



Configuring the Embedded Event Manager

This chapter describes how to configure the EEM to detect and handle critical events on a device.

This chapter includes the following sections:

- [Information About EEM, page 7-1](#)
- [Licensing Requirements for EEM, page 7-6](#)
- [Prerequisites for EEM, page 7-6](#)
- [Guidelines and Limitations, page 7-6](#)
- [Default Settings, page 7-7](#)
- [Configuring EEM, page 7-7](#)
- [Verifying the EEM Configuration, page 7-15](#)
- [Configuration Examples for EEM, page 7-15](#)
- [Additional References, page 7-16](#)
- [Feature History for EEM, page 7-16](#)

Information About EEM

Embedded Event Manager monitors events that occur on your device and takes action to recover or troubleshoot these events, based on your configuration.

This section includes the following topics:

- [EEM Overview, page 7-2](#)
- [Policies, page 7-2](#)
- [Event Statements, page 7-3](#)
- [Action Statements, page 7-4](#)
- [VSH Script Policies, page 7-5](#)
- [Environment Variables, page 7-5](#)
- [High Availability, page 7-6](#)

EEM Overview

EEM consists of three major components:

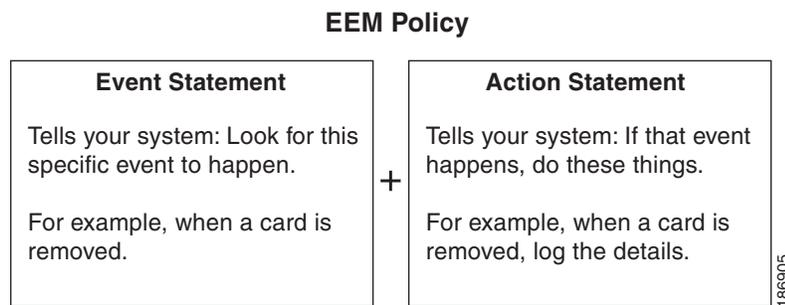
- Event statements—Events to monitor from another Cisco NX-OS component that may require some action, workaround, or notification.
- Action statements—Actions that EEM can take, such as sending an e-mail, or disabling an interface, to recover from an event.
- Policies—A combination of an event statement and an action statement. When the specified event occurs, the configured action is executed.

Policies

An EEM policy consists of an event statement and one or more action statements. The event statement defines the event to look for as well as the filtering characteristics for the event. The action statement defines the action EEM takes when the event occurs.

Figure 7-1 shows the two basic statements in an EEM policy.

Figure 7-1 EEM Policy Statements



You can configure EEM policies using the CLI or using a VSH script.



Note

EEM policy matching is not supported on MDS switches.

EEM maintains event logs on the supervisor.

Cisco NX-OS has a number of preconfigured system policies. These system policies define many common events and actions for the device. System policy names begin with two underscore characters (__).

The following are some of the preconfigured system policies available in Cisco MDS 9000 Series Switches and all the three policies are over-ridable:

- Zone
 - `__zone_dbsize_max_per_vsan`: Syslog warning when Zone database size exceeds the maximum limit for a vsan.
 - `__zone_members_max_per_sw`: Syslog warning when Zone member count exceeds the maximum limit for the switch.
 - `__zone_zones_max_per_sw`: Syslog warning when Zone count exceeds the maximum limit for the switch.

- `__zone_zonesets_max_per_sw` : Syslog warning when Zoneset count exceeds the maximum limit for the switch.
- Fabric Login (FLOGI)
 - `__flogi_fcids_max_per_switch`: Syslog warning when the number of flogis in the switch exceeds maximum limit.
 - `__flogi_fcids_max_per_module`: Syslog warning when the number of flogis in the module exceeds maximum limit.
 - `__flogi_fcids_max_per_intf`: Syslog warning when the number of flogis on the interface exceeds maximum limit.

**Note**

During an In Service Software Upgrade (ISSU), EEM syslog messages for FLOGI are not printed in the terminal.

- Fibre Channel Name Server (FCNS)
 - `__fcns_entries_max_per_switch` : Configuring max limit for Name server entries verified across all VSANs per switch.

Action: Display a syslogUser

**Note**

User should not configure an event for a different component's policy.

You can create user policies to suit your network. Actions defined by the user policies are executed along with the actions defined by the system policies. To configure a user policy, see the [“Defining a User Policy Using the CLI” section on page 7-7](#).

