

Main page: [Cisco Unified Presence, Release 7.x](#)

Contents

- [1 Previous Topic](#)
- [2 Alert Messages](#)
- [3 Preconfigured Alerts](#)
 - ◆ [3.1 Related Topics](#)
- [4 Alert Fields](#)
 - ◆ [4.1 Table 1: Alert Customization](#)
 - ◆ [4.2 Related Topics](#)
- [5 Alert Logs](#)
 - ◆ [5.1 Related Topics](#)

Previous Topic

- [How to Work with Alerts in RTMT](#)

- [Alert Messages](#)

- [Preconfigured Alerts](#)

- [Alert Fields](#)

- [Alert Logs](#)

Alert Messages

The system generates alert messages to notify administrator when a predefined condition is met, such as when an activated service goes from up to down. Alerts can be sent out as email/epage.

RTMT, which supports alert defining, setting, and viewing, contains preconfigured and user-defined alerts. Although you can perform configuration tasks for both types, you cannot delete preconfigured alerts (whereas you can add and delete user-defined alerts).

The Alert menu comprises the following menu options:

- Alert Central-This option comprises the history and current status of every alert in the system.
Note: You can also access Alert Central by clicking the Alert Central icon in the hierarchy tree in the system drawer.
- Set Alert/Properties-This menu option allows you to set alerts and alert properties.
- Remove Alert-This menu category allows you to remove an alert.

Cisco_Unified_Presence,_Release_7.x_--_About_Alerts

- Enable Alert-With this menu category, you can enable alerts.
- Disable Alert-You can disable an alert with this category.
- Suspend cluster/node Alerts-This menu category allows you to temporarily suspend alerts on a particular Cisco Unified Presence node or on the entire cluster.
- Clear Alerts-This menu category allows you to reset an alert (change the color of an alert item from to black) to signal that an alert has been taken care of. After an alert has been raised, its color will automatically change to in RTMT and will stay that way until you manually clear the alert.
- Clear All Alerts-This menu category allows you to clear all alerts.
- Alert Detail-This menu category provides detailed information on alert events.
- Config Email Server-In this category, you can configure your email server to enable alerts.
- Config Alert Action-This category allows you to set actions to take for specific alerts; you can configure the actions to send the alerts to desired email recipients.

In RTMT, you configure alert notification for perfmon counter value thresholds and set alert properties for the alert, such as the threshold, duration, frequency, and so on.

You can locate Alert Central under the Tools hierarchy tree in the quick launch. Alert Central provides both the current status and the history of all the alerts in the system.

Preconfigured Alerts

The Real-Time Monitoring Tool (RTMT) displays both preconfigured alerts and custom alerts in Alert Central. RTMT organizes the alerts under different tabs-System, CUP, and Custom.

You can enable or disable preconfigured and custom alerