

Defining Preferences and Using Configuration, Diagnostic, and File Management Tools

This chapter describes the preferences and tools available for configuration, problem diagnosis, and file management, and includes the following sections:

- [Preferences, page 3-1](#)
- [Configuration Tools, page 3-3](#)
- [Diagnostic Tools, page 3-7](#)
- [File Management Tools, page 3-18](#)

Preferences

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

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

-
- Step 1** In the main ASDM application window, choose **Tools > Preferences**.
- The Preferences dialog box appears, with three tabs: General, Rules Table, and Syslog.
- Step 2** Click one of these tabs to define your settings: the **General** tab to specify general preferences; the **Rules Tables** tab to specify preferences for the Rules table; and the **Syslog** tab to specify the appearance of syslog messages displayed in the Home pane and to enable the display of a warning message for NetFlow-related syslog messages.
- Step 3** On the General tab, specify the following:
- a. Check the **Preview commands before sending them to the device** check box to view CLI commands generated by ASDM.
 - b. Check the **Enable cumulative (batch) CLI delivery** check box to send multiple commands in a single group to the adaptive security appliance.
 - c. Check the **Warn that configuration in ASDM is out of sync with the configuration in ASA** check box to be notified when the startup configuration and the running configuration are no longer in sync with each other.
 - d. Check the **Confirm before exiting ASDM** check box to display a prompt when you try to close ASDM to confirm that you want to exit. This option is checked by default.
 - e. Check the **Show configuration restriction message to read-only user** check box to display the following message to a read-only user at startup. This option is checked by default.

"You are not allowed to modify the ASA configuration, because you do not have sufficient privileges."

- f. Check the **Enable screen reader support (requires ASDM restart)** check box to enable screen readers to work. You must restart ASDM to enable this option.
- g. To allow the Packet Capture Wizard to display captured packets, enter the name of the network sniffer application or click **Browse** to find it.

Step 4 On the Rules Tables tab, specify the following:

- a. Display settings let you change the way rules are displayed in the Rules table.
 - Check the **Auto-expand network and service object groups with specified prefix** check box to display the network and service object groups automatically expanded based on the Auto-Expand Prefix setting.
 - In the Auto-Expand Prefix field, specify the prefix of the network and service object groups to expand automatically when displayed.
 - Check the **Show members of network and service object groups** check box to display members of network and service object groups and the group name in the Rules table. If the check box is not checked, only the group name is displayed.
 - In the Limit Members To field, enter the number of network and service object groups to display. When the object group members are displayed, then only the first *n* members are displayed.
 - Check the **Show all actions for service policy rules** check box to display all actions in the Rules table. When unchecked, a summary appears.
- b. Deployment settings let you configure the behavior of the security appliance when deploying changes to the Rules table.
 - Check the **Issue "clear xlate" command when deploying access lists** check box to clear the NAT table when deploying new access lists. This setting ensures the access lists that are configured on the security appliance are applied to all translated addresses.
- c. Access Rule Hit Count Settings let you configure the frequency for which the hit counts are updated in the Access Rules table. Hit counts are applicable for explicit rules only. No hit count will be displayed for implicit rules in the Access Rules table.
 - Check the **Update access rule hit counts automatically** check box to have the hit counts automatically updated in the Access Rules table.
 - In the Update Frequency field, specify the frequency in seconds in which the hit count column is updated in the Access Rules table. Valid values are 10 - 86400 seconds.

Step 5 On the Syslog tab, specify the following:

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

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

**Note**

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

Modes

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

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

Configuration Tools

This section includes the following topics:

- [Reset Device to the Factory Default Configuration, page 3-3](#)
- [Save Running Configuration to TFTP Server, page 3-4](#)
- [Save Internal Log Buffer to Flash, page 3-5](#)
- [Command Line Interface, page 3-5](#)
- [Show Commands Ignored by ASDM on Device, page 3-6](#)

Reset Device to the Factory Default Configuration

The default configuration provides the minimum commands required to connect to the adaptive security appliance using ASDM.

**Note**

This feature is available only for routed firewall mode; transparent mode does not support IP addresses for interfaces. In addition, this feature is available only in single context mode; a security appliance with a cleared configuration does not have any defined contexts to configure automatically using this feature.

To reset the adaptive security appliance to the factory default configuration, perform the following steps:

Step 1 In the main ASDM application window, choose **File > Reset Device to the Factory Default Configuration**.

The Reset Device to the Default Configuration dialog box appears.

- Step 2** Enter the Management IP address of the management interface, instead of using the default address, 192.168.1.1. For an adaptive security appliance with a dedicated management interface, the interface is called “Management0/0.” For other adaptive security appliances, the configured interface is Ethernet 1 and called “inside.”
- Step 3** Choose the Management (or Inside) Subnet Mask from the drop-down list.
- Step 4** To save this configuration to internal flash memory, choose **File > Save Running Configuration to Flash**.

Selecting this option saves the running configuration to the default location for the startup configuration, even if you have previously configured a different location for the [System Time](#). When the configuration was cleared, this path was also cleared. The next time you reload the adaptive security appliance after restoring the factory configuration, the device boots from the first image in internal flash memory. If an image in internal flash memory does not exist, the adaptive security appliance does not boot.

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 feature stores a copy of the current running configuration file on a TFTP server.

