CHAPTER 18

logging asdm through logout message Commands

logging asdm

To send syslog messages to the ASDM log buffer, use the **logging asdm** command in global configuration mode. To disable logging to the ASDM log buffer, use the **no** form of this command.

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the ASDM log buffer. For information about creating lists, see the **logging list** command.

Defaults

ASDM logging is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Before any messages are sent to the ASDM log buffer, you must enable logging using the **logging enable** command.

When the ASDM log buffer is full, the adaptive security appliance deletes the oldest message to make room in the buffer for new messages. To control the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

The following example shows how to enable logging, send log buffer messages of severity levels 0, 1, and 2 to the ASDM, and how to set the ASDM log buffer size to 200 messages:

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages that it contains.
logging asdm-buffer-size	Specifies the number of ASDM messages retained in the ASDM log buffer
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging configuration.

logging asdm-buffer-size

To specify the number of syslog messages retained in the ASDM log buffer, use the **logging asdm-buffer-size** command in global configuration mode. To reset the ASDM log buffer to its default size of 100 messages, use the **no** form of this command.

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

Syntax Description

num_of_msgs	Specifies the number of syslog messages that the adaptive security appliance retains in the ASDM log buffer.

Defaults

The default ASDM syslog buffer size is 100 messages.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When the ASDM log buffer is full, the adaptive security appliance deletes the oldest message to make room in the buffer for new messages. To control whether logging to the ASDM log buffer is enabled or to control the kind of syslog messages retained in the ASDM log buffer, use the **logging asdm** command.

The ASDM log buffer is a different buffer than the log buffer enabled by the **logging buffered** command.

Examples

The following example shows how to enable logging, sendmessages of severity levels 0, 1, and 2 to the ASDM log buffer, and how to set the ASDM log buffer size to 200 messages:

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: level critical, 48 messages logged
```

Related Commands

Command	Description
clear logging asdm	Clears the ASDM log buffer of all messages that it contains.
logging asdm	Enables logging to the ASDM log buffer.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the currently running logging configuration.

logging buffered

To enable the adaptive security appliance to send syslog messages to the log buffer, use the **logging buffered** command in global configuration mode. To disable logging to the log buffer, use the **no** form of this command.

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the log buffer. For information about creating lists, see the **logging list** command.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- The buffer size is 4 KB.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the log buffer, you must enable logging using the **logging enable** command.

New messages append to the end of the buffer. When the buffer fills up, the adaptive security appliance clears the buffer and continues adding messages to it. When the log buffer is full, the adaptive security appliance deletes the oldest message to make room in the buffer for new messages. You can have buffer contents automatically saved each time the contents of the buffer have "wrapped", which means that all the messages since the last save have been replaced by new messages. For more information, see the **logging flash-bufferwrap** and **logging ftp-bufferwrap** commands.

At any time, you can save the contents of the buffer to flash memory. For more information, see the **logging savelog** command.

You can view syslog messages that have been sent to the buffer with the **show logging** command.

Examples

The following example configures logging to the buffer for severity level 0 and level 1 events:

```
hostname(config)# logging buffered alerts
hostname(config)#
```

The following example creates a list named" notif-list" with a maximum severity level of 7 and configures logging to the buffer for syslog messages identified by the "notif-list" list:

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
logging savelog	Saves the contents of the log buffer to flash memory.

logging buffer-size

To specify the size of the log buffer, use the **logging buffer-size** command in global configuration mode. To reset the log buffer to its default size of 4 KB of memory, use the **no** form of this command.

logging buffer-size *bytes*

no logging buffer-size *bytes*

Syntax Description

bytes	Sets the amount of memory used for the log buffer, in bytes. For example, if you specify 8192, the adaptive security appliance uses 8 KB of memory for the log buffer.

Defaults

The default log buffer size is 4 KB of memory.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To see whether the adaptive security appliance is using a log buffer of a size other than the default buffer size, use the **show running-config logging** command. If the **logging buffer-size** command is not shown, then the adaptive security appliance uses a log buffer of 4 KB.

For more information about how the adaptive security appliance uses the buffer, see the **logging buffered** command.

Examples

The following example enables logging, enables the logging buffer, and specifies that the adaptive security appliance uses 16 KB of memory for the log buffer:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to flash memory when the log buffer is full.
logging savelog	Saves the contents of the log buffer to flash memory.

logging class

To configure the maximum severity level per logging destination for a message class, use the **logging class** command in global configuration mode. To remove a message class severity level configuration, use the **no** form of the command.

logging class *class destination level* [*destination level . . .*]

no logging class *class*

Syntax Description

class	Specifies the message class whose maximum severity levels are configured per destination. For valid values of *class*, see the "Usage Guidelines" section that follows.
destination	Specifies a logging destination for *class*. For the destination, the *level* determines the maximum severity level sent to *destination*. For valid values of *destination*, see the "Usage Guidelines" section that follows.
level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action is needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.

Defaults

By default, the adaptive security appliance does not apply severity levels on a logging destination and message class basis. Instead, each enabled logging destination receives messages for all classes at the severity level determined by the logging list or severity level specified when you enabled the logging destination.

Command Modes

The following table shows the modes in which you may enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Added **eigrp** to valid class values.
8.2(1)	Added **dap** to valid class values.

Usage Guidelines

Valid values for *class* include the following:

- **auth**—User authentication.
- **bridge**—Transparent firewall.
- **ca**—PKI certificate authority.
- **config**—Command interface.
- **dap—**Dynamic Access Policies.
- **eap**—Extensible Authentication Protocol (EAP). Logs the following types of events to support Network Admission Control: EAP session state changes, EAP status query events, and a hexadecimal dump of EAP header and packet contents.
- **eapoudp**—Extensible Authentication Protocol (EAP) over UDP. Logs EAPoUDP events to support Network Admission Control, and generates a complete record of EAPoUDP header and packet contents.
- **eigrp**—EIGRP routing.
- **email**—Email proxy.
- **ha**—Failover.
- **ids**—Intrusion detection system.
- **ip**—IP stack.
- **ipaa—**IP address assignment
- **nac**—Network Admission Control. Logs the following types of events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.
- **np**—Network processor.
- **ospf**—OSPF routing.
- **rip**—RIP routing.
- **session**—User session.
- **snmp**—SNMP.
- **sys**—System.
- **vpn**—IKE and IPSec.
- **vpnc**—VPN client.
- **vpnfo**—VPN failover.
- **vpnlb**—VPN load balancing.

Valid logging destinations are as follows:

- **asdm**—To learn about this destination, see the **logging asdm** command.
- **buffered**—To learn about this destination, see the **logging buffered** command.

- **console**—To learn about this destination, see the **logging console** command.
- **history**—To learn about this destination, see the **logging history** command.
- **mail**—To learn about this destination, see the **logging mail** command.
- **monitor**—To learn about this destination, see the **logging monitor** command.
- **trap**—To learn about this destination, see the **logging trap** command.

Examples

The following example specifies that, for failover-related messages, the maximum severity level for the ASDM log buffer is 2 and the maximum severity level for the syslog buffer is 7:

```
hostname(config)# logging class ha asdm 2 buffered 7
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging console

To enable the adaptive security appliance to display syslog messages in console sessions, use the **logging console** command in global configuration mode. To disable the display of syslog messages in console sessions, use the **no** form of this command.

logging console [*logging_list* | *level*]

no logging console

Note We recommend that you do not use this command, because it may cause many syslog messages to be dropped due to buffer overflow. For more information, see the "Usage Guidelines" section that follows.

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the console session. For information about creating lists, see the **logging list** command.

Defaults

The adaptive security appliance does not display syslog messages in console sessions by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Before any messages are sent to the console, you must enable logging using the **logging enable** command.

Caution Using the **logging console** command could significantly degrade system performance. Instead, use the **logging buffered** command to start logging and the **show logging** command to view the messages. To make viewing the most current messages easier, use the **clear logging buffer** command to clear the buffer.

Examples

The following example shows how to enable syslog messages of severity levels 0, 1, 2, and 3 to appear in console sessions:

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging debug-trace

To redirect debugging messages to logs as syslog message 711001 issued at severity level 7, use the **logging debug-trace** command in global configuration mode. To stop sending debugging messages to logs, use the **no** form of this command.

logging debug-trace

no logging debug-trace

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the adaptive security appliance does not include debugging output in syslog messages.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Debugging messages are generated as severity level 7 messages. They appear in logs with the syslog message number 711001, but do not appear in any monitoring session.

Examples

The following example shows how to enable logging, send log messages to the system log buffer, redirect debugging output to logs, and turn on debugging of disk activity.

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

The following is sample output of a debugging message that could appear in the logs:

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging device-id

To configure the adaptive security appliance to include a device ID in non-EMBLEM-format syslog messages, use the **logging device-id** command in global configuration mode. To disable the use of a device ID, use the **no** form of this command.

logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

no logging device-id {**context-name** | **hostname** | **ipaddress** *interface_name* | **string** *text*}

Syntax Description

context-name	Specifies the name of the current context as the device ID.
hostname	Specifies the hostname of the adaptive security appliance as the device ID.
ipaddress *interface_name*	Specifies the device ID or the IP address of the interface in *interface_name*. If you use the **ipaddress** keyword, syslog messages sent to an external server include the IP address of the interface specified, regardless of which interface the adaptive security appliance uses to send the log data to the external server.
string *text*	Specifies the characters included in *text* as the device ID, which can be up to 16 characters long. You cannot use white space characters or any of the following characters: • &—ampersand • '—single quote • "—double quote • <—less than • >—greater than • ?—question mark

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you use the **ipaddress** keyword, the device ID becomes the specified adaptive security appliance interface IP address, regardless of the interface from which the message is sent. This keyword provides a single, consistent device ID for all messages that are sent from the device.

Examples

The following example shows how to configure a host named “secappl-1”:

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

The hostname appears at the beginning of syslog messages, as shown in the following message:

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging emblem

To use the EMBLEM format for syslog messages sent to destinations other than a syslog server, use the **logging emblem** command in global configuration mode. To disable the use of EMBLEM format, use the **no** form of this command.

logging emblem

no logging emblem

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the adaptive security appliance does not use EMBLEM format for syslog messages.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed to be independent of the **logging host** command.

Usage Guidelines

The **logging emblem** command lets you to enable EMBLEM-format logging for all logging destinations other than syslog servers. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

To enable EMBLEM-format logging for syslog servers, use the **format emblem** option with the **logging host** command.

Examples

The following example shows how to enable logging and enable the use of EMBLEM-format for logging to all logging destinations except syslog servers:

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging enable

To enable logging for all configured output locations, use the **logging enable** command in global configuration mode. To disable logging, use the **no** form of this command.

logging enable

no logging enable

Syntax Description

This command has no arguments or keywords.

Defaults

Logging is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was changed from the **logging on** command.

Usage Guidelines

The **logging enable** command allows you to enable or disable sending syslog messages to any of the supported logging destinations. You can stop all logging with the **no logging enable** command.

You can enable logging to individual logging destinations with the following commands:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Examples

The following example shows how to enable logging. The output of the **show logging** command illustrates how each possible logging destination must be enabled separately:

```
hostname(config)# logging enable
hostname(config)# show logging
Syslog logging: enabled
```

```
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Deny Conn when Queue Full: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging facility

To specify the logging facility used for messages sent to syslog servers, use the **logging facility** command in global configuration mode. To reset the logging facility to its default of 20, use the **no** form of this command.

logging facility *facility*

no logging facility

Syntax Description

facility	Specifies the logging facility; valid values are 16 through 23.

Defaults

The default facility is 20 (LOCAL4).

Command Modes

The following table shows the modes in which you can enter the command, with the exceptions noted in the Syntax Description section.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Syslog servers file messages based on the *facility* number in the message. There are eight possible facilities: 16 (LOCAL0) through 23 (LOCAL7).

Examples

The following example shows how to specify that the adaptive security appliance indicate the logging facility as 16 in syslog messages. The output of the **show logging** command includes the facility being used by the adaptive security appliance:

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
```

```
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging flash-bufferwrap

To enable the adaptive security appliance to write the log buffer to flash memory every time the buffer is full of messages that have never been saved, use the **logging flash-bufferwrap** command in global configuration mode. To disable writing of the log buffer to flash memory, use the **no** form of this command.

logging flash-bufferwrap

no logging flash-bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Writing the log buffer to flash memory is disabled.
- The buffer size is 4 KB.
- Minimum free flash memory is 3 MB.
- Maximum flash memory allocation for buffer logging is 1 MB.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

For the adaptive security appliance to write the log buffer to flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to flash memory. To enable logging to the buffer, use the **logging buffered** command.

While the adaptive security appliance writes log buffer contents to flash memory, it continues storing any new event messages to the log buffer.

The adaptive security appliance creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

The availability of flash memory affects how the adaptive security appliance saves syslog messages using the **logging flash-bufferwrap** command. For more information, see the **logging flash-maximum-allocation** and the **logging flash-minimum-free** commands.

Examples

The following example shows how to enable logging, enable the log buffer, and enable the adaptive security appliance to write the log buffer to flash memory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
copy	Copies a file from one location to another, including to a TFTP or FTP server.
delete	Deletes a file from the disk partition, such as saved log files.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.

logging flash-maximum-allocation

To specify the maximum amount of flash memory that the adaptive security appliance uses to store log data, use the **logging flash-maximum-allocation** command in global configuration mode. To reset the maximum amount of flash memory used for this purpose to its default size of 1 MB of flash memory, use the **no** form of this command.

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

Syntax Description

kbytes	The largest amount of flash memory, in kilobytes, that the adaptive security appliance can use to save log buffer data.

Defaults

The default maximum flash memory allocation for log data is 1 MB.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command determines how much flash memory is available for the **logging savelog** and **logging flash-bufferwrap** commands.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** causes flash memory use for log files to exceed the maximum amount specified by the **logging flash-maximum-allocation** command, the adaptive security appliance deletes the oldest log files to free sufficient memory for the new log file. If there are no files to delete or if, after all old files are deleted, free memory is too small for the new log file, the adaptive security appliance fails to save the new log file.

To see whether the adaptive security appliance has a maximum flash memory allocation of a size different than the default size, use the **show running-config logging** command. If the **logging flash-maximum-allocation** command is not shown, then the adaptive security appliance uses a maximum of 1 MB for saved log buffer data. The memory allocated is used for both the **logging savelog** and **logging flash-bufferwrap** commands.

For more information about how the adaptive security appliance uses the log buffer, see the **logging buffered** command.

Examples

The following example shows how to enable logging, enable the log buffer, enable the adaptive security appliance to write the log buffer to flash memory, with the maximum amount of flash memory used for writing log files set to approximately 1.2 MB of memory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to flash memory when the log buffer is full.
logging flash-minimum-free	Specifies the minimum amount of flash memory that must be available for the adaptive security appliance to permit writing of the log buffer to flash memory.

logging flash-minimum-free

To specify the minimum amount of free flash memory that must exist before the adaptive security appliance saves a new log file, use the **logging flash-minimum-free** command in global configuration mode. This command affects how much free flash memory must exist before the adaptive security appliance saves log files created by the **logging savelog** and **logging flash-bufferwrap** commands. To reset the minimum required amount of free flash memory to its default size of 3 MB, use the **no** form of this command.

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

Syntax Description

kbytes	The minimum amount of flash memory, in kilobytes, that must be available before the adaptive security appliance saves a new log file.

Defaults

The default minimum free flash memory is 3 MB.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The logging flash-minimum-free command specifies how much flash memory the **logging savelog** and **logging flash-bufferwrap** commands must preserve at all times.

If a log file to be saved by **logging savelog** or **logging flash-bufferwrap** would cause the amount of free flash memory to fall below the limit specified by the **logging flash-minimum-free** command, the adaptive security appliance deletes the oldest log files to ensure that the minimum amount of memory remains free after saving the new log file. If there are no files to delete or if, after all old files are deleted, free memory would still be below the limit, the adaptive security appliance fails to save the new log file.

Examples

The following example shows how to enable logging, enable the log buffer, enable the adaptive security appliance to write the log buffer to flash memory, and specifies that the minimum amount of free flash memory must be 4000 KB:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.
logging flash-bufferwrap	Writes the log buffer to flash memory when the log buffer is full.
logging flash-maximum-allocation	Specifies the maximum amount of flash memory that can be used for writing log buffer contents.

logging flow-export-syslogs enable | disable

To enable all of the syslog messages that NetFlow captures, use the **logging flow-export-syslogs enable** command in global configuration mode. To disable all of the syslog messages that NetFlow captures, use the **logging flow-export-syslogs disable** command in global configuration mode.

logging flow-export-syslogs {enable | disable}

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all syslogs that are captured by NetFlow are enabled.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

If the security appliance is configured to export NetFlow data, to improve performance, we recommend that you disable redundant syslog messages (those also captured by NetFlow) by entering the **logging flow-export-syslogs disable** command. The syslog messages that will be disabled are as follows:

Syslog Message	Description
106015	A TCP flow was denied because the first packet was not a SYN packet.
106023	A flow that is denied by an ingress ACL or an egress ACL that is attached to an interface through the **access-group** command.
106100	A flow that is permitted or denied by an ACL.
302013 and 302014	A TCP connection and deletion.
302015 and 302016	A UDP connection and deletion.
302017 and 302018	A GRE connection and deletion.
302020 and 302021	An ICMP connection and deletion.
313001	An ICMP packet to the security appliance was denied.
313008	An ICMPv6 packet to the security appliance was denied.
710003	An attempt to connect to the security appliance was denied.

Note Although this is a configuration mode command, it is not stored in the configuration. Only the **no logging message xxxxxx** commands are stored in the configuration.

Examples

The following example shows how to disable redundant syslog messages that NetFlow captures and the sample output that appears:

