Alarms

Overview

Cisco Unified Serviceability and Cisco Unified IM and Presence Serviceability alarms provide information on runtime status and the state of the system, so you can troubleshoot problems that are associated with your system; for example, to identify issues with the Disaster Recovery System. Alarm information, which includes an explanation and recommended action, also includes the application name, machine name, and so on, to help you perform troubleshooting and also applies to clusters.

You configure the alarm interface to send alarm information to multiple locations, and each location can have its own alarm event level (from Debug to Emergency). You can direct alarms to the Syslog Viewer (local syslog), Syslog file (remote syslog), an SDL trace log file (for Cisco CallManager and CTIManager services only), or to all destinations.

When a service issues an alarm, the alarm interface sends the alarm information to the locations that you configure and that are specified in the routing list in the alarm definition (for example, SDI trace). The system can either forward the alarm information, as is the case with SNMP traps, or write the alarm information to its final destination (such as a log file).

You can configure alarms for services, such as Cisco Database Layer Monitor, on a particular node, or you configure alarms for a particular service on all nodes in the cluster.

Note Cisco Unity Connection SNMP does not support traps.

Tip For the Remote Syslog Server, do not specify a Unified Communications Manager server, which cannot accept syslog messages from other servers.

You use the Trace and Log Central option in the Cisco Unified Real-Time Monitoring Tool (Unifed RTMT) to collect alarms that get sent to an SDL trace log file (for Cisco CallManager and CTIManager services only). You use the SysLog Viewer in Unifed RTMT to view alarm information that gets sent to the local syslog.

Alarm Configuration

You can configure alarms for services, such as Cisco Database Layer Monitor, in Cisco Unified Serviceability. Then, you configure the location or locations, such as Syslog Viewer (local syslog), where you want the system to send the alarm information. With this option, you can do the following:

- Configure alarms for services on a particular server or on all servers (Unified Communications Manager clusters only)
- Configure different remote syslog servers for the configured services or servers
- Configure different alarm event level settings for different destinations

Cisco Syslog Agent enterprise parameters in Cisco Unified Communications Manager Administration allow you to forward all alarms that meet or exceed the configured threshold to a remote syslog server with these two settings: remote syslog server name and syslog severity. To access these Cisco Syslog Agent parameters, go to the applicable window for your configuration:

Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting** > **Enterprise Parameters**.
Cisco IM and Presence	In Cisco Unified Communications Manager IM and Presence Administration, choose **System** > **Enterprise Parameters**.

The alarms include system (OS/hardware platform), application (services), and security alarms.

Note If you configure both the Cisco Syslog Agent alarm enterprise parameters and application (service) alarms in Cisco Unified Serviceability, the system can send the same alarm to the remote syslog twice.

If local syslog is enabled for an application alarm, the system sends the alarm to the enterprise remote syslog server only when the alarm exceeds both the local syslog threshold and the enterprise threshold.

If remote syslog is also enabled in Cisco Unified Serviceability, the system forwards the alarm to the remote syslog server by using the application threshold that is configured in Cisco Unified Serviceability, which may result in the alarm being sent to the remote syslog server twice.

The event level/severity settings provide a filtering mechanism for the alarms and messages that the system collects. This setting helps to prevent the Syslog and trace files from becoming overloaded. The system forwards only alarms and messages that exceed the configured threshold.

For more information about the severity levels attached to alarms and events, see the Alarm Definitions, on page 3.

Alarm Definitions

Used for reference, alarm definitions describe alarm messages: what they mean and how to recover from them. You search the Alarm Definitions window for alarm information. When you click any service-specific alarm definition, a description of the alarm information (including any user-defined text that you have added) and a recommended action display.

You can search for alarm definitions of all alarms that display in the Serviceability GUI. To aid you with troubleshooting problems, the definitions, which exist in a corresponding catalog, include the alarm name, description, explanation, recommended action, severity, parameters and monitors.

When the system generates an alarm, it uses the alarm definition name in the alarm information, so you can identify the alarm. In the alarm definition, you can view the routing list, which specifies the locations where the system can send the alarm information. The routing list may include the following locations, which correlate to the locations that you can configure in the Alarm Configuration window:

- Unified Communications Manager only: SDL - The system sends the alarm information to the SDL trace if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- SDI - The system sends the alarm information to the SDI trace if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- Sys Log - The system sends the alarm information to the remote syslog server if you enable the alarm for this option, specify an event level in the Alarm Configuration window, and enter a server name or IP address for the remote syslog server.
- Event Log - The system sends the alarm information to the local syslog, which you can view in the SysLog Viewer in the Cisco Unified Real-Time Monitoring Tool (Unified RTMT), if you enable the alarm for this option and specify an event level in the Alarm Configuration window.
- Data Collector - The system sends the alarm information to the real-time information system (RIS data collector) for alert purposes only. You cannot configure this option in the Alarm Configuration window.
- SNMP Traps - System generates an SNMP trap. You cannot configure this option in the Alarm Configuration window.

Tip If the SNMP Traps location displays in the routing list, the system forwards the alarm information to the CCM MIB SNMP agent, which generates traps according to the definition in CISCO-CCM-MIB.

The system sends an alarm if the configured alarm event level for the specific location 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, the system does not send the alarm to the corresponding location.

For each alarm definition, you can include an additional explanation or recommendation. All administrators have access to the added information. You directly enter information into the User Defined Text pane that displays in the Alarm Details window. Standard horizontal and vertical scroll bars support scrolling. Cisco Unified Serviceability adds the information to the database.

Alarm Information

You view alarm information to determine whether problems exist. The method that you use to view the alarm information depends on the destination that you chose when you configured the alarm. You can view alarm information that is sent to the SDL trace log file (Unified Communications Manager) by using the Trace and Log Central option in Unified RTMT or by using a text editor. You can view alarm information that gets sent to local syslog by using the SysLog Viewer in Unified RTMT.

Set Up Alarms

Perform the following steps to configure alarms.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, Cisco Unity Connection Administrationor Cisco Unified IM and Presence Administration, configure the Cisco Syslog Agent enterprise parameters to send system, application (services), and security alarms/messages to a remote syslog server that you specify. Skip this step to configure application (services) alarms/messages in Cisco Unified Serviceability.

Step 2 In Cisco Unified Serviceability, configure the servers, services, destinations, and event levels for the applications (services) alarm information that you want to collect.

Step 3 (Optional) Add a definition to an alarm.

- All services can go to the SDI log (but must be configured in Trace also).
- All services can go to the SysLog Viewer.
- Unified Communications Manager only: Only the Cisco CallManager and Cisco CTIManager services use the SDL log.
- To send syslog messages to the Remote Syslog Server, check the Remote Syslog destination and specify a host name. If you do not configure the remote server name, Cisco Unified Serviceability does not send the Syslog messages to the remote syslog server.

  Tip Do not configure a Unified Communications Manager server as a remote Syslog server.

Step 4 If you chose an SDL trace file as the alarm destination, collect traces and view the information with the Trace and Log Central option in Unified RTMT.

Step 5 If you chose local syslog as the alarm destination, view the alarm information in the SysLog Viewer in Unified RTMT.

Step 6 See the corresponding alarm definition for the description and recommended action.

Alarm Service Setup

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:

Unified Communications Manager	In Cisco Unified Communications Manager Administration, choose **System** > **Enterprise Parameters**.
Cisco Unity Connection	In Cisco Unity Connection Administration, choose **System Setting** > **Enterprise Parameters**.
Cisco IM and Presence	In Cisco Unified Communications Manager IM and Presence Administration, choose **System** > **Enterprise Parameters**.

Next, configure the remote syslog server names (Remote Syslog Server Name 1, Remote Syslog Server Name 2, Remote Syslog Server Name 3, Remote Syslog Server Name 4, and Remote Syslog Server Name 5) and syslog severity. Ensure that you specify valid IP addresses while configuring the server names. The syslog severity is applicable to all the remote syslog servers that you configure. Then click **Save**. For the valid values to enter, click the **?** button. If no server name is specified, Cisco Unified Serviceability does not send the Syslog messages.

Caution While configuring remote syslog servers in Unified Communications Manager, do not add duplicate entries for remote syslog server names. If you add duplicate entries, the Cisco Syslog Agent will ignore the duplicate entries while sending messages to the remote syslog servers.

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

Set Up Alarm 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, choose the server for which you want to configure the alarm; then, click **Go**.

Step 3 From the Service Group drop-down list, 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 Service groups.

Step 4 From the Service drop-down list, 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 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 Communications Manager only: If you want to do so, you can apply the alarm configuration for the service to all nodes 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 Alarm configuration settings, 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**.

