# Embedded Event Manager Commands

This module describes the commands that are used to set the Embedded Event Manager (EEM) operational attributes and monitor EEM operations.

The Cisco IOS XR software EEM functions as the central clearing house for the events detected by any portion of Cisco IOS XR software High Availability Services. The EEM is responsible for fault detection, fault recovery, and process the reliability statistics in a system. The EEM is policy driven and enables you to configure the high-availability monitoring features of the system to fit your needs.

The EEM monitors the reliability rates achieved by each process in the system. You can use these metrics during testing to identify the components that do not meet their reliability or availability goals, which in turn enables you to take corrective action.

To use commands of this module, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using any command, contact your AAA administrator for assistance.

For detailed information about the EEM concepts, configuration tasks, and examples, see the *Configuring and Managing Embedded Event Manager Policies* module in *Cisco IOS XR System Monitoring Configuration Guide for the Cisco XR 12000 Series Router*.

- show event manager statistics-table, page 33

# event manager directory user

To specify a directory name for storing user library files or user-defined Embedded Event Manager (EEM) policies, use the **event manager directory user** command in Global Configuration mode. To disable the use of a directory for storing user library files or user-defined EEM policies, use the **no** form of this command.

**event manager directory user** {**library** *path*| **policy** *path*}

**no event manager directory user** {**library** *path*| **policy** *path*}

## Syntax Description

| | |
|---|---|
| **library** | Specifies a directory name for storing user library files. |
| *path* | Absolute pathname to the user directory on the flash device. |
| **policy** | Specifies a directory name for storing user-defined EEM policies. |

## Command Default

No directory name is specified for storing user library files or user-defined EEM policies.

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **fault manager userlibdirectory** and **fault manager userpolicydirectory** commands were replaced with the **event manager directory user** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

Cisco IOS XR software supports only the policy files that are created by using the Tool Command Language (TCL) scripting language. The TCL software is provided in the Cisco IOS XR software image when the EEM is installed on the network device. Files with the .tcl extension can be EEM policies, TCL library files, or a special TCL library index file named tclindex. The tclindex file contains a list of user function names and library files that contain the user functions (procedures). The EEM searches the user library directory when the TCL starts to process the tclindex file.

**User Library**

A user library directory is needed to store user library files associated with authoring EEM policies. If you do not plan to write EEM policies, you do not have to create a user library directory.

To create user library directory before identifying it to the EEM, use the **mkdir** command in EXEC mode. After creating the user library directory, use the **copy** command to copy the .tcl library files into the user library directory.

**User Policy**

A user policy directory is essential to store the user-defined policy files. If you do not plan to write EEM policies, you do not have to create a user policy directory. The EEM searches the user policy directory when you enter the **event manager policy** *policy-name* **user** command.

To create a user policy directory before identifying it to the EEM, use the **mkdir** command in EXEC mode. After creating the user policy directory, use the **copy** command to copy the policy files into the user policy directory.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read, write |

## Examples

This example shows how to set the pathname for a user library directory to /usr/lib/tcl on disk0:

```
RP/0/0/CPU0:router(config)# event manager directory user library disk0:/usr/lib/tcl
```

This example shows how to set the location of the EEM user policy directory to /usr/fm_policies on disk0:

```
RP/0/0/CPU0:router(config)# event manager directory user policy disk0:/usr/fm_policies
```

## Related Commands

| Command | Description |
|---|---|
| event manager policy, on page 7 | Registers an EEM policy with the EEM. |
| show event manager directory user, on page 16 | Displays the directory name for storing user library and policy files. |

# event manager environment

To set an Embedded Event Manager (EEM) environment variable, use the **event manager environment** command in Global Configuration mode. To remove the configuration, use the **no** form of this command.

**event manager environment** *var-name* [ *var-value* ]

**no event manager environment** *var-name*

## Syntax Description

| | |
|---|---|
| *var-name* | Name assigned to the EEM environment configuration variable. |
| *var-value* | (Optional) Series of characters, including embedded spaces, to be placed in the environment variable *var-name*. |

## Command Default

None

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **fault manager environment** command was replaced with the **event manager environment** command.<br>The *var-value* argument was changed from required to optional. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

Environment variables are available to EEM policies when you set the variables using the **event manager environment** command. They become unavailable when you remove them with the **no** form of this command.

By convention, the names of all the environment variables defined by Cisco begin with an underscore character (_) to set them apart, for example, _show_cmd.

Spaces can be used in the *var-value* argument. This command interprets everything after the *var-name* argument uptil the end of the line in order to be a part of the *var-value* argument.

Use the show event manager environment, on page 18 command to display the name and value of all EEM environment variables before and after they have been set using the **event manager environment** command.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read, write |

## Examples

This example shows how to define a set of EEM environment variables:

```
RP/0/0/CPU0:router(config)# event manager environment _cron_entry 0-59/2 0-23/1 * * 0-7
RP/0/0/CPU0:router(config)# event manager environment _show_cmd show eem manager policy
registered
RP/0/0/CPU0:router(config)# event manager environment _email_server alpha@cisco.com
RP/0/0/CPU0:router(config)# event manager environment _email_from beta@cisco.com
RP/0/0/CPU0:router(config)# event manager environment _email_to beta@cisco.com
RP/0/0/CPU0:router(config)# event manager environment _email_cc
```

## Related Commands

| Command | Description |
|---|---|
| show event manager environment, on page 18 | Displays the name and value for all the EEM environment variables. |

# event manager policy

To register an Embedded Event Manager (EEM) policy with the EEM, use the **event manager policy** command in Global Configuration mode. To unregister an EEM policy from the EEM, use the **no** form of this command.

**event manager policy** *policy-name* **username** *username* [**persist-time** [*seconds*| **infinite**]| **type** {**system**| **user**}]

**no event manager policy** *policy-name* [**username** *username*]

**event manager policy** <*name of policy file*> **username** <*val*> [**persist-time <val>**{**system**| **user**}[**checksum**| {**md5**| **sha-1**}| <*checksum_val*>]][**secure-mode**| {**trust**| **cisco rsa-2048**}]

## Syntax Description

| | |
|---|---|
| *policy-name* | Name of the policy file. |
| **username** *username* | Specifies the username used to run the script. This name can be different from that of the user who is currently logged in, but the registering user must have permissions that are a superset of the username that runs the script. Otherwise, the script is not registered, and the command is rejected.<br>In addition, the username that runs the script must have access privileges to the commands issued by the EEM policy being registered. |
| **persist-time** [*seconds* \| **infinite**] | (Optional) The length of the username authentication validity, in seconds. The default time is 3600 seconds (1 hour). The *seconds* range is 0 to 4294967294. Enter 0 to stop the username authentication from being cached. Enter the **infinite** keyword to stop the username from being marked as invalid. |
| **type** | (Optional) Specifies the type of policy. |
| **system** | (Optional) Registers a system policy defined by Cisco. |
| **user** | (Optional) Registers a user-defined policy. |
| **checksum**{**md5sha-1**} | Specifies a script that is verified against checksum policies. |
| **secure-mode**{**trustcisco rsa-2048**} | Specifies a script that is verified against Cisco signing server in secure mode. |

## Command Default

The default persist time is 3600 seconds (1 hour).

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |

| Release | Modification |
|---|---|
| Release 3.3.0 | Support was added for the required keyword and argument **username** *username* .<br>Support was added for the optional keyword and argument **persist-time** [ *seconds* \| **infinite** ]. |
| Release 3.6.0 | The **fault manager policy** command was replaced with the **event manager policy** command.<br>The **type** keyword was added. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |
| Release 5.2.0 | Support added for verifying scripts against digital signatures, checksum, third party scripts and Cisco signing server. |

## Usage Guidelines

The EEM schedules and runs policies on the basis of an event specification that is contained within the policy itself. When the **event manager policy** command is invoked, the EEM examines the policy and registers it to be run when the specified event occurs. An EEM script is available to be scheduled by the EEM until the **no** form of this command is entered.

**Note** AAA authorization (such as the **aaa authorization** command with the **eventmanager** and **default** keywords) must be configured before the EEM policies can be registered. The **eventmanager** and **default** keywords must be configured for policy registration. See the *Configuring AAA Services on* the Cisco IOS XR Softwaremodule of *Cisco IOS XR System Security Configuration Guide for the Cisco XR 12000 Series Router* for more information on AAA authorization configuration.

**Username**

Enter the username that should execute the script with the **username** *username* keyword and argument. This name can be different from the user who is currently logged in, but the registering user must have permissions that are a superset of the username that runs the script. Otherwise, the script will not be registered, and the command will be rejected. In addition, the username that runs the script must have access privileges to the commands issued by the EEM policy being registered.

**Persist-time**

When a script is first registered, the configured **username** for the script is authenticated. If authentication fails, or if the AAA server is down, the script registration fails.

After the script is registered, the username is authenticated each time a script is run.

If the AAA server is down, the username authentication can be read from memory. The **persist-time** determines the number of seconds this username authentication is held in memory.