You can also override some system policies. The override policies replace the system policies. You can override the event or the actions.

Use the **show event manager system-policy** command to view the preconfigured system policies and determine which policies that you can override.

To configure an overriding policy, see the [“Overriding a Policy” section on page 7-13](#).

**Note**

- You should use the **show running-config eem** command to check the configuration of each policy. An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.
- Your override policy should always include an event statement. An override policy without an event statement overrides all possible events in the system policy.

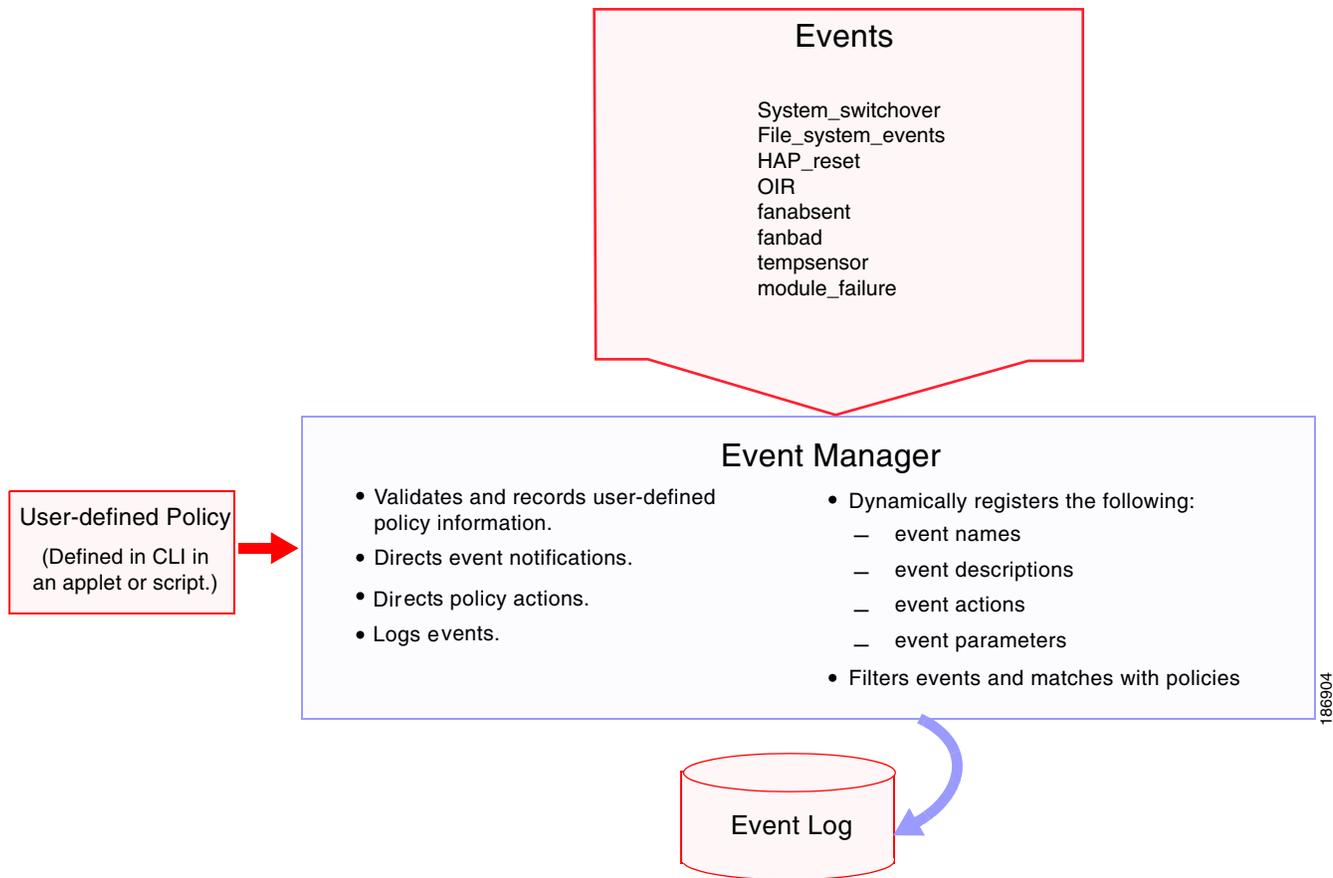
Event Statements

An event is any device activity for which some action, such as a workaround or a notification, should be taken. In many cases, these events are related to faults in the device such as when an interface or a fan malfunctions.

