CHAPTER 4

Configuring Embedded Event Manager

This chapter describes how to configure Embedded Event Manager (EEM) to detect and handle critical events on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as the Cisco CG-OS router).

This chapter includes the following sections:

- Information About EEM, page 4-1
- Prerequisites for EEM, page 4-5
- Guidelines and Limitations, page 4-6
- Default Settings, page 4-7
- Configuring EEM, page 4-7
- Verifying the Configuration, page 4-16
- Configuration Examples, page 4-17
- Feature History, page 4-17

Information About EEM

EEM 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 4-2
- Policies, page 4-2
- Event Statements, page 4-3
- Action Statements, page 4-4
- VSH Script Policies, page 4-4
- Environment Variables, page 4-4
- EEM Event Correlation, page 4-5
- Stateless Restarts, page 4-5
- Prerequisites for EEM, page 4-5

EEM Overview

EEM consists of three major components:

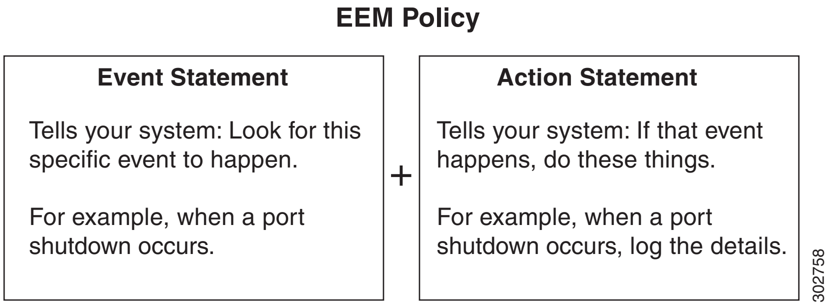
- Event statements—Events to monitor from another Cisco CG-OS component that might require some action, workaround, or notification.
- Action statements —An action that EEM can take, such as sending an e-mail, or disabling an interface, to recover from an event.
- Policies—An event paired with one or more actions to troubleshoot or recover from the event.

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 4-1 shows the two basic statements in an EEM policy.

Figure 4-1 EEM Policy Statements



Tells your system: Look for this specific event to happen.

For example, when a port shutdown occurs.

Tells your system: If that event happens, do these things.

For example, when a port shutdown occurs, log the details.

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

EEM gives you a device-wide view of policy management. You configure EEM policies on the supervisor, and EEM pushes the policy to the correct module based on the event type. EEM takes any actions for a triggered event either locally on the module or on the supervisor (the default option).

EEM maintains event logs on the Cisco CG-OS router.

Cisco CG-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 (__).

You can create user policies to suit your network. If you create a user policy, any actions in your policy occur after EEM triggers any system policy actions related to the same event as your policy. To configure a user policy, see Defining a User Policy, page 4-8.

You can also override some system policies. The overrides that you configure take the place of the system policy. 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, page 4-14.

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.

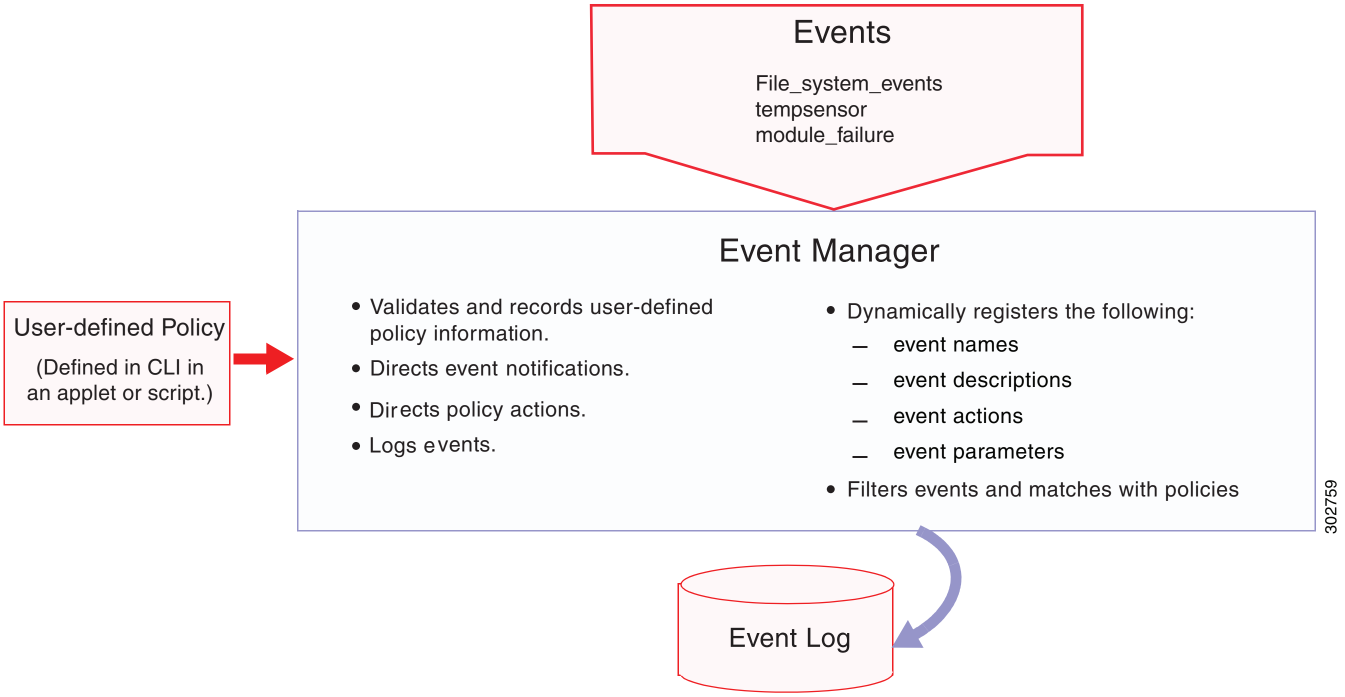
Note Your override policy should always include an event statement. An override policy without an event statement overrides all possible events in the system policy.

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 4-2 EEM Overview


Events
File_system_events
tempsensor
module_failure
Event Manager
Validates and records user-defined policy information.
Directs event notifications.
Directs policy actions.
Logs events.
Dynamically registers the following:
event names
event descriptions
event actions
event parameters
Filters events and matches with policies
User-defined Policy
(Defined in CLI in an applet or script.)
Event Log
302759

Event statements specify the event that triggers a policy to run.

You can configure multiple event triggers. For more information on configuring multiple events, see the EEM Event Correlation, page 4-5.

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

Note If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the event default action statement.

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 shutdown of any module.
- Reload the device.
- Shut down specified modules because the power is over budget.
- Generate a syslog message.
- Generate an SNMP notification.
- Use the default action for the system policy.

Note If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. 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.

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 VSH script policy, copy it to the device and activate it. To configure a policy in a VSH script, see the Defining a Policy using a VSH Script, page 4-13.

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 4-1 shows a sample action statement to force a module 1 shutdown, with a reset reason of “EEM action.”

Example 4-1 Action Statement

```
router (config-eem-policy)# action 1.0 forceshut module 1 reset-reson “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 4-2.

Example 4-2 Action Statement with Environment Variable

```
router (config-eem-policy)# action 1.0 foreshut 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, page 4-7.

EEM Event Correlation

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.

Note For information on configuring EEM event correlation, see Defining a User Policy, page 4-8.

Stateless Restarts

Cisco CG-OS software supports stateless restarts for EEM. After a reboot of the Cisco CG-OS router, the CG-OS software applies the running configuration.

Prerequisites for EEM

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

Guidelines and Limitations

Command Rules

The following rules apply to regular command expressions: all keywords must be expanded, and only the * symbol can be used for argument replacement.

Policies

The maximum number of configurable EEM policies is 500.

Action statements within your user policy or overriding policy must not negate each other or adversely affect the associated system policy.

