAA Access**.

About the ASDM Interface

The ASDM interface is designed to provide easy access to the many features that the adaptive security appliance supports. The ASDM interface includes the following components:

- Menu Bar—Provides quick access to files, tools, wizards, and help. Many menu items also have keyboard shortcuts.

- **Toolbar**—Lets you navigate ASDM. From the toolbar you can access the home pane, configuration, and monitoring panes. You can also get help and navigate between panes.
- **Status Bar**—Shows the time, connection status, user, and privilege level.
- **Device List**—Displays a list of devices that you can access through ASDM. For more information, see [Device List, page 1-10](#).
- **Addresses/Services/Time Ranges**—Displays a dockable pane that shows various objects you can use in the rules tables when you create access, filter, and service rules.
- **Navigation**—Displays a dockable pane that lets you navigate the Configuration and Monitoring screens.

**Note**

Tool tips have been added for various parts of the GUI, including wizards, and the configuration and monitoring panes.

This section includes the following topics:

- [Menus, page 1-4](#)
- [Toolbar, page 1-8](#)
- [Status Bar, page 1-9](#)
- [Common Buttons, page 1-10](#)
- [Keyboard Shortcuts, page 1-11](#)
- [Enabling Extended Screen Reader Support, page 1-13](#)

Menus

You can access the ASDM menus using the mouse or keyboard. See [Keyboard Shortcuts, page 1-11](#) for more information about accessing the menu bar from the keyboard. ASDM has the following menus:

- [File Menu, page 1-4](#)
- [View Menu, page 1-5](#)
- [Tools Menu, page 1-6](#)
- [Wizards Menu, page 1-6](#)
- [Window Menu, page 1-7](#)
- [Help Menu](#)

File Menu

The File menu manages adaptive security appliance configurations, and includes the following items:

- **Refresh ASDM with the Running Configuration on the Device**—Loads a copy of the running configuration to ASDM. Click **Refresh** to make sure ASDM has a current copy of the running configuration.
- **Reset Device to the Factory Default Configuration**—Restores the configuration to the factory default. See the [Reset Device to the Factory Default Configuration](#) dialog box for more information.
- **Show Running Configuration in New Window**—Displays the current running configuration in a new window.

- Save Running Configuration to Flash—Writes a copy of the running configuration to Flash memory.
- Save Running Configuration to TFTP Server—Stores a copy of the current running configuration file on a TFTP server. See the [Save Running Configuration to TFTP Server](#) dialog box for more information.
- Save Running Configuration to Standby Unit—Sends a copy of the running configuration file on the primary unit to the running configuration of a failover standby unit.
- Save Internal Log Buffer to Flash—Saves the internal log buffer to Flash memory.
- Print—Prints the current page. We recommend landscape page orientation when you print rules. If you use Internet Explorer, permission to print is already granted when you originally accepted the signed applet.
- Clear ASDM Cache—Removes local ASDM images. ASDM downloads images locally when you connect to ASDM.
- Clear Internal Log Buffer—Empties the system log message buffer.
- Exit—Closes ASDM.

View Menu

The View menu lets you display various parts of the ASDM interface. Certain items are dependent on the current view. You cannot select items that cannot be displayed in the current view. For example, the Latest ASDM Syslog Messages pane is only available when the home view is displayed.

- Home—Displays the home view.
- Configuration—Displays the configuration view.
- Monitoring—Displays the monitoring view.
- Device List—Displays a list of devices in a dockable pane. For more information, see [Device List, page 1-10](#).
- Navigation—Shows and hides the display of the Navigation pane in the configuration and monitoring views.
- Latest ASDM Syslog Messages—Shows and hides the display of the Latest ASDM Syslog Messages pane in the home view.
- Addresses—Shows and hides the display of the Addresses pane. The Addresses pane is only available for the Access Rules, NAT Rules, Service Policy Rules, AAA Rules, and Filter Rules panes in the configuration view.
- Services—Shows and hides the display of the Services pane. The Services pane is only available for the Access Rules, NAT Rules, Service Policy Rules, AAA Rules, and Filter Rules panes in the configuration view.
- Time Ranges—Shows and hides the display of the Time Ranges pane. The Time Ranges pane is only available for the Access Rules, Service Policy Rules, AAA Rules, and Filter Rules panes in the configuration view.
- Global Pools—Shows and hides the display of the Global Pools pane. The Global Pools pane is only available for the NAT Rules pane in the configuration view.
- Find—Locates an item for which you are searching, such as a feature or the ASDM Assistant.
- Back—See [Common Buttons](#) for more information.
- Forward—See [Common Buttons](#) for more information.
- Reset Layout—Returns the layout to the default configuration.

- Office Look and Feel—Changes the screen fonts and colors to the Microsoft Office settings.

Tools Menu

The Tools menu provides you with the following series of tools to use with ASDM:

- Command Line Interface—Provides a text-based tool for sending commands to the adaptive security appliance and viewing the results. See the [Command Line Interface](#) dialog box for more information.
- Show Commands Ignored by ASDM on Device—Displays unsupported commands that have been ignored by ASDM. See the [Show Commands Ignored by ASDM on Device](#) dialog box for more information.
- Packet Tracer—Lets you trace a packet from a specified source address and interface to a destination. You can specify the protocol and port of any type of data and view the lifespan of a packet, with detailed information about actions taken on it. See the [Packet Tracer](#) dialog box for more information.
- Ping—Lets you verify the configuration and operation of the adaptive security appliance and surrounding communications links, as well as perform basic testing of other network devices. See the [Ping](#) dialog box for more information.
- Traceroute—Lets you determine the route packets will take to their destination. See the [Traceroute](#) dialog box for more information.
- File Management—Lets you view, move, copy, and delete files stored in Flash memory. You can also create a directory in Flash memory. See the [File Management](#) dialog box for more information. You can also display the [File Transfer](#) dialog box to transfer files between various file systems, including TFTP, Flash memory, and your local PC.
- Upgrade Software from Local Computer—Lets you choose an adaptive security appliance image, ASDM image, or another image on your PC, and upload the file to Flash memory. See the [Upgrade Software from Local Computer](#) dialog box for more information.
- Upgrade Software from Cisco.com—Lets you upgrade adaptive security appliance software and ASDM software through a wizard. See the [Upgrade Software from Cisco.com Wizard](#) for more information.
- Upload ASDM Assistant Guide—Lets you upload an XML file to Flash memory that contains information used in the ASDM Assistant. You can download these files from Cisco.com. See the [Upload ASDM Assistant Guide](#) dialog box for more information.
- System Reload—Lets you restart the ASDM and reload the saved configuration into memory. See the [System Reload](#) dialog box for more information.
- Administrator's Alerts to Clientless SSL VPN Users—Lets an administrator send an alert message to clientless SSL VPN users. See the [Administrator's Alert to Clientless SSL VPN Users](#) dialog box for more information.
- Preferences—Changes the behavior of specified ASDM functions between sessions. See the [Preferences](#) dialog box for more information.
- ASDM Java Console—Shows the Java console. See the [ASDM Java Console](#) dialog box for more information.

Wizards Menu

The Wizards menu lets you run a wizard to configure multiple features.

- Startup Wizard—This wizard walks you, step-by-step, through the initial configuration of your adaptive security appliance. For more information, see [Using the Startup Wizard](#).
- IPsec VPN Wizard—This wizard enables you to configure an IPsec VPN policy on your adaptive security appliance. For more information, see the [VPN Wizard](#).
- SSL VPN Wizard—This wizard enables you to configure an SSL VPN policy on your adaptive security appliance. For more information, see the [VPN Wizard](#).
- High Availability and Scalability Wizard— This wizard allows you to configure failover on your adaptive security appliance. For more information, see [High Availability](#).
- Packet Capture Wizard— This wizard allows you to configure packet capture on your adaptive security appliance. The wizard runs one packet capture on each ingress and egress interface. After you run the capture, you can save the capture on your computer, and then examine and analyze the capture with a packet analyzer. For more information, see the [Packet Capture Wizard](#).

Window Menu

The Window menu enables you to move between ASDM windows. The active window appears as the selected window.

Help Menu

The Help menu provides links to online Help, as well as information about ASDM and the adaptive security appliance.

- Help Topics—Opens a new browser window with help organized by contents, screen name, and indexed in the left frame. Use these methods to find help for any topic, or search using the Search tab.
- Help for Current Screen—Opens context-sensitive help about that screen. The wizard runs the screen, pane, or dialog box that is currently open. You can also click the question mark (?) help icon for context-sensitive help.
- Release Notes—Opens the most current version of the *Cisco ASDM Release Notes* on Cisco.com. The Release Notes contain the most current information about ASDM software and hardware requirements, and the most current information about changes in the software.
- Getting Started—Opens the Getting Started help topic to help you begin using ASDM.
- VPN 3000 Migration Guide—Opens this document on Cisco.com to help you upgrade from Version 7.2 to 8.0(2).
- Glossary—Contains definitions of terms and acronyms.
- Feature Search—Lets you search for a function in ASDM. The Search feature looks through the titles of each pane and presents you with a list of matches, and gives you a hyperlink directly to that pane. If you need to switch quickly between two different panes you found, click the **Back** and **Forward** buttons. You can also click the **Search** icon on the ASDM [Toolbar, page 1-8](#).
- How Do I?—Opens the ASDM Assistant, which lets you search downloadable content from Cisco.com, with details about performing certain tasks.
- Icon Legend—Provides a list of icons used in ASDM and explains what they represent.
- About Cisco Adaptive Security Appliance (ASA)—Displays information about the adaptive security appliance, including the software version, hardware set, configuration file loaded at startup, and software image loaded at startup. This information is helpful in troubleshooting.