EEM defines event filters so only critical events or multiple occurrences of an event within a specified time period trigger an associated action.

Figure 7-2 shows events that are handled by EEM.

Figure 7-2 EEM Overview



Event statements specify the event that triggers a policy to run. You can configure only one event statement per policy.

EEM schedules and runs policies on the basis of event statements. EEM examines the event and action commands and runs them as defined.

Action Statements

Action statements describe the action triggered by a policy. Each policy can have multiple action statements. If no action is associated with a policy, EEM still observes events but takes no actions.

EEM supports the following actions in action statements:

- Execute any CLI commands.
- Update a counter.
- Log an exception.
- Force the shut down of any module.
- Reload the device.

- Shut down specified modules because the power is over budget.
- Generate a syslog message.
- Generate a Call Home event.
- Generate an SNMP notification.
- Use the default action for the system policy.

**Note**

If you want to allow the triggered event to process the default actions also, you must explicitly configure an EEM action with **event-default** or **policy-default**, based on the type of policy. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy. If the event-default action statement is not added, EEM will not allow the CLI command to execute.

**Note**

Verify that your action statements within your user policy or overriding policy do not negate each other or adversely affect the associated system policy.

VSH Script Policies

You can also write policies in a VSH script, using a text editor. These policies have an event statement and action statement(s) just as other policies, and these policies can either augment or override system policies. After you write your script policy, copy it to the device and activate it. To configure a policy in a script, see the [“Defining a Policy Using a VSH Script” section on page 7-12](#).

Environment Variables

You can define environment variables for EEM that are available for all policies. Environment variables are useful for configuring common values that you can use in multiple policies. For example, you can create an environment variable for the IP address of an external e-mail server.

You can use an environment variable in action statements by using the parameter substitution format.

[Example 7-1](#) shows a sample action statement to force a module 1 shutdown, with a reset reason of “EEM action.”

Example 7-1 Action Statement

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason "EEM action"
```

If you define an environment variable for the shutdown reason, called default-reason, you can replace that reset reason with the environment variable, as shown in [Example 7-2](#).

Example 7-2 Action Statement with Environment Variable

```
switch (config-eem-policy)# action 1.0 forceshut module 1 reset-reason $default-reason
```

You can reuse this environment variable in any policy. For more information on environment variables, see the [“Defining an Environment Variable” section on page 7-14](#).

EEM Event Correlation

Beginning with Cisco NX-OS Release 5.2, you can trigger an EEM policy based on a combination of events. First, you use the **tag** keyword to create and differentiate multiple events in the EEM policy. Then using a set of boolean operators (**and**, **or**, **andnot**), along with the count and time, you can define a combination of these events to trigger a custom action.

High Availability

Cisco NX-OS supports stateless restarts for EEM. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Licensing Requirements for EEM

The following table shows the licensing requirements for this feature:

| Product | License Requirement |
|---------|---|
| NX-OS | EEM requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. |

Prerequisites for EEM

EEM has the following prerequisites:

- You must have network-admin user privileges to configure EEM.

Guidelines and Limitations

EEM has the following configuration guidelines and limitations:

- Action statements within your user policy or overriding policy should not negate each other or adversely affect the associated system policy.
- If you want to allow the triggered event to process the default actions also, you must explicitly configure an EEM action with **event-default** or **policy-default**, based on the type of policy. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.
- An override policy that consists of an event statement and no action statement triggers no action and no notification of failures.

- An override policy without an event statement overrides all possible events in the system policy.
- When more than one event statement is included in an EEM policy, each event statement must have a **tag** keyword with a unique tag argument.
- Although multiple overriding is blocked at application-level (FCNS/zone/FLOGI), blank applets can be saved by overriding the system policy.

Default Settings

Table 7-1 lists the default settings for EEM parameters.

Table 7-1 Default EEM Parameters

| Parameters | Default |
|-----------------|---------|
| system policies | active |

Configuring EEM

This section includes the following topics:

- [Defining a User Policy Using the CLI, page 7-7](#)
- [Defining a Policy Using a VSH Script, page 7-12](#)
- [Registering and Activating a VSH Script Policy, page 7-13](#)
- [Overriding a Policy, page 7-13](#)

Defining a User Policy Using the CLI

You can define a user policy using the CLI.

Detailed Steps

To define a user policy using the CLI, follow these steps:

| | Command | Purpose |
|--------|--|--|
| Step 1 | <code>config t</code> | Enters configuration mode. |
| Step 2 | <code>event manager applet <i>applet-name</i></code> | Registers the applet with EEM and enters applet configuration mode. The <i>applet-name</i> can be any case-sensitive alphanumeric string up to 29 characters. |
| Step 3 | <code>description <i>policy-description</i></code> | (Optional) Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks. |
| Step 4 | <code>event <i>event-statement</i></code> | Configures the event statement for the policy. See the “ Configuring Event Statements ” section on page 7-8. |

| | Command | Purpose |
|--------|--|--|
| Step 5 | <code>tag tagname1 {and andnot or} tagname2 [{and andnot or} tagname3 [{and andnot or} tagname4]] happens occurs in seconds</code> | (Optional) Correlates multiple events in the policy. The range for <i>occurs</i> is from 1 to 4294967295. The range for <i>seconds</i> is from 0 to 4294967295 seconds. |
| Step 6 | <code>action action-statement</code> | Configures an action statement for the policy. See the “Configuring Action Statements” section on page 7-11. Repeat Step 5 for multiple action statements. |
| Step 7 | <code>show event manager policy internal name</code> | (Optional) Displays information about the configured policy. |
| Step 8 | <code>copy running-config startup-config</code> | (Optional) Saves this configuration change. |

Configuring Event Statements

Detailed Steps

To configure an event statement, use one the following commands in EEM configuration mode:

| Command | Purpose |
|--|---|
| <code>event cli [tag tag_name] match expression [count repeats time seconds]</code> | Triggers an event if you enter a CLI command that matches the regular expression. The <code>tag tag_name</code> keyword-argument pair identifies this specific event when multiple events are included in the policy. The <i>repeats</i> range is from 1 to 65000. The time range, in seconds, is from 0 to 4294967295, where 0 indicates no time limit. |
| <code>event counter name counter entry-val entry entry-op {eq ge gt le lt ne} [exit-val exit exit-op {eq ge gt le lt ne}]</code> | Triggers an event if the counter crosses the entry threshold (based on the entry operation—greater than, less than, and so on.) The event resets immediately. Optionally, you can configure the event to reset after the counter passes the exit threshold. The <i>counter</i> name can be any case-sensitive, alphanumeric string up to 28 characters. The <i>entry</i> and <i>exit</i> value ranges are from 0 to 2147483647. |
| <code>event fanabsent [fan number] time seconds</code> | Triggers an event if a fan is removed from the device for more than the configured time, in seconds. The <i>fan number</i> range is dependent on different switches (for example for 9513 switches the range is from 1 to 2, for 9506/9509 switches the range is 1). The <i>seconds</i> range is from 10 to 64000. |

| Command | Purpose |
|--|---|
| <code>event fanbad [fan number] time seconds</code> | Triggers an event if a fan fails for more than the configured time, in seconds. The fan <i>number</i> range is dependent on different switches (for example for 9513 switches the range is from 1 to 2, for 9506/9509 switches the range is 1). The <i>seconds</i> range is from 10 to 64000. |
| <code>event memory {critical minor severe}</code> | Triggers an event if a memory threshold is crossed. |
| <code>event module-failure type failure-type module {slot all} count repeats [time seconds]</code> | Triggers an event if a module experiences the failure type configured. The <i>slot</i> range is dependent on different switches (for example for 9513 switches the range is from 1 to 13, for 9509 switches the range is 1 to 9). The <i>repeats</i> range is from 0 to 4294967295. The <i>seconds</i> range is from 0 to 4294967295. |
| <code>event oir {fan module powersupply} {anyoir insert remove} [number]</code> | Triggers an event if the configured device element (fan, module, or power supply) is inserted or removed from the device. You can optionally configure a specific fan, module, or power supply number. The <i>number</i> range is as follows: <ul style="list-style-type: none"> • Fan number is dependent on different switches. • Module number is dependent on different switches. • Power supply number range is from 1 to 2. |
| <code>event policy-default count repeats [time seconds]</code> | Uses the event configured in the system policy. Use this option for overriding policies. The <i>repeats</i> range is from 1 to 65000. The <i>seconds</i> range is from 0 to 4294967295. |
| <code>event poweroverbudget</code> | Triggers an event if the power budget exceeds the capacity of the configured power supplies. |
| <code>event snmp oid oid get-type {exact next} entry-op {eq ge gt le lt ne} entry-val entry [exit-comb {and or}] exit-op {eq ge gt le lt ne} exit-val exit exit-time time polling-interval interval</code> | Triggers an event if the SNMP OID crosses the entry threshold (based on the entry operation—greater than, less than, and so on.) The event resets immediately, or optionally you can configure the event to reset after the counter passes the exit threshold. The OID is in dotted decimal notation. The <i>entry</i> and <i>exit</i> value ranges are from 0 to 18446744073709551615. The time range is from 0 to 2147483647. The interval range is from 1 to 2147483647. |

| Command | Purpose |
|--|---|
| <pre>event syslog {occurs occurs number pattern syslog pattern period time intervals priority syslog priority tag tag_name }</pre> | <p>Triggers an event based on a message logged in the syslog logfile.</p> <p><i>occurs occurs number</i>-Specifies the number of occurrences. The range is from 1 to 65000.</p> <p><i>pattern syslog pattern</i>-Specifies the syslog pattern. Normal regular expression pattern matching is used. The maximum size is 256 alphanumerical characters.</p> <p><i>period time intervals</i>-Specifies the maximum time interval between messages. The range is from 0 to 4294967295 seconds.</p> <p><i>priority syslog priority</i>-Specifies the syslog priority.</p> <ul style="list-style-type: none"> •alerts—Specifies the alert log message •critical—Specifies the critical log message •debugging—Specifies the debugging message •emergencies—Specifies the emergency log message •errors-Specifies the error log message •informational—Specifies the informational log message •notification—Specifies the notification log message •pattern—Specifies the pattern matching •warnings—Specifies the warning message <p><i>tag tag_name</i>-Specifies the tag name. Maximum size is 29 alphanumerical characters.</p> <p>The tag <i>tag_name</i> keyword argument pair identifies this specific event when multiple events are included in the policy.</p> |
| <pre>event temperature [module slot] [sensor number] threshold {any major minor}</pre> | <p>Triggers an event if the temperature sensor exceeds the configured threshold. The <i>slot</i> range is dependent on different switches. The <i>sensor range</i> is from 1 to 8 on MDS modules, but current MDS modules use the range from 1 to 3 only, some modules use the range from 1 to 2.</p> |

Configuring Action Statements

Detailed Steps

To configure action statements, use the following commands in EEM configuration mode:

| Command | Purpose |
|--|--|
| action <i>number</i> [. <i>number2</i>] cli <i>command1</i> [<i>command2</i> ...] [local] | Executes the configured CLI commands. You can optionally execute the commands on the module where the event occurred. The action label is in the format <i>number1.number2</i> . <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. |
| action <i>number</i> [. <i>number2</i>] counter <i>name</i> <i>counter value val op</i> { dec inc nop set } | Modifies the counter by the configured value and operation. The action label is in the format <i>number1.number2</i> . <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. The counter name can be any case-sensitive, alphanumeric string up to 28 characters. The <i>val</i> can be an integer from 0 to 2147483647 or a substituted parameter. |
| action <i>number</i> [. <i>number2</i>] event-default | Executes the default action for the associated event. The action label is in the format <i>number1.number2</i> . <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. |
| action <i>number</i> [. <i>number2</i>] exceptionlog module <i>module</i> syserr <i>error</i> devid <i>id</i> errtype <i>type</i> errcode <i>code</i> phylayer <i>layer</i> ports <i>list</i> harderror <i>error</i> [desc <i>string</i>] | Logs an exception if the specific conditions are encountered when an EEM applet is triggered. |
| action <i>number</i> [. <i>number2</i>] forceshut [module <i>slot</i> xbar <i>xbar-number</i>] reset-reason <i>seconds</i> | Forces a module, crossbar, or the entire system to shut down. The action label is in the format <i>number1.number2</i> . <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. The <i>slot</i> range is dependent on different switches. The <i>xbar-number</i> range is from 1 to 2 and is only available on MDS 9513 modules. The reset reason is a quoted alphanumeric string up to 80 characters. |
| action <i>number</i> [. <i>number2</i>] overbudgetshut [module <i>slot</i> [- <i>slot</i>]] | Forces one or more modules or the entire system to shut down because of a power overbudget issue. <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. The <i>slot</i> range is dependent on different switches. |

| Command | Purpose |
|--|---|
| <code>action number[.number2] policy-default</code> | Executes the default action for the policy that you are overriding. The action label is in the format <code>number1.number2</code> . <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. |
| <code>action number[.number2] reload [module slot [- slot]]</code> | Forces one or more modules or the entire system to reload. <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. The <i>slot</i> range is dependent on different switches. |
| <code>action number[.number2] snmp-trap {[intdata1 data [intdata2 data] [strdata string]}</code> | Sends an SNMP trap with the configured data. <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. The <i>data</i> arguments can be any number up to 80 digits. The <i>string</i> can be any alphanumeric string up to 80 characters. |