You cannot override event statements. You can only override specific action statements (see Overriding a Policy, page 4-14)

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.

If you want to allow a triggered event to process any default actions, then you must configure the EEM policy to allow the default action. 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.

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.

Default action execution is not supported for policies that are configured with tagged events.

Event Correlation

EEM event correlation is supported only on the Cisco CG-OS Router, not on individual interfaces.

EEM event correlation is not supported across different interfaces within a single policy.

EEM event correlation supports up to four event statements in a single policy. The event types can be the same or different, but only these event types are supported: cli, counter, syslog, and track.

EEM event correlation does not override the system default policies.

Default Settings

Table 4-1 lists the default settings for EEM parameters.

Table 4-1 Default EEM Parameters

Parameters	Default
System policies	Active

Configuring EEM

You can create policies that contain actions to take based on system policies. To display information about the system policies, use the **show event manager system-policy** command.

This section includes the following topics:

- Defining an Environment Variable, page 4-7
- Defining a User Policy, page 4-8
- Defining a Policy using a VSH Script, page 4-13
- Registering and Activating a VSH Script Policy, page 4-13
- Overriding a Policy, page 4-14
- Configuring Syslog as EEM Publisher, page 4-15

Defining an Environment Variable

You can define a variable to serve as a parameter in an EEM policy.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

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

EXAMPLE

This example shows how to define an environment variable on the Cisco CG-OS router.

```
router# configure terminal
router(config)# event manager environment emailto “admin@anyplace.com”
router(config)# copy running-config startup-config
```

Defining a User Policy

To define a user policy you must define both an event and action statement.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager applet** *applet-name*	Registers the applet with EEM and enters applet configuration mode. The *applet-name* can be any case-sensitive alphanumeric string up to 29 characters.
Step 3	**description** *policy-description*	(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	**event** *event-statement*	Configures the event statement for the policy and enters the EEM configuration mode. For a list of all supported events statements, see Configuring Event Statements, page 4-9. Repeat Step 4 for multiple event statements.
Step 5	**tag** *tag* {**and** | **andnot** | **or**} *tag* [**and** | **andnot** | **or** {*tag*}] {**happens** *occurs* **in** *seconds*}	(Optional) Correlates multiple events in the policy. The range for the *occurs* argument is from 1 to 4294967295. The range for the *seconds* argument is from 0 to 4294967295 seconds.
Step 6	**action** *number*[.*number2*] *action-statement*	Configures an action statement for the policy. For a list of all supported action statements, See Configuring Action Statements, page 4-12. Repeat Step 6 for multiple action statements.
	(Optional) **action** *number*[.*number2*] *action-statement* >> *filename*	Enter this action statement for the policy if you want to export the output of an action statement to a specified flash or a directory. **Note**: The router does not have a default file to log these outputs.

	Command	Purpose
Step 7	**show event manager policy-state** *name* [**module** *module-id*]	(Optional) Displays information about the status of the configured policy.
Step 8	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to define a user policy.

```
router# configure terminal
router(config)# event manager applet monitorShutdown
router(config-applet)# description "Monitors interface shutdown."
router(config-applet)# event cli match "shutdown"
router(config-applet)# tag one or two happens 1 in 10000
router(config-applet)# action 1.0 cli show interface e 2/1 >> action.txt
router(config-applet)# copy running-config startup-config
```

Configuring Event Statements

Use one or more of the following commands in EEM configuration mode to configure an event statement as shown in Step 4 of the Defining a User Policy section.