To save the running configuration to a TFTP server, perform the following steps:

- Step 1** In the main ASDM application window, choose **File > Save Running Configuration to TFTP Server**. The Save Running Configuration to TFTP Server dialog box appears.
- Step 2** Enter the TFTP server IP address and file path on the TFTP server in which the configuration file will be saved, and then click **Save Configuration**.



Note To configure default TFTP settings, choose **Configuration > Device Management > Management Access > File Access > TFTP Client**. After you have configured this setting, the TFTP server IP address and file path on the TFTP server appear automatically in this 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
•	•	•	•	•

Save Internal Log Buffer to Flash

This feature lets you save the internal log buffer to flash memory.

To save the internal log buffer to flash memory, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **File > Save Internal Log Buffer to Flash**.
The Enter Log File Name dialog box appears.
 - Step 2** Choose the first option to save the log buffer with the default filename, LOG-YYYY-MM-DD-hhmmss.txt.
 - Step 3** Choose the second option to specify a filename for the log buffer.
 - Step 4** Enter the filename for the log buffer, and then click **OK**.
-

Command Line Interface

This feature provides a text-based tool for sending commands to the adaptive security appliance and viewing the results.

The commands you can enter with the CLI tool depend on your user privileges. See the section, [About Authorization](#) for more information. Review your privilege level in the status bar at the bottom of the main ASDM application window to ensure that you have the required privileges to execute privileged-level CLI commands.



Note

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

To use the CLI tool, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Command Line Interface**.
The Command Line Interface dialog box appears.
 - Step 2** Choose the type of command (single line or multiple line) that you want, and then choose the command from the drop-down list, or type it in the field provided.
 - Step 3** Click **Send** to execute the command.
 - Step 4** To enter a new command, click **Clear Response**, and then choose (or type) another command to execute.
 - Step 5** Check the **Enable context-sensitive help (?)** check box to provide context-sensitive help for this feature. Uncheck this check box to disable the context-sensitive help.

- Step 6** After you have closed the Command Line Interface dialog box, if you changed the configuration, click **Refresh** to view the changes in ASDM.

Modes

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

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

Command Errors

If an error occurs because you entered an incorrect command, the incorrect command is skipped and the remaining commands are processed. A message displays in the Response area to inform you whether any error occurred, as well as other related information.



Note

ASDM supports almost all CLI commands. See the *Cisco Security Appliance Command Reference* for a list of commands.

Interactive Commands

Interactive commands are not supported in the CLI tool. To use these commands in ASDM, use the **noconfirm** keyword if available, as shown in the following command:

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

Avoiding Conflicts with Other Administrators

Multiple administrative users can update the running configuration of the adaptive security appliance. Before using the ASDM CLI tool to make configuration changes, check for other active administrative sessions. If more than one user is configuring the adaptive security appliance at the same time, the most recent changes take effect.

To view other administrative sessions that are currently active on the same adaptive security appliance, choose **Monitoring > Properties > Device Access**.

Show Commands Ignored by ASDM on Device

This feature lets you show the list of commands that ASDM does not support. Typically, ASDM ignores them. ASDM does not change or remove these commands from your running configuration. See [Unsupported Commands](#) for more information.

To display the list of unsupported commands for ASDM, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Show Commands Ignored by ASDM on Device**.
- Step 2** Click **OK** when you are done.
-

Modes

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

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

Diagnostic Tools

ASDM provides a set of diagnostic tools to help you in troubleshooting problems. This section includes the following topics:

- [Packet Tracer, page 3-7](#)
- [Ping, page 3-8](#)
- [Traceroute, page 3-11](#)
- [Administrator's Alert to Clientless SSL VPN Users, page 3-12](#)
- [ASDM Java Console, page 3-13](#)
- [Packet Capture Wizard, page 3-13](#)

Packet Tracer

The packet tracer tool provides packet tracing for packet sniffing and network fault isolation, as well as detailed information about the packets and how they are processed by the adaptive security appliance. If a configuration command 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, the following message is displayed:

```
"packet dropped due to bad ip header (reason)."
```

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

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

To open the packet tracer, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > Packet Tracer**.
The Cisco ASDM Packet Tracer dialog box appears.
- Step 2** Choose the source interface for the packet trace from the drop-down list.
- Step 3** Specify the protocol type for the packet trace. Available protocol types are ICMP, IP, TCP, and UDP.
- Step 4** Enter the source address for the packet trace in the Source IP Address field.
- Step 5** Choose the source port for the packet trace from the drop-down list.
- Step 6** Enter the destination IP address for the packet trace in the Destination IP Address field.
- Step 7** Choose the destination port for the packet trace from the drop-down list.
- Step 8** Click **Start** to trace the packet.
The Information Display Area shows detailed messages about the packet trace.



Note To display a graphical representation of the packet trace, check the **Show animation** check box.

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 tool is useful for verifying the configuration and operation of the adaptive security appliance and surrounding communications links, as well as for testing other network devices.

A ping is sent to an IP address and it returns a reply. This process enables network devices to discover, identify, and test each other.

The Ping tool uses ICMP (as described in RFC-777 and RFC-792) to define an echo request and reply transaction between two network devices. 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.

To use the Ping tool, perform the following steps:

Step 1 In the main ASDM application window, choose **Tools > Ping**.

The Ping dialog box appears.

Step 2 Enter the destination IP address for the ICMP echo request packets in the IP Address field.



Note If a hostname has been assigned in the Configuration > Firewall > Objects > IP Names pane, you can use the hostname in place of the IP address.