| <code>action number[.number2] syslog [priority prio-val] msg error-message</code> | Sends a customized syslog message at the configured priority. <i>number</i> can be any number up to 16 digits. The range for <i>number2</i> is from 0 to 9. The <i>error-message</i> can be any quoted alphanumeric string up to 80 characters. |

**Note**

If you want to allow the triggered event to process the default actions also, you must explicitly configure an EEM action with **event-default** or **policy-default**, based on the type of policy. For example, if you match a CLI command in a match statement, you must add the **event-default** action statement to the EEM policy or EEM will not allow the CLI command to execute. You can bypass all CLI-based EEM policies using **terminal event-manager bypass** command. To revert use **terminal no event-manager bypass** command.

Defining a Policy Using a VSH Script

Detailed Steps

To define a policy using a VSH script, follow these steps:

-
- Step 1** In a text editor, list the CLI commands that define the policy.
 - Step 2** Name the text file and save it.
 - Step 3** Copy the file to the following system directory:
bootflash://eem/user_script_policies
-

Registering and Activating a VSH Script Policy

Detailed Steps

To register and activate a policy defined in a VSH script, follow these steps:

| | Command | Purpose |
|--------|---|---|
| Step 1 | <code>config t</code> | Enters configuration mode. |
| Step 2 | <code>event manager policy <i>policy-script</i></code> | Registers and activates an EEM script policy. The <i>policy-script</i> can be any case-sensitive alphanumeric string up to 29 characters. |
| Step 3 | <code>show event manager internal policy <i>name</i></code> | (Optional) Displays information about the configured policy. |
| Step 4 | <code>copy running-config startup-config</code> | (Optional) Saves this configuration change. |

Overriding a Policy

Detailed Steps

To override a system policy, follow these steps:

| | Command | Purpose |
|--------|---|---|
| Step 1 | <code>config t</code> | Enters configuration mode. |
| Step 2 | <code>show event manager policy-state <i>system-policy</i></code> | (Optional) Displays information about the system policy that you want to override, including thresholds. Use the <code>show event manager system-policy</code> command to find the system policy names. |
| Step 3 | <code>[no] event manager applet <i>applet-name</i> override <i>system-policy</i></code> | Overrides a system policy and enters applet configuration mode. The <i>applet-name</i> can be any case-sensitive alphanumeric string up to 29 characters. The <i>system-policy</i> must be one of the existing system policies. |
| Step 4 | <code>description <i>policy-description</i></code> | (Optional) Configures a descriptive string for the policy. The string can be any alphanumeric string up to 80 characters. Enclose the string in quotation marks. |
| Step 5 | <code>[no] event <i>event-statement</i></code> | Configures the event statement for the policy. See the “Configuring Event Statements” section on page 7-8 . Using the <code>no</code> keyword deletes the overridden event, if any. |

 **Note**

- Deleting an overridden policy does not remove the default system policy.
- You can modify an overridden policy by changing the respective Zone, FCNS, or FLOGI limit values.

| | Command | Purpose |
|--------|---|---|
| Step 6 | <code>action action-statement</code> | Configures an action statement for the policy. See the “Configuring Action Statements” section on page 7-11. Repeat Step 6 for multiple action statements. |
| | |  <p>Note</p> <ul style="list-style-type: none"> Zone, FLOGI, and FCNS support only syslog message generation as the action. If an action is not configured, the default action associated with the default system policy is executed. If an action is configured, both the configured and default actions are executed. This functionality is applicable only to Zone, FLOGI, and FCNS system policies. |
| Step 7 | <code>show event manager policy-state name</code> | (Optional) Displays information about the configured policy. |
| Step 8 | <code>copy running-config startup-config</code> | (Optional) Saves this configuration change. |



Note Multiple overrides for Zone, FLOGI, and FCNS EEM policies are not allowed.

Defining an Environment Variable

Detailed Steps

To define a variable to serve as a parameter in an EEM policy, follow these steps:

| | Command | Purpose |
|--------|---|---|
| Step 1 | <code>config t</code> | Enters configuration mode. |
| Step 2 | <code>event manager environment variable-name variable-value</code> | Creates an environment variable for EEM. The <i>variable-name</i> can be any case-sensitive alphanumeric string up to 29 characters. The <i>variable-value</i> can be any quoted alphanumeric string up to 39 characters. |
| Step 3 | <code>show event manager environment</code> | (Optional) Displays information about the configured environment variables. |
| Step 4 | <code>copy running-config startup-config</code> | (Optional) Saves this configuration change. |

Verifying the EEM Configuration

To display EEM configuration information, perform one of the following tasks:

| Command | Purpose |
|--|---|
| <code>show event manager environment</code> [<i>variable-name</i> / all] | Displays information about the event manager environment variables. |
| <code>show event manager event-types</code> [<i>event</i> all <i>module slot</i>] | Displays information about the event manager event types. |
| <code>show event manager history events</code> [detail] [maximum <i>num-events</i>] [severity {catastrophic minor moderate severe}] | Displays the history of events for all policies. |
| <code>show event manager policy internal</code> [<i>policy-name</i>] [inactive] | Displays information about the configured policies. |
| <code>show event manager policy-state</code> <i>policy-name</i> | Displays information about policy state, including thresholds. |
| <code>show event manager script system</code> [<i>policy-name</i> / all] | Displays information about the script policies. |
| <code>show event manager system-policy</code> [all] | Displays information about the predefined system policies. |
| <code>show running-config eem</code> | Displays information about the running configuration for EEM. |
| <code>show startup-config eem</code> | Displays information about the startup configuration for EEM. |

Configuration Examples for EEM

This example overrides the `__lcm_module_failure` system policy by changing the threshold for just module 3 hitless upgrade failures. This example also sends a syslog message. The settings in the system policy, `__lcm_module_failure`, apply in all other cases.