What to do next

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 Unified Communications Manager Assistant service, Cisco Extension Mobility service, and the Cisco Web Dialer service, choose the **JavaApplications** catalog in the Alarm Messages Definitions window described in Alarm definitions.

Set Up Alarm 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

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, choose the server for which you want to configure the alarm; then, click **Go**.

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

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

Step 5 Unified Commuications Manager only: If you want to do so, you can apply the alarm configuration for the service to all nodes 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 Alarm configuration settings, which includes descriptions for monitors and event levels.

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

Service Groups

The following table lists the services that correspond to the options in the Service Group drop-down list in the Alarm Configuration window.

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

Table 1: Service Groups in Alarm Configuration

Service Group	Services
CM Services	Cisco CTIManager, Cisco CallManager, 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, Cisco Headset Service, and Cisco TFTP
CTI Services	Cisco IP Manager Assistant and Cisco WebDialer Web Service
CDR Services	Cisco CAR Scheduler, Cisco CDR Agent, and Cisco CDR Repository Manager

Service Group	Services
Database and Admin Services	Cisco Bulk Provisioning Service and Cisco Database Layer Monitor
Performance and Monitoring Services	Cisco AMC Service and Cisco RIS Data Collector
Directory Services	Cisco DirSync
Backup and Restore Services	Cisco DRF Local and Cisco DRF Master
System Services	Cisco Trace Collection Service
Platform Services	Cisco Tomcat and Cisco Smart License Manager

Alarm Configuration Settings

The following table describes all alarm configuration settings, even though the service may not support the settings.

Table 2: Alarm Configuration Settings

Name	Description
Server	From the drop-down list, choose the server (node) 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 list, 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 list, 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 displays both active and inactive services.
Unified Communications Manager and Cisco Unified Communications Manager IM and Presence Service only: Apply to All Nodes	To apply the alarm settings for the service to all nodes in a cluster, check the check box.

Name	Description
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*.
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 a backup or newly configured node is used. To prevent too many alarms flooding the system, you can check the **Exclude End Point Alarms** check box. This ensures that the endpoint phone-related events get logged into a separate file. **Exclude End Point Alarms** check box is displayed only for the CallManager services, and is not checked by default. You need to check the **Apply to All Nodes** also, when you check this check box. The configuration options for endpoint alarms are listed in Alarm configuration settings. **Tip** Do not specify a Unified Communications Manager or a Cisco Unified Communications Manager IM and Presence Service node as the destination because the node does not accept syslog messages from another node.

Name	Description
Remote Syslog Servers	In each of the Server Name 1, Server Name 2, Server Name 3, Server Name 4, and Server Name 5 fields, 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 Cisco Unified Operations Manager, specify the Cisco Unified Operations Manager as the server name. **Tip** Do not specify a Unified Communications Manager or a Cisco Unified Communications Manager IM and Presence Service node as the destination because the node does not accept syslog messages from another node.
Enable Alarm for SDI Trace	The SDI trace library serves as the alarm destination. To log alarms, 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 Set up trace parameters.
Unified Communications Manager and Unified Communications Manager 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 Set up trace parameters.

Name	Description
Alarm Event Level	From the drop-down list, 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 that 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 Technical Assistance Center engineers use for debugging.

The following tables describe the 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

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

Alarm Definitions and User-Defined Description Additions

This section provides procedural information to search, view, and create user information for alarm definitions that display in the Serviceability interface.

View Alarm Definitions and Add User-Defined Descriptions

This section describes how to search for and view an alarm definitions.

Tip Unified Communications Manager and Cisco Unity Connection only: You can view Cisco Unity Connection alarm definitions in Cisco Unity Connection Serviceability. You cannot add user-defined descriptions to alarm definitions in Cisco Unity Connection Serviceability.

Cisco Unity Connection also uses certain alarm definitions in Cisco Unified Serviceability, and they must be viewed in Cisco Unified Serviceability. Be aware that alarms that are associated with the catalogs in System catalogs are available for viewing.

Before you begin

Review the description of alarm definition catalogs.

Procedure

Step 1 Select **Alarm** > **Definitions**.

Step 2 Perform one of the following actions:

- Select an alarm as follows:
  - Select an alarm catalog from the **Find alarms where** drop-down list, for example, a System Alarm catalog or IM and Presence alarm catalog.
  - Select the specific catalog name from the **Equals** drop-down list.
- Enter the alarm name in the **Enter Alarm Name** field.

