



# CHAPTER 1

## Welcome to ASDM

---

Welcome to ASDM, a browser-based, Java applet used to configure and monitor the software on security appliances. ASDM is loaded from the security appliance, then used to configure, monitor, and manage the device.

For more information about this release, see the following topics:

- [Important Notes](#)
- [New in This Release](#)
- [Unsupported Commands](#)
- [About the ASDM Window](#)
- [About the Help Window](#)
- [Home Page](#)

## Important Notes

- **CLI Command Support**—With a few exceptions, almost all CLI commands are fully supported by ASDM. For a list of commands ASDM does not support, see [Unsupported Commands](#).
- **Multiple ASDM Sessions**—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 5 concurrent ASDM sessions in single, routed mode. Only one session per browser per PC or workstation is supported for a particular security appliance. In multiple context mode, five concurrent ASDM sessions are supported per context, up to a limit of 32 connections total per security appliance.
- **Security Appliance Release**—This release of ASDM requires Version 7.1 and does not run with earlier security appliance releases.
- **Caveats**—Use the Bug Toolkit on [cisco.com](http://www.cisco.com) to view current caveat information. You can access Bug Toolkit at:  
[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)
- **Changing OS Color Schemes**—If you change the color scheme of your operating system while ASDM is running, you should restart ASDM or some ASDM screens might not display correctly.
- If you enable TCP normalization, the default action for packets that exceed MSS has changed from drop to allow (the **exceed-mss** command).

# New in This Release

This section contains the following topics:

- [Features Introduced in the 5.2\(1\) Release, page 1-2](#)
- [Features Introduced in the 5.2\(2\) Release, page 1-2](#)
- [Features Introduced in the 5.2\(3\) Release, page 1-3](#)
- [Features Introduced in the 5.2\(4\) Release, page 1-4](#)

For a complete list of new platform and ASDM features, refer to the *Cisco ASDM Release Notes* on Cisco.com.

## Features Introduced in the 5.2(1) Release

See the following topics for more information about the new features in the 5.2(1) release:

- Enhanced and new inspection engines. See [Service Policy Rules, page 21-1](#) and [Global Objects, page 6-1](#).
- Sub-second failover and the High Availability and Scalability Wizard. See [Failover, page 12-1](#).
- Packet Tracer tool. See [Packet Tracer, page 1-13](#).
- Traceroute tool. See [Traceroute, page 1-17](#).
- Expanded VPN Support:
  - ZoneLabs Integrity Server. See [Zone Labs Integrity Server, page 27-60](#).
  - Easy VPN Remote. See [Easy VPN Remote, page 27-61](#).
  - Online Certificate Status Protocol (OCSP) support. See [Add/Edit Trustpoint Configuration > Revocation Check Tab, page 32-11](#) and [Add/Edit Trustpoint Configuration > OCSP Rules Tab, page 32-13](#).
- RIP routing enhancements. See [RIP, page 14-21](#).
- Static Route Tracking/Dual ISP support. See [Static Routes, page 14-28](#).
- Web Cache Communication Protocol (WCCP) support. See [WCCP, page 25-2](#).
- ASA 5505 adaptive security appliance Power over Ethernet port support. See [Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance, page 5-13](#).

## Features Introduced in the 5.2(2) Release

See the following topics for more information about the new features in the 5.2(2) release:

- IDM Integration. See [Accessing IDM from ASDM, page 34-1](#).
- AIP SSM Password Reset. See [Resetting the AIP SSM Password, page 34-2](#).
- CSC SSM Password Reset. See [Restoring the Default Password, page 35-12](#).
- Additional Multicast Feature Support:
  - PIM neighbor-filter. See [Neighbor Filter, page 15-13](#).
  - PIM bidir-neighbor-filter. See [Bidirectional Neighbor Filter, page 15-14](#).

- PIM old-register-checksum. See the Generate IOS compatible register messages check box in [Rendezvous Points](#), page 15-16.
- Multicast Boundary. See [MBoundary](#), page 15-8.
- MFIB forwarding. See PIM bidir-neighbor-filter. See [MForwarding](#), page 15-10.
- Support for HTTP/HTTPS interactive authentication. See [Configuring Advanced AAA Features](#), page 19-12.
- Added DNS (User Principle Name) to the Primary DN Field for tunnel groups. See [Add/Edit Tunnel Group > General Tab > Authorization Tab](#), page 27-44.
- Per-interface authorization server groups for tunnel groups. See [Add/Edit Tunnel Group > General Tab > Authorization Tab](#), page 27-44.
- Support for Virtual Telnet Server. See [Virtual Access](#), page 11-11.

## Features Introduced in the 5.2(3) Release

See the following topics for more information about the new features in the 5.2(3) release:

- 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.
- Added Enable DNS Guard checkbox to DNS Client panel for interfaces. See [Configuration > Properties > DNS](#).
- Added **redirect-fqdn** command to support DNS-based load balancing.
- Added support in Client Software Location list to allow client updates from Linux or Mac systems. See [Configuration > Remote Access VPN > Network \(Client\) Access > Advanced > IPSec > Upload Software > Client Software](#).
- Added new checkbox Cache Static Content to allow users to cache the static content. See [Configuration>VPN>WebVPN>Cache](#).
- Support for two new options, **broadcast-flag** and **client-id interface** *interface* in the **dhcp-client** command. See [Configuration > Interfaces > Add or Edit Interfaces > Obtain Addresses via DHCP](#).
- ASDM now reporting Damage Cleanup Services events and statistics.
- ASDM banner includes 'Continue' and 'Disconnect' button at startup. To configure banner with these buttons, see [Configuration > Properties > Device Administration > Banner](#).
- Added support for new ESMTP parameter **allow-tls [action log]** in the ESMTP policy map. When parameter is on, traffic on an ESMTP session will not be inspected after the exchange of client's STARTTLS command and server's 220 reply code. To implement this parameter, see [Configuration Global Objects > Inspect Maps > ESMTP](#). After map is inspected or edited, select the entry and click **Advanced View** to access the ESMTP policy map parameter.
- Added the **inspect waas** command to support WAAS inspection. See [Service Policy Rule > Protocol Inspection](#).
- Added new command, **smartcard-removal-disconnect [enable | disable]** in group policy configuration mode, to specify that tunnels stay connected when the SmartCard is removed. Currently, the default behavior is that tunnels are disconnected when a SmartCard is removed.

