

Embedded Event Manager

This chapter describes how to configure the Embedded Event Manager (EEM).

- Information About the EEM, page 50-1
- Licensing Requirements for the EEM, page 50-2
- Guidelines and Limitations, page 50-3
- Creating an Event Manager Applet, page 50-3
- Configuring a Syslog Event, page 50-4
- Configuring a Watchdog (Periodic) Timer Event, page 50-4
- Configuring a Countdown (One-shot) Timer Event, page 50-4
- Configuring an Absolute (Once-A-Day) Timer Event, page 50-5
- Configuring a Crash Event, page 50-5
- Configuring an Action on an Event Manager Applet, page 50-5
- Configuring Destinations for Output from an Action, page 50-6
- Running an Event Manager Applet, page 50-7
- Invoking an Event Manager Applet Manually, page 50-7
- Configuration Examples for the EEM, page 50-8
- Monitoring the EEM, page 50-8
- Feature History for the EEM, page 50-9

Information About the EEM

The EEM feature enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions.

- Supported Events, page 50-2
- Configuring Actions, page 50-2
- Configuring Output Destinations, page 50-2

Supported Events

The EEM supports the following events:

- Syslog—The ASA uses syslog message IDs to identify syslog messages that trigger an event manager applet. You may configure multiple syslog events, but the syslog message IDs may not overlap within a single event manager applet.
- Timers—You may use timers to trigger events. You may configure each timer only once for each event manager applet. Each event manager applet may have up to three timers. The three types of timers are the following:
  - Watchdog (periodic) timers trigger an event manager applet after the specified time period following the completion of the applet's actions and restart automatically.
  - Countdown (one-shot) timers trigger an event manager applet once after the specified time period and do not restart unless they are removed, then re-added.
  - Absolute (once-a-day) timers cause an event to occur once a day at a specified time, and restart automatically. The time-of-day format is in hh:mm:ss.

  You may configure only one timer event of each type for each event manager applet.
- None—The none event is triggered when you run an event manager applet manually using the CLI or ASDM.
- Crash—The crash event is triggered when the ASA crashes. Regardless of the value of the **output** command, the **action** commands are directed to the crashinfo file. The output is generated before the **show tech** command.

Configuring Actions

When an event manager applet is triggered, the actions on the event manager applet are performed. Each action has a number that is used to specify the sequence of the actions. The sequence number must be unique within an event manager applet. You may configure multiple actions for an event manager applet. The commands are typical CLI commands, such as **show blocks**.

Configuring Output Destinations

- You may send the output from the actions to a specified location using the **output** command. Only one output value may be enabled at any one time. The default value is **output none**. This value discards any output from the **action** commands. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled.

Licensing Requirements for the EEM

The following table shows the licensing requirements for this feature:

Model	License Requirement
ASAv	Standard or Premium License.
All other models	Base License.

Guidelines and Limitations

This section includes the guidelines and limitations for this feature.

Context Mode Guidelines

Supported in single mode only. Not suported in multiple context mode.

Firewall Mode Guidelines

Supported in routed and transparent firewall modes.

Additional Guidelines

- During a crash, the state of the ASA is generally unknown. Some commands may not be safe to run during this condition.
- The name of an event manager applet may not contain spaces.
- You cannot modify the None event and Crashinfo event parameters.
- Performance may be affected because syslog messages are sent to the EEM for processing.
- The default output is **output none** for each event manager applet. To change this setting, you must enter a different output value.
- You may have only one output option defined for each event manager applet.

Creating an Event Manager Applet

To create an event manager applet that links events with actions and output, perform the following steps:

	Command	Purpose
Step 1	**event manager applet** *name* **Example:** `ciscoasa(config)# event manager applet exampleapplet1`	Creates an event manager applet and enters event manager applet configuration mode. The *name* argument may be up to 32 alphanumeric characters long. Spaces are not allowed. To remove an event manager applet, enter the **no event manager applet** command.
Step 2	**description** *text* **Example:** `ciscoasa(config-applet)# description applet1example`	Describes an event manager applet. The *text* argument may be up to 256 characters long. You may include spaces in description text if it is placed within quotes.

Configuring a Syslog Event

To configure a syslog event, enter the following command:

Command	Purpose
event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*] **Example:** `ciscoasa(config-applet)# event syslog id 106201`	Identifies a single syslog message or a range of syslog messages that trigger an event manager applet. The *nnnnnn* argument identifies the syslog message ID. The **occurs** *n* keyword-argument pair indicates the number of times that the syslog message must occur for an event manager applet to be invoked. The default is 1 occurrence every 0 seconds. Valid values are from 1 - 4294967295. The **period** *seconds* keyword-argument pair indicates the number of seconds in which the event must occur, and limits how frequently an event manager applet is invoked to at most once in the configured period. Valid values are from 0 - 604800. A value of 0 means that no period is defined. To remove a syslog message or range of syslog messages, enter the **no event syslog id** command.

Configuring a Watchdog (Periodic) Timer Event

To configure a watchdog (periodic) timer event, enter the following command:

Command	Purpose
event timer watchdog time *seconds* **Example:** `ciscoasa(config-applet)# event timer watchdog time 30`	Causes an event to occur once per configured period and restart automatically. The number of seconds may range from 1 - 604800. To remove a watchdog timer event, enter the **no event timer watchdog time** command.

Configuring a Countdown (One-shot) Timer Event

To configure a countdown (one-shot) timer event, enter the following command:

Command	Purpose
event timer countdown time *seconds* **Example:** `ciscoasa(config-applet)# event timer countdown time 60`	Causes an event to occur once and not restart unless it is removed, then re-added. The number of seconds may range from 1 - 604800. **Note** This timer reruns when you reboot if it is the startup configuration. To remove a countdown timer event, enter the **no event timer watchdog time** command.

Configuring an Absolute (Once-A-Day) Timer Event

To configure an absolute (once-a-day) timer event, enter the following command:

Command	Purpose
event timer absolute time *hh:mm:ss* **Example:** `ciscoasa(config-applet)# event timer absolute time 10:30:20`	Causes an event to occur once a day at a specified time and restart automatically. The time-of-day format is in hh:mm:ss. The time range is from 00:00:00 (midnight) to 23:59:59. To remove an absolute timer event, enter the **no event timer absolute time** command.

Configuring a Crash Event

To configure a crash event, enter the following command:

Command	Purpose
event crashinfo **Example:** `ciscoasa(config-applet)# event crashinfo`	Triggered when the ASA crashes. Regardless of the value of the **output** command, the **action** commands are directed to the crashinfo file. The output is generated before the **show tech** command. To remove a crash event, enter the **no event crashinfo** command.

Configuring an Action on an Event Manager Applet

To configure an action on an event manager applet, enter the following command:

Command	Purpose
action *n* **cli command** "*command*" **Example:** `ciscoasa(config-applet)# action 1 cli command "show version"`	Configures an action on an event manager applet. The *n* option is an action ID. Valid IDs range from 0 - 4294967295. The value of the *command* option must be in quotes; otherwise, an error occurs if the command consists of more than one word. The command runs in global configuration mode as a user with privilege level 15 (the highest). The command may not accept any input, because it is disabled. Use the **noconfirm** option if the command has it available. To remove the configured action, enter the **no action** *n* command.

Configuring Destinations for Output from an Action

To configure specific destinations for sending output from an action, enter one of the following commands:

None Option

Command	Purpose
output none **Example:** `ciscoasa(config-applet)# output none`	Discards any output from the **action** commands, which is the default setting.

Console Option

Command	Purpose
output console **Example:** `ciscoasa(config-applet)# output console`	Sends the output of the **action** commands to the console. **Note** Running this command affects performance. To remove the console as an output destination, enter the **no output console** command.

New File Option

Command	Purpose
output file new **Example:** `ciscoasa(config-applet)# output file new`	Sends the output of the **action** commands to a new file for each event manager applet that is invoked. The filename has the format of eem-*applet-timestamp*.log, in which *applet* is the name of the event manager applet and *timestamp* is a dated timestamp in the format of YYYYMMDD-hhmmss. To remove the new file as an output destination, enter the **no output file new** command.

New Set of Rotated Files Option

Command	Purpose
output file rotate *n* **Example:** `ciscoasa(config-applet)# output file rotate 50`	Creates a set of files that are rotated. When a new file is to be written, the oldest file is deleted, and all subsequent files are renumbered before the first file is written. The newest file is indicated by 0, and the oldest file is indicated by the highest number (*n*-1). The *n* option is the rotate value. Valid values range from 2 - 100. The filename format is eem-*applet-x*.log, in which *applet* is the name of the applet, and *x* is the file number. To remove the file rotation, enter the **no output file rotate** command.

Single Overwritten File Option

Command	Purpose
output file overwrite *filename* **Example:** `ciscoasa(config-applet)# output file overwrite examplefile1`	Writes the **action** command output to a single file, which is overwritten every time. The *filename* argument is a local (to the ASA) filename. This command may also use FTP, TFTP, and SMB targeted files. To remove the overwrite action, enter the **no output file overwrite** command.

Single Appended File Option

Command	Purpose
output file append *filename* **Example:** `ciscoasa(config-applet)# output file append examplefile1`	Writes the **action** command output to a single file, but that file is appended to every time. The *filename* argument is a local (to the ASA) filename. To remove the append action, enter the **no output file append** command.

Running an Event Manager Applet

To run an event manager applet, enter the following command:

Command	Purpose
event manager run *applet* **Example:** `ciscoasa# event manager run exampleapplet1`	Runs an event manager applet that has been configured with the **event none** command. If you run an event manager applet that has not been configured with the **event none** command, an error occurs. The *applet* argument is the name of the event manager applet.

Invoking an Event Manager Applet Manually

To invoke an event manager applet manually, enter the following command:

Command	Purpose
event none **Example:** `ciscoasa(config-applet)# event none`	Invokes an event manager applet manually. To remove the manual invocation of an event manager applet, enter the **no event none** command.

Configuration Examples for the EEM

The following example shows an event manager applet that records block leak information every hour and writes the output to a rotating set of log files, keeping a day's worth of logs:

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description “Log block usage”
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command “show blocks old”
```

The following example shows an event manager applet that reboots the ASA every day at 1 am, saving the configuration as needed:

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description “Reboot every night”
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command “reload save-config noconfirm”
```

The following example shows event manager applets that disable the given interface between midnight and 3 am.

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description “Disable the interface at midnight”
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command “interface GigabitEthernet 0/0”
ciscoasa(config-applet)# action 2 cli command “shutdown”
ciscoasa(config-applet)# action 3 cli command “write memory”

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description “Enable the interface at 3am”
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command “interface GigabitEthernet 0/0”
ciscoasa(config-applet)# action 2 cli command “no shutdown”
ciscoasa(config-applet)# action 3 cli command “write memory”
```

Monitoring the EEM

To monitor the EEM, enter one of the following commands at the ASA CLI or use the CLI tool in ASDM by choosing **Tools > Command Line Interface**:

Command	Purpose
clear configure event manager	Removes the event manager running configuration.
clear configure event manager applet *appletname*	Removes the named event manager applet from the configuration.
show counters protocol eem	Shows the counters for the event manager.
show event manager	Shows information about the configured event manager applets, including hit counts and when the event manager applets were last invoked.
show running-config event manager	Shows the running configuration of the event manager.

Feature History for the EEM

Table 50-1 lists each feature change and the platform release in which it was implemented.

Table 50-1 Feature History for the EEM

Feature Name	Platform Releases	Feature Information
Embedded Event Manager (EEM)	9.2(1)	The EEM feature enables you to debug problems and provides general purpose logging for troubleshooting. There are two components: events to which the EEM responds or listens, and event manager applets that define actions as well as the events to which the EEM responds. You may configure multiple event manager applets to respond to different events and perform different actions. We introduced or modified the following commands: **event manager applet**, **description**, **event syslog id**, **event none**, **event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}, **event crashinfo**, **action cli command**, **output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}, **show running-config event manager**, **event manager run**, **show event manager**, **show counters protocol eem**, **clear configure event manager**, **debug event manager**, **debug menu eem**.