Step 3 Select **Find**.

Step 4 Perform one of the following actions if multiple pages of alarm definitions exist:

- To select another page, select the appropriate navigation button at the bottom of the **Alarm Message Definitions** window.
- To change the number of alarms that display in the window, select a different value from the **Rows per Page** drop-down list.

Step 5 Select the alarm definition for which you want alarm details.

Step 6 Enter text in the **User Defined Text** field if you want to add information to the alarm, and then select **Save**.

Tip If you add text in the **User Defined Text** field, you can select **Clear All** at any time to delete the information that you entered.

Step 7 Select **Save**.

Step 8 Select **Back to Find/List Alarms** from the Related Links drop-down list if you want to return to the **Alarm Message Definitions** window.

Step 9 Select **Go**.

System Alarm Catalog Descriptions

The following table contains the System Alarm Catalog alarm descriptions. The System Alarm Catalog supports Unified Communications Manager and Cisco Unity Connection.

Table 3: System Catalogs

Name	Description
ClusterManagerAlarmCatalog	All cluster manager alarm definitions that are related to the establishment of security associations between servers in a cluster.
DBAlarmCatalog	All Cisco database alarm definitions
DRFAlarmCatalog	All Disaster Recovery System alarm definitions
GenericAlarmCatalog	All generic alarm definitions that all applications share
JavaApplications	All Java Applications alarm definitions. **Tip** You cannot configure JavaApplications alarms by using the alarm configuration GUI. For Unified Communications Manager and Cisco Unity Connection, you generally configure these alarms to go to the Event Logs; for Unified Communications Manager, you can configure these alarms to generate SNMP traps to integrate with CiscoWorks LAN Management Solution. Use the registry editor that is provided with your operating system to view or change alarm definitions and parameters.
EMAlarmCatalog	Alarms for Extension Mobility
LoginAlarmCatalog	All login-related alarm definitions
LpmTctCatalog	All log partition monitoring and trace collection alarm definitions
RTMTAlarmCatalog	All Cisco Unified Real-Time Monitoring Tool alarm definitions
SystemAccessCatalog	All alarm definitions that are used for tracking whether SystemAccess provides all thread statistic counters together with all the process statistic counters.
ServiceManagerAlarmCatalogs	All service manager alarm definitions that are related to the activation, deactivation, starting, restarting, and stopping of services.
TFTPAlarmCatalog	All Cisco TFTP alarm definitions

Name	Description
TVSAlarmCatalog	Alarms for Trust Verification Service
TestAlarmCatalog	All alarm definitions that are used for sending test alarms through SNMP traps from the command line interface (CLI). For information on the CLI, refer to the *Command Line Interface Reference Guide for Cisco Unified Solutions*. **Tip** Cisco Unity Connection SNMP does not support traps in either Unified Communications Manager and Cisco Unity Connection systems.
CertMonitorAlarmCatalog	All certificate expiration definitions.
CTLproviderAlarmCatalog	Alarms for Certificate Trust List (CTL) Provider service
CDPAlarmCatalog	Alarms for Cisco Discovery Protocol (CDP) service
IMSAlarmCatalog	All user authentication and credential definitions.
SLMAlarmCatalog	Alarms for Cisco Smart Licensing

CallManager Alarm Catalog Descriptions

The information in this section does not apply to Cisco Unity Connection.

The following table contains the CallManager Alarm Catalog descriptions.

Table 4: CallManager Alarm Catalog

Name	Description
CallManager	All Cisco CallManager service alarm definitions
CDRRepAlarmCatalog	All CDRRep alarm definitions
CARAlarmCatalog	All CDR analysis and reporting alarm definitions
CEFAlarmCatalog	All Cisco Extended Functions alarm definitions
CMIAlarmCatalog	All Cisco messaging interface alarm definitions
CtiManagerAlarmCatalog	All Cisco computer telephony integration (CTI) manager alarm definitions
IpVmsAlarmCatalog	All IP voice media streaming applications alarm definitions
TCDSRVAlarmCatalog	All Cisco telephony call dispatcher service alarm definitions

Name	Description
Phone	Alarms for phone-related tasks, such as downloads
CAPFAlarmCatalog	Alarms for Certificate Authority Proxy Function (CAPF) service
SAMLSSOAlarmCatalog	Alarms for SAML Single Sign On feature.

