CHAPTER 4

Configuring Alarms

This chapter contains the following topics:

Configuring the Cisco Syslog Agent Enterprise Parameters

You can configure the Cisco Syslog Agent enterprise parameters to send system, application, and security alarms/messages that exceed the configured threshold to a remote syslog server that you specify. To access the Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Cisco Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Cisco Unified Communications Manager Business Edition 5000	In Cisco Unified Communications Manager Administration, choose **System > Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting > Enterprise Parameters**.

Next, configure the remote syslog server name and syslog severity. Then click **Save**. For the valid values to enter, click the **?** button. If the server name is not specified, Cisco Unified Serviceability does not send the Syslog messages.

Note Do not configure a Cisco Unified Communications Manager as a remote syslog server. The Cisco Unified Communications Manager server does not accept Syslog messages from another server.

Configuring an Alarm for a Service

This section describes how to add or update an alarm for a feature or network service that you manage through Cisco Unified Serviceability.

Note Cisco recommends that you do not change SNMP Trap and Catalog configurations.

Cisco Unity Connection also uses alarms, which are available in Cisco Unity Connection Serviceability. You cannot configure alarms in Cisco Unity Connection Serviceability. For details, see the *Cisco Unity Connection Serviceability Administration Guide*.

Refer to your online OS documentation for more information on how to use your standard registry editor.

Procedure

Step 1 Choose **Alarm > Configuration**.

The Alarm Configuration window displays.

Step 2 From the Server drop-down list box, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Service Group drop-down list box, choose the category of service, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.

Tip For a list of services that correspond to the service groups, see Table 4-1.

Step 4 From the Service drop-down list box, choose the service for which you want to configure the alarm; then, click **Go**.

Only services that support the service group and your configuration display.

Tip The drop-down list box displays active and inactive services.

In the Alarm Configuration window, a list of alarm monitors with the event levels displays for the chosen service.In addition, the Apply to All Nodes check box displays.

Step 5 *Unified CM only*: If you want to do so, you can apply the alarm configuration for the service to all servers in the cluster by checking the **Apply to All Nodes** check box, provided your configuration supports clusters.

Step 6 Configure the settings, as described in Table 4-2, which includes descriptions for monitors and event levels.

Step 7 To save your configuration, click the **Save** button.

Note To set the default, click the **Set Default** button; then, click **Save**.

Services That Use Cisco Tomcat

The following services use Cisco Tomcat for alarm generation:

- Cisco Extension Mobility Application
- Cisco IP Manager Assistant
- Cisco Extension Mobility
- Cisco Web Dialer Web

The system login alarm AuthenticationFailed also uses Cisco Tomcat. To generate alarms for these services, perform the following procedure.

Procedure

Step 1 In Cisco Unified Serviceability, choose **Alarm > Configuration**.

Step 2 From the Server drop-down list box, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Services Group drop-down list box, choose **Platform Services**; then, click **Go**.

Step 4 From the Services drop-down list box, choose **Cisco Tomcat**; then, click **Go**.

Step 5 *Unified CM only*: If you want to do so, you can apply the alarm configuration for the service to all servers in the cluster by checking the **Apply to All Nodes** check box, if your configuration supports clusters.

Step 6 Configure the settings, as described in Table 4-2, which includes descriptions for monitors and event levels.

Step 7 To save your configuration, click the **Save** button.

Tip The system sends the alarm if the configured alarm event level for the specific destination in the Alarm Configuration window is equal to or lower than the severity that is listed in the alarm definition. For example, if the severity in the alarm definition equals WARNING_ALARM, and, in the Alarm Configuration window, you configure the alarm event level for the specific destination as Warning, Notice, Informational, or Debug, which are lower event levels, the system sends the alarm to the corresponding destination. If you configure the alarm event level as Emergency, Alert, Critical, or Error, which are higher severity levels, the system does not send the alarm to the corresponding location.

To access the alarm definitions for the Cisco Extension Mobility Application service, Cisco IP Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer Web Service, choose the **JavaApplications** catalog in the Alarm Messages Definitions window described in Chapter 5, "Viewing and Updating Alarm Definitions".

Additional Information

See the "Related Topics" section on page 4-8.

Service Groups in Alarm Configuration

Table 4-1 lists the services that correspond to the options in the Service Group drop-down list box in the Alarm Configuration window.

Note Not all listed service groups and services apply to all system configurations.

Table 4-1 Service Groups in Alarm Configuration

Service Group	Services	Notes
CM Services	Cisco CTIManager, Cisco CallManager, Cisco CallManager Cisco IP Phone Service, Cisco DHCP Monitor Service, Cisco Dialed Number Analyzer, Cisco Dialed Number Analyzer Server, Cisco Extended Functions, Cisco IP Voice Media Streaming App, Cisco Messaging Interface, and Cisco Tftp	For a description of these services, see the "Understanding Services" section on page 9-1.
CDR Services	Cisco CDR Agent and Cisco CDR Repository Manager	For a description of these services, see the "Understanding Services" section on page 9-1.
Database and Admin Services	Cisco Bulk Provisioning Service, Cisco Database Layer Monitor, and Cisco License Manager	For a description of these services, see the "Understanding Services" section on page 9-1.
Performance and Monitoring Services	Cisco AMC Service and Cisco RIS Data Collector	For a description of these services, see the "Understanding Services" section on page 9-1.
Directory Services	Cisco DirSync	For a description of this service, see the "Understanding Services" section on page 9-1.
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master	For a description of these services, see the "Understanding Services" section on page 9-1.
System Services	Cisco Trace Collection Service	For a description of these services, see the "Understanding Services" section on page 9-1.
Platform Services	Cisco Tomcat	For a description of this service, see the "Understanding Services" section on page 9-1.

Alarm Configuration Settings

Table 4-2 describes all alarm configuration settings, even though the service may not support the settings. For related procedures, see the "Related Topics" section on page 4-8.

Table 4-2 Alarm Configuration Settings

Name	Description
Server	From the drop-down box, choose the server for which you want to configure the alarm; then, click **Go**.
Service Group	Cisco Unity Connection supports only the following service groups: Database and Admin Services, Performance and Monitoring Services, Backup and Restore Services, System Services, and Platform Services. From the drop-down box, choose the category of services, for example, Database and Admin Services, for which you want to configure the alarm; then, click **Go**.
Service	From the Service drop-down box, choose the service for which you want to configure the alarm; then, click **Go**. Only services that support the service group and your configuration display. **Tip** The drop-down list box displays active and inactive services.
Unified CM only: Apply to All Nodes	To apply the alarm settings for the service to all servers in a cluster, check the check box.
Enable Alarm for Local Syslogs	The SysLog viewer serves as the alarm destination. The program logs errors in the Application Logs within SysLog Viewer and provides a description of the alarm and a recommended action. You can access the SysLog Viewer from the Cisco Unified Real-Time Monitoring Tool. For information on viewing logs with the SysLog Viewer, refer to the *Cisco Unified Real-Time Monitoring Tool Administration Guide*.

Table 4-2 Alarm Configuration Settings (continued)

Name	Description
Enable Alarm for Remote Syslogs	The Syslog file serves as the alarm destination. Check this check box to enable the Syslog messages to be stored on a Syslog server and to specify the Syslog server name. If this destination is enabled and no server name is specified, Cisco Unified Serviceability does not send the Syslog messages. The configured AMC primary and failover collectors use the remote syslog settings. The remote syslog settings used by the collectors are those configured on the respective individual nodes. If the remote syslog is only configured on AMC primary collector without configuring remote syslog on AMC failover collector and failover occurs in AMC primary collector, then no remote syslogs will be generated. You must configure exactly the same settings on all nodes, to send the remote syslog alarms to the same remote syslog server. When failover occurs in AMC controller or when the collector configuration changes to a different node, the remote syslog settings on backup or newly configured node is used. To prevent too many alarms flooding the system, you can check the **Exclude End Point Alarms** checkbox. This ensures that the endpoint phone-related events get logged into a separate file. Exclude End Point Alarms checkbox is displayed only for the Call Manager services, and is not selected by default. You need to select the **Apply to All Nodes** also, while selecting this checkbox. The configuration options for endpoint alarms are given in Table 4-4. **Tip** In the Server field, enter the name or IP address of the remote Syslog server that you want to use to accept Syslog messages. For example, if you want to send the alarms to CiscoWorks Lan Management Solution, specify the CiscoWorks Lan Management Solution server name. **Tip** Do not specify a Cisco Unified Communications Manager server as the destination because the Cisco Unified Communications Manager server does not accept Syslog messages from another server.
Enable Alarm for SDI Trace	The SDI trace library serves as the alarm destination. To log alarms in the SDI trace log file, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see the "Configuring Trace Parameters" section on page 7-1.

Table 4-2 Alarm Configuration Settings (continued)

Name	Description
Unified CM and Unified CM BE only: Enable Alarm for SDL Trace	The SDL trace library serves as the alarm destination. This destination applies only to the Cisco CallManager service and the CTIManager service. Configure this alarm destination by using Trace SDL configuration. To log alarms in the SDL trace log file, check this check box and check the Trace On check box in the Trace Configuration window for the chosen service. For information on configuring settings in the Trace Configuration window in Cisco Unified Serviceability, see the "Configuring Trace Parameters" section on page 7-1.
Alarm Event Level	From the drop-down list box, choose one of the following options: • **Emergency**—This level designates system as unusable. • **Alert**—This level indicates that immediate action is needed. • **Critical**—The system detects a critical condition. • **Error**—This level signifies an error condition exists. • **Warning**—This level indicates that a warning condition is detected. • **Notice**—This level designates a normal but significant condition. • **Informational**—This level designates information messages only. • **Debug**—This level designates detailed event information that Cisco TAC engineers use for debugging.

Table 4-3 describes the default alarm configuration settings.

Table 4-3 Default Alarm Configuration Settings

	Local Syslogs	Remote Syslogs	SDI Trace	SDL Trace
Enable Alarm	Checked	Unchecked	Checked	Checked
Alarm Event Level	Error	Disabled	Error	Error

Table 4-4 End point Alarm Configuration Options

Exclude End Point Alarms	Local Syslog	Alternate Syslog	Remote Syslog	Syslog Severity and Strangulate Alert	Syslog Traps
Checked	No	Yes	No	No	No
Unchecked	No	Yes	Yes	Yes	Yes

Where to Find More Information

Related Topics

- Configuring the Cisco Syslog Agent Enterprise Parameters, page 4-1
- Configuring an Alarm for a Service, page 4-2
- Service Groups in Alarm Configuration, page 4-3
- Alarm Configuration Settings, page 4-4
- Understanding Alarms, page 3-1

Additional Cisco Documentation

- *Cisco Unified Real-Time Monitoring Tool Administration Guide*
- *Unified CM BE and Connection only*: *Cisco Unity Connection Serviceability Administration Guide*