Step 3 (Optional) Choose the security appliance interface that transmits the echo request packets from the drop-down list. If it is not specified, the security appliance checks the routing table to find the destination address and uses the required interface.

Step 4 Click **Ping** to send an ICMP echo request packet from the specified or default interface to the specified IP address and start the response timer.

The response appears in the Ping Output area. Three attempts are made to ping the IP address, and results display the following fields:

- The IP address of the device pinged or a device name, if available. The name of the device, if assigned Hosts/Networks, may be displayed, even if **NO response** is the result.
- When the ping is transmitted, a millisecond timer starts with a specified maximum, or timeout value. This timer is useful for testing the relative response times of different routes or activity levels.
- 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)
```

Step 5 To enter a new IP address, click **Clear Screen** to remove the previous response from the Ping output area.

Modes

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

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

Using the Ping Tool

Administrators can use the ASDM Ping interactive diagnostic tool in these ways:

- 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—The Ping tool can ping an interface on another security appliance 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 an adaptive security appliance interface to a network device that is suspected to be functioning incorrectly. If the interface is configured correctly and an echo is not received, there may be problems with the device.
- Pinging to test intermediate communications—A ping may be initiated from an adaptive security appliance interface to a network device that is known to be functioning correctly and returning echo requests. If the echo is received, the correct 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 an adaptive security appliance, and not necessarily because of no response from the IP address being pinged. Before using the Ping tool to ping from, to, or through an adaptive security appliance interface, perform the following basic checks:

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

Pinging from a Security Appliance Interface

For basic testing of an interface, you can initiate a ping from an adaptive security appliance interface to a network device that you know is functioning correctly and returning replies via the intermediate communications path. For basic testing, make sure you do the following:

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

Pinging to a Security Appliance Interface

When you try to ping to an adaptive security appliance interface, verify that the pinging response (ICMP echo reply) is enabled for that interface by choosing **Tools > Ping**. When pinging is disabled, the adaptive 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

To verify that other types of network traffic from “known good” sources is being passed through the adaptive security appliance, choose **Monitoring > Interfaces > Interface Graphs** or an SNMP management station.

To enable internal hosts to ping external hosts, configure ICMP access correctly for both the inside and outside interfaces by choosing **Configuration > Firewall > Objects > IP Names**.

Traceroute

The Traceroute tool helps you to determine the route that packets will take to their destination. The tool prints the result of each probe sent. Every line of output corresponds to a TTL value in increasing order. The following table lists the output symbols printed by this tool.

Output Symbol	Description
*	No response was received for the probe within the timeout period.
nn msec	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 unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

To use the Traceroute tool, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Traceroute**.
The Traceroute dialog box appears.
- Step 2** Enter the name of the host to which the route is traced. If the hostname is specified, define it by choosing **Configuration > Firewall > Objects > IP Names**, or configure a DNS server to enable this tool to resolve the hostname to an IP address.
- Step 3** Enter the amount of time in seconds to wait for a response before the connection times out. The default is three seconds.
- Step 4** Type the destination port used by the UDP probe messages. The default is 33434.
- Step 5** Enter the number of probes to be sent at each TTL level. The default is three.

- Step 6** Specify the minimum and maximum TTL 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 traceroute terminates when the packet reaches the destination or when the maximum value is reached.
- Step 7** Check the **Specify source interface or IP address** check box. Choose the source interface or IP address for the packet trace from the drop-down list. 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 adaptive security appliance.
- Step 8** Check the **Reverse Resolve** check box to have the output display the names of hops encountered if name resolution is configured. Leave this check box unchecked to have the output display IP addresses.
- Step 9** Check the **Use ICMP** check box to specify the use of ICMP probe packets instead of UDP probe packets.
- Step 10** Click **Trace Route** to start the traceroute.
The Traceroute Output area displays detailed messages about the traceroute results.
- Step 11** Click **Clear Output** to start a new traceroute.

Modes

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

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

Administrator's Alert to Clientless SSL VPN Users

This feature lets you send an alert message to clientless SSL VPN users (for example, about connection status).

To send an alert message, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Administrator's Alert Message to Clientless SSL VPN Users**.
The Administrator's Alert Message to Clientless SSL VPN Users dialog box appears.
- Step 2** Enter the new or edited alert content that you want to send, and then click **Post Alert**.
- Step 3** To remove current alert content and enter new alert content, click **Cancel Alert**.

Modes

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

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

ASDM Java Console

You can use the ASDM Java console to view and copy logged entries in a text format, which can help you troubleshoot ASDM errors. To access this tool, in the main ASDM application window, choose **Tools > ASDM Java Console**.

To show the virtual machine memory statistics, enter **m** in the console.

To perform garbage collection, enter **g** in the console.

To monitor memory usage, open the Windows Task Manager and double-click the **asdm_launcher.exe** file.



Note