- About Cisco ASDM 6.0—Displays information about ASDM such as the software version, hostname, privilege level, operating system, device type, and Java version.

Toolbar

The Toolbar below the menus provides access to the home view, configuration view, and monitoring view. It also lets you choose between the system and security contexts in multiple context mode, and provides navigation and other commonly used functions.

- System/Contexts—Click the down arrow to open the context list in a left-hand pane, and click the up arrow to restore the context drop-down list. After you have expanded this list, click the left arrow to collapse the pane, and the right arrow to restore the pane. To manage the system, choose **System** from the list. To manage a context, choose one from the list.
- Home—Displays the [Home Pane](#), which lets you view important information about your adaptive security appliance such as the status of your interfaces, the version you are running, licensing information, and performance. See the Home pane for more information. In multiple mode, the system does not have a Home pane.
- Configuration—Configures the adaptive security appliance. Choose a feature button in the left-hand pane to configure that feature.
- Monitoring—Monitors the adaptive security appliance. Choose a feature button in the left-hand pane to monitor that feature.
- Back—Takes you back to the last pane of ASDM you visited.
- Forward—Takes you forward to the last pane of ASDM you visited.
- Search—Lets you search for a feature in ASDM. The Search function looks through the titles of each pane and presents you with a list of matches, and gives you a hyperlink directly to that pane. If you need to switch quickly between two different panes you found, click **Back** or **Forward**. See the [ASDM Assistant](#) for more information.
- Refresh—Refreshes ASDM with the current running configuration, except for graphs in any of the monitoring graphs.
- Save—Saves the running configuration to the startup configuration for write-accessible contexts only.
- Help—Shows context-sensitive help for the screen that is currently open.

ASDM Assistant

The ASDM Assistant dialog box lets you search for useful ASDM procedural help about certain tasks. You must first upload the ASDM Assistant Guide through the Tools menu to make the help available. See the [Upload ASDM Assistant Guide](#) dialog box for more information.

This dialog box provides a two-pane window that lets you enter queries on the left-hand pane, lists the available links to information that result from those queries, and then displays the information that you selected or additional links on the right-hand pane.

The How Do I? tab lets you select specific areas on which to search. The Search tab lets you enter terms and features about which you want more information and specify the type of results you want.

How Do I? Tab

Fields

- Show tasks—Choose the type of information you want from the drop-down list. The available types are Security Policy, ASDM, Administration, and All.

Search Tab

Fields

- For—Enter the term about which you want more information.
- How Do I?—Check this check box to include downloadable content from Cisco.com, with details about performing certain tasks.
- Features—Check to include features about which you want more details.
- Include—Select from the following options the information you want to include: Exact Phrase, Any Word, or All Words.
- Exclude—Specify the information that you want to exclude.
- Search—Click to start the query.

Status Bar

The status bar appears at the bottom of the ASDM window, and shows the following areas from left to right.

- Status—Shows the status of the configuration (for example, “Device configuration loaded successfully.”).
- User Name—Shows the username of the ASDM user. If you logged in without a username, the username is “admin.”
- User Privilege—Shows the privilege of the ASDM user.
- Commands Ignored by ASDM—Click the icon to show a list of commands from your configuration that ASDM did not process. These commands will not be removed from the configuration. See [Show Commands Ignored by ASDM on Device](#) for more information.
- Status of Connection to Device—Shows the ASDM connection status to the adaptive security appliance. See [Connection to Device](#) for more information.
- Save to Flash Needed—Shows that you made configuration changes in ASDM, but that you still must save the running configuration to the startup configuration.
- Refresh Needed—Shows that you need to refresh the configuration from the adaptive security appliance to ASDM, because the configuration on the adaptive security appliance changed (for example, you made a change to the configuration through the CLI).
- SSL Secure—Shows that the connection to ASDM is secure because it uses SSL.
- Time—Shows the time that is set on the switch that contains the adaptive security appliance.

Connection to Device

ASDM maintains a constant connection to the adaptive security appliance to maintain up-to-date monitoring and home pane data. This dialog box shows the status of the connection. When you make a configuration change, ASDM opens a second connection for the duration of the configuration, and then closes it; however, this dialog box does not represent the second connection.

Device List

The device list is a dockable pane. You can click one of the three buttons in the header to maximize or restore this pane, make it a floating pane that you can move, hide the pane, or close the pane. This pane is available in the home, configuration, monitoring, and system views. You can use this pane to switch to another device; however, that device must run the same version of ASDM that you are currently running. To display the pane fully, you must have at least two devices listed.



Note

You cannot switch to another device that runs a different version of ASDM.

To use this pane to connect to another device, perform the following steps:

-
- Step 1** Click **Add** to add another device to the list.
The Add Device dialog box appears.
- Step 2** In the Device/IP Address/Name field, type the device name or IP address of the device, and then click **OK**.
- Step 3** Click **Delete** to remove a selected device from the list.
- Step 4** Click **Connect** to connect to another device.
The Enter Network Password dialog box appears.
- Step 5** Type your username and password in the applicable fields, and then click **Login**.
-

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

Common Buttons

These buttons appear on many ASDM panes:

- **Apply**—Sends changes made in ASDM to the adaptive security appliance and applies them to the running configuration.
- **Save**—Writes a copy of the running configuration to Flash memory.

- **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After you click **Reset**, click **Refresh** to make sure that information from the current running configuration is displayed.
- **Restore Default**—Clears the selected settings and returns to the default settings.
- **Cancel**—Discards changes and returns to the previous pane.
- **Enable**—Displays read-only statistics for a feature.
- **Close**—Closes an open dialog box.
- **Clear**—Removes information from a field or box, or removes a check from a check box.
- **Back**—Returns you to the previous pane.
- **Forward**—Takes you to the next pane.
- **Help**—Displays help for the selected pane.

Keyboard Shortcuts

You can use the keyboard to navigate the ASDM interface.

Table 1-2 lists the keyboard shortcuts you can use to move across the three main areas of the ASDM interface.

Table 1-2 Navigating ASDM

To display the	Windows/Linux	MacOS
Home Page	Ctrl+H	Shift+Command+H
Configuration Page	Ctrl+G	Shift+Command+G
Monitoring Page	Ctrl+M	Shift+Command+M
Help	F1	Command+?
Back	Alt+Left Arrow	Command+[
Forward	Alt+Rightarrow	Command+]
Refresh the display	F5	Command+R
Cut	Ctrl+X	Command+X
Copy	Ctrl+C	Command+C
Paste	Ctrl+V	Command+V
Save the configuration	Ctrl+S	Command+S
Popup menus	Shift+F10	—
Close a secondary window	Alt+F4	Command+W
Find	Ctrl+F	Command+F
Exit	Alt+F4	Command+Q
Exit a table or text area	Ctrl_Shift or Ctrl+Shift+Tab	Ctrl+Shift or Ctrl+Shift+Tab

Table 1-3 lists the keyboard shortcut you can use to navigate within a pane.

Table 1-3 *Moving the Focus*

To move the focus to the	Press
next field	Tab
previous field	Shift+Tab
next field when the focus is in a table	Ctrl+Tab
previous field when the focus is in a table	Shift+Ctrl+Tab
next tab (when a tab has the focus)	Right Arrow
previous tab (when a tab has the focus)	Left Arrow
next cell in a table	Tab
previous cell in a table	Shift+Tab
next pane (when multiple panes are displayed)	F6
previous pane (when multiple panes are displayed)	Shift+F6

Table 1-4 lists the keyboard shortcuts you can use with the Log Viewers.

Table 1-4 *Log Viewer Keyboard Shortcuts*

To display the	Windows/Linux	MacOS
Pause and Resume Real-Time Log Viewer	Ctrl+U	Command+.
Refresh Log Buffer Window	F5	Command+R
Clear Internal Log Buffer	Ctrl+Delete	Command+Delete
Copy Selected Log Entry	Ctrl+C	Command+C
Save Log	Ctrl+S	Command+S
Print	Ctrl+P	Command+P
Close a secondary window	Alt+F4	Command+W

Table 1-5 lists the keyboard shortcuts you can use to access menu items.

Table 1-5 *Log Viewer Keyboard Shortcuts*

To access the	Windows/Linux
Menu Bar	Alt
Next Menu	Right Arrow
Previous Menu	Left Arrow
Next Menu Option	Down Arrow
Previous Menu Option	Up Arrow
Selected Menu Option	Enter

Enabling Extended Screen Reader Support

By default, labels and descriptions are not included in tab order when you press the Tab key to navigate a pane. Some screen readers, such as JAWS, only read screen objects that have the focus. You can include the labels and descriptions in the tab order by enabling extended screen reader support.

To enable extended screen reader support, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Preferences**.
The Preferences dialog box appears.
- Step 2** On the General tab, check the **Enable screen reader support** check box.
- Step 3** Click **OK**.
- Step 4** Restart ASDM to activate screen reader support.
-

Organizational Folder

Some nodes in the navigation tree for the configuration and monitoring screens do not have associated configuration or monitoring panes. They are used to organize related configuration and monitoring items. Clicking on these folders displays a list of sub-items in the right-hand pane. You can click the name of a sub-item to go to that item.

About the Help Window

This section includes the following topics:

- [Header Buttons](#), page 1-13
- [Browser Window](#), page 1-14

Header Buttons

Click the applicable button to obtain the information you need.

- **About ASDM**—Displays information about ASDM, including the hostname, version number, device type, adaptive security appliance software version number, privilege level, username, and operating system being used.
- **Search**—Searches for information among online help topics.
- **Using Help**—Describes the most efficient methods for using online help.
- **Glossary**—Lists terms found in ASDM and adaptive security appliance devices.
- **Left-Pane Links**—Moves through online help topics.
- **Contents**—Displays a table of contents.
- **Screens**—Lists help files by screen name.
- **Index**—Provides an index of help topics found in ASDM online help.
- **Right-Pane Help Content**—Displays the help for the selected topic.

Browser Window

When you open help and a help page is already open, the new help page will appear in the same browser window. If no help page is open, then the help page will appear in a new browser window.

If Internet Explorer is the default browser, the help page may appear either in the last-visited browser window or in a new browser window, according to your browser settings. You can control this behavior in Internet Explorer by choosing **Tools > Internet Options > Advanced > Reuse windows for launching shortcuts**.

Home Pane

The ASDM home pane lets you view important information about your adaptive security appliance. Status information on the home pane is updated every ten seconds. This pane usually has two tabs: Device Dashboard and Firewall Dashboard.

If you have a CSC SSM installed in your adaptive security appliance, the Content Security tab also appears on the home pane. The additional tab displays status information about the CSC SSM software.

If you have IPS software installed in your adaptive security appliance, the Intrusion Prevention tab also appears on the home pane. The additional tab displays status information about the IPS software.

This section includes the following topics:

- [Device Dashboard Tab, page 1-15](#)
- [Firewall Dashboard Tab, page 1-17](#)
- [Content Security Tab, page 1-18](#)
- [Intrusion Prevention Tab, page 1-20](#)

Fields

- Latest ASDM Syslog Messages—Shows the most recent system messages generated by the adaptive security appliance, up to a maximum of 100 messages.

Click the square icon in the header to expand the logging pane. Click the double square icon in the header to return to the default size. Drag the divider up or down to resize the pane. You can also right-click an event and choose **Clear Content**, to clear the current messages; **Save Content**, to save the current messages to a file on your PC, **Copy**, to copy the content; and **Color Settings**, to change the background and foreground colors of system messages according to their severity. Click one of the four buttons in the header on the right-hand side to maximize or restore the pane, make it a floating pane that you can move, hide the pane, or close the pane.

- Enable Logging—Click to enable logging and display system log messages.
- Stop message display—Click the red icon on the right-hand side to stop updating the display of system log messages.
- Resume message display—Click the green icon on the right-hand side to continue updating the display of system log messages.
- Configure ASDM Syslog Filters—Click the filters icon on the right-hand side to open the [Logging Filters](#) pane.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Device Dashboard Tab

The Device Dashboard tab lets you view, at a glance, important information about your adaptive security appliance, such as the status of your interfaces, the version you are running, licensing information, and performance.

Fields

- Device Information—Includes two tabs to show device information.
 - General—Shows the following information:
 - Host Name—*Display only*. Shows the adaptive security appliance hostname. See [Device Name/Password](#) to set the hostname.
 - ASA Version—*Display only*. Shows the adaptive security appliance software version.
 - Device Uptime—*Display only*. Shows how long the adaptive security appliance has been running.
 - ASDM Version—*Display only*. Shows the ASDM version.
 - Device Type—*Display only*. Shows the adaptive security appliance model.
 - Firewall Mode—*Display only*. Shows the firewall mode, either Routed or Transparent. See [Firewall Mode Overview](#) for more information.
 - Total Flash—*Display only*. Shows the total amount of available Flash memory.
 - Context Mode—*Display only*. Shows the context mode, either Single or Multiple. See [Security Context Overview](#) for more information.
 - Total Memory—*Display only*. Shows the total amount of available RAM.
 - License—*Display only*. Shows the level of support for licensed features on the adaptive security appliance. Shows the following information:
 - License—*Display only*. Shows the type of license, either Base or Premium.
 - Number of days until a time-based license expires, if applicable.
 - Inside Hosts—*Display only*. Shows inside hosts (ASA 5505 only).
 - Max VLANs—*Display only*. Shows the maximum number of VLANs allowed.
 - Failover—*Display only*. Shows the failover configuration, either Active/Active or Active/Standby.
 - Security Contexts—*Display only*. Shows the maximum numbers of security contexts allowed.
 - Dual ISP Support—*Display only*. Shows dual ISP support, if enabled (ASA 5505 only).
 - GTP/GPRS—*Display only*. Shows whether GTP/GPRS is enabled or disabled.
 - Encryption—*Display only*. Shows the type of encryption enabled.

VPN Peers—*Display only*. Shows the number of VPN peers allowed. This entry is blank if no VPN peers are supported.

Clientless SSL VPN Peers—*Display only*. Shows the number of clientless SSL VPN peers allowed.

- VPN Tunnels Status—Routed, single mode only. Shows the following information:
 - IKE—*Display only*. Shows the number of connected IKE tunnels.
 - IPSec—*Display only*. Shows the number of connected IPSec tunnels.
 - Clientless SSL VPN—*Display only*. Shows the number of clientless, connected SSL VPN tunnels.
 - SSL VPN Client—*Display only*. Shows the number of connected SSL VPN client tunnels.
- System Resources Status—Shows the following CPU and memory usage statistics:
 - CPU—*Display only*. Shows the current percentage of CPU being used.
 - CPU Usage (percent)—*Display only*. Shows the CPU usage for the last five minutes.
 - Memory—*Display only*. Shows the current amount of memory being used in MB.
 - Memory Usage (MB)—*Display only*. Shows the memory usage for the last five minutes in MB.
- Interface Status—Shows the status of each interface. If you select an interface row, the input and output throughput in Kbps shows under the table.
 - Interface—*Display only*. Shows the interface name.
 - IP Address/Mask—*Display only*. Routed mode only. Shows the IP address and subnet mask of the interface.
 - Line—*Display only*. Shows the administrative status of the interface. A red icon is displayed if the line is down, and a green icon is displayed if the line is up.
 - Link—*Display only*. Shows the link status of the interface. A red icon is displayed if the link is down, and a green icon is displayed if the link is up.
 - Kbps—*Display only*. Shows the current number of throughput in Kbps that cross the interface.
- Traffic Status—Shows graphs for connections per second for all interfaces and for the traffic throughput of the lowest security interface.
 - Connections per Second Usage—*Display only*. Shows the UDP and TCP connections per second during the last five minutes. This graph also shows the current number of connections by type, UDP, TCP, and the total.
 - Name Interface Traffic Usage (Kbps)—*Display only*. Shows the traffic throughput for the lowest security interface. If you have multiple interfaces at the same level, then ASDM shows the first interface alphabetically. This graph also shows the current throughput by type, input Kbps, and output Kbps.
- Latest ASDM Syslog Messages—Shows the latest system messages generated by the adaptive security appliance.
 - Stop Message Display—Stops logging to ASDM.
 - Resume Message Display—Continues logging to ASDM.
 - Configure ASDM Filters—Configures logging filters.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Firewall Dashboard Tab

The Firewall Dashboard tab lets you view important information about the traffic passing through your security appliance, including the number of connections, NAT translations, dropped packets, attacks, and top usage statistics.

The Traffic Overview statistics are enabled by default. If you disable basic threat detection (see the [“Configuring Basic Threat Detection”](#) section on page 27-1), then this tab includes an Enable button that lets you enable basic threat detection.

The Top 10 Access Rules are also enabled by default. If you disable threat detection statistics for access rules (see the [“Configuring Threat Statistics”](#) section on page 27-4), then this tab includes an Enable button that lets you enable statistics for access rules.

The Top Usage Status statistics are disabled by default. This tab includes Enable buttons that let you enable the features, or you can enable them according to the [“Configuring Threat Statistics”](#) section on page 27-4. The Top 10 Services Enable button enables statistics for both ports and protocols (both must be enabled for the display). The Top 10 Sources and Top 10 Destinations Enable buttons enable statistics for hosts.



Caution

Enabling statistics can affect the security appliance performance, depending on the type of statistics enabled. Enabling statistics for hosts affects performance in a significant way; if you have a high traffic load, you might consider enabling this type of statistics temporarily. Enabling statistics for ports, however, has modest impact.

Fields

- Traffic Overview—*Display only*. Shows runtime statistics, including the number of connections, NAT translations, and dropped packets.
 - Connection Statistics—*Display only*. Shows the number of connections and NAT translations.
 - Dropped Packets Rate—*Display only*. Shows the rate of dropped packets per second caused by access list denials and application inspections.
 - Possible Scan and SYN Attack Rates—*Display only*. Shows the rate of dropped packets per second that are identified as part of a scanning attack, or that are incomplete sessions detected, such as TCP SYN attack detected or no data UDP session attack detected.
- Top 10 Access Rules—*Display only*. Shows the most active access rules.
 - Interval—Lets you view information based on the interval you choose. Available values are Last 1 hour, Last 8 hours, and Last 24 hours.
 - Based on—*Display only*. Shows that this statistic shows number of packet hits only.
 - Display—Lets you view the same information in three different formats: Table, Pie, or Bar.
 - Interface—Shows the interface to which the rule is applied.
 - Rule#—Shows the rule number used.

- Hits—Shows the number of packet hits that occurred.
- Source—Shows the source IP address.
- Dest—Shows the destination IP address.
- Service—Shows the service (protocol or port) for the connection.
- Action—Shows whether the rule is a permit or deny rule.

In the Table view, you can select a rule in the list and right-click the rule to display a popup menu item, **Show Rule**. Choose this item to go to the Access Rules table and select that rule in this table.

- Top Usage Status—Provides usage status for hosts (source and destinations), and ports and protocols.
 - Interval—Lets you view information based on the interval you choose. Available values are Last 1 hour, Last 8 hours, and Last 24 hours.
 - Based On—Shows the statistics in Packet Hits or Bytes.
 - Display—Lets you view the same information in three different formats: Table, Pie, or Bar.
 - Top 10 Services—Shows statistics for the top 10 services, including the combined statistics of TCP/UDP port and IP protocol types.
 - Top 10 Sources—Shows the top 10 host source addresses.
 - Top 10 Destinations—Shows the top 10 host destination addresses.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	—	—

Content Security Tab

The Content Security tab lets you view important information about the Content Security and Control (CSC) SSM. This pane appears only if a CSC SSM is installed in the adaptive security appliance.

For an introduction to the CSC SSM, see [About the CSC SSM](#).



Note

If you have not completed the CSC Setup Wizard by choosing **Configuration > Trend Micro Content Security > CSC Setup**, you cannot access the panes under Home > Content Security. Instead, a dialog box appears and lets you access the Setup Wizard directly from this location.

Fields

- Device Information—Shows the following details:
 - Model—*Display only*. Shows the type of SSM installed in your adaptive security appliance.
 - Mgmt IP—*Display only*. Shows the IP address of the management interface for the CSC SSM.
 - Version—*Display only*. Shows the CSC SSM software version.

- Last Update—*Display only*. Shows the date of the last software update obtained from Trend Micro.
- Daily Node #—*Display only*. Shows the number of network devices for which the CSC SSM provided services in the preceding 24 hours. ASDM updates this field at midnight.
- Base License—*Display only*. Shows the license status for basic features of the CSC SSM, such as anti-virus, anti-spyware, and FTP file blocking. The license expiration date appears. If the license has expired, the expiration date appears. If no license is configured, the field shows “Not Available.”
- Plus License—*Display only*. Shows the license status for advanced features of the CSC SSM, such as anti-spam, anti-phishing, e-mail content filtering, and URL blocking and filtering. The license expiration date appears. If the license has expired, the expiration date appears. If no license is configured, the field shows “Not Available.”
- Licensed Nodes—*Display only*. Shows the maximum number of network devices for which your CSC SSM is licensed to provide services.
- System Resources Status—Shows the following CPU and memory usage statistics for the CSC SSM:
 - CPU—*Display only*. Shows the current percentage of CPU being used.
 - CSC SSM CPU Usage (percent)—*Display only*. Shows the CPU usage for the last five minutes.
 - Memory—*Display only*. Shows the current amount of memory being used in MB.
 - CSC SSM Memory Usage (MB)—*Display only*. Shows the memory usage for the last five minutes in MB.
- Threat Summary—Shows aggregated data about threats detected by the CSC SSM.
 - Threat Type—*Display only*. Lists five threat types: Virus, Spyware, URL Blocked, URL Filtered, and Spam.
 - Today—*Display only*. Shows the number of threats detected for each threat type in the past 24 hours.
 - Last 7 Days—*Display only*. Shows the number of threats detected for each threat type in the past seven days.
 - Last 30 Days—*Display only*. Shows the number of threats detected for each threat type within the past 30 days.
- Email Scan—Shows graphs for scanned e-mails and e-mail virus and spyware detected.
 - Email Scanned Count—*Display only*. Shows the number of e-mails scanned as separate graphs by e-mail protocol (SMTP or POP3), and as a combined graph for both supported e-mail protocols. The graphs display data in ten-second intervals.
 - Email Virus and Spyware—*Display only*. Shows the number of viruses and e-mails detected in e-mail scans as separate graphs by threat type (virus or spyware). The graphs display data in ten-second intervals.
- Latest CSC Security Events—Shows in real-time the security event messages received from the CSC SSM.
 - Time—*Display only*. Shows the time that an event occurred.
 - Source—*Display only*. Shows the IP address or hostname from which the threat came.
 - Threat/Filter—*Display only*. Shows the type of threat or, in the case of a URL filter event, the filter that triggered the event.

- Subject/File/URL—*Display only*. Shows the subject of e-mails that contain a threat, the names of FTP files that contain a threat, or blocked or filtered URLs.
- Receiver/Host—*Display only*. Shows the recipient of e-mails that contain a threat or the IP address or hostname of a threatened node.
- Sender—*Display only*. Shows the source of e-mails that contain a threat.
- Content Action—*Display only*. Shows the action that is taken on the message or file content, such as delivering the content unaltered, deleting attachments, or cleaning attachments before delivering them.
- Msg Action—*Display only*. Shows the action that is taken on the message, such as delivering the message unchanged, delivering the message after deleting attachments, or not delivering the message.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

Intrusion Prevention Tab

The Intrusion Prevention tab lets you view important information about IPS. This tab appears only when you have IPS software running on the AIP SSM that is installed on the adaptive security appliance.

For more information about intrusion prevention, see [Configuring IPS](#).

Connecting to IPS

To connect to the IPS software on the AIP SSM, perform the following steps:

-
- Step 1** From the main ASDM application window, click the **Intrusion Prevention** tab.
 - Step 2** In the Connecting to IPS dialog box, choose one of the following options:
 - Management IP Address—Connects to the IP address of the management port on the SSM.
 - Other IP Address or Hostname—Connects to an alternate IP address or hostname on the SSM.
 - Step 3** Enter the port number in the Port field, and then click **Continue**.
 - Step 4** In the Enter Network Password dialog box, type your username and password in the applicable fields, and then click **Login**.
-

Fields

- Device Information—Shows the following information:
 - Host Name—*Display only*. Shows the IPS hostname.

- IPS Version—*Display only*. Shows the IPS software version.
- IDM Version—*Display only*. Shows the IDM software version.
- Bypass Mode—*Display only*. Shows the bypass mode, which can be set to On or Off.
- Missed Packets Percentage—*Display only*. Shows the percentage of missed packets.
- IP Address—*Display only*. Shows the IP address of the adaptive security appliance.
- Device Type—*Display only*. Shows the type and model of the adaptive security appliance.
- Total Data Storage—*Display only*. Shows the total amount of available data storage in MB.
- Total Sensing Interface—*Display only*. Shows the total number of sensing interfaces.
- System Resources Status—Shows the following CPU and memory usage statistics for the IPS software:
 - *Display only*. Percentage of CPU resources currently being used.
 - *Display only*. Average percentage of CPU resources being used.
 - *Display only*. Amount of memory currently being used.
 - *Display only*. Average amount of memory being used.
 - *Display only*. Amount of free memory and total memory available.
- Interface Status—Shows the following information:
 - Interface—*Display only*. Shows the type of interface to which you are connected. Choose an interface to view the sent and received packet counts.
 - Link—*Display only*. Shows the link status, which can be Up or Down.
 - Enabled—*Display only*. Shows the current connection status, which can be Yes (Enabled) or No (Not Enabled).
 - Speed—*Display only*. Shows the current connection speed.
 - Mode—*Display only*. Shows the current mode, which can be Management or Paired.
- Alert Summary—*Display only*. Lists the alerts, with assigned values of High, Med, Low, and Info, and the assigned threat rating.
- Alert Profile—*Display only*. Shows the alerts received in a color-coded graph, with assigned values of High (red), Med (yellow), Low (green), and Info (blue), and the assigned threat rating (magenta).
- Auto-Refresh every 10 seconds—Check this check box to refresh the current pane automatically every ten seconds.
- Refresh Page—Click to refresh the currently open pane manually.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

System Home Pane

The ASDM system home pane lets you view important status information about your adaptive security appliance. Many of the details available on the ASDM system home pane are available elsewhere in ASDM, but this pane shows at-a-glance how your adaptive security appliance is running. Status information on the system home pane is updated every ten seconds.

**Note**

This pane is available only in the security context.

Fields

- Device List—Displays the list of devices to which you can connect. For more information, see [Device List, page 1-10](#).
- Interface Status—Shows the following information:
 - Interface—*Display only*. Shows the type of interface to which you are connected. Choose an interface to view the total amount of traffic through the interface.
 - Contexts—*Display only*. Shows the current contexts of users (for example, admin).
 - Line—*Display only*. Shows the line status, which can be Up or Down.
 - Link—*Display only*. Shows the link status, which can be Up or Down.
 - Kbps—*Display only*. Shows the current connection speed in kilobits per second.
- CPU Status—Shows the following CPU and context usage statistics:
 - Total Usage tab—*Display only*. Shows the total percentage of CPU usage and the total percentage of CPU usage history in seconds.
 - Context Usage tab—*Display only*. Shows the total percentage of context usage in three formats: a table, or a pie or bar chart. The tabular view provides a filtering feature to show only the top five or top ten users of a specific resource. In addition, this view can show peak usage.
- Connection Status—Shows the following connection usage and context connection usage statistics:
 - Total Connections tab—*Display only*. Shows the total number of connections.
 - Context Connections tab—*Display only*. Shows the total number of context connections in three formats: a table, or a pie or bar chart. The tabular view provides a filtering feature to show only the top five or top ten users of a specific resource. In addition, this view can show peak usage.
- Memory Status—Shows the following CPU and context usage statistics:
 - Total Usage tab—*Display only*. Shows the total amount of memory usage in MB and the total amount of memory usage history in MB.
 - Context Usage tab—*Display only*. Shows the total amount of memory usage in various contexts in MB in three formats: a table, or a pie or bar chart. The tabular view provides a filtering feature to show only the top five or top ten users of a specific resource. In addition, this view can show peak usage.

Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	•