- If the AAA server is down and the **persist-time** has not expired, the username is authenticated from memory, and the script runs.
- If the AAA server is down, and the **persist-time** has expired, user authentication fails, and the script does not run.

**Note** EEM attempts to contact the AAA server and refresh the username reauthenticate whenever the configured **refresh-time** expires. See the event manager refresh-time, on page 11 command for more information.

These values can be used for the **persist-time**:

- The default **persist-time** is 3600 seconds (1 hour). Enter the **event manager policy** command without the **persist-time** keyword to set the **persist-time** to 1 hour.
- Enter zero to stop the username authentication from being cached. If the AAA server is down, the username is not authenticated and the script does not run.
- Enter **infinite** to stop the username from being marked as invalid. The username authentication held in the cache will not expire. If the AAA server is down, the username is authenticated from the cache.

### Type

If you enter the **event manager policy** command without specifying the **type** keyword, the EEM first tries to locate the specified policy file in the system policy directory. If the EEM finds the file in the system policy directory, it registers the policy as a system policy. If the EEM does not find the specified policy file in the system policy directory, it looks in the user policy directory. If the EEM locates the specified file in the user policy directory, it registers the policy file as a user policy. If the EEM finds policy files with the same name in both the system policy directory and the user policy directory, the policy file in the system policy directory takes precedence, and the policy file is registered as a system policy.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read, write |

## Examples

This example shows how to register a user-defined policy named cron.tcl located in the user policy directory:

```
RP/0/0/CPU0:router(config)# event manager policy cron.tcl username joe
```

## Related Commands

| Command | Description |
|---|---|
| event manager environment, on page 5 | Specifies a directory for storing user library files. |
| event manager refresh-time, on page 11 | Specifies the time between the system attempts to contact the AAA server and refresh the username reauthentication. |
| show event manager environment, on page 18 | Displays the name and value for all EEM environment variables. |
| show event manager policy available, on page 26 | Displays EEM policies that are available to be registered. |
| show event manager policy registered, on page 28 | Displays the EEM policies that are already registered. |

# event manager refresh-time

To define the time between user authentication refreshes in Embedded Event Manager (EEM), use the **event manager refresh-time** command in Global Configuration mode. To restore the system to its default condition, use the **no** form of this command.

**event manager refresh-time** *seconds*

**no event manager refresh-time** *seconds*

## Syntax Description

| | |
|---|---|
| *seconds* | Number of seconds between user authentication refreshes, in seconds. Range is 10 to 4294967295. |

## Command Default

The default refresh time is 1800 seconds (30 minutes).

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 3.3.0 | This command was introduced. |
| Release 3.6.0 | The **fault manager refresh-time** command was replaced with the **event manager refresh-time** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

EEM attempts to contact the AAA server and refresh the username reauthentication whenever the configured **refresh-time** expires.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read, write |

## Examples

This example shows how to set the refresh time:

```
RP/0/0/CPU0:router(config)# event manager refresh-time 1900
```

# event manager run

To manually run an Embedded Event Manager (EEM) policy, use the **event manager run** command in EXEC mode.

**event manager run** *policy* [*argument* [... [ *argument15* ]]]

## Syntax Description

| | |
|---|---|
| *policy* | Name of the policy file. |
| [*argument*[...[*argument15*]]] | Argument that you want to pass to the policy. The maximum number of arguments is 15. |

## Command Default

No registered EEM policies are run.

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.6.0 | This command was introduced. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

EEM usually schedules and runs policies on the basis of an event specification that is contained within the policy itself. The **event manager run** command allows policies to be run manually.

You can query the arguments in the policy file by using the **TCL** command *event_reqinfo* , as shown in this example:

```
array set arr_einfo [event_reqinfo] set argc $arr_einfo(argc) set arg1
          $arr_einfo(arg1)
```

Use the event manager policy, on page 7 command to register the policy before using the **event manager run** command to run the policy. The policy can be registered with none as the event type.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This example of the **event manager run** command shows how to manually run an EEM policy named policy-manual.tcl:

```
RP/0/0/CPU0:router# event manager run policy-manual.tcl parameter1 parameter2 parameter3
RP/0/0/CPU0:Sep 20 10:26:31.169 : user-plocy.tcl[65724]: The reqinfo of arg2 is parameter2.

RP/0/0/CPU0:Sep 20 10:26:31.170 : user-plocy.tcl[65724]: The reqinfo of argc is 3.
RP/0/0/CPU0:Sep 20 10:26:31.171 : user-plocy.tcl[65724]: The reqinfo of arg3 is parameter3.

RP/0/0/CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_type_string
is none.
RP/0/0/CPU0:Sep 20 10:26:31.172 : user-plocy.tcl[65724]: The reqinfo of event_pub_sec is
1190283990.
RP/0/0/CPU0:Sep 20 10:26:31.173 : user-plocy.tcl[65724]: The reqinfo of event_pub_time is
1190283990.
RP/0/0/CPU0:Sep 20 10:26:31.173 : user-plocy.tcl[65724]: The reqinfo of event_id is 3.
RP/0/0/CPU0:Sep 20 10:26:31.174 : user-plocy.tcl[65724]: The reqinfo of arg1 is parameter1.

RP/0/0/CPU0:Sep 20 10:26:31.175 : user-plocy.tcl[65724]: The reqinfo of event_type is 16.
RP/0/0/CPU0:Sep 20 10:26:31.175 : user-plocy.tcl[65724]: The reqinfo of event_pub_msec is
830
```

## Related Commands

| Command | Description |
|---|---|
| event manager policy, on page 7 | Registers an EEM policy with the EEM. |

# event manager scheduler suspend

To suspend the Embedded Event Manager (EEM) policy scheduling execution immediately, use the **event manager scheduler suspend** command in Global Configuration mode. To restore a system to its default condition, use the **no** form of this command.

**event manager scheduler suspend**

**no event manager scheduler suspend**

## Syntax Description

This command has no keywords or arguments.

## Command Default

Policy scheduling is active by default.

## Command Modes

Global Configuration mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **fault manager schedule-policy suspend** command was replaced with the **event manager scheduler suspend** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

Use the **event manager scheduler suspend** command to suspend all the policy scheduling requests, and do not perform scheduling until you enter the **no** form of this command. The **no** form of this command resumes policy scheduling and runs pending policies, if any.

It is recommended that you suspend policy execution immediately instead of unregistering policies one by one, for the following reasons:

- Security—If you suspect that the security of your system has been compromised.
- Performance—If you want to suspend policy execution temporarily to make more CPU cycles available for other functions.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read, write |

## Examples

This example shows how to disable policy scheduling:

```
RP/0/0/CPU0:router(config)# event manager scheduler suspend
```

This example shows how to enable policy scheduling:

```
RP/0/0/CPU0:router(config)# no event manager scheduler suspend
```

## Related Commands

| Command | Description |
|---|---|
| event manager policy, on page 7 | Registers an EEM policy with the EEM. |

# show event manager directory user

To display the current value of the EEM user library files or user-defined Embedded Event Manager (EEM) policies, use the **show event manager directory user** command in EXEC mode.

**show event manager directory user** {**library**| **policy**}

## Syntax Description

| | |
|---|---|
| **library** | Specifies the user library files. |
| **policy** | Specifies the user-defined EEM policies. |

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager userlibdirectory** and **show fault manager userpolicydirectory** commands were replaced with the **show event manager directory user** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

Use the **show event manager directory user** command to display the current value of the EEM user library or policy directory.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager directory user** command:

```
RP/0/0/CPU0:router# show event manager directory user library
disk0:/fm_user_lib_dir

RP/0/0/CPU0:router# show event manager directory user policy
disk0:/fm_user_pol_dir
```

## Related Commands

| Command | Description |
|---|---|
| event manager directory user, on page 3 | Specifies the name of a directory that is to be used for storing either the user library or the policy files. |

# show event manager environment

To display the names and values of the Embedded Event Manager (EEM) environment variables, use the **show event manager environment** command in EXEC mode.

**show event manager environment** [**all**| *environment-name*]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Specifies all the environment variables. |
| *environment-name* | (Optional) Environment variable for which data is displayed. |

## Command Default

All environment variables are displayed.

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager environment** command was replaced with the **show event manager environment** command. |

## Usage Guidelines

Use the **show event manager environment** command to display the names and values of the EEM environment variables.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager environment** command:

```
RP/0/0/CPU0:router# show event manager environment

No.  Name                           Value
1    _email_cc
2    _email_to                      mosnerd@cisco.com
3    _show_cmd                      show event manager policy registered
4    _cron_entry                    0-59/2 0-23/1 * * 0-7
5    _email_from                    mosnerd@cisco.com
6    _email_server                  zeta@cisco.com
```

This table describes the significant fields in the display.

***Table 1: show event manager environment Field Descriptions***

| Field | Description |
|---|---|
| No. | Number of the EEM environment variable. |
| Name | Name of the EEM environment variable. |
| Value | Value of the EEM environment variable. |

## Related Commands

| Command | Description |
|---|---|
| event manager environment, on page 5 | Specifies a directory to use for storing user library files. |

# show event manager metric hardware

To display the Embedded Event Manager (EEM) reliability data for the processes running on a particular node, use the **show event manager metric hardware** command in EXEC mode.