The maximum memory allocation allowed is 256 MB.

Modes

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

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

Packet Capture Wizard

You can use the Packet Capture Wizard to configure and run captures for troubleshooting errors. The captures can use access lists to limit the type of traffic captured, the source and destination addresses and ports, and one or more interfaces. The wizard runs one capture on each of the ingress and egress interfaces. You can save the captures on your PC to examine them in a packet analyzer.



Note

This tool does not support clientless SSL VPN capture.


To configure and run captures, perform the following steps:

- Step 1** In the main ASDM application window, choose **Wizards > Packet Capture Wizard**.
The Overview of Packet Capture screen appears, with a list of the tasks that the wizard will guide you through to complete.
- Step 2** Click **Next** to display the Ingress Traffic Selector screen.

- Step 3** Choose the ingress interface (inside or outside) from the drop-down list.
- Step 4** Enter the source host IP address and choose the network IP address from the drop-down list.
- Step 5** Choose the protocol from the drop-down list.
- Step 6** Depending on the selected protocol, you also need to define both the source port services and destination port services. Choose one of the following options:
- All Services
 - Service group, which you choose from the drop-down list
 - Service, which you choose according to a set of predefined parameters
- Step 7** Click **Next** to display the Egress Traffic Selector screen.
- Step 8** Choose the egress interface from the drop-down list.
- Step 9** Enter the source host IP address and choose the network IP address from the drop-down list.



Note The source port services and destination port services are read-only based on the choices you made in the Ingress Traffic Selector screen.

- Step 10** Click **Next** to display the Buffers screen. The buffer size is the maximum amount of memory that the capture can use to store packets. The packet size is the longest packet that the capture can hold. We recommend that you use the longest packet size to capture as much information as possible.
- Step 11** Enter the packet size. The valid size ranges from 14 - 1522 bytes.
- Step 12** Enter the buffer size. The valid size ranges from 1534 - 33554432 bytes.
- Step 13** Check the **Use circular buffer** check box to store captured packets.
- 
-
- Note** When you choose this setting, if all the buffer storage is used, the capture will start overwriting the oldest packets.
-
- Step 14** Click **Next** to display the Summary screen, which shows the traffic selectors and buffer parameters that you have entered.
- Step 15** Click **Next** to display the Run Capture screen, and then click **Start** to begin capturing packets. Click **Stop** to end the capture.
- Step 16** Click **Get Capture Buffer** to determine how much buffer space you have remaining. Click **Clear Buffer on Device** to remove the current content and allow room in the buffer to capture more packets.
- Step 17** Click **Save captures** to display the Save Capture dialog box. Select the format in which you want to include the captures: **ASCII** or **PCAP**. You have the option of saving either the ingress capture, the egress capture, or both.
- Step 18** To save the ingress packet capture, click **Save Ingress Capture** to display the Save capture file dialog box. Specify the storage location on your PC, and click **Save**.
- Step 19** To save the egress packet capture, click **Save Egress Capture** to display the Save capture file dialog box. Specify the storage location on your PC, and click **Save**.
- Step 20** Click **Close**, and then click **Finish** to exit the wizard.
-

Modes

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

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

Field Information for the Packet Capture Wizard

This section includes the following topics:

- [Ingress Traffic Selector, page 3-15](#)
- [Egress Traffic Selector, page 3-16](#)
- [Buffers, page 3-16](#)
- [Summary, page 3-17](#)
- [Run Captures, page 3-17](#)
- [Save Captures, page 3-18](#)

Ingress Traffic Selector

The Ingress Traffic Selector dialog box lets you configure the ingress interface, source and destination hosts/networks, and the protocol for packet capture.

Fields

- Ingress Interface—Specifies the ingress interface name.
- Source Host/Network—Specifies the ingress source host and network.
- Destination Host/Network—Specifies the ingress destination host and network.
- Protocol—Specifies the protocol type to capture (ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp, or udp).
 - ICMP type—Specifies the ICMP type for ICMP protocol only (all, alternate address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute, or unreachable).
 - Source/Destination Port Services—Specifies source and destination port services for TCP and UDP protocols only.
 - All Services—Specifies all services.
 - Service Group—Specifies a service group.
 - Service—Specifies a service (aol, bgp, chargen, cifx, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nntp, panywhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp, or whois).

Modes

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

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

Egress Traffic Selector

The Egress Traffic Selector dialog box lets you configure the egress interface, source and destination hosts/networks, and source and destination port services for packet capture.

Fields

- Egress Interface—Specifies the egress interface name.
- Source Host/Network—Specifies the egress source host and network.
- Destination Host/Network—Specifies the egress destination hose and network.
- Protocol—Specifies the protocol type selected during the ingress configuration.

Modes

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

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

Buffers

The Buffers dialog box lets you configure the packet size, buffer size, and whether to use the circular buffer for packet capture.

Fields

- Packet Size—Specifies longest packet that the capture can hold. Use the longest size available to capture as much information as possible.
- Buffer Size—Specifies the maximum amount of memory that the capture can use to store packets.
- Use circular buffer—Specifies whether to use the circular buffer to store packets. When the circular buffer has used all of the buffer storage, the capture will write over the oldest packets first.

Modes

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

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

Summary

The Summary dialog box shows the traffic selectors and the buffer parameters for the packet capture.

Fields

- Traffic Selectors—Shows the capture and access list configuration specified in the previous steps.
