



CHAPTER 44

Monitoring Properties

This chapter includes the following sections:

- [Monitoring AAA Servers, page 44-1](#)
- [Monitoring Device Access, page 44-4](#)
- [Connection Graphs](#)
- [CRL](#)
- [DNS Cache](#)
- [IP Audit](#)
- [System Resources Graphs](#)
- [WCCP](#)

Monitoring AAA Servers

This section includes the following topics:

- [Viewing AAA Server Statistics, page 44-1](#)
- [Updating the Operational State of an AAA Server, page 44-2](#)
- [Fields Used to Monitor AAA Servers, page 44-3](#)

Viewing AAA Server Statistics

Use this procedure to view statistics for AAA Servers.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM Startup Wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).

Procedure

To view AAA Server statistics, perform the following steps.

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click **AAA Servers**.
The AAA Servers dialog box opens in the right-hand pane, displaying a list of the configured AAA servers.
- Step 4** Click the row for the server whose statistics you want to monitor.
Statistics for the selected server display in the lower portion of the dialog box.
-

Updating the Operational State of an AAA Server

Use this procedure to update the operational state of an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM Startup Wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).

Procedure

To update the state of an AAA Server, perform the following steps.

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click **AAA Servers**.
The AAA Servers dialog box opens in the right-hand pane, displaying a list of the AAA servers that are configured on the security appliance.
- Step 4** Click the row for the server to update.
Statistics for the selected server display in the lower portion of the dialog box.
- Step 5** Click **Update Server Statistics**.
The Update Server Statistics dialog box opens.
- Step 6** From the AAA Server Status selection list, choose the operational state to apply to this server.
The security appliance is updated with the server current state.
- Step 7** Click **OK**.

The dialog box closes.

Fields Used to Monitor AAA Servers

The following table describes the fields for monitoring AAA Servers.

Field	Description
Server Group	The name of the server group where the server resides.
Protocol	The protocol used by the AAA server group.
IP Address	The IP address for the AAA server.
Status	The operational status of the AAA server. <ul style="list-style-type: none"> Active Failed
Statistics	The lower portion of the AAA Servers dialog box shows the following current information about the selected server: <ul style="list-style-type: none"> Server port and/or hostname Number of pending requests Average round trip time Number of authentication requests Number of authorization requests Number of accounting requests Number of retransmissions Number of accepts Number of rejects Number of challenges Number of malformed responses Number of bad authenticators Number of timeouts Number of unrecognized responses
Clear Server Statistics	Zeroes the counters for the selected server's statistics.
Update Server Status	Opens the Update Server Status dialog box for changing the operational state of the AAA server.
Refresh	Refreshes the dialog box display.

Modes

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

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

Monitoring Device Access

This section includes the following topics:

- [Monitoring User Lockouts](#)
- [Monitoring Authenticated Users](#)
- [Monitoring Active Sessions](#)
- [Fields Used to Monitor Device Access](#)

Monitoring User Lockouts

This section includes the following topics:

- [Viewing Lockouts, page 44-4](#)
- [Removing All User Lockouts, page 44-5](#)
- [Removing One User Lockout, page 44-6](#)

Viewing Lockouts

Use this procedure to view information about users who were locked out of the security appliance after failing to successfully authenticate with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-18](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To view information about user lockouts, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.

The monitoring functions display in the left-hand Navigation pane.

- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **AAA Local Locked Out Users**.
The AAA Local Locked Out Users dialog box opens in the right-hand pane, displaying a list of users who failed to successfully authenticate with an AAA server.
-

Removing All User Lockouts

Use this procedure to remove the lockouts of all users who were locked out of the security appliance after failing to successfully authenticate with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-18](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To clear all user lockouts from the security appliance, perform the following steps:

- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **AAA Local Locked Out Users**.
The AAA Local Locked Out Users dialog box opens in the right-hand pane, displaying a list of users who failed to successfully authenticate with an AAA server.
- Step 5** Click **Refresh**.
The display is refreshed with current lockout information.
- Step 6** Review the refreshed list to make sure that you want to remove all lockouts.
- Step 7** Click **Clear All Lockouts**.

All lockouts from the security appliance are removed and usernames removed from the list.

Removing One User Lockout

Use this procedure to remove a lockout for one user who was locked out of the security appliance after failing to successfully authenticate with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-18](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To remove a user lockout, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **AAA Local Locked Out Users**.
The AAA Local Locked Out Users dialog box opens in the right-hand pane, displaying a list of users who failed to successfully authenticate with an AAA server.
- Step 5** Select the username from the list.
The row is highlighted.
- Step 6** Click **Clear Selected Lockout**.
The lockout is removed for this user and the row is removed from the list.
-

Monitoring Authenticated Users

Use this procedure to monitor users who have successfully authenticated with an AAA server.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-18](#).
- You have already configured authentication for the security appliance using the section, [About Authentication, page 14-2](#).

Procedure

To monitor information about users who have successfully authenticated, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **Authenticated Users**.
The Authenticated Users dialog box opens in the right-hand pane, displaying a list of users who have successfully authenticated with an AAA server.
-

Monitoring Active Sessions

This section includes the following procedures:

- [Viewing Active Sessions, page 44-7](#)
- [Disconnecting an Active Session, page 44-9](#)

Viewing Active Sessions

Use this procedure to view the sessions that are currently connected to the security appliance.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-18](#).

- You have already configured the security appliance access for the session traffic you want to monitor. See the procedures in one of the following sections:
 - [Configuring Device Access for ASDM, Telnet, or SSH, page 16-1](#)
 - [Configuring CLI Parameters, page 16-2](#)

Procedure

To monitor active sessions, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **ASDM/HTTPS/Telnet/SSH Sessions**.
A dialog box opens in the right-hand pane, displaying the list of currently active connections.
The following table describes the fields for monitoring active ASDM/HTTPS/Telnet sessions.

Field	Description
Type	The type of connection (ASDM/HTTPS/Telnet).
Session ID	The name of a currently connected ASDM/HTTPS/Telnet session.
IP Address	The IP address of the host or network that is currently connected to the security appliance.
Disconnect	Disconnects the selected ASDM/HTTPS/Telnet session from the security appliance.
Refresh	Refreshes the dialog box display.

The following table describes the fields for monitoring active SSH sessions.

Field	Description
Client	The client type for the selected SSH session.
User	The user name for the selected SSH session.
State	The state of the selected SSH session.
Version	The version of SSH used to connect to the security appliance.
Encryption (In)	The inbound encryption method used for the selected session.
Encryption (Out)	The outbound encryption method used for the selected session.
HMAC (In)	The configured HMAC for the selected inbound SSH session.
HMAC (Out)	The configured HMAC for the selected outbound SSH session.
SID	The session ID of the selected session.
Disconnect	Disconnects an active SSH session connected to the security appliance.
Refresh	Refreshes the dialog box display.

Modes

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

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

Disconnecting an Active Session

Use this procedure to disconnect an active ASDM/HTTPS, SSH, or Telnet session that is currently connected to the security appliance.

Prerequisites

- You are connected to the security appliance using ASDM.
- You have already completed the initial security appliance configurations included in the ASDM startup wizard. For more information, see [Using the Startup Wizard, page 5-1](#).
- You have already configured the servers and server groups that are being managed by the security appliance. For more information, see the [Summary of Support, page 14-3](#).
- You have already configured the user accounts that are being managed by the security appliance Local server. For more information, see [Adding a User Account, page 14-18](#).
- You have already configured the security appliance access. See the procedures in one of the following sections:
 - [Configuring Device Access for ASDM, Telnet, or SSH, page 16-1](#)
 - [Configuring CLI Parameters, page 16-2](#)

Procedure

To disconnect an active security appliance session, perform the following steps:

-
- Step 1** From the ASDM toolbar, click **Monitoring**.
The monitoring functions display in the left-hand Navigation pane.
- Step 2** Click **Properties**.
The Properties Navigation pane opens.
- Step 3** Click the plus (+) symbol next to Device Access.
The list of Device Access functions expands below it.
- Step 4** Click **ASDM/HTTPS/Telnet/SSH Sessions**.
A dialog box opens in the right-hand pane, displaying a table which lists the currently active connections.
- Step 5** In the table, select the session you want to disconnect.
The row is highlighted.
- Step 6** Click **Disconnect**.
The session is disconnected from the security appliance, and removed from the table.
-

Fields Used to Monitor Device Access

This section includes the following topics:

- [Fields for Monitoring User Lockouts, page 44-10](#)
- [Fields for Monitoring Users Who Have Authenticated with a Server, page 44-11](#)

Fields for Monitoring User Lockouts

The following table describes the fields for monitoring locked out users.

Field	Description
Lock Time	The amount of time that the user has been locked out of the system.
Failed Attempts	The number of authentication attempts that the user failed.
User	A list of usernames of those users who are currently locked out of the security appliance because they were unable to successfully authenticate with the authentication server.
Clear Selected Lockout	Removes the lockout for the selected username and removes the username from the list.
Clear All Lockouts	Removes the lockout for all usernames in the list. Note We recommend that you refresh the list of locked out users and review it before clearing all lockouts.
Refresh	Refreshes the dialog box display.

Modes

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

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

Fields for Monitoring Users Who Have Authenticated with a Server

The following table describes the fields for monitoring authenticated users.

Field	Description
User	The usernames of users who have successfully authenticated with an authentication server.
IP Address	The IP addresses of users who have successfully authenticated with an authentication server.
Dynamic ACL	The dynamic access list of the user authenticated to use the security appliance.
Inactivity Timeout	The amount of time that the user connection must remain inactive before the session times out and the user is disconnected.
Absolute Timeout	The amount of time that the user can remain connected before the session closes and the user is disconnected.
Refresh	Refreshes the dialog box display.

Modes

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

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

Connection Graphs

The Connection Graphs pane lets you view connection information about the security appliance in graph format. You can view information about NAT and performance monitoring information, including UDP connections, AAA performance, and inspection information. This section includes the following topics:

- [Perfmon](#)
- [Xlates](#)

Perfmon

The Perfmon pane lets you view the performance information in a graphical format. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - AAA Perfmon—Displays the security appliance AAA performance information.
 - Inspection Perfmon—Displays the security appliance inspection performance information.
 - Web Perfmon—Displays the security appliance web performance information, including URL access and URL server requests.
 - Connections Perfmon—Displays the security appliance connections performance information.
 - Xlate Perfmon—Displays the security appliance NAT performance information.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

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

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

Xlates

This pane lets you view the active Network Address Translations in a graphical format. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - Xlate Utilization—Displays the security appliance NAT utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected entry from the Selected Graphs list.

- Show Graphs—Click to display a new or updated graph window.

Modes

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

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

CRL

This pane allows you to view or clear associated CRLs of selected CA certificates.

Fields

- CA Certificate Name—Choose the name of the selected certificate from the drop-down list.
- View CRL—Click to view the selected CRL.
- Clear CRL—Click to clear the selected CRL from the cache.
- CRL Info—*Display only*. Displays detailed CRL information.

Modes

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

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

DNS Cache

The security appliance provides a local cache of DNS information from external DNS queries that are sent for certain clientless SSL VPN and certificate commands. Each DNS translation request is first looked for in the local cache. If the local cache has the information, the resulting IP address is returned. If the local cache can not resolve the request, a DNS query is sent to the various DNS servers that have been configured. If an external DNS server resolves the request, the resulting IP address is stored in the local cache along with its corresponding hostname.

Important Notes

- DNS cache entries are time stamped. The time stamp will be used to age out unused entries. When the entry is added to the cache, the time stamp is initialized. Each time the entry is accessed, the timestamp is updated. At a configured time interval, the DNS cache will check all entries and purge those entries whose time exceeds a configured age-out timer.

- If new entries arrive but there is no room in the cache because the size was exceeded or no more memory is available, the cache will be thinned by one third, based on the entries age. The oldest entries will be removed.

Fields

- Host— Shows the DNS name of the host.
- IP Address—Shows the address that resolves to the hostname.
- Permanent—Indicates whether the entry was made though a **name** command.
- Idle Time—Specifies the time elapsed since the security appliance last referred to that entry.
- Active—Indicates whether the entry has aged out. If there is not adequate space in cache, this entry may be deleted.
- Clear Cache—Click to clear the entire DNS cache.

Modes

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

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

IP Audit

The IP Audit pane lets you view the number of packets that match informational and attack signatures that are shown in graphical or tabular form. Each graph type shows the combined packets for all interfaces that have this feature enabled.

Fields

- Available Graphs—Lists the types of signatures available for monitoring. See [IP Audit Signatures](#) for detailed information about each signature type. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.
 - IP Options—Shows the packet count for the following signatures:
 - Bad Options List (1000)
 - Timestamp (1002)
 - Provide s, c, h, tcc (1003)
 - SATNET ID (1005)
 - IP Route Options—Shows the packet count for the following signatures:
 - Loose Source Route (1004)
 - Record Packet Route (1001)
 - Strict Source Route (1006)
 - IP Attacks—Shows the packet count for the following signatures:
 - IP Fragment Attack (1100)

- Impossible IP Packet (1102)
- IP Teardrop (1103)
- ICMP Requests—Shows the packet count for the following signatures:
 - Echo Request (2004)
 - Time Request (2007)
 - Info Request (2009)
 - Address Mask Request (2011)
- ICMP Responses—Shows the packet count for the following signatures:
 - Echo Reply (2000)
 - Source Quench (2002)
 - Redirect (2003)
 - Time Exceeded (2005)
 - Parameter Problem (2006)
- ICMP Replies—Shows the packet count for the following signatures:
 - Unreachable (2001)
 - Time Reply (2008)
 - Info Reply (2010)
 - Address Mask reply (2012)
- ICMP Attacks—Shows the packet count for the following signatures:
 - Fragmented ICMP (2150)
 - Large ICMP (2151)
 - Ping of Death (2154)
- TCP Attacks—Shows the packet count for the following signatures:
 - No Flags (3040)
 - SYN & FIN Flags Only (3041)
 - FIN Flag Only (3042)
- UDP Attacks—Shows the packet count for the following signatures:
 - Bomb (4050)
 - Snork (4051)
 - Chargen (4052)
- DNS Attacks—Shows the packet count for the following signatures:
 - Host Info (6050)
 - Zone Transfer (6051)
 - Zone Transfer High Port (6052)
 - All Records (6053)
- FTP Attacks—Shows the packet count for the following signatures:
 - Improper Address (3153)
 - Improper Port (3154)

- RPC Requests to Target Hosts—Shows the packet count for the following signatures:
 - Port Registration (6100)
 - Port Unregistration (6101)
 - Dump (6102)
- YP Daemon Portmap Requests—Shows the packet count for the following signatures:
 - ypserv Portmap Request (6150)
 - ybind Portmap Request (6151)
 - yppasswdd Portmap Request (6152)
 - ypupdated Portmap Request (6153)
 - ypxfrd Portmap Request (6154)
- Miscellaneous Portmap Requests—Shows the packet count for the following signatures:
 - mountd Portmap Request (6155)
 - rexdb Portmap Request (6175)
- Miscellaneous RPC Calls—Shows the packet count for the following signatures:
 - rexdb Attempt (6180)
- RPC Attacks—Shows the packet count for the following signatures:
 - statd Buffer Overflow (6190)
 - Proxied RPC (6103)
- Add—Click to add the selected graph type to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.
- Selected Graphs—Lists the graph types you want to show in the Selected Graphs list.

Modes

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

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

System Resources Graphs

This pane lets you view the status of the security appliance memory, CPU, and block utilization. This section includes the following topics:

- [Blocks](#)
- [CPU](#)
- [Memory](#)

Blocks

This pane lets you view the free and used memory blocks. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs —Lists the components you can graph.
 - Blocks Used—Displays the security appliance used memory blocks.
 - Blocks Free—Displays the security appliance free memory blocks.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected statistic type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

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

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

CPU

This pane lets you view the CPU utilization. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - CPU Utilization—Displays the security appliance CPU utilization.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

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

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

Memory

This pane lets you view the memory utilization. You can choose up to four types of statistics to show in one graph window. You can open multiple graph windows at the same time.

Fields

- Available Graphs—Lists the components you can graph.
 - Free Memory—Displays the security appliance free memory.
 - Used Memory—Displays the security appliance used memory.
- Graph Window Title—Shows the graph window name to which you want to add a graph type. To use an existing window title, select one from the drop-down list. To display graphs in a new window, enter a new window title.
- Add—Click to move the selected entries in the Available Graphs list to the Selected Graphs list.
- Remove—Click to remove the selected graph type from the Selected Graphs list.
- Show Graphs—Click to display a new or updated graph window.

Modes

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

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

WCCP

The Web Cache Communication Protocol redirects IPv4 traffic flows to web caches in real-time. In ASDM, you can monitor packet redirection of an interface using WCCP. WCCP also provides load balancing, scaling, fault tolerance, and fail safe services. Load balancing is provided by hashing based on the destination IP address. The hash values are used to choose the egress interface for any traffic flow.

This protocol also enables the security appliance and WCCP clients to form service groups to support a service. This section includes the following topics:

- [Service Groups](#)
- [Redirection](#)

Service Groups

This pane allows you to view and refresh the service group, the display mode, and hash settings, which include the source and destination IP addresses and the source and destination port numbers.

Fields

- Service Group—Choose the applicable service group from the drop-down list.
- Display Mode—Choose the display mode from the drop-down list.
- Destination IP Address—Specify the destination IP address.
- Source IP Address—Specify the source IP address.
- Destination Port—Specify the destination port number.
- Source Port—Specify the source port number.
- WCCP Service Groups—*Display-only*. Shows the selected WCCP service group information.

For example:

```
Global WCCP information:
  Router information:
  Router Identifier:          -not yet determined-
  Protocol Version:          2.0

  Service Identifier: web-cache
  Number of Cache Engines:   0
  Number of routers:         0
  Total Packets Redirected:  0
  Redirect access-list:     -none-
  Total Connections Denied Redirect: 0
  Total Packets Unassigned:  0
  Group access-list:        -none-
  Total Messages Denied to Group: 0
  Total Authentication failures: 0
  Total Bypassed Packets Received: 0

  Service Identifier: 1
  Number of Cache Engines:   0
  Number of routers:         0
  Total Packets Redirected:  0
  Redirect access-list:     -none-
  Total Connections Denied Redirect: 0
  Total Packets Unassigned:  0
  Group access-list:        -none-
  Total Messages Denied to Group: 0
  Total Authentication failures: 0
  Total Bypassed Packets Received: 0
```

Redirection

This pane allows you to view and refresh WCCP interface statistics in either a summary or detailed format.

Fields

- Show Summary—Choose this option to display statistics in a summary format.
- Show Details—Choose this option to display statistics in a detailed format.

- WCCP Interface Statistics—*Display-only*. Shows the current WCCP interface statistics.

For example:

WCCP interface configuration details:

```
Management0/0
Output services: 0
Input services: 1
Static:          None
Dynamic:         001
Mcast services: 0
Exclude In:     FALSE
```