**show event manager metric hardware location** {*node-id*| **all**}

## Syntax Description

| | |
|---|---|
| **location** | Specifies the location of the node. |
| *node-id* | EEM reliability data for the specified node. The *node-id* argument is entered in the *rack/slot/module* notation. |
| **all** | Specifies all the nodes. |

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager metric hardware** command was replaced with the **show event manager metric environment** command. |

## Usage Guidelines

No specific guidelines impact the use of this command.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager metric hardware** command:

```
RP/0/0/CPU0:router# show event manager metric hardware location 0/0/CPU0

=====================================

node: 0/0/CPU0

Most recent online: Mon Sep 10 21:45:02 2007
```

```
Number of times online: 1
Cumulative time online: 0 days, 09:01:07

Most recent offline: n/a
Number of times offline: 0
Cumulative time offline: 0 days, 00:00:00
```

This table describes the significant fields shown in the display.

***Table 2: show event manager metric hardware location Field Descriptions***

| Field | Description |
|---|---|
| node | Node with processes running. |
| Most recent online | The last time the node was started. |
| Number of times online | Total number of times the node was started. |
| Cumulative time online | Total amount of time the node was available. |
| Most recent offline | The last time the process was terminated abnormally. |
| Number of times offline | Total number of times the node was terminated. |
| Cumulative time offline | Total amount of time the node was terminated. |

## Related Commands

| Command | Description |
|---|---|
| show processes | Displays information about active processes. |

# show event manager metric process

To display the Embedded Event Manager (EEM) reliability metric data for processes, use the **show event manager metric process** command in EXEC mode.

**show event manager metric process** {**all**| *job-id*| *process-name*} **location** {**all**| *node-id*}

## Syntax Description

| | |
|---|---|
| **all** | Specifies all the processes. |
| *job-id* | Process associated with this job identifier. The value ranges from 0-4294967295. |
| *process-name* | Process associated with this name. |
| **location** | Specifies the location of the node. |
| **all** | Displays hardware reliability metric data for all the nodes. |
| *node-id* | Hardware reliability metric data for a specified node. Displays detailed Cisco Express Forwarding information for the designated node. The *node-id* argument is entered in the *rack/slot/module* notation. |

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager metric process** command was replaced with the **show event manager metric process** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

The system maintains a record of when processes start and end. This data is used as the basis for reliability analysis.

Use the **show event manager metric process** command to obtain availability information for a process or group of processes. A process is considered available when it is running.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is sample output from the **show event manager metric process** command:

```
RP/0/0/CPU0:router# show event manager metric process all location all

====================================
job id: 88, node name: 0/4/CPU0
process name: wd-critical-mon, instance: 1
--------------------------------
last event type: process start
recent start time: Wed Sep 19 13:31:07 2007
recent normal end time: n/a
recent abnormal end time: n/a
number of times started: 1
number of times ended normally: 0
number of times ended abnormally: 0
most recent 10 process start times:
--------------------------
Wed Sep 19 13:31:07 2007
--------------------------

most recent 10 process end times and types:

cumulative process available time: 21 hours 1 minutes 31 seconds 46 milliseconds
cumulative process unavailable time: 0 hours 0 minutes 0 seconds 0 milliseconds
process availability:  1.000000000
number of abnormal ends within the past 60 minutes (since reload): 0
number of abnormal ends within the past 24 hours (since reload): 0
number of abnormal ends within the past 30 days (since reload): 0
====================================
job id: 54, node name: 0/4/CPU0
process name: dllmgr, instance: 1
--------------------------------
last event type: process start
recent start time: Wed Sep 19 13:31:07 2007
recent normal end time: n/a
recent abnormal end time: n/a
number of times started: 1
number of times ended normally: 0
number of times ended abnormally: 0
most recent 10 process start times:
--------------------------
Wed Sep 19 13:31:07 2007
--------------------------

most recent 10 process end times and types:

cumulative process available time: 21 hours 1 minutes 31 seconds 41 milliseconds
cumulative process unavailable time: 0 hours 0 minutes 0 seconds 0 milliseconds
process availability:  1.000000000
number of abnormal ends within the past 60 minutes (since reload): 0
number of abnormal ends within the past 24 hours (since reload): 0
number of abnormal ends within the past 30 days (since reload): 0
```

This table describes the significant fields shown in the display.