- Buffer Parameters—Shows the buffer parameters specified in the previous step.

Modes

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

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

Run Captures

The Run Captures dialog box lets you start and stop the capture session. You can also view the capture buffer, launch a network analyzer application, save the packet captures, and clear the buffer.

Fields

- Start—Starts the packet capture session on selected interfaces.
- Stop—Stops the packet capture session on selected interfaces.
- Get Capture Buffer—Specifies to show a snapshot of the captured packets on the interface.
- Ingress—Shows the capture buffer on the ingress interface.
 - Launch Network Sniffer Application—Launches the packet analysis application specified in Tools > Preferences for analyzing the ingress capture.
- Egress—Shows the capture buffer on the egress interface.
 - Launch Network Sniffer Application—Launches the packet analysis application specified in Tools > Preferences for analyzing the egress capture.
- Save Captures—Lets you save the ingress and egress captures in either ASCII or PCAP format.
- Clear Buffer on Device—Clears the buffer on the device.

Modes

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

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

Save Captures

The Save Captures dialog box lets you save the ingress and egress packet captures to ASCII or PCAP file format for further packet analysis.

Fields

- ASCII—Specifies to save the capture buffer in ASCII format.
- PCAP—Specifies to save the capture buffer in PCAP format.
- Save ingress capture—Lets you specify a file to save the ingress packet capture.
- Save egress capture—Lets you specify a file to save the egress packet capture.

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 Tools

ASDM provides a set of file management tools to help you perform basic file management tasks. This section includes the following topics:

- [File Management, page 3-19](#)
- [Manage Mount Points, page 3-20](#)
- [Add/Edit a CIFS/FTP Mount Point, page 3-20](#)
- [Accessing a CIFS Mount Point, page 3-21](#)
- [Upgrade Software from Local Computer, page 3-22](#)
- [File Transfer, page 3-23](#)
- [Upgrade Software from Cisco.com Wizard, page 3-24](#)
- [ASDM Assistant, page 3-26](#)
- [System Reload, page 3-26](#)
- [Backup and Restore, page 3-27](#)

File Management

The File Management tool lets you view, move, copy, and delete files stored in flash memory, transfer files, and to manage files on remote storage devices (mount points).


Note

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

To use the file management tools, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**.
The File Management dialog box appears.
- The Folders pane displays the available folders on disk.
 - Flash Space shows the total amount of flash memory and how much memory is available.
 - The Files area displays the following information about files in the selected folder:
 - Path
 - Filename
 - Size (bytes)
 - Time Modified
 - Status, which indicates whether a selected file is designated as a boot configuration file, boot image file, ASDM image file, SVC image file, CSD image file, or APCF image file.
- Step 2** Click **View** to display the selected file in your browser.
- Step 3** Click **Cut** to cut the selected file for pasting to another directory.
- Step 4** Click **Copy** to copy the selected file for pasting to another directory.
- Step 5** Click **Paste** to paste the copied file to the selected destination.
- Step 6** Click **Delete** to remove the selected file from flash memory.
- Step 7** Click **Rename** to rename a file.
- Step 8** Click **New Directory** to create a new directory for storing files.
- Step 9** Click **File Transfer** to open the File Transfer dialog box. See [File Transfer, page 3-23](#) for more information.
- Step 10** Click **Mount Points** to open the Manage Mount Points dialog box. See [Manage Mount Points, page 3-20](#) 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
•	•	•	—	•

Manage Mount Points

This feature lets you configure remote storage (mount points) for network file systems using a CIFS or FTP connection. The dialog box lists the mount-point name, connection type, server name or IP address, and the enabled setting (yes or no). You can add, edit, or delete mount points. For more information, see [Add/Edit a CIFS/FTP Mount Point, page 3-20](#). You can access the CIFS mount point after it has been created. For more information, see [Accessing a CIFS Mount Point, page 3-21](#).


Note

On a PIX 535 security appliance in single, routed mode, the Manage Mount Point feature is not available.

Add/Edit a CIFS/FTP Mount Point

To add a CIFS mount point, perform the following steps:

-
- Step 1** Click **Add**, and then choose **CIFS Mount Point**.
The Add CIFS Mount Point dialog box appears.
The Enable mount point check box is automatically checked, which is the default setting.
 - Step 2** Enter the mount-point name, server name or IP address, and share name in the applicable fields.
 - Step 3** In the Authentication section, enter the NT domain, username and password, and then confirm the password.
 - Step 4** Click **OK**.
-

To add an FTP mount point, perform the following steps:

-
- Step 1** Click **Add**, and then choose **FTP Mount Point**.
The Add FTP Mount Point dialog box appears.
The Enable mount point check box is automatically checked, which is the default setting.
 - Step 2** Enter the mount-point name and the server name or IP address in the applicable fields.
 - Step 3** In the FTP Mount Options area, click the **Active Mode** or **Passive Mode** option.
 - Step 4** Enter the path to mount the remote storage.
 - Step 5** In the Authentication area, enter the NT domain, username and password, and then confirm the password.
 - Step 6** Click **OK**.
-

To edit a CIFS mount point, perform the following steps:

-
- Step 1** Choose the CIFS mount-point you want to modify, and click **Edit**.
The Edit CIFS Mount Point dialog box appears.



Note You cannot change the CIFS mount-point name.

Step 2 Make the changes to the remaining settings, and click **OK** when you are done.

To edit an FTP mount point, perform the following steps:

Step 1 Choose the FTP mount-point you want to modify, and click **Edit**.

The Edit FTP Mount Point dialog box appears.



Note You cannot change the FTP mount-point name.

Step 2 Make the changes to the remaining settings, and click **OK** when you are done.

Accessing a CIFS Mount Point

To access a CIFS mount point after it has been created, perform the following steps:

Step 1 Start the security appliance CLI.

Step 2 Create the mount by entering the **mount <name of mount> type cifs** command.

Step 3 Enter the **show run mount** command.

The following output appears:



Note In this example, win2003 is the name of the mount.