- **event gold module** {*slot* | **all**} **test** *test-name* [**severity** {**major** | **minor** | **moderate**}] **testing-type** {**bootup** | **monitoring** | **ondemand** | **scheduled**} **consecutive-failure** *count*
- **event memory** {**critical** | **minor** | **severe**}
- **event module** [**tag** *tag*] **status** {**online** | **offline** | **any**} **module** {**all** | *module-num*}
- **event module-failure** [**tag** *tag*] **type** *failure-type* **module** {*slot* | **all**} **count** *repeats* [**time** *seconds*]
- **event policy-default count** [*int count*] [**time** *seconds*]
- **event snmp** [**tag** *tag*] **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*
- **event temperature** [**module** *slot*] [*sensor number*]

DETAILED STEPS

Command	Purpose
event cli [tag *tag*] **match** *expression* [**count** *repeats* | **time** *seconds*]	Triggers an event if you enter a command that matches the regular expression. **Note**: When using the **event cli match** command, you always use quotes to enclose the expression such as **event cli match** "**show ip int br**" **count 3 time 0** The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *repeats* range is from 1 to 65000. The time range, in seconds, is from 0 to 4294967295, where 0 indicates no time limit.
event counter [**tag** *tag*] **name** *counter* **entry-val** *entry* **entry-op {eq | ge | gt | le | lt | ne}** **[exit-val** *exit* **exit-op {eq | ge | gt | le | lt | ne}]**	Triggers an event if the counter crosses the entry threshold based on the entry operation. The event resets immediately. Optionally, you can configure the event to reset after the counter passes the exit threshold. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *counter* name can be any case-sensitive, alphanumeric string up to 28 characters. The *entry* and *exit* value ranges are from 0 to 2147483647.

Command	Purpose
event track [tag *tag*] *object-number* **state** {**any** | **down** | **up**}	Triggers an event if the tracked object is in the configured state. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. The *object-numbe*r range is from 1 to 500.
event syslog [**tag** *tag*] [**occurs** | **pattern** *msg-text* | **period** | **priority** [**0-7** | **emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **informational** | **debugging**]]	Monitors an event. The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. **occurs** Specifies the number of occurrences. The range is from 1 to 65000. **pattern** *msg-txt*– Specifies the matching regular expression (regex). The pattern can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, it is enclosed with double quotation marks. **period**–Specifies the time interval during which the event occurs. The range is from 0 to 4294967295. **priority**–Specifies the priority level of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level. If this keyword is selected, the priority level argument must be defined. The range of values are 0 to 7. **emergencies**–Specifies that the system is unusable. **alerts** Specifies that immediate action is needed. **critical**–Specifies critical conditions. **errors**–Specifies error conditions. **warnings**–Specifies warming conditions. **notifications**–Specifies normal but significant conditions. **informational**–Specifies informational messages. This is the default. **debugging**–Specifies debugging messages

EXAMPLE

This example shows how to configure an event statement.

```
router# configure terminal
router (config-applet)# event cli match "shutdown"
router (config-applet)# event counter name mycounter entry-val 20 gt
router (config-applet)# event track 1 state down
```

Configuring Action Statements

Use the one or more of the following commands in EEM configuration mode to configure action statements as shown in Step 6 of the Defining a User Policy section.

Command	Purpose
action *number*[**.***number2*] **cli** *command1* [*command2...*] [**local**]	Runs the configured CLI commands. You can optionally run the commands on the module where the event occurred. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *number[.number2]* **counter name** counter **value** *val* **op** {**dec | inc | nop | set**}	Modifies the counter by the configured value and operation. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The counter name can be any case-sensitive, alphanumeric string up to 28 characters. The *val* can be an integer from 0 to 2147483647 or a substituted parameter.
action *number[.number2]* **event-default**	Executes the default action for the associated event. The action label is in the format number1.number2. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9.
action *number*[*.number2*] **syslog** [**priority** *prio-val*] **msg** *error-message*	Sends a customized syslog message at the configured priority. *number* can be any number up to 16 digits. The range for *number2* is from 0 to 9. The *error-message* can be any quoted alphanumeric string up to 80 characters.

Note When you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the default action. For example, if you match a CLI command in a match statement, then you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute. You can use the **terminal event-manager bypass** command to allow all EEM policies with CLI matches to execute the CLI command.

Defining a Policy using a VSH Script

You can define a policy using a VSH script.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

Ensure that you are logged in with administrator privileges.

Ensure that your script name is the same name as the script filename.