- Increased VLAN range for the ASA 5505--The ASA 5505 adaptive security appliance now supports VLAN IDs between 1 and 4090. Originally, only VLAN IDs between 1 and 1001 were supported.

## Features Introduced in the 5.2(4) Release

See the following topics for more information about the new features in the 5.2(4) release:

- Network Objects-- You can now add true network objects that you can use in firewall rules. Objects can be named, and when you edit an object, the change is inherited wherever the object is used. Also, when you create a rule, the networks that you specify in the rule are automatically added to the network object list so you can reuse them elsewhere. You can name and edit these automatic entries as well. See Configuration > Objects > Network Objects/Groups.
- QoS Traffic Shaping--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. To manage networks with differing line speeds, you can configure the security appliance to transmit packets at a fixed slower rate. See the Configuration > Security Policy > Service Policy Rules pane, 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.

See the **crypto ipsec security-association replay** command, which lets you configure the IPSec anti-replay window size. One side-effect of priority queueing is packet re-ordering. For IPSec packets, out-of-order packets that are not within the anti-replay window generate warning syslog messages. These warnings become false alarms in the case of priority queueing. This new command avoids possible false alarms.

- Timeout for SIP provisional media--You can now configure the timeout for SIP provisional media on the Configuration > Properties > Timeouts pane.
- Rate and burst limit sizes for ICMP messages can now be adjusted from the Configuration > Properties > ICMP Rules pane.
- TCP normalization enhancements--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.
  - TCP invalid ACK check
  - TCP packet sequence past window check
  - TCP SYN-ACK with data check

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 the Configuration > Global Objects > TCP Maps pane. The following non-configurable actions have changed from drop to clear for these packet types:

- Bad option length in TCP
- TCP Window scale on non-SYN
- Bad TCP window scale value
- Bad TCP SACK ALLOW option

# Unsupported Commands

ASDM supports almost all commands available for the security appliance, but some commands in an existing configuration are ignored by ASDM. Most of these commands can remain in your configuration; see [Show Commands Ignored by ASDM on Device](#) for the ignored commands in your configuration.

In the case of the **alias** command, ASDM enters into Monitor-only mode until you remove the command from your configuration.

This section contains the following topics:

- [Ignored and View-Only Commands](#)
- [Effects of Unsupported Commands](#)
- [Other CLI Limitations](#)

## Ignored and View-Only Commands

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

Unsupported Commands	ASDM Behavior
<b>access-list</b>	Ignored if not used.
<b>capture</b>	Ignored
<b>established</b>	Ignored.
<b>failover timeout</b>	Ignored.
<b>ipv6</b> , any IPv6 addresses	Ignored.
<b>pager</b>	Ignored.
<b>pim accept-register route-map</b>	Ignored. Only the <b>list</b> option can be configured using ASDM
<b>prefix-list</b>	Ignored if not used in an OSPF area.
<b>route-map</b>	Ignored.
<b>service-policy global</b>	Ignored if it uses a <b>match access-list</b> class. For example: <pre>access-list myacl line 1 extended permit ip any any class-map mycm match access-list mycl policy-map mypm class mycm inspect ftp service-policy mypm global</pre>
<b>switchport trunk native vlan</b>	Ignored in Ethernet interface mode.
<b>sysopt nodnsalias</b>	Ignored.
<b>sysopt uauth allow-http-cache</b>	Ignored.

Unsupported Commands	ASDM Behavior
<b>terminal</b>	Ignored.
<b>virtual</b>	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 all other configuration is available.
- If ASDM loads an existing running configuration and finds other unsupported commands, ASDM operation is unaffected. To view the unsupported commands, see Options > Show Commands Ignored by ASDM on Device.
- If ASDM loads an existing running configuration and finds the **alias** command, it enters Monitor-only mode.

Monitor-only mode allows access to the following functions:

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

To exit Monitor-only mode, use the CLI tool or access the security appliance console, and remove the **alias** command. You can use outside NAT instead of the **alias** command. See the *Cisco 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 3 by your system administrator, which allows Monitor-only mode. For more information, see Configuration > Properties > Device Administration > User Accounts and Configuration > Device Access > AAA Access.

## Other CLI Limitations

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

```
ip address inside 192.168.2.1 255.255.0.255
```

## About the ASDM Window

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

- **Menus**—Provides quick access to files, tools, options and help.
- **Toolbar**—Lets you navigate ASDM. From the toolbar you can access the home page, configuration, and monitoring panels. You can also search for features, save the configuration, get help and navigate back and forth between panels. The Home, Configuration, and Monitoring buttons each

open a panel with a variety of useful tools. The home page offers much information at a glance. Configuration and monitoring offer a useful category tree along the left side of the frame, for access to more detailed configuration or monitoring information.

- [Status Bar](#)—Shows the time, connection status, user, and privilege level.