```
server kmmwin2003
share sharefolder
username webvpnuser2
password *****
status enable
```

Step 4 Enter the **dir** command to list all enabled mounts as subdirectories, which is similar to mounting a drive on the Windows PC. For example, in the following output, FTP2003:, FTPLINUX:, and win2K: are configured mounts.

The following is sample output from the **dir** command:

```
FTP2003: Directory or file name
FTPLINUX: Directory or file name
WIN2003: Directory or file name
all-filesystems List files on all filesystems
disk0: Directory or file name
disk1: Directory or file name
flash: Directory or file name
system: Directory or file name
win2K: Directory or file name
```

- Step 5** Enter the **dir** command for that mount (for example, **dir WIN2003**), and copy files to and from flash (disk0:) to any of the listed mounts.

The following is sample output from the **dir WIN2003** command.

```
Directory of WIN2003:/
---- 14920928 08:33:36 Apr 03 2009 1_5_0_01-windows-i586-p.exe
---- 33 11:27:16 Jun 07 2007 AArenameIE70
---- 28213021 15:15:22 Apr 03 2009 atest2(3).bin
---- 61946730 12:09:40 Mar 17 2009 atest2.bin
---- 5398366 14:52:10 Jul 28 2008 atest222.bin
---- 2587728 10:07:44 Dec 06 2005 cCITRIXICA32t.exe
---- 1499578 15:26:50 Dec 02 2005 ccore.exe
---- 61946728 11:40:36 Dec 09 2005 CIFSTESTT.bin
---- 2828 13:46:04 May 11 2009 ClientCert.pfx
d--- 16384 14:48:28 Mar 20 2007 cookiefolder
---- 4399 15:58:46 Jan 06 2006 Cookies.plist
---- 2781710 12:35:00 Dec 12 2006 coreftplitel.3.exe
---- 0 10:22:52 Jul 13 2007 coreftplitel.3.exe.download
---- 245760 15:13:38 Dec 21 2005 Dbgview.exe
---- 1408249 11:01:34 Dec 08 2005 expect-5.21r1b1-setup.exe
d--- 16384 14:49:14 Jul 28 2008 folder157
---- 101 09:33:48 Dec 12 2005 FxSasser.log
---- 2307104 09:54:12 Dec 12 2005 ica32t.exe
---- 8732552 10:14:32 Apr 29 2009 iclientSetup_IFen_flex51.exe
d--- 16384 08:32:46 Apr 03 2009 IE8withVistaTitan
---- 15955208 08:34:18 Aug 14 2007 j2re.exe
---- 16781620 13:38:22 Jul 23 2008 jre-1_5_0_06-windows-i586-p.exe
<--- More --->
```

Upgrade Software from Local Computer

The Upgrade Software from Local Computer tool lets you upload an image file from your PC to the flash file system to upgrade the adaptive security appliance.

To upgrade software from your PC, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software from Local Computer dialog box appears.
- Step 2** Choose the image file to upload from the drop-down list.
- Step 3** Enter the local path to the file on your PC or click **Browse Local Files** to find the file on your PC.
- Step 4** Enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 5** Click **Image to Upload**. The uploading process might take a few minutes; make sure you wait until it is finished.

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

The File Transfer tool lets you transfer files from either a local or remote location. You can transfer a local file on your computer or a flash file system to and from the security appliance. You can transfer a remote file to and from the security appliance using HTTP, HTTPS, TFTP, FTP, or SMB.

To transfer files between your local computer and a flash file system, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**.
The File Management dialog box appears.
- Step 2** Click the down arrow next to **File Transfer**, and then click **Between Local PC and Flash**.
The File Transfer dialog box appears.
- Step 3** Select and *drag* the file(s) from either your local computer or the flash file system that you want to upload or download to the desired location. Alternatively, select the file(s) from either your local computer or the flash file system that you want to upload or download, and click the right arrow or left arrow to transfer the file(s) to the desired location.
- Step 4** Click **Close** when you are done.
-

To transfer files between a remote server and a flash file system, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**.
The File Management dialog box appears.
- Step 2** Click the down arrow next to **File Transfer**, and then click **Between Remote Server and Flash**.
The File Transfer dialog box appears.
- Step 3** To transfer a file from a remote server, click the **Remote server** option.
- Step 4** Define the source file to be transferred.
- a. Choose the path to the location of the file, including the IP address of the server.
 - b. Enter the port number or type (if FTP) of the remote server. Valid FTP types are the following:
 - 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
- Step 5** To transfer the file from the flash file system, click the **Flash file system** option.
- Step 6** Enter the path to the location of the file or click **Browse Flash** to find the file location.

- Step 7** In addition, you can copy a file from your startup configuration, running configuration, or an SMB file system through the CLI. For instructions about using the **copy** command, see the *Cisco Security Appliance Command Line Configuration Guide*.
- Step 8** Define the destination of the file to be transferred.
- To transfer the file to the flash file system, choose the **Flash file system** option.
 - Enter the path to the location of the file or click **Browse Flash** to find the file location.
- Step 9** To transfer a file to a remote server, choose the **Remote server** option.
