



Alarm Filtering Support in the Cisco Entity Alarm MIB

First Published: November 14, 2008
Last Updated: March 12, 2008

The Alarm Filtering Support in the Cisco Entity Alarm MIB feature implements the alarm filter profile capability defined in CISCO-ENTITY-ALARM-MIB. Also implemented are configuration commands to control the severity of syslog messages and SNMP notifications triggered by the alarms.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Information About Alarm Filtering Support in the Cisco Entity Alarm MIB”](#) section on [page 2](#).

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 2](#)
- [Restrictions for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 2](#)
- [Information About Alarm Filtering Support in the Cisco Entity Alarm MIB, page 2](#)
- [How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications, page 3](#)
- [Configuration Examples for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 5](#)
- [Additional References, page 6](#)



- [Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 7](#)
- [Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB, page 7](#)

Prerequisites for Alarm Filtering Support in the Cisco Entity Alarm MIB

- SNMP is configured on your routing devices.
- Familiarity with the ENTITY-MIB and the CISCO-ENTITY-ALARM-MIB.

Restrictions for Alarm Filtering Support in the Cisco Entity Alarm MIB

- The CISCO-ENTITY-ALARM-MIB supports reporting of alarms for physical entities only. For line cards, alarms are reported at the physical interface or port level.

Information About Alarm Filtering Support in the Cisco Entity Alarm MIB

To configure alarm filtering in the Cisco Entity Alarm MIB, you should understand the following concepts:

- [CISCO-ENTITY-ALARM-MIB, page 2](#)
- [ceAlarmGroup, page 2](#)
- [ceAlarmFilterProfileTable, page 3](#)
- [ceAlarmFilterProfile, page 3](#)

CISCO-ENTITY-ALARM-MIB

The CISCO-ENTITY-ALARM-MIB provides a management client with the capability to monitor alarms generated by physical entities in a network that are identified in the entPhysicalTable of the Entity-MIB (RFC 2737). Examples of these physical entities are chassis, fans, modules, ports, slots, and power supplies. The management client interfaces with an SNMP agent to request access to objects defined in the CISCO-ENTITY-ALARM-MIB.

ceAlarmGroup

The ceAlarmGroup is a group in the CISCO-ENTITY-ALARM-MIB that defines objects that provide current statuses of alarms and the capability to instruct an agent to stop (cut off) signaling for any or all external audible alarms.

Following are the objects in ceAlarmGroup:

- ceAlarmCriticalCount
- ceAlarmMajorCount
- ceAlarmMinorCount
- ceAlarmCutoff
- ceAlarmFilterProfile
- ceAlarmSeverity
- ceAlarmList

ceAlarmFilterProfileTable

The ceAlarmFilterProfileTable filters alarms according to configured alarm lists. The filtered alarms are then sent out as SNMP notifications or syslog messages, based on the alarm list enabled for each alarm type. This table is defined in the CISCO-ENTITY-ALARM-MIB and implemented in the group ceAlarmGroup.

ceAlarmFilterProfile

An alarm filter profile controls the alarm types that an agent monitors and signals for a corresponding physical entity. The ceAlarmFilterProfile object holds an integer value that uniquely identifies an alarm filter profile associated with a corresponding physical entity. When the value is zero, the agent monitors and signals all alarms associated with the corresponding physical entity.

How to Configure Alarm Filtering for Syslog Messages and SNMP Notifications

This section contains the following tasks:

- [Configuring Alarm Filtering for Syslog Messages, page 3](#) (optional)
- [Configuring Alarm Filtering for SNMP Notifications, page 4](#) (optional)

Configuring Alarm Filtering for Syslog Messages

Perform this task to configure the alarm severity threshold for generating syslog messages. When you perform this task, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **logging alarm** [*severity*]
4. **show facility-alarm status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	logging alarm [<i>severity</i>] Example: Router(config)# logging alarm 2	Configures the alarm severity threshold for generating syslog messages. All alarms at and above this threshold are sent as syslog messages.
Step 4	show facility-alarm status Example: Router(config)# show facility-alarm status	Generates output that shows information about each alarm depending on the severity level that is set.

Configuring Alarm Filtering for SNMP Notifications

Perform this task to configure the alarm severity threshold for generating SNMP notifications. When you perform this task, the alarm severity threshold is included in the running configuration and automatically applied when the configuration is reloaded.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps alarms** [*severity*]
4. **show facility-alarm status**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>snmp-server enable traps alarms [severity]</pre> <p>Example: Router(config)# snmp-server enable traps alarms 2</p>	Configures the alarm severity threshold for generating SNMP notifications. All alarms at and above this threshold are sent as SNMP notifications.
Step 4	<pre>show facility-alarm status</pre> <p>Example: Router(config)# show facility-alarm status</p>	Generates output that shows information about each alarm depending on the severity level that is set.

Configuration Examples for Alarm Filtering Support in the Cisco Entity Alarm MIB

This section provides the following configuration examples:

- [Configuring Alarm Filtering for Syslog Messages: Example, page 5](#)
- [Configuring Alarm Filtering for SNMP Notifications: Example, page 5](#)

Configuring Alarm Filtering for Syslog Messages: Example

The following example shows how to configure an alarm filter for syslog messages:

```
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# logging alarm 2
Router(config)# exit
Router#
Router# show facility-alarm status

System Totals Critical: 1 Major: 0 Minor: 0
Source Severity Description [Index]
-----
Fa0/0 CRITICAL Physical Port Link Down [0]
Fa0/1 INFO Physical Port Administrative State Down [1]
AT6/0 INFO Physical Port Administrative State Down [8]
```

Configuring Alarm Filtering for SNMP Notifications: Example

The following example shows how to configure an alarm filter for SNMP notifications:

```
Router#
Router# enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# snmp-server enable traps alarms 2
Router(config)#
Router(config)# exit
Router#
Router# show facility-alarm status
```

```

System Totals Critical: 1 Major: 0 Minor: 0
Source Severity Description [Index]
-----
Fa0/0 CRITICAL Physical Port Link Down [0]
Fa0/1 INFO Physical Port Administrative State Down [1]
AT6/0 INFO Physical Port Administrative State Down [8]

```

Additional References

The following sections provide references related to the Alarm Filtering Support in the Cisco Entity Alarm MIB feature.

Related Documents

Related Topic	Document Title
Network management configuration tasks	Cisco IOS Network Management Configuration Guide
Network management commands	Cisco IOS Network Management Command Reference

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.”	—

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> ENTITY-MIB CISCO-ENTITY-ALARM-MIB 	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2737	<i>Entity MIB (Version 2)</i>

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/techsupport

Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Alarm Filtering Support in the Cisco Entity Alarm MIB

Feature Name	Releases	Feature Information
Alarm Filtering Support in the Cisco Entity Alarm MIB	12.4(4)T 12.2(33)SRB 12.2(33)SB 12.2(33)SXI	<p>The Alarm Filtering Support in the Cisco Entity Alarm MIB feature implements the alarm filter profile capability defined in CISCO-ENTITY-ALARM-MIB. Also implemented are configuration commands to control the severity of syslog messages and SNMP notifications triggered by the alarms.</p> <p>This feature was introduced in Cisco IOS Release 12.4(4)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXI.</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2005-2008 Cisco Systems, Inc. All rights reserved.