## Menus

ASDM includes the following menus:

- [File Menu](#)
- [Options Menu](#)
- [Tools Menu](#)
- [Wizards Menu](#)
- [Help Menu](#)

## File Menu

The File menu manages 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. Use 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 [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 log buffer to flash memory.
- [Print](#)—Prints the current panel. We recommend landscape page orientation when printing rules. If ASDM is running in Netscape Communicator and the user has not yet granted print privileges to the Java applet, a security dialog appears requesting Print privileges. Click **Grant** to grant the applet printing privileges. When using Internet Explorer, permission to print is already granted when you originally accepted the signed applet.
- [Clear ASDM Cache](#)—Clears the local ASDM images. ASDM downloads an image locally when you connect to ASDM.
- [Clear Internal Log Buffer](#)—Clears the system log message buffer.
- [Exit](#)—Exits ASDM.

## Reset Device to the Factory Default Configuration

The default configuration includes the minimum commands required to connect to the security appliance using ASDM. This feature is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces, and setting the interface IP address is one of the actions this feature takes. This feature is also only available in single context mode; a security appliance with a cleared configuration does not have any defined contexts to automatically configure using this feature.

This feature clears the current running configuration and then configures several commands. The configured interface depends on your platform. For a platform with a dedicated management interface, the interface is named “management.” For other platforms, the configured interface is Ethernet 1 and named “inside.”

The following commands apply to the dedicated management interface, Management 0/0 (for a platform without a dedicated management interface, the interface is Ethernet 1):

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

If you set the IP address in this dialog box, then the **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.

After you restore the factory default configuration, save it to internal Flash memory using the File > Save Running Configuration to Flash item. This menu item saves the running configuration to the default location for the startup configuration, even if you previously configured the [Boot Image/Configuration](#) to set a different location; when the configuration was cleared, this path was also cleared.



### Note

This command also clears the [Add Boot Image](#) configuration, if present, along with the rest of the configuration. The [Add Boot Image](#) pane lets you boot from a specific image, including an image on the external Flash memory card. The next time you reload the security appliance after restoring the factory configuration, it boots from the first image in internal Flash memory; if you do not have an image in internal Flash memory, the security appliance does not boot.

### Fields

- Use this address for the “*Interface\_ID*” interface which will be named as “*name*”—Manually sets the IP address of the management interface, instead of using the default address, 192.168.1.1. For a platform with a dedicated management interface, the interface is named “management.” For other platforms, the configured interface is Ethernet 1 and named “inside.”
- Management IP Address—Sets the management interface IP address.
- Management subnet mask—Sets the subnet mask of the interface. If you do not set a mask, the security appliance uses the mask appropriate for the IP address class.

### Modes

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

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

### Save Running Configuration to TFTP Server

This dialog box stores a copy of the current running configuration file on a TFTP server.

#### Fields

- TFTP Server IP Address—Enter the IP address of the TFTP server.
- Configuration File Path—Enter path on the TFTP server where the file will be saved.

#### Modes

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

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

### Enter Log File Name

Saves the log buffer to flash memory.

#### Fields

- Use default file name—Saves the log buffer using LOG-YYYY-MM-DD-hhmmss.txt as the file name.
- Use user-specified file name—Saves the log buffer using a file name that you specify.
- Field Name—Enter the file name for the saved log buffer.

### Options Menu

The Options menu lets you set ASDM preferences.

- 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.
- Preferences—Changes the behavior of some ASDM functions between sessions using your web browser cookie feature. See the [Preferences](#) dialog box for more information.

## Show Commands Ignored by ASDM on Device

Some commands are unsupported in ASDM. Typically, they are ignored when encountered by ASDM, and are displayed in the list of unparsed commands invoked by Show Commands Ignored by ASDM on Device.

ASDM does not change or remove these commands from your configuration. See [Unsupported Commands](#) for more information.

### Modes

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

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

## Preferences

The Preferences dialog box lets you change the behavior of some ASDM functions between sessions by using your web browser cookie feature.

### Fields

- General tab—Sets general preferences.
  - Preview commands before sending to the device check box—Lets you view CLI commands generated by ASDM.
  - Enable Large Fonts (Requires ASDM Restart) check box—Increases the ASDM icon font size, after closing ASDM and reconnecting. Not all fonts are affected.
  - Confirm before exiting from ASDM check box—Displays a prompt when you try to close ASDM to confirm that you want to exit. This option is checked by default.
- Rules Table tab—Sets preferences for the Rules Table.
  - Display settings—Lets you change the way rules are displayed in the Rules Table.
  - Auto expand network and service object groups with specified prefix—Displays the network and service object groups automatically expanded based on the Auto Expand-Prefix.
  - Auto Expand-Prefix—Specifies the prefix of the network and service object groups to automatically expand when displayed.
  - Show members of network and service object groups—Select to display members of network and service object groups and the group name in the rules table. If the check box is not selected, only the group name is displayed.
  - Limit members to—Enter the number of network and service object groups to display. When the object group members are displayed, then display only the first *nn* members.
  - Show all actions for service policy rules—Select to display all action in the rules table. When cleared, a summary is displayed.
  - Deployment Settings—Lets you configure the behavior the security appliance has when deploying changes to the rules table.

- Issue clear xlate command when deploying access lists—Check to clear the NAT table when deploying a new access lists. This ensures the access lists that are configured on the security appliance are applied to all translated addresses.
- Show filter panel by default—Displays the filter panel by default.
- Show rule diagram panel by default—Displays the rule diagram by default.
- Applications Inspections tab—Sets Application Inspection map options.
  - Prompt to add inspect map before applying changes—Enables a prompt that reminds you the inspection map has not yet been added.
  - Make advanced view the default inspect view—Select to make the advanced view the default application inspection view.
- Ask to make advanced view the default view—Enables a dialog box that asks to make the advanced view the default application inspection view. Clear to disable the prompt.
- Syslog Color Settings tab—Sets the background and text colors for system log messages displayed on the Home page.
  - Severity column—Lists each severity level.
  - Background Color column—Shows the background color for messages for each severity level. To change the color, click the appropriate row. The Pick a Color dialog box appears.
  - Foreground Color column—Shows the foreground (text) color for messages for each severity level. To change the color, click the appropriate row. The Pick a Color dialog box appears.
  - Restore Default button—Restores the default settings of white background and colored text.

**Note**

Each time a preference is checked or unchecked, the change is written to the .conf file and becomes available for all the other ASDM sessions running on the workstation at the time. Restarting ASDM maintains your preferences.

**Modes**

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

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

**Tools Menu**

The Tools menu provides you with troubleshooting tools on ASDM. Here you can upload new software to the ASDM, check connectivity, or issue commands at the command line.

- Command Line Interface—Provides a text-based tool for sending commands to the security appliance and viewing the results. See the [Command Line Interface](#) 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 see the lifespan of a packet with detailed information about actions taken on it. See the [Packet Tracer](#) dialog box for more information.
- Ping—Provides a useful tool for verifying the configuration and operation of the security appliance and surrounding communications links, as well as 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 bring up the [File Transfer](#) dialog box to transfer files between various file systems, including TFTP, Flash memory, and your local PC.
- Upload ASDM Assistant Guide—Lets you upload an XML file to Flash memory that contains information used in the ASDM Assistant. These files can be downloaded from Cisco.com.
- Upgrade Software—Lets you choose a security appliance image, ASDM image, or other image file on your PC, and upload it to Flash memory. See the [Upload Image from Local PC](#) dialog box for more information.
- System Reload—Lets you restart the system and reload the saved configuration into memory. See the [System Reload](#) dialog box for more information.
- IPS/CSC Password Reset—Resets the password of an installed AIP SSM or CSC SSM to the default (cisco). See the [“Resetting the AIP SSM Password” section on page 34-2](#) and the [“Restoring the Default Password” section on page 35-12](#) for more information.
- ASDM Java Console—Shows the Java console.

## Command Line Interface

The Command Line Interface dialog box provides a text-based tool for sending commands to the security appliance and viewing the results.



### Note

---

Commands entered via the ASDM CLI tool might function differently from commands entered through a terminal connection to the security appliance.

---

## Command Errors

If an error occurs because you entered an incorrect command, the offending command is skipped and the remaining commands are processed anyway. A message displays in the Response box to let you know what, if any, errors were encountered as well as other pertinent information.



### Note

---

Refer to the *Cisco ASA 5500 Series Command Reference* for a list of commands. With a few exceptions, almost all CLI commands are fully supported by ASDM.

---

## Interactive Commands

Interactive commands are not supported in the Command Line Interface dialog box. To use these commands in ASDM, use the **noconfirm** keyword if available, as follows:

```
crypto key generate rsa modulus 1024 noconfirm
```

## Avoiding Conflicts with Other Administrators

Multiple administrative users can update the running configuration of the security appliance. Before using the ASDM Command Line Interface tool to make configuration changes, check for other active administrative sessions. If more than one user is configuring the security appliance at the same time, the last changes take effect. (Click the **Monitoring** tab to view other administrative sessions that are currently active on the same security appliance.)

## Viewing Configuration Changes in ASDM

If you change the configuration using the Command Line Interface tool, click the **Refresh** button to view the changes in ASDM.

### Prerequisites

The commands you can enter at the Command Line Interface tool depends on your user privileges. See the [Authorization Tab](#). Review your privilege level in the status bar at the bottom of the main ASDM window to ensure you have privileges to execute privileged-level CLI commands.

### Fields

- **Command**—Sends commands to the security appliance.
  - **Single Line**—Lets you enter single commands, one at a time. The most recent commands entered are listed, or you can type a new command.
  - **Multiple Line**—Lets you enter multiple command lines.
  - **Enable context sensitive help (?)**—Shows CLI help for a command if you enter a question mark (?) after it. You do not need to press enter; the help displays as soon as you type a ?.  
Clearing this check box causes ASDM to escape the question mark character before sending it to the device, allowing you to enter the question mark as part of a text string without causing the command line help to display.
- **Response**—Displays the results of the commands you entered in the command box.
- **Send**—Sends all commands to the security appliance.
- **Clear Response**—Clears all text displayed in the Response box.

### Modes

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

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

## Packet Tracer

The packet tracer tool provides packet tracing capabilities for packet sniffing and network fault isolation.

The tool provides detailed information about the packets and how they are processed by the security appliance. In the instance that a command from the configuration did not cause the packet to drop, the packet tracer tool will provide information about the cause in an easily readable manner. For example if a packet was dropped because of an invalid header validation, a message is displayed that says, “packet dropped due to bad ip header (reason).”

In addition to capturing packets, it is possible to trace the lifespan of a packet through the security appliance to see if it is behaving as expected. The packet tracer tool lets you do the following:

- Debug all packet drops in production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet along with the CLI lines which caused the rule addition.
- Show a time line of packet changes in a data path.
- Inject tracer packets into the data path.

**Fields**

- **Interface**—Specifies the source interface for the packet trace.
- **Packet type**—Specifies the protocol type for the packet trace. Available protocol types are *icmp*, *rawip*, *tcp* or *udp*.
  - **Source IP**—Specifies the source address for the packet trace.
  - **Source Port**—Specifies the source port for the packet trace.
  - **Destination IP** —Specifies the destination address for the packet trace.
  - **Destination Port**—Specifies the destination port for the packet trace.
- **Start** —Starts the packet trace.
- **Clear**—Clears all fields.
- **Show animation**—Check to display graphically the packet trace.
- **Information Display Area**—Displays detailed messages about the packet trace.

**Modes**

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

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

**Ping**

The Ping dialog box provides a useful tool for verifying the configuration and operation of the security appliance and surrounding communications links, as well as basic testing of other network devices.

A ping is the network equivalent of sonar for submarines. A ping is sent to an IP address and it returns an echo, or reply. This simple process enables network devices to discover, identify, and test each other.

The Ping tool uses ICMP described in RFC-777 and RFC-792. ICMP defines an *echo* and *echo reply* transaction between two network devices, which has become known as a ping. The *echo* (request) packet is sent to the IP address of a network device. The receiving device reverses the source and destination address and sends the packet back as the *echo reply*.

## Using the Ping Tool

Administrators can use the ASDM Ping tool as an interactive diagnostic aid in several ways, for example:

- Loopback testing of two interfaces—A ping may be initiated from one interface to another on the same security appliance, as an external loopback test to verify basic “up” status and operation of each interface.
- Pinging to a security appliance interface—An interface on another security appliance may be pinged by the Ping tool or another source to verify that it is up and responding.
- Pinging through a security appliance—Ping packets originating from the Ping tool may pass through an intermediate security appliance on their way to a device. The echo packets will also pass through two of its interfaces as they return. This procedure can be used to perform a basic test of the interfaces, operation, and response time of the intermediate unit.
- Pinging to test questionable operation of a network device—A ping may be initiated from a security appliance interface to a network device that is suspected to be functioning improperly. If the interface is configured properly and an echo is not received, there may be problems with the device.
- Pinging to test intermediate communications—A ping may be initiated from a security appliance interface to a network device which is known to be functioning properly and returning echo requests. If the echo is received, the proper operation of any intermediate devices and physical connectivity is confirmed.

## Troubleshooting the Ping Tool

When pings fail to receive an echo, it may be the result of a configuration or operational error in a security appliance, and not always due to “NO response” from the IP address being pinged. Before using the Ping tool to ping *from*, *to* or *through* a security appliance interface, verify the following:

### Basic Interface Checks

- Verify that interfaces are configured properly in Configuration > Properties > Interfaces.
- Verify that devices in the intermediate communications path, such as switches or routers, are properly delivering other types of network traffic.
- Make sure that traffic of other types from “known good” sources is being passed. Use Monitoring > Interface Graphs.

### Pinging from a security appliance interface

For basic testing of an interface, a ping may be initiated from a security appliance interface to a network device which, by other means, is known to be functioning properly and returning echoes via the intermediate communications path.

- Verify receipt of the ping from the security appliance interface by the “known good” device. If it is not received, there may be a problem with the transmit hardware or configuration of the interface.
- If the security appliance interface is configured properly and it does not receive an echo from the “known good” device, there may be problems with the interface hardware receive function. If a different interface with “known good” receive capability can receive an echo after pinging the same “known good” device, the hardware receive problem of the first interface is confirmed.

### Pinging to an security appliance interface

When attempting to ping *to* an security appliance interface, verify that pinging response (ICMP *echo reply*), is enabled for that interface in the Configuration > Properties > Administration > ICMP panel. When pinging is disabled, the security appliance cannot be detected by other devices or software applications, and will not respond to the ASDM Ping tool.

### Pinging through the security appliance

- First, verify that other types of network traffic from “known good” sources is being passed through through the security appliance. Use Monitoring > Interface Graphs, or an SNMP management station.
- To enable internal hosts to ping external hosts, ICMP access must be configured correctly for both the inside and outside interfaces in Configuration > Access Rules.

### Fields

- IP Address—The destination IP address for the ICMP echo request packets.



**Note** If a host name has been assigned in the **Configuration > Network Objects/Groups** pane, you can use the host name in place of the IP address.

- Interface—(Optional). The security appliance interface that transmits the *echo* request packets is specified. If it is not specified, the security appliance checks the routing table to find the destination address and uses the required interface.
- Ping Output—The result of the ping. When you click **Ping**, three attempts are made to ping the IP address, and three results display the following fields:
  - Reply IP address/Device name—The IP address of the device pinged or a device name, if available. The name of the device, if assigned as a Network Object, may be displayed, even if **NO response** is the result.
  - Response time/timeout (ms)—When the ping is transmitted, a millisecond timer starts with a specified maximum, or timeout value. This is useful for testing the relative response times of different routes or activity levels, for example.

#### Example Ping Output:

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

If the ping fails, the output is as follows:

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
```

```
????
```

```
Success rate is 0 percent (0/5)
```

- Ping—Sends an ICMP *echo* request packet from the specified or default interface to the specified IP address and starts the response timer.
- Clear Screen—Clears the output on the screen from previous ping command attempts.

### Modes

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

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

## Traceroute

The Traceroute dialog box provides a useful tool to determine the route packets will take to their destination.

### Traceroute Output

The traceroute tool prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following are the output symbols printed by the traceroute tool:

Output Symbol	Description
*	No response was received for the probe within the timeout period.
<i>nn msec</i>	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachable.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

### Fields

- Hostname or IP address—Specifies the hostname of the host to which the route is traced. If the hostname is specified, define it with **Configuration > Global Objects/Groups**, or configure a DNS server to enable traceroute to resolve the hostname to an IP address.
- Timeout—Specifies the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
- Port—Specifies the destination port used by the UDP probe messages. The default is 33434.
- Probe—Specifies the number of probes to be sent at each TTL level. The default count is 3.
- Min & Max TTL—Specifies the minimum and maximum time to live values for the first probes. The minimum default is one, but it can be set to a higher value to suppress the display of known hops. The maximum default is 30. The tool terminates when the traceroute packet reaches the destination or when the maximum value is reached.
- Destination Port—Specifies the destination port used by the UDP probe messages. The default is 33434.
- Specify Source Interface or IP Address—Specifies the source interface or IP address for the packet trace. This IP address must be the IP address of one of the interfaces. In transparent mode, it must be the management IP address of the security appliance.
- Reverse Resolve—When checked, the output displays the names of hops encountered if name resolution is configured. If left unchecked, the output displays IP addresses.
- Use ICMP—Specifies the use of ICMP probe packets instead of UDP probe packets.

- Traceroute Output—Displays detailed messages about the traceroute.
- Traceroute—Starts the traceroute.
- Clear—Clears all fields.

### Modes

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

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

## File Management

Lets you view, move, copy and delete files stored on Flash memory. You can also create a directory in Flash memory.

In multiple context mode, this tool is only available in the system.

### Fields

- Folders—Displays the folders available in disk.
  - Flash Space—Shows the size of Flash and how much is available.
  - Total—Shows the total size of Flash memory.
  - Available—Shows how much memory is available.
- Files—Displays information about the files in the selected folder.
  - Path—Shows the selected path
  - Filename
  - Size (bytes)
  - Time Modified
  - Status
- View—Displays the selected file in your browser.
- Cut—Cuts the selected file for pasting to another directory.
- Copy—Copies the selected file for pasting to another directory.
- Paste—Pastes the copied file to the selected destination.
- Delete—Deletes the selected file from Flash.
- Rename—Lets you rename the file.
- New Directory—Creates a new directory for storing files.
- File Transfer—Opens the [File Transfer](#) dialog box.

### Modes

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

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

## Upload Image from Local PC

The Upload Image from Local PC dialog box lets you choose a security appliance image file, ASDM image, or other images on your PC, and upload it to Flash memory.

### Fields

- Image to upload—Select which image type to upload.
- Local File Path—Enter the path to the file on your PC.
  - Browse Local—Select to browse to the file on your PC.
- Flash File System Path—Enter the path to copy the file in Flash memory.
  - Browse Local—Select to browse to the directory or file in Flash memory.

### Modes

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

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

## File Transfer

File Transfer lets you copy files to and from your security appliance using HTTPS, TFTP, FTP or by browsing for a local image.

### Fields

- Source File—Select the source file to be transferred.
  - Remote Server—Select to transfer a file from a remote server.
    - Path—Enter the path to the location of the file, including the IP address of the server.
    - Port/Type—Enter the port number or type (if FTP) of the remote server. Valid FTP types are:
      - ap—ASCII files in passive mode.
      - an—ASCII files in non-passive mode.
      - ip—Binary image files in passive mode.
      - in—Binary image files in non-passive mode.
  - Flash File System—Select to copy the file from Flash memory.
    - Path—Enter the path to the location of the file.

- Browse Flash—Select to browse to the file location on your security appliance where the file will be copied from.
  - Local Computer—Select to copy the file from the local PC.
    - Path—Enter the path to the location of the file.
    - Browse Localhost—Browses the local PC for the file to be transferred.
- Destination File—Select the destination file to be transferred. Depending on the source destination, the Flash File System or the Remote Server will automatically be selected.
  - Flash File System—Transfers the file to Flash memory.
    - Path—Enter the path to the location of the file.
    - Browse Flash—Select to browse to the file location on your security appliance where the file will be transferred.
  - Remote Server—Transfers a file to a remote server.
    - Path—Enter the path to the location of the file.
    - Type—For FTP transfers, enter the type. Valid types are:
      - ap—ASCII files in passive mode.
      - an—ASCII files in non-passive mode.
      - ip—Binary image files in passive mode.
      - in—Binary image files in non-passive mode.
- Transfer File—Starts the file transfer.

### Modes

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

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

### Upload ASDM Assistant Guide

Upload ASDM Assistant Guide lets you upload an XML file to flash that contains useful ASDM procedural help about certain tasks. You can obtain these files from Cisco.com. Once loaded the files are available in the Search field in the File Menu.

### Fields

- File to upload—The name of the XML file located on your computer, typically obtained from Cisco.com
- Flash File System Path—The path in the Flash memory where the XML file is loaded.
- Upload File—Starts the upload.

### Modes

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

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

## System Reload

System Reload lets you restart the system and reload the saved configuration into memory. The System Reload dialog box lets you choose when the system should be reloaded, whether you should save the running configuration to Flash memory, and send a message to connected users at reload.

### Fields

- Reload Scheduling—Lets you configure when the reload will take place.
  - Configuration State—Select whether to save the running configuration or not at reload.
    - Save the Running Configuration at Time of Reload—Select to save the running configuration at reload.
    - Reload Without Saving the Running Configuration—Select to discard configuration changes to the running configuration at reload.
- Reload Start Time—Lets you select the time of the reload.
  - Now—Select to perform an immediate reload.
  - Delay by—Lets you delay the reload by a select amount of time. Enter the time to elapse before the reload in hours and minutes or minutes.
  - Schedule at—Lets you schedule the reload to take place at a specific time and date. Enter the time of day the reload is to take place, and select the date of the scheduled reload.
- Reload Message—Enter a message to be sent to open instances of ASDM at reload.
- On Reload Failure Force Immediate Reload after—If the reload fails, the amount of time elapsed in hours and minutes or minutes before a reload is attempted again.
- Schedule Reload—Schedules the reload as configured.
- Reload Status—Displays the status of the reload.
- Cancel Reload—Cancels the scheduled reload.
- Refresh—Refreshes the Reload Status display.
- Details—Displays the details of the scheduled reload.

### Modes

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

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

## Wizards Menu

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

- **Startup Wizard**—The ASDM Startup Wizard walks you, step by step, through the initial configuration of your security appliance. As you click through the configuration screens, you will be prompted to enter information about your security appliance. The Startup Wizard will apply these settings, so you should be able to start using your security appliance right away.
- **VPN Wizard**—The VPN Wizard is a simple way to get a VPN policy configured on your security appliance.
- **High Availability and Scalability Wizard**—Use this wizard to get failover configured on your security appliance.

## Help Menu

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

- **Help Topics**—Opens a new browser window with help arranged by contents, screen name, and indexed in the left frame. Use these to find help for any topic, or search using the Search tab above.
- **Help for Current Screen**—Opens context sensitive help about the screen, panel 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 *Release Notes for Cisco ASDM* on the web. The Release Notes contain the latest information about ASDM software and hardware requirements, and the latest information about changes in the software.
- **Getting Started**—Brings up the Getting Started help topic to help you get started using ASDM.
- **Glossary**—Contains definitions of terms and acronyms.
- **Feature Matrix**—Opens the most current version of the *Release Notes for Cisco ASDM* on the web, which includes the latest licensing information.
- **Feature Search**—Lets you search for a function in ASDM. The Search feature looks through the titles of each panel and presents you with a list of matches, and gives you a hyperlink directly to that panel. If you need to switch quickly between two different panels you found in Search, use the Back and Forward buttons. You can also click the Search icon on the ASDM [Toolbar](#).
- **How do I?**—Opens the ASDM Assistant, which lets you search downloadable content with from Cisco.com, with details about performing certain tasks.
- **Legend**—Provides a list of icons found in ASDM and explains what they represent.
- **About Cisco Platform**—Displays an extensive list of information about the security appliance, including software versions, hardware sets, configuration file loaded at startup, and software image loaded at startup. This information is helpful in troubleshooting.
- **About Cisco ASDM 5.2**—Displays information about ASDM such as the ASDM software version, hostname, privilege level, operating system, browser type, and Java version.

## Toolbar

The Toolbar at the top of the ASDM window, below the menus, provides access to the home page, configuration pages, and monitoring pages. 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 the up arrow to restore the context drop-down list. When expanded, click the left arrow to collapse the pane all the way left, and the right arrow to restore the pane. To manage the system, select System from the list. To manage a context, select the context from the list.
- **Home**—Displays the Home page, which lets you view at a glance important information about your security appliance such as the status of your interfaces, the version you are running, licensing information, and performance. See [Home Page](#) for more information. In multiple mode, the system does not have a Home page.
- **Configuration**—Configures the security appliance. Choose a feature button in the left-hand pane to configure that feature.
- **Monitoring**—Monitors the security appliance. Choose a feature button in the left-hand pane to monitor that feature.
- **Back**—Takes you back to the last panel of ASDM you visited.
- **Forward**—Takes you forward to the last panel of ASDM you visited.
- **Search**—Lets you search for a function in ASDM. The Search feature looks through the titles of each panel and presents you with a list of matches, and gives you a hyperlink directly to that panel. If you need to switch quickly between two different panels you found in Search, use Back and Forward.
- **Refresh**—Refreshes ASDM with the current running configuration by selecting. This button does not refresh the graphs in any of the monitoring graphs.
- **Save**—Saves the running configuration to the startup configuration. If you have a context that is not write accessible, for example on HTTP, then this button does not save the running configuration.
- **Help**—Shows context-sensitive help for the screen that is currently open.

## Status Bar

The status bar appears at the bottom of the ASDM window. The areas below appear from left to right on the status bar.

- **Status**—Shows the status of the configuration, such as “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**—When you click the icon, ASDM shows a list of commands from your configuration that ASDM did not process. They 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 security appliance. See [Connection to Device](#) for more information.
- **Save to Flash Needed**—Shows that you made configuration changes in ASDM, but that you have not yet saved the running configuration to the startup configuration.
- **Refresh Needed**—Shows that you need to refresh the configuration from the security appliance to ASDM because the configuration changed on the security appliance. For example, you made a change to the configuration at 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 security appliance.

## Connection to Device

ASDM maintains a constant connection to the security appliance to maintain up-to-date monitoring and home page data. This dialog box shows the status of this connection. When you make a configuration change, ASDM opens a second connection for the duration of the configuration, and then closes it. That connection is not represented by this dialog box.

## Buttons That Appear on Many Panels

These buttons appear on many ASDM panels:

- **Apply**—Sends changes made in ASDM to the security appliance and applies them to the running configuration. Click **Save** to write a copy of the running configuration to Flash memory. Use the File menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby unit.
- **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After Reset, use Refresh to make sure that information from the current running configuration is displayed.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Displays help for the selected panel.

## About the Help Window

This section contains the following topics:

- [Header Buttons](#)
- [Notes](#)

## Header Buttons

Use the header buttons to navigate through the help to find the topic you are looking for.