- Enter the path to the location of the file.
 - For FTP transfers, enter the type. Valid types are the following:
 - 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
- Step 10** Click **Transfer** to start the file transfer.
- The Enter Username and Password dialog box appears.
- Step 11** Enter the username, password, and domain (if required) for the remote server.
- Step 12** Click **OK** to continue the file transfer.
- The file transfer process might take a few minutes; make sure that you wait until it is finished.
- Step 13** Click **Close** when the file transfer is finished.

Modes

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

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

Upgrade Software from Cisco.com Wizard

The Upgrade Software from Cisco.com Wizard lets you automatically upgrade the ASDM and adaptive security appliance to more current versions.



Note

This feature is not available in the user or admin context mode in a single security context.

In this wizard, you can do the following:

- Download the list of available releases from Cisco.com.
- Select an ASDM image file or ASA image file for upgrade.
- Upgrade the images you have selected.

- Reload the firewall if you have upgraded the ASA image (optional).

**Note**

You must upgrade incrementally from one version to the next (for example, from Version 6.1 to 6.2, from Version 6.1(3) to 6.1(5), and so on). You cannot upgrade from Version 5.2(3) to 6.1(3).

To upgrade software from Cisco.com, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Cisco.com**.
The Upgrade Software from Cisco.com Wizard appears. The Overview screen describes the steps in the image upgrade process.
- Step 2** Click **Next** to continue.
The Authentication screen appears.
- Step 3** Enter your assigned Cisco.com user name and the Cisco.com password, and then click **Next**.
The Image Selection screen appears.
- Step 4** Choose one or both of the two options listed.
- Check the **Upgrade the ASA version** check box to specify the most current adaptive security appliance image to which you want to upgrade.
 - Check the **Upgrade the ASDM version** check box to specify the most current ASDM version to which you want to upgrade.

**Note**

If the ASA version list or the ASDM version list is empty, a statement appears informing you that no new ASA or ASDM images are available. If you see this statement, you can exit the wizard.

- Step 5** Click **Next** to continue.
The Selected Images screen appears.
- Step 6** Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.
The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.
The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the adaptive security appliance.
If you upgraded the adaptive security appliance version and the upgrade succeeded, an option to save the configuration and reload the adaptive security appliance appears.
- Step 7** Click **Yes**.
For the upgrade versions to take effect, you must save the configuration, reload the adaptive security appliance, and restart ASDM.

**Note**

You do not need to restart the wizard after you have completed one incremental upgrade. You can return to [Step 3](#) of the wizard to upgrade to the next higher version, if any.

- Step 8** Click **Finish** to exit the wizard when the upgrade is finished.

Modes

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

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

ASDM Assistant

The ASDM Assistant tool lets you search and view useful ASDM procedural help about certain tasks.

To access information, choose **View > ASDM Assistant > How Do I?** or enter a search request from the Look For field in the menu bar. From the Find drop-down list, choose **How Do I?** to begin the search.

**Note**

This feature is not available on the PIX security appliance.

To view the ASDM Assistant, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **View > ASDM Assistant**.
The ASDM Assistant pane appears.
- Step 2** In the Search field, enter the information that you want to find, and click **Go**.
The requested information appears in the Search Results pane.
- Step 3** Click any links that appear in the Search Results and Features sections to obtain more details.
-

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

The System Reload tool lets you schedule a system reload or cancel a pending reload.

To schedule a reload, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > System Reload**.

- Step 2** In the Reload Scheduling section, define the following reload scheduling settings:
- For the Configuration State, choose either to save the running configuration at reload time or to discard configuration changes to the running configuration at reload time.
 - For the Reload Start Time, you can select from the following options:
 - Click **Now** to perform an immediate reload.
 - Click **Delay by** to delay the reload by a specified amount of time. Enter the time to elapse before the reload in hours and minutes or only minutes.
 - Click **Schedule at** to schedule the reload to occur at a specific time and date. Enter the time of day the reload is to occur, and select the date of the scheduled reload.
 - In the Reload Message field, enter a message to send to open instances of ASDM at reload time.
 - Check the **On reload failure force immediate reload after** check box to show the amount of time elapsed in hours and minutes or only minutes before a reload is attempted again.
 - Click **Schedule Reload** to schedules the reload as configured.
- Step 3** The Reload Status area displays the status of the reload.
- Click **Cancel Reload** to stop a scheduled reload.
 - Click **Refresh** to refresh the Reload Status display after a scheduled reload is finished.
 - Click **Details** to display the details of a 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
•	•	•	—	•

Backup and Restore

The Backup and Restore features options on the Tools menu let you back up and restore the security appliance configuration, Cisco Secure Desktop image, and SSL VPN Client images and profiles.

ASDM lets you choose the file types to back up, compresses them into a single zip file, then transfers the zip file to the directory you choose on your computer. Similarly, to restore files, you choose the source zip file on your computer and then choose the file types to be restored.

Go to the section that applies:

- [Backing Up Configurations](#)
- [Restoring Configurations](#)

Backing Up Configurations

To back up configurations and images to a .zip file to be transferred to your local computer, perform the following steps:

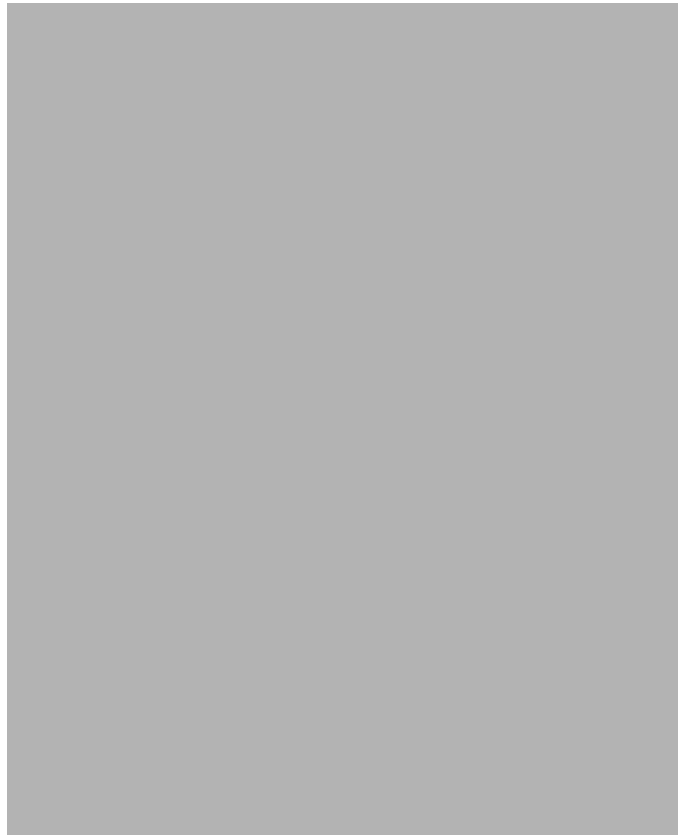
-
- Step 1** Create a folder on your computer to store backup files so they will be easy to find if you have to restore later.
- Step 2** Choose **Tools > Backup Configurations**.
ASDM opens the Backup Configurations dialog box.



By default, all files are checked and will be backed up if they are available. If you want to back up all of the files in the list, go to Step 5.

- Step 3** Uncheck the **Backup All** check box if you want to specify the configurations to back up.
- Step 4** Check the options to customize the backup.
- Step 5** Click **Browse Local Directory**.
The Select dialog box appears.
- Step 6** Choose the path on your computer to specify the target destination for the zip file to package the backup.
- Step 7** Click **Select**.
The path appears in the Local File field.
- Step 8** Enter the name of the destination backup file after the path.
- Step 9** Click **Backup**.

ASDM displays a status window. When the backup completes, ASDM closes it and opens the Backup Statistics window.



This window shows the status of each backup.



Note Backup “failure messages” are most likely the consequence of no configuration present for the types indicated.

Step 10 Click **OK** to close the window.

Modes

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

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

Restoring Configurations

You can specify configurations and images to restore from a zip file on your local computer. Before proceeding, please note the following restrictions:

- The zip file you restore must be created from the Tools > Backup Configurations option.
- Although you can use the Tools > Backup Configurations option to back up a running configuration, the Tools > Restore Configurations option does not support restore the running configuration. Instead, unzip and transfer the running-config.cfg file to the security appliance file system, enter the **copy running-config.cfg startup-config** command, and restart the security appliance to load it to memory.
- We support configuration restorals using backups made from the same security appliance type. Although you may want to try the following types of restorals, we do not support them:
 - Restoral of components other than the running configuration to any other type in the ASA 5500-series.
 - Restoral of a 5520 running configuration to a 5540, or vice-versa.
 - Restoral of a 5520 running configuration to a 5550, or vice-versa, only if they both have a 4-port SSM.
 - Restoral from one 5520, 5540, or 5580 running configuration to another type in this group only if they both have the same interfaces in the same slots.
- The DAP configuration may depend on a specific running configuration, URL-list, and CSD configuration.
- The CSD configuration may depend on the version of the CSD image.

To restore selected elements of the security appliance configuration, Cisco Secure Desktop image, or SSL VPN Client images and profiles, perform the following steps:

Step 1 Choose Tools > Restore Configurations.

The first Restore Configurations dialog box opens.



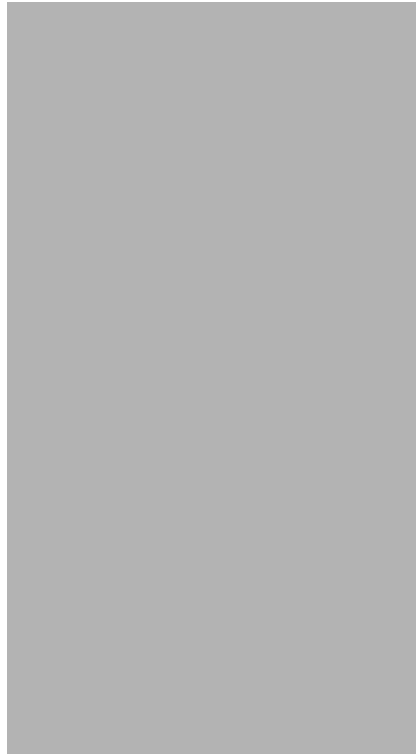
Note Later in the procedure, you have an opportunity to choose the configuration elements to restore; this window lets you choose the file from which to restore them.

Step 2 Click **Browse Local Directory**, choose the zip file on your local computer that contains the configuration to restore, then click **Select**.

ASDM shows the path and the zip filename in the Local File box.

Step 3 Click **Next**.

The second Restore Configuration dialog box opens.



By default, all files are checked; ASDM restores them if they are available.

Step 4 Use the default options, or uncheck them and check the specific configurations and images you want to restore.

Step 5 Click **Restore**.

ASDM displays a status window until the restore operation completes.

Modes

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

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