*Table 3: show event manager metric process Field Descriptions*

| Field | Description |
|---|---|
| job id | Number assigned as the job identifier. |
| node name | Node with the process running. |
| process name | Name of the process running on the node. |
| instance | Instance or thread of a multithreaded process. |
| comp id | Component of which the process is a member. |
| version | Specific software version or release of which the process is a member. |
| last event type | Last event type on the node. |
| recent end type | Most recent end type. |
| recent start time | Last time the process was started. |
| recent normal end time | Last time the process was stopped normally. |
| recent abnormal end time | Last time the process was terminated abnormally. |
| recent abnormal end type | Reason for the last abnormal process termination. For example, the process was aborted or crashed. |
| number of times started | Number of times the process has been started. |
| number of times ended normally | Number of times the process has been stopped normally. |
| number of times ended abnormally | Number of times the process has stopped abnormally. |
| most recent 10 process start times | Times of the last ten process starts. |
| cumulative process available time | Total time the process has been available. |
| cumulative process unavailable time | Total time the process has been out of service due to a restart, abort, communication problems, and so on. |
| process availability | Uptime percentage of the process (time running—the duration of any outage). |
| number of abnormal ends within the past 60 minutes | Number of times the process has stopped abnormally within the last 60 minutes. |

| Field | Description |
|---|---|
| number of abnormal ends within the past 24 hours | Number of times the process has stopped abnormally within the last 24 hours. |
| number of abnormal ends within the past 30 days | Number of times the process has stopped abnormally within the last 30 days. |

## Related Commands

| Command | Description |
|---|---|
| show processes | Displays information about active processes. |

# show event manager policy available

To display Embedded Event Manager (EEM) policies that are available to be registered, use the **show event manager policy available** command in EXEC mode.

**show event manager policy available** [**system**| **user**]

## Syntax Description

| | |
|---|---|
| **system** | (Optional) Displays all the available system policies. |
| **user** | (Optional) Displays all the available user policies. |

## Command Default

If this command is invoked with no optional keywords, it displays information for all available system and user policies.

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager policy available** command was replaced with the **show event manager policy available** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

Use the **show event manager policy available** command to find out what policies are available to be registered just prior to using the **event manager policy** command to register policies.

This command is also useful if you forget the exact name of a policy that is required for the **event manager policy** command.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager policy available** command:

```
RP/0/0/CPU0:router# show event manager policy available
```

```
No.  Type    Time Created                 Name
1    system  Tue Jan 12 09:41:32 2004     pr_sample_cdp_abort.tcl
2    system  Tue Jan 12 09:41:32 2004     pr_sample_cdp_revert.tcl
3    system  Tue Jan 12 09:41:32 2004     sl_sample_intf_down.tcl
4    system  Tue Jan 12 09:41:32 2004     tm_sample_cli_cmd.tcl
5    system  Tue Jan 12 09:41:32 2004     tm_sample_crash_hist.tcl
6    system  Tue Jan 12 09:41:32 2004     wd_sample_proc_mem_used.tcl
7    system  Tue Jan 12 09:41:32 2004     wd_sample_sys_mem_used.tcl
```

This table describes the significant fields shown in the display.

***Table 4: show event manager policy available Field Descriptions***

| Field | Description |
|---|---|
| No. | Number of the policy. |
| Type | Type of policy. |
| Time Created | Time the policy was created. |
| Name | Name of the policy. |

## Related Commands

| Command | Description |
|---|---|
| event manager policy, on page 7 | Registers an EEM policy with the EEM. |
| show event manager policy registered, on page 28 | Displays the EEM policies that are already registered. |

# show event manager policy registered

To display the Embedded Event Manager (EEM) policies that are already registered, use the **show event manager policy registered** command in EXEC mode.

**show event manager policy registered**[**event-type** *type*] [**system**| **user**] [**time-ordered**| **name-ordered**]

## Syntax Description

| | |
|---|---|
| **event-type** *type* | (Optional) Displays the registered policies for a specific event type, where the valid *type* options are as follows:<br>• **application—**Application event type<br>• **counter—**Counter event type<br>• **hardware—**Hardware event type<br>• **oir—**Online insertion and removal (OIR) event type<br>• **process-abort—**Process abort event type<br>• **process-start—**Process start event type<br>• **process-term—**Process termination event type<br>• **process-user-restart—**Process user restart event type<br>• **process-user-shutdown—**Process user shutdown event type<br>• **statistics—**Statistics event type<br>• **syslog—**Syslog event type<br>• **timer-absolute—**Absolute timer event type<br>• **timer-countdown—**Countdown timer event type<br>• **timer-cron—**Clock daemon (cron) timer event type<br>• **timer-watchdog—**Watchdog timer event type<br>• **wdsysmon—**Watchdog system monitor event type |
| **system** | (Optional) Displays the registered system policies. |
| **user** | (Optional) Displays the registered user policies. |
| **time-ordered** | (Optional) Displays the policies according to registration time. |
| **name-ordered** | (Optional) Displays the policies in alphabetical order according to policy name. |

## Command Default

If this command is invoked with no optional keywords or arguments, it displays the registered EEM policies for all the event types. The policies are displayed according to the registration time.