- **About ASDM**—Displays information about ASDM.
- **Search**—Lets you search the help topics.
- **Using Help**—Describes the best way to get the most out of online help.
- **Glossary**—Lists a glossary of terms found in ASDM and networking.

**Left-Pane Tabs**—Help navigate the online help.

- **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.

## Notes

When help is invoked in applet mode and if there is any help page already open, the new help page will appear in the same browser window. If there is no help page already open, then the help page will appear in a new browser window.

When help is invoked in application mode and if Netscape is the default browser, each time help is invoked the help page will appear in a new browser window. If IE is the default browser, based on the user setting, the help page may appear either in the last visited browser window or in a new browser window. This behavior of IE can be controlled by using the option Tools > Internet Options > Advanced > Reuse window for launching shortcuts.

## Home Page

The ASDM home pane lets you view, at a glance, important information about your security appliance. If you have an SSM installed in your security appliance, an additional tab appears on the home page. The additional tab displays status information about the software on the SSM.

For more information about configuring these areas, see the following:

- [Home](#)
- [Home > Content Security Tab](#)

### Modes

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

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

## Home

The ASDM home pane lets you view, at a glance, important information about your security appliance, such as the status of your interfaces, the version you are running, licensing information, and performance.

Many of the details available on the ASDM home page are available elsewhere in ASDM, but this is a useful and quick way to see how your security appliance is running. Status information on the Home pane is updated every ten seconds.

### Fields

- Device Information—Includes two tabs to show device information.
  - General—Shows the following information:
    - Host Name—*Display only*. Shows the security appliance hostname. See [Device](#) to set the hostname.

*Platform Version—Display only.* Shows the security appliance software version.

*Device Uptime—Display only.* Shows how long the security appliance has been running.

*ASDM Version—Display only.* Shows the ASDM version.

*Device Type—Display only.* Shows the security appliance model.

*Firewall Mode—Display only.* Shows the firewall mode, either Routed or Transparent. See [Firewall Mode Overview](#) for more information.

*Context Mode—Display only.* Shows the context mode, either Single or Multiple. See [Security Context Overview](#) for more information.

*Total Flash—Display only.* Shows the total amount of Flash memory (the internal Flash memory plus the external Flash memory card, if available) in MB.

*Total Memory—Display only.* Shows the total RAM.

- *License—Display only.* Shows the level of support for licensed features on the security appliance.
- *VPN Status—Routed, single mode only.* Shows the following information:
  - *IKE Tunnels—Display only.* Shows the number of connected IKE tunnels.
  - *IPSec Tunnels—Display only.* Shows the number of connected IPSec tunnels.
- *System Resources Status—Shows the following CPU and memory usage statistics:*
  - *CPU—Display only.* Shows the current percentage of CPU being utilized.
  - *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 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.
  - *Current Kbps—Display only.* Shows the current number of kilobits per second 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 over the last 5 minutes. This graph also shows the current number of connections by type, UDP, TCP, and 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 security appliance.
  - Stop Message Display—Stops logging to ASDM.
  - Resume Message Display—Resumes logging to ASDM.

### Modes

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

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

## Home > Content Security Tab

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

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



### Note

If you have not completed the Setup Wizard in Configuration > Trend Micro Content Security > CSC Setup, you cannot access the panels under Home > Content Security. Instead, a dialog box appears and lets you access the Setup Wizard directly from Home > Content Security.

### Fields

- Device Information—Shows the following information:
  - Model—Shows the type of SSM installed in your security appliance.
  - Mgmt IP—Shows the IP address of the management interface for the CSC SSM.
  - Version—Shows the CSC SSM software version.
  - Last Update—Shows the date of the last software update obtained from Trend Micro.
  - Daily Node #—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—Shows license status for basic features of the CSC SSM, such as anti-virus, anti-spyware, and FTP file blocking features. The date that the license is due to expire appears. If the license has expired, the date of expiry appears. If no license is configured, the field shows Not Available.
  - Plus License—Shows license status for advanced features of the CSC SSM, such as anti-spam, anti-phishing, email content filtering, and URL blocking and filtering features. The date that the license is due to expire appears. If the license has expired, the date of expiry appears. If no license is configured, the field shows Not Available.
  - Licensed Nodes—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—Shows the current percentage of CPU being utilized.
  - CSC SSM CPU Usage (percent)—Shows the CPU usage for the last five minutes.
  - Memory—Shows the current amount of memory being used in MB.
  - CSC SSM Memory Usage (MB)—Shows the memory usage for the last five minutes in MB.
- Threat Summary—Shows aggregate data about threats detected by the CSC SSM.
  - Threat Type—Lists four threat types: Virus, Spyware, URL Filtered, and URL Blocked.
  - Today—Shows the number of threats detected for each threat type within the past 24 hours.
  - Last 7 Days—Shows the number of threats detected for each threat type within the past 7 days.
  - Last 30 Days—Shows the number of threats detected for each threat type within the past 30 days.
- Email Scan—Shows graphs for emails scanned and email virus and spyware detected.
  - Email Scanned Count—Shows the number of emails scanned, as separate graphs by email protocol (SMTP or POP3) and as a combined graph for both supported email protocols. The graphs display data in ten-second intervals.
  - Email Virus and Spyware—Shows the number of viruses and emails detected in email 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, security event messages received from the CSC SSM.
  - Time—Displays the time an event occurred.
  - Source—Displays the IP address or hostname from which the threat came.
  - Threat/Filter—Displays the type of threat or, in the case of a URL filter event, the filter that triggered the event.
  - Subject/File/URL—Displays the subject of emails containing a threat, the names of FTP file containing a threat, or URLs blocked or filtered.
  - Receiver/Host—Displays the recipient of emails containing a threat or the IP address or hostname of a node threatened.
  - Sender—Displays the sender of emails containing a threat.
  - Content Action—Displays the action taken upon the content of the message or file, such as delivering the content unaltered, deleting attachments, or cleaning attachments before delivering them.
  - Msg Action—Displays the action taken upon 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
•	•	•	•	—