DETAILED STEPS

Step 1 In a text editor, list the 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

You can register and activate a policy defined in a VSH script.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

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

EXAMPLE

This example shows how to register and activate a VSH script policy.

```
router# configure terminal
router(config)# event manager policy moduleScript
router(config)# copy running-config startup-config
```

Overriding a Policy

You can override actions statements for a gold system policy.

BEFORE YOU BEGIN

Make sure that you are in the default VDC. The Cisco CG-OS router does not support any VDCs beyond the default.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager applet** *applet-name* **override** *system-policy*	Overrides a system policy and enters applet configuration mode. The *applet-name* can be any case-sensitive alphanumeric string up to 29 characters. The *system-policy* must be one of the existing system policies.
Step 3	**description** *policy-description*	(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	**action** *number action-statement*	Configures an action statement for the policy. For details on action statements, see Configuring Action Statements, page 4-12. Repeat Step 6 in that section to create multiple action statements.
Step 5	**show event manager policy-state** *name*	(Optional) Displays information about the configured policy.
Step 6	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to override an action statement for a gold system policy.

```
router# configure terminal
router(config)# event manager applet gold module all test monday test-type bootup
                  consecutive-failure 3
router(config-applet)# action 1.0 syslog priority warnings msg "Gold Module bootup
                       consecutive failures."
router(config)# copy running-config startup-config
```

Configuring Syslog as EEM Publisher

You can monitor syslog messages from the router.

Note The maximum number of searchable strings to monitor syslog messages is 10.

BEFORE YOU BEGIN

EEM should be available for registration by syslog.

The syslog daemon must be configured and executed.

Note The maximum number of searchable strings to monitor syslog messages is 10.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**event manager applet** *applet-name*	Registers an applet with EEM and enters applet configuration mode.
Step 3	**event syslog** [**tag** *tag*] {**occurs** *number* | **period** *seconds* | **pattern** *msg-text* | **priority** *priority*}	Monitors syslog messages and invokes the policy based on the search string in the policy. • The **tag** *tag* keyword-argument pair identifies this specific event when multiple events are included in the policy. • The **occurs** *number* keyword-argument pair specifies the number of occurrences. The range is from 1 to 65000. • The **period** *seconds* keyword-argument pair specifies the interval during which the event occurs. The range is from 1 to 4294967295. • The **pattern** *msg-text* keyword-argument pair specifies the matching regular expression. The pattern can contain character text, an environment variable, or a combination of the two. If the string contains embedded blanks, it is enclosed in quotation marks. • The **priority** *priority* keyword-argument pair specifies the priority of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure EEM as a publisher.

```
router# configure terminal
router (config-applet)# event manager applet abc
router (config-applet)# event syslog occurs 10
router (config-applet)# copy running-config startup-config
```

Verifying the Configuration

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

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

Configuration Examples

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

This example shows how to override the real_time clock.

```
event manager applet realtime override __real_time_clock
    action 1.0 syslog priority warnings msg Override policy real time clock
    action 1.1 policy-default
```

This example creates an EEM policy that allows the CLI to execute but triggers an SNMP notification when the user enters configuration mode on the router.

```
event manager applet TEST
    event cli match “conf t”
    action 1.0 snmp-trap strdata “Configuration change”
    action 2.0 event-default
```

This example shows how to correlate multiple events in an EEM policy and execute the policy based on a combination of the event triggers. In this example, the software triggers the EEM policy if one of the specified syslog patterns occurs within 120 seconds.

```
event manager applet eem-correlate
    event syslog tag one pattern “copy bootflash:* running-config.*”
    event syslog tag two pattern “copy run start”
    event syslog tag three pattern “hello”
    tag one or two or three happens 1 in 120
    action 1.0 reload module 1
```

Feature History

Table 4-2 Feature History for Embedded Event Manager

Feature Name	Release	Feature Information
Embedded Event Manager	Cisco CG-OS Release CG2(1)	Initial support of the feature on the CGR 1000 Series Routers.