IM and Presence Alarm Catalog Descriptions

The following table contains the IM and Presence Service Alarm Catalog description.

Table 5: IM and Presence Service Alarm Catalog

Name	Description
CiscoUPSConfigAgent	All Config Agent alarms that notify the IM and Presence Service SIP Proxy of configuration changes in the IM and Presence Service IDS database.
CiscoUPInterclusterSyncAgent	All Intercluster Sync Agent alarms that synchronize end user information between IM and Presence Service clusters for intercluster routing.
CiscoUPSPresenceEngine	All Presence Engine alarms that collect information regarding the availability status and communications capabilities of a user.
CiscoUPSSIPProxy	All SIP Proxy alarms that are related to routing, requestor identification, and transport interconnection.
CiscoUPSSOAP	All simple object access protocol (SOAP) alarms that provide a secure SOAP interface to and from external clients using HTTPS.
CiscoUPSSyncAgent	All Sync Agent alarms that keep the IM and Presence Service data synchronized with Unified Communications Manager data.
CiscoUPXCP	All XCP alarms that collect information on the status of XCP components and services on IM and Presence Service.
CiscoUPServerRecoveryManager	All server recovery manager alarms that relate to the failover and fallback process between nodes in a presence redundancy group.
CiscoUPReplWatcher	All ReplWatcher alarms that monitor IDS Replication State.
CiscoUPXCPConfigManager	All Cisco XCP Config Manager alarm definitions that relate to XCP components.

Alarm information, which includes an explanation and recommended action, also includes the application name, server name, and other information, to help you perform troubleshooting, even for problems that are not on your local IM and Presence Service node.

For more information about the alarms that are specific to the IM and Presence Service, see *System Error Messages for IM and Presence on Cisco Unified Communications Manager*.

Default Alarms in CiscoSyslog File

The following table contains the description of the default alarms that are triggered in the CiscoSyslog file without any alarm configurations:

Table 6: Default Alarms in CiscoSyslog File

Name	Description
CLM_IPSecCertUpdated	The IPSec self-signed cert from a peer node in the cluster has been imported due to a change.
CLM_IPAddressChange	The IP address of a peer node in the cluster has changed.
CLM_PeerState	The ClusterMgr session state with another node in the cluster has changed to the current state.
CLM_MsgIntChkError	ClusterMgr has received a message which has failed a message integrity check. This can be an indication that another node in the cluster is configured with the wrong security password.
CLM_UnrecognizedHost	ClusterMgr has received a message from an IP address which is not configured as a node in this cluster.
CLM_ConnectivityTest	Cluster Manager detected a network error.
ServiceActivated	This service is now activated.
ServiceDeactivated	This service is now deactivated.
ServiceActivationFailed	Failed to activate this service.
ServiceDeactivationFailed	Failed to deactivate this service.
ServiceFailed	The Service has terminated abruptly. Service Manager will try to restart it.
ServiceStartFailed	Failed to start this service. Service Manager will attempt to start the service again.
ServiceStopFailed	Unable to stop the specified service after serveral retries. The service will be marked stopped.
ServiceRestartFailed	Unable to restart the specified service.

Name	Description
ServiceExceededMaxRestarts	Service failed to start, even after the max restarts attempts.
FailedToReadConfig	Failed to read configuration file. Configuration file might be corrupted.
MemAllocFailed	Failure to allocate memory.
SystemResourceError	System call failed.
ServiceManagerUnexpectedShutdown	Service Manager restarted successfully after an unexpected termination.
OutOfMemory	The process has requested memory from the operating system, and there was not enough memory available.
CREATE-DST-RULE-FILE-CLI	New DST rules file is generated from cli. Phones need to be restarted.Not restarting the phones would result in wrong DST start / stop dates.
CREATE-DST-RULE-FILE-BOOTUP	New DST rules file is generated during bootup. Phones need to be restarted.Not restarting the phones would result in wrong DST start / stop dates.
CREATE-DST-RULE-FILE-CRON	New DST rules file is generated from cron. Phones need to be restarted.Not restarting the phones would result in wrong DST start / stop dates.
PermissionDenied	An operation could not be completed because the process did not have authority to perform it.
ServiceNotInstalled	An executable is trying to start but cannot because it is not configured as a service in the service control manager. The service name is %s.
ServiceStopped	A service has stopped.
ServiceStarted	A service has started.
ServiceStartupFailed	A service has started.
FileWriteError	Failed to write into the primary file path.