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager policy registered** command was replaced with the **show event manager policy registered** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

The output of the **show event manager policy registered** command is most beneficial if you are writing and monitoring the EEM policies. The output displays registered policy information in two parts. The first line in each policy description lists the index number assigned to the policy, policy type (system or user), type of event registered, time at which the policy was registered, and name of the policy file. The remaining lines of each policy description display information about the registered event and how the event is to be handled, and come directly from the Tool Command Language (TCL) command arguments that make up the policy file.

Registered policy information is documented in the Cisco publication *Writing Embedded Event Manager Policies Using Tcl*.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager policy registered** command:

```
RP/0/0/CPU0:router# show event manager policy registered

No.       Type    Event Type          Time Registered              Name
1         system  proc abort          Wed Jan 16 23:44:56 2004     test1.tcl
 version 00.00.0000 instance 1 path {cdp}
 priority normal maxrun_sec 20 maxrun_nsec 0
2         system  timer cron          Wed Jan 16 23:44:58 2004     test2.tcl
 name {crontimer1}
 priority normal maxrun_sec 20 maxrun_nsec 0
3         system  proc abort          Wed Jan 16 23:45:02 2004     test3.tcl
 path {cdp}
 priority normal maxrun_sec 20 maxrun_nsec 0
4         system  syslog              Wed Jan 16 23:45:41 2004     test4.tcl
 occurs 1 pattern {test_pattern}
 priority normal maxrun_sec 90 maxrun_nsec 0
5         system  timer cron          Wed Jan 16 23:45:12 2004     test5.tcl
 name {crontimer2}
 priority normal maxrun_sec 30 maxrun_nsec 0
6         system  wdsysmon           Wed Jan 16 23:45:15 2004     test6.tcl
 timewin_sec 120 timewin_nsec 0 sub1 mem_tot_used {node {localhost} op gt
 val 23000}
```

```
 priority normal maxrun_sec 40 maxrun_nsec 0
7         system  wdsysmon            Wed Jan 16 23:45:19 2004      test7.tcl
 timewin_sec 120 timewin_nsec 0 sub1 mem_proc {node {localhost} procname
 {wdsysmon} op gt val 80 is_percent FALSE}
 priority normal maxrun_sec 40 maxrun_nsec 0
```

This is the sample of a script that is signed by Cisco:

```
script    system  timer watchdog     Off   Fri Apr 23 14:03:27 2010  script_signed_cisco.tcl

     name {clistimer} time 30.000
     nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Secu 2048 Dsig Cisco
```

This is the sample of a script that is signed by third party:

```
script    system  timer watchdog      Off   Fri Apr 23 14:03:27 2010  script_signed.tcl
     name {clistimer} time 30.000
     nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Secu Trust Dsig
Tcl_trustpoint
```

This is the sample of a script that is verified against a configured checksum:

```
script    user    timer watchdog      Off   Fri Apr 23 14:03:27 2010  test3_3rd_signed.tcl
     name {clistimer} time 30.000
     nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Secu none Cksm MD5
```

This is the sample of a script that is signed by a combination of security levels. If a SHA-1 or MD5 script is verified and registered, the checksum information displays as Cksm sha1 or Cksm md5. The following example shows a SHA-1 checksum signed by Tcl_trustpoint:

```
script    user    timer watchdog      Off   Fri Apr 23 14:03:27 2010  test3_3rd_signed.tcl
 name {clistimer} time 30.000
 nice 0 queue-priority normal maxrun 0.000 scheduler rp_primary Cksm sha1 Dsig Tcl_trustpoint
```

This table describes the significant fields displayed in the example.

***Table 5: show event manager policy registered Field Descriptions***

| Field | Description |
|---|---|
| No. | Number of the policy. |
| Type | Type of policy. |
| Event Type | Type of the EEM event for which the policy is registered. |
| Time Registered | Time at which the policy was registered. |
| Name | Name of the policy. |

## Related Commands

| Command | Description |
|---|---|
| event manager policy,  on page 7 | Registers an EEM policy with the EEM. |

# show event manager refresh-time

To display the time between the user authentication refreshes in the Embedded Event Manager (EEM), use the **show event manager refresh-time** command in EXEC mode.