```
event manager applet example2 override __lcm_module_failure
 event module-failure type hitless-upgrade-failure module 3 count 2
  action 1 syslog priority errors msg module 3 "upgrade is not a hitless upgrade!"
  action 2 policy-default
```

This example modifies an overridden policy by changing the number of FCNS database entries to 1500. It also generates both the configured and the default syslog messages of the default system policy.

```
event manager applet fcns_policy override __fcns_entries_max_per
_switch
 event fcns entries max-per-switch 1500
  action 1.0 syslog priority warnings msg FCNS DB entries have reached the EEM limit
```

This example deletes the event of an overridden policy:

```
no event manager applet zone_policy
```

This example creates an EEM policy that allows the CLI command to execute but triggers an SNMP notification when a user enters configuration mode on the device:

```
event manager applet TEST
 event cli match "conf t"
```

```
action 1.0 snmp-trap strdata "Confiiguration change"
action 2.0 event-default
```

**Note**

You must add the **event-default** action statement to the EEM policy or EEM will not allow the CLI command to execute.

Additional References

For additional information related to implementing EEM, see the following section:

- [MIBs, page 7-16](#)

MIBs

| MIBs | MIBs Link |
|--|--|
| <ul style="list-style-type: none"> • CISCO-EMBEDDED-EVENT-MGR-MIB | To locate and download MIBs, go to the following URL: http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html |

Feature History for EEM

[Table 7-2](#) lists the release history for this feature. Only features that were introduced or modified in Release 3.x or a later release appear in the table.

Table 7-2 Feature History for EEM

| Feature Name | Releases | Feature Information |
|------------------------------|----------|--|
| Embedded Event Manager (EEM) | 4.1(3) | New chapter on configuring Embedded Event Manager (EEM) has been added. |
| EEM—Zone, FCNS, and FLOGI | 6.2(11) | This feature enables users to configure custom limits for default Zone, FCNS, and FLOGI system policies. |