```
hostname(config)# logging flow-export-syslogs disable

hostname(config)# show running-config logging

no logging message xxxxx1
no logging message xxxxx2
```

where the *xxxxx1* and *xxxxx2* are syslog messages that are redundant because the same information has been captured through NetFlow. This command is like a command alias, and will convert to a batch of **no logging message xxxxxx** commands. After you have disabled the syslog messages, you can enable them individually with the **logging message xxxxxx** command, where *xxxxxx* is the specific syslog message number.

Related Commands

Commands	Description
flow-export destination *interface-name ipv4-address | hostname udp-port*	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate *minutes*	Controls the interval at which the template information is sent to the NetFlow collector.
show flow-export counters	Displays a set of runtime counters for NetFlow.

logging from-address

To specify the sender e-mail address for syslog messages sent by the adaptive security appliance, use the **logging from-address** command in global configuration mode. All sent syslog messages appear to come from the address you specify. To remove the sender e-mail address, use the **no** form of this command.

logging from-address *from-email-address*

no logging from-address *from-email-address*

Syntax Description

from-email-address	Source e-mail address, that is, the e-mail address that syslog messages appear to come from (for example, cdb@example.com).

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Sending syslog messages by e-mail is enabled by the **logging mail** command.

The address specified with this command need not correspond to an existing e-mail account.

Examples

To enable logging and set up the adaptive security appliance to send syslog messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging mail	Enables the adaptive security appliance to send syslog messages by e-mail and determines which messages are sent by e-mail.
logging recipient-address	Specifies the e-mail address to which syslog messages are sent.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.

logging ftp-bufferwrap

To enable the adaptive security appliance to send the log buffer to an FTP server every time the buffer is full of messages that have never been saved, use the **logging ftp-bufferwrap** command in global configuration mode. To disable sending the log buffer to an FTP server, use the **no** form of this command.

logging ftp-bufferwrap

no logging ftp-bufferwrap

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Logging to the buffer is disabled.
- Sending the log buffer to an FTP server is disabled.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

When you enable **logging ftp-bufferwrap**, the adaptive security appliance sends log buffer data to the FTP server that you specify with the **logging ftp-server** command. While the adaptive security appliance sends log data to the FTP server, it continues storing any new event messages to the log buffer.

For the adaptive security appliance to send log buffer contents to an FTP server, you must enable logging to the buffer; otherwise, the log buffer never has data to be written to flash memory. To enable logging to the buffer, use the **logging buffered** command.

The adaptive security appliance creates log files with names that use a default time-stamp format, as follows:

```
LOG-YYYY-MM-DD-HHMMSS.TXT
```

where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Examples

The following example shows how to enable logging, enable the log buffer, specify an FTP server, and enable the adaptive security appliance to write the log buffer to an FTP server. The example specifies an FTP server whose hostname is logserver-352. The server can be accessed with the username, logsupervisor and password, 1luvMy10gs. Log files are to be stored in the /syslogs directory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-server	Specifies FTP server parameters for use with the **logging ftp-bufferwrap** command.

logging ftp-server

To specify details about the FTP server that the adaptive security appliance sends log buffer data to when **logging ftp-bufferwrap** is enabled, use the **logging ftp-server** command in global configuration mode. To remove all details about an FTP server, use the **no** form of this command.

logging ftp-server *ftp_server path username* [*0* | *8*] *password*

no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) user password will follow.
8	(Optional) Specifies that an encrypted user password will follow.
ftp-server	External FTP server IP address or hostname. **Note** If you specify a hostname, be sure DNS is operating correctly on your network.
password	The password for the username specified.
path	Directory path on the FTP server where the log buffer data is to be saved. This path is relative to the FTP root directory. For example: `/security_appliances/syslogs/appliance107`
username	A username that is valid for logging in to the FTP server.

Defaults

No FTP server is specified by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
8.2(2)	Support for password encryption has been added.

Usage Guidelines

You can only specify one FTP server. If a logging FTP server is already specified, using the **logging ftp-server** command replaces this FTP server configuration with the new one that you enter.

The adaptive security appliance does not verify the FTP server information that you specify. If you misconfigure any of the details, the adaptive security appliance fails to send log buffer data to the FTP server.

During bootup or upgrade of the adaptive security appliance, single-digit passwords and passwords startingwith a digit followed by a whitespace are not supported. For example, 0 pass and 1 are invalid passwords.

Examples

The following example shows how to enable logging, enable the log buffer, specify an FTP server, and enable the adaptive security appliance to write the log buffer to an FTP server. This example specifies an FTP server whose hostname is logserver-352. The server can be accessed with the username, logsupervisor and passwor,d 1luvMy10gs. Log files are to be stored in the /syslogs directory:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

The following example shows how to enter an encrypted password:

```
hostname(config)# logging ftp-server logserver /path1 user1 8 JPAGWzIIFVlheXv2I9nglfytOzHU
```

The following example shows how to enter an unencrypted (clear text) password:

```
hostname(config)# logging ftp-server logserver /path1 user1 0 pass1
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all syslog messages that it contains.
logging buffered	Enables logging to the log buffer.
logging buffer-size	Specifies log buffer size.
logging enable	Enables logging.
logging ftp-bufferwrap	Sends the log buffer to an FTP server when the log buffer is full.

logging history

To enable SNMP logging and specify which messages are to be sent to SNMP servers, use the **logging history** command in global configuration mode. To disable SNMP logging, use the **no** form of this command.

logging history [*logging_list* | *level*]

no logging history

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the SNMP server. For information about creating lists, see the **logging list** command.

Defaults

The adaptive security appliance does not log to SNMP servers by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging history** command allows you to enable logging to an SNMP server and to set the SNMP message level or event list.

Examples

The following example shows how to enable SNMP logging and specify that messages of severity levels 0, 1, 2, and 3 are sent to the SNMP server configured:

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
snmp-server	Specifies SNMP server details.

logging host

To define a syslog server, use the **logging host** command in global configuration mode. To remove a syslog server definition, use the **no** form of this command.

logging host *interface_name syslog_ip* [**tcp/***port* | **udp/***port*] [**format emblem**] [**secure**] [**permit-hostdown**]

logging host *interface_name syslog_ip*

[**no**] **logging host** *interface_name syslog_ip* [**tcp/***port* | **udp/***port*] [**format emblem**] [**secure**]

[**no**] **logging host** *interface_name syslog_ip*

Syntax Description

format emblem	(Optional) Enables EMBLEM format logging for the syslog server.
interface_name	Specifies the interface on which the syslog server resides.
permit-hostdown	Allows the adaptive security appliance to continue TCP logging when the syslog server is down or unreachable.
port	Indicates the port that the syslog server listens to for messages. Valid port values are 1025 through 65535 for either protocol.
secure	Specifies that the connection to the remote logging host should use SSL/TLS. This option is valid only if the protocol selected is TCP. **Note** A secure logging connection can only be established with a SSL/TLS-capable syslog server. If a SSL/TLS connection cannot be established, all new connections will be denied. You may change this default behavior by entering the **logging permit-hostdown** command.
syslog_ip	Specifies the IP address of the syslog server.
tcp	Specifies that the adaptive adaptive security appliance should use TCP to send messages to the syslog server.
udp	Specifies that the adaptive adaptive security appliance should use UDP to send messages to the syslog server.

Defaults

The default protocol is UDP.

The default port numbers are as follows:

- UDP—514
- TCP —1470

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.
8.0(2)	The **secure** keyword was added.

Usage Guidelines

The **logging host** *ip_address* **format emblem** command allows you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for UDP syslog messages only. If you enable EMBLEM-format logging for a particular syslog server, then the messages are sent to that server. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. However, you can only specify a server to receive either UDP or TCP syslog messages, not both.

Note When the **tcp** option is used in the **logging host** command, the adaptive security appliance will drop connections across the firewall if the syslog server is unreachable.

You can display only the *port* and *protocol* values that you previously entered by using the **show running-config logging** command and finding the command in the listing—TCP is listed as 6, and UDP is listed as 17. TCP ports work only with the syslog server. The *port* must be the same port on which the syslog server listens.

Note An error message occurs if you try to use the **logging host** command and the **secure** keyword with UDP.

Examples

The following example shows how to send syslog messages of severity levels 0, 1, 2, and 3 to a syslog server on the inside interface that uses the default protocol and port number:

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging list

To create a logging list to use in other commands to specify messages by various criteria (logging level, event class, and message IDs), use the **logging list** command in global configuration mode. To remove the list, use the **no** form of this command.

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[**-***end_id*]}

no logging list *name*

Syntax Description

class *event_class*	(Optional) Sets the class of events for syslog messages. For the level specified, only syslog messages of the class specified are identified by the command. See the “Usage Guidelines” section for a list of classes.
level *level*	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
message *start_id*[**-***end_id*]	Specified a message ID or range of IDs. To look up the default level of a message, use the **show logging** command or see the *Cisco ASA 5500 Series System Log Messages*.
name	Sets the logging list name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Logging commands that can use lists are the following:

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

Possible values for the *event_class* include the following:

- **auth**—User authentication.
- **bridge**—Transparent firewall.
- **ca**—PKI certificate authority.
- **config**—Command interface.
- **eap**—Extensible Authentication Protocol (EAP). Logs the following types of events to support Network Admission Control: EAP session state changes, EAP status query events, and a hexadecimal dump of EAP header and packet contents.
- **eapoudp**—Extensible Authentication Protocol (EAP) over UDP. Logs EAPoUDP events to support Network Admission Control, and generates a complete record of EAPoUDP header and packet contents.
- **email**—Email proxy.
- **ha**—Failover.
- **ids**—Intrusion detection system.
- **ip**—IP stack.
- **nac**—Network Admission Control. Logs the following types of events: initializations, exception list matches, ACS transactions, clientless authentications, default ACL applications, and revalidations.
- **np**—Network processor.
- **ospf**—OSPF routing.
- **rip**—RIP routing.
- **session**—User session.
- **snmp**—SNMP.
- **sys**—System.
- **vpn**—IKE and IPSec.
- **vpnc**—VPN client.
- **vpnfo**—VPN failover.
- **vpnlb**—VPN load balancing.

Examples

The following example shows how to use the logging list command:

```
hostname(config)# logging list my-list 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

The preceding example states that syslog messages that match the criteria specified will be sent to the logging buffer. The criteria specified in this example are:

- Syslog message IDs that fall in the range of 100100 to 100110
- All syslog messages with critical level or higher (emergency, alert, or critical)
- All VPN class syslog messages with warning level or higher (emergency, alert, critical, error, or warning)

If a syslog message satisfies any one of these conditions, it is logged to the buffer.

Note When you design list criteria, the criteria can specify overlapping sets of messages. Syslog messages matching more than one set of criteria are logged normally.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging mail

To enable the adaptive security appliance to send syslog messages by e-mail and to determine which messages are sent by e-mail, use the **logging mail** command in global configuration mode. To disable e-mailing of syslog messages, use the **no** form of this command.

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the e-mail recipient. For information about creating lists, see the **logging list** command.

Defaults

Logging to e-mail is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

E-mailed syslog messages appear in the subject line of the e-mails sent.

Examples

To set up the adaptive security appliance to send syslog messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the e-mail address from which e-mailed syslog messages appear to come.
logging list	Creates a reusable list of message selection criteria.
logging recipient-address	Specifies the e-mail address to which e-mailed syslog messages are sent.
smtp-server	Configures an SMTP server.

logging message

To specify the logging level of a syslog message, use the **logging message** command with the **level** keyword in global configuration mode. To reset the logging level of a message to its default level, use the **no** form of this command. To prevent the adaptive security appliance from generating a particular syslog message, use the **no** form of the **logging message** command (without the **level** keyword) in global configuration mode. To let the adaptive security appliance generate a particular syslog message, use the **logging message** command (without the **level** keyword). These two versions of the **logging message** command can be used in parallel. See the "Examples" section that follows.

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

Syntax Description

level *level*	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
syslog_id	The ID of the syslog message that you want to enable or disable or whose severity level you want to modify. To look up the default level of a message, use the **show logging** command or see the *Cisco ASA 5500 Series System Log Messages*.

Defaults

By default, all syslog messages are enabled and the severity levels of all messages are set to their default levels.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can use the **logging message** command for two purposes:

- To control whether a message is enabled or disabled.
- To control the severity level of a message.

You can use the **show logging** command to determine the level currently assigned to a message and whether the message is enabled.

Examples

The series of commands in the following example illustrate the use of the **logging message** command to control both whether a message is enabled and the severity level of the messages:

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

Command	Description
clear configure logging	Clears all logging configuration or message configuration only.
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging monitor

To enable the adaptive security appliance to display syslog messages in SSH and Telnet sessions, use the **logging monitor** command in global configuration mode. To disable the display of syslog messages in SSH and Telnet sessions, use the **no** form of this command.

logging monitor [*logging_list* | *level*]

no logging monitor

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the SSH or Telnet session. For information about creating lists, see the **logging list** command.

Defaults

The adaptive security appliance does not display syslog messages in SSH and Telnet sessions by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging monitor** command enables syslog messages for all sessions in the current context; however, in each session, the **terminal** command controls whether syslog messages appear in that session.

Examples

The following example shows how to enable the display of syslog messages in console sessions. The use of the **errors** keyword indicates that messages of severity levels 0, 1, 2, and 3 should display in SSH and Telnet sessions. The **terminal** command enables the messages to appear in the current session:

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.
terminal	Sets terminal line parameters.

logging permit-hostdown

To make the status of a TCP-based syslog server irrelevant to new user sessions, use the **logging permit-hostdown** command in global configuration mode. To cause the adaptive security appliance to deny new user sessions when a TCP-based syslog server is unavailable, use the **no** form of this command.

logging permit-hostdown

no logging permit-hostdown

Syntax Description

This command has no arguments or keywords.

Defaults

By default, if you have enabled logging to a syslog server that uses a TCP connection, the adaptive security appliance does not allow new network access sessions when the syslog server is unavailable for any reason.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you are using TCP as the logging transport protocol for sending messages to a syslog server, the adaptive security appliance denies new network access sessions as a security measure if the adaptive security appliance is unable to reach the syslog server. You can use the **logging permit-hostdown** command to remove this restriction.

Examples

The following example makes the status of TCP-based syslog servers irrelevant to whether the adaptive security appliance permits new sessions. When the **logging permit-hostdown** command includes in its output the **show running-config logging** command, the status of TCP-based syslog servers is irrelevant to new network access sessions.

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging trap	Enables logging to syslog servers.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging queue

To specify how many syslog messages the adaptive security appliance may hold in its queue before processing them according to the logging configuration, use the **logging queue** command in global configuration mode. To reset the logging queue size to the default of 512 messages, use the **no** form of this command.

logging queue *queue_size*

no logging queue *queue_size*

Syntax Description

queue_size	The number of syslog messages permitted in the queue used for storing syslog messages before processing them. Valid values are from 0 to 8192 messages, depending on the platform type. If the logging queue is set to zero, the queue will be the maximum configurable size (8192 messages), depending on the platform. On the ASA-5505, the maximum queue size is 1024, On the ASA-5510, it is 2048, and on all other platforms, it is 8192 ..

Defaults

The default queue size is 512 messages.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.
8.2(2)	The maximum queue size for the ASA 5505 has been set to 1024 messages. The maximum queue size for the ASA 5510 has been set to 2048 messages.

Usage Guidelines

When traffic is so heavy that the queue fills up, the adaptive security appliance may discard messages. On the ASA-5505, the maximum queue size is 1024. On the ASA-5510, it is 2048. On all other platforms, it is 8192 .

Examples

The following example shows how to display the output of the **logging queue** and **show logging queue** commands:

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

In this example, the **logging queue** command is set to 0, which means that the queue is set to the maximum of 8192. The syslog messages in the queue are processed by the adaptive security appliance in the manner dictated by the logging configuration, such as sending syslog messages to mail recipients, saving them to flash memory, and so forth.

The output of this example **show logging queue** command shows that 5 messages are queued, 3513 messages was the largest number of messages in the queue at one time since the adaptive security appliance was last booted, and that 1 message was discarded. Even though the queue was set for unlimited messages, the message was discarded because no block memory was available to add the message to the queue.

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging rate-limit

To limit the rate at which syslog messages are generated, use the **logging rate-limit** command in privileged EXEC mode. To disable rate limiting, use the **no** form of this command in privileged EXEC mode.

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

[no] logging rate-limit [**unlimited** | {*num* [*interval*]}} **message** *syslog_id*] **level** *severity_level*

Syntax Description

interval	(Optional) Time interval (in seconds) to use for measuring the rate at which messages are generated. The valid range of values for *interval* is 0 through 2147483647.
level *severity_level*	Applies the set rate limits on all syslog messages that belong to a certain severity level. All syslog messages at a specified severity level are rate-limited individually. The valid range for *severity_level* is 1 through 7.
message	Suppresses reporting of this syslog message.
num	Number of syslog messages that can be generated during the specified time interval. The valid range of values for *num* is 0 through 2147483647.
syslog_id	ID of the syslog message to be suppressed. The valid range of values is 100000-999999.
unlimited	Disables rate limiting, which means that there is no limit on the logging rate.

Defaults

The default setting for *interval* is 1.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The syslog message severity levels are as follows:

- 0—System is unusable
- 1—Immediate action needed
- 2—Critical Conditions
- 3—Error Conditions

- 4—Warning Conditions
- 5—Normal but significant conditions
- 6—Informational Messages
- 7—Debugging Messages

Examples

To limit the rate of syslog message generation, you can enter a specific message ID. The following example shows how to limit the rate of syslog message generation using a specific message ID and time interval:

```
hostname(config)# logging rate-limit 100 600 message 302020
```

This example suppresses syslog message 302020 from being sent to the host after the rate limit of 100 is reached in the specified interval of 600 seconds.

To limit the rate of syslog message generation, you can enter a specific severity level. The following example shows how to limit the rate of syslog message generation using a specific severity level and time interval.

```
hostname(config)# logging rate-limit 1000 600 level 6
```

This example suppresses all syslog messages under severity level 6 to the specified rate limit of 1000 in the specified time interval of 600 seconds. Each syslog message in severity level 6 has a rate limit of 1000.

Related Commands

Command	Description
clear running-config logging rate-limit	Resets the logging rate limit setting to its default.
show logging	Shows the messages currently in the internal buffer or to shows logging configuration settings.
show running-config logging rate-limit	Shows the current logging rate limit setting.

logging recipient-address

To specify the receiving e-mail address for syslog messages sent by the adaptive security appliance, use the **logging recipient-address** command in global configuration mode. To remove the receiving e-mail address, use the **no** form of this command. You can configure up to 5 recipient addresses. If you want, each recipient address can have a different message level than that specified by the **logging mail** command.

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

Syntax Description

address	Specifies recipient e-mail address when sending syslog messages by e-mail.
level	Indicates that a severity level follows.
level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages. **Note** We do not recommend using a severity level greater than 3 with the **logging recipient-address** command. Higher severity levels are likely to cause dropped syslog messages because of buffer overflow. The message severity level specified by a **logging recipient-address** command overrides the message severity level specified by the **logging mail** command. For example, if a **logging recipient-address** command specifies a severity level of 7 but the **logging mail** command specifies a severity level of 3, the adaptive security appliance sends all messages to the recipient, including those of severity levels 4, 5, 6, and 7.

Defaults

The default value is set to the errors logging level.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Sending syslog messages by e-mail is enabled by the **logging mail** command.

You can configure up to 5 **logging recipient-address** commands. Each command can have a different severity level than the others. This command is useful when you want more urgent messages to go to a larger number of recipients than less urgent messages are sent to.

Examples

To set up the adaptive security appliance to send syslog messages by e-mail, use the following criteria:

- Send messages that are critical, alerts, or emergencies.
- Send messages using ciscosecurityappliance@example.com as the sender address.
- Send messages to admin@example.com.
- Send messages using SMTP, the primary servers pri-smtp-host, and secondary server sec-smtp-host.

Enter the following commands:

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

Related Commands

Command	Description
logging enable	Enables logging.
logging from-address	Specifies the e-mail address from which syslog messages appear to come.
logging mail	Enables the adaptive security appliance to send syslog messages by e-mail and determines which messages are sent by e-mail.
smtp-server	Configures an SMTP server.
show logging	Displays the enabled logging options.

logging savelog

To save the log buffer to flash memory, use the **logging savelog** command in privileged EXEC mode.

logging savelog [*savefile*]

Syntax Description

savefile	(Optional) Saved flash memory file name. If you do not specify the file name, the adaptive security appliance saves the log file using a default time-stamp format, as follows: LOG-*YYYY-MM-DD-HHMMSS*.TXT where *YYYY* is the year, *MM* is the month, *DD* is the day of the month, and *HHMMSS* is the time in hours, minutes, and seconds.

Defaults

The defaults are as follows:

- Buffer size is 4 KB.
- Minimum free flash memory is 3 MB.
- Maximum flash memory allocation for buffer logging is 1 MB.
- The default log file name is described in the “Syntax Description” section.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Before you can save the log buffer to flash memory, you must enable logging to the buffer; otherwise, the log buffer never has data to be saved to flash memory. To enable logging to the buffer, use the **logging buffered** command.

Note The **logging savelog** command does not clear the buffer. To clear the buffer, use the **clear logging buffer** command.

Examples

The following example enables logging and the log buffer, exits global configuration mode, and saves the log buffer to flash memory using the file name, latest-logfile.txt:

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

Related Commands

Command	Description
clear logging buffer	Clears the log buffer of all system log messages it contains.
copy	Copies a file from one location to another, including to a TFTP or FTP server.
delete	Deletes a file from the disk partition, such as saved log files.
logging buffered	Enables logging to the log buffer.
logging enable	Enables logging.

logging standby

To enable the failover standby adaptive security appliance to send the syslog messages of this adaptive security appliance to logging destinations, use the **logging standby** command in global configuration mode. To disable syslog messaging and SNMP logging, use the **no** form of this command.

logging standby

no logging standby

Syntax Description

This command has no arguments or keywords.

Defaults

The **logging standby** command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can enable **logging standby** to ensure that the syslog messages of the failover standby adaptive security appliance stay synchronized if failover occurs.

Note Using the **logging standby** command causes twice as much traffic on shared logging destinations, such as syslog servers, SNMP servers, and FTP servers.

Examples

The following example enables the adaptive security appliance to send syslog messages to the failover standby adaptive security appliance. The output of the **show logging** command reveals that this feature is enabled:

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
```

```
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

Related Commands

Command	Description
failover	Enables the failover feature.
logging enable	Enables logging.
logging host	Defines a syslog server.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging timestamp

To specify that syslog messages should include the date and time that the messages was generated, use the **logging timestamp** command in global configuration mode. To remove the date and time from syslog messages, use the **no** form of this command.

logging timestamp

no logging timestamp

Syntax Description

This command has no arguments or keywords.

Defaults

The adaptive security appliance does not include the date and time in syslog messages by default.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logging timestamp** command makes the adaptive security appliance include a timestamp in all syslog messages.

Examples

The following example enables the inclusion of timestamp information in all syslog messages:

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

logging trap

To specify which syslog messages the adaptive security appliance sends to a syslog server, use the **logging trap** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

logging trap [*logging_list* | *level*]

no logging trap

Syntax Description

level	Sets the maximum severity level for syslog messages. For example, if you set the severity level to 3, then the adaptive security appliance generates syslog messages for severity levels 3, 2, 1, and 0. You can specify either the number or the name, as follows: • **0** or **emergencies**—System is unusable. • **1** or **alerts**—Immediate action needed. • **2** or **critical**—Critical conditions. • **3** or **errors**—Error conditions. • **4** or **warnings**—Warning conditions. • **5** or **notifications**—Normal but significant conditions. • **6** or **informational**—Informational messages. • **7** or **debugging**—Debugging messages.
logging_list	Specifies the list that identifies the messages to send to the syslog server. For information about creating lists, see the **logging list** command.

Defaults

No default syslog message trap is defined.

Command Modes

The following table shows the modes in which you can enter the command.

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If you are using TCP as the logging transport protocol, the adaptive security appliance denies new network access sessions as a security measure if the adaptive security appliance is unable to reach the syslog server, if the syslog server is misconfigured, or if the disk is full.

UDP-based logging does not prevent the adaptive security appliance from passing traffic if the syslog server fails.

Examples

The following example shows how to send syslog messages of severity levels 0, 1, 2, and 3 to a syslog server that resides on the inside interface and uses the default protocol and port number.

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

Related Commands

Command	Description
logging enable	Enables logging.
logging host	Defines a syslog server.
logging list	Creates a reusable list of message selection criteria.
show logging	Displays the enabled logging options.
show running-config logging	Displays the logging-related portion of the running configuration.

login

To log into privileged EXEC mode using the local user database (see the username command) or to change user names, use the **login** command in user EXEC mode.

login

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

From user EXEC mode, you can log in to privileged EXEC mode as any username in the local database using the **login** command. The **login** command is similar to the **enable** command when you have enable authentication turned on (see the **aaa authentication console** command). Unlike enable authentication, the **login** command can only use the local username database, and authentication is always required with this command. You can also change users using the **login** command from any CLI mode.

To allow users to access privileged EXEC mode (and all commands) when they log in, set the user privilege level to 2 (the default) through 15. If you configure local command authorization, then the user can only enter commands assigned to that privilege level or lower. See the **aaa authorization command** for more information.

Caution If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged EXEC mode, you should configure command authorization. Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged EXEC mode.

Examples

The following example shows the prompt after you enter the **login** command:

```
hostname> login
```

```
Username:
```

Related Commands

Command	Description
aaa authorization command	Enables command authorization for CLI access.
aaa authentication console	Requires authentication for console, Telnet, HTTP, SSH, or **enable** command access.
logout	Logs out of the CLI.
username	Adds a user to the local database.

login-button

To customize the Login button of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **login-button** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default login button text is "Login".

The default login button style is:

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the Login button with the text “OK”:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-button text OK
```

Related Commands

Command	Description
login-title	Customizes the title of the WebVPN page login box.
group-prompt	Customizes the group prompt of the WebVPN page login box.
password-prompt	Customizes the password prompt of the WebVPN page login box.
username-prompt	Customizes the username prompt of the WebVPN page login box.

login-message

To customize the login message of the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **login-message** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default login message is “Please enter your username and password”.

The default login message style is background-color:#CCCCCC;color:black.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

In the following example, the login message text is set to “username and password”:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-message text username and password
```

Related Commands

Command	Description
login-title	Customizes the title of the login box on the WebVPN page.
username-prompt	Customizes the username prompt of the WebVPN page login.
password-prompt	Customizes the password prompt of the WebVPN page login.
group-prompt	Customizes the group prompt of the WebVPN page login.

login-title

To customize the title of the login box on the WebVPN page displayed to WebVPN users, use the **login-title** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

Syntax Description

text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default login text is "Login".

The default HTML style of the login title is background-color: #666666; color: white.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example configures the login title style:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
bold
```

Related Commands

Command	Description
login-message	Customizes the login message of the WebVPN login page.
username-prompt	Customizes the username prompt of the WebVPN login page.
password-prompt	Customizes the password prompt of the WebVPN login page.
group-prompt	Customizes the group prompt of the WebVPN login page.

logo

To customize the logo on the WebVPN page displayed to WebVPN users when they connect to the security appliance, use the **logo** command from webvpn customization mode. To remove a logo from the configuration and reset the default (the Cisco logo), use the **no** form of this command.

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

Syntax Description

file	Indicates you are supplying a file containing a logo.
none	Indicates that there is no logo. Sets a null value, thereby disallowing a logo. Prevents inheriting a logo.
path	The path of the filename. The possible paths are disk0:, disk1:, or flash:
value	Specifies the filename of the logo. Maximum length is 255 characters, with no spaces. File type must be JPG, PNG, or GIF, and must be less than 100 KB.

Defaults

The default logo is the Cisco logo.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

If the filename you specify does not exist, an error message displays. If you remove a logo file but the configuration still points to it, no logo displays.

The filename cannot contain spaces.

Examples

In the following example, the file cisco_logo.gif contains a custom logo:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

Related Commands

Command	Description
title	Customizes the title of the WebVPN page.
page style	Customizes the WebVPN page using Cascading Style Sheet (CSS) parameters.

logout

To exit from the CLI, use the **logout** command in user EXEC mode.

logout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **logout** command lets you log out of the adaptive security appliance. You can use the **exit** or **quit** commands to go back to unprivileged mode.

Examples

The following example shows how to log out of the adaptive security appliance:

```
hostname> logout
```

Related Commands

Command	Description
login	Initiates the log-in prompt.
exit	Exits an access mode.
quit	Exits configuration or privileged mode.

logout-message

To customize the logout message of the WebVPN logout screen that is displayed to WebVPN users when they logout from WebVPN service, use the **logout-message** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default logout message text is “Goodbye”.

The default logout message style is background-color:#999999;color:black.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
WebVPN customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example configures the logout message style:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style:
italic; font-weight: bold
```

Related Commands

Command	Description
logout-title	Customizes the logout title of the WebVPN page.
group-prompt	Customizes the group prompt of the WebVPN page login box.
password-prompt	Customizes the password prompt of the WebVPN page login box.
username-prompt	Customizes the username prompt of the WebVPN page login box.