**show event manager refresh-time**

## Syntax Description

This command has no keywords or arguments.

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.3.0 | This command was introduced. |
| Release 3.6.0 | The **show fault manager refresh-time** command was replaced with the **show event manager refresh-time** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

The output of the **show event manager refresh-time** command is the refresh time, in seconds.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager refresh-time** command:

```
RP/0/0/CPU0:router# show event manager refresh-time
Output:
1800 seconds
```

## Related Commands

| Command | Description |
|---|---|
| event manager refresh-time, on page 11 | Specifies the time between the system attempts to contact the AAA server, and refreshes the username reauthentication. |

# show event manager statistics-table

To display the currently supported statistic counters maintained by the Statistic Event Detector, use the **show event manager statistics-table** command in EXEC mode.

**show event manager statistics-table** {*stats-name*| **all**}

## Syntax Description

| | |
|---|---|
| *stats-name* | Specific statistics type to be displayed. There are three statistics types:<br>• generic (ifstats-generic)<br>• interface table (ifstats-iftable)<br>• data rate (ifstats-datarate) |
| **all** | Displays the possible values for the *stats-name* argument.<br>Displays the output for all the statistics types. |

## Command Default

None

## Command Modes

EXEC mode

## Command History

| Release | Modification |
|---|---|
| Release 3.2 | This command was introduced. |
| Release 3.6.0 | The **show fault manager statistics-table** command was replaced with the **show event manager statistics-table** command. |
| Release 3.7.0 | Task ID was changed from fault-mgr to eem. |

## Usage Guidelines

Use the **show event manager statistics-table all** command to display the output for all the statistics types.

## Task ID

| Task ID | Operations |
|---|---|
| eem | read |

## Examples

This is a sample output of the **show event manager statistics-table all** command:

```
RP/0/0/CPU0:router# show event manager statistics-table all

Name                      Type      Description
ifstats-generic           bag       Interface generic stats
ifstats-iftable           bag       Interface iftable stats
ifstats-datarate          bag       Interface datarate stats
```

This is a sample output providing more detailed information on the ifstats-iftable interface statistics table:

```
RP/0/0/CPU0:router# show event manager statistics-table ifstats-iftable

Name                      Type      Description
PacketsReceived           uint64    Packets rcvd
BytesReceived             uint64    Bytes rcvd
PacketsSent               uint64    Packets sent
BytesSent                 uint64    Bytes sent
MulticastPacketsReceived uint64    Multicast pkts rcvd
BroadcastPacketsReceived uint64    Broadcast pkts rcvd
MulticastPacketsSent      uint64    Multicast pkts sent
BroadcastPacketsSent      uint64    Broadcast pkts sent
OutputDropsCount          uint32    Total output drops
InputDropsCount           uint32    Total input drops
InputQueueDrops           uint32    Input queue drops
RuntPacketsReceived       uint32    Received runt packets
GiantPacketsReceived      uint32    Received giant packets
ThrottledPacketsReceived uint32    Received throttled packets
ParityPacketsReceived     uint32    Received parity packets
UnknownProtocolPacketsReceiveduint32    Unknown protocol pkts rcvd
InputErrorsCount          uint32    Total input errors
CRCErrorCount             uint32    Input crc errors
InputOverruns             uint32    Input overruns
FramingErrorsReceived     uint32    Framing-errors rcvd
InputIgnoredPackets       uint32    Input ignored packets
InputAborts               uint32    Input aborts
OutputErrorsCount         uint32    Total output errors
OutputUnderruns           uint32    Output underruns
OutputBufferFailures      uint32    Output buffer failures
OutputBuffersSwappedOut   uint32    Output buffers swapped out
Applique                  uint32    Applique
ResetCount                uint32    Number of board resets
CarrierTransitions        uint32    Carrier transitions
AvailabilityFlag          uint32    Availability bit mask
NumberOfSecondsSinceLastClearCountersuint32    Seconds since last clear counters
LastClearTime             uint32    SysUpTime when counters were last cleared (in seconds)
```

This table describes the significant fields displayed in the example.

*Table 6: show event manager statistics-table Field Descriptions*

| Field | Description |
|---|---|
| Name | Name of the statistic.<br>When the **all** keyword is specified, there are three types of statistics displayed:<br>• ifstats-generic<br>• ifstats-iftable<br>• ifstats-datarate<br>When a statistics type is specified, the statistics for the statistic type are displayed. |
| Type | Type of statistic. |
| Description | Description of the statistic. |

## Related Commands

| Command | Description |
|---|---|
| event manager policy, on page 7 | Registers an EEM policy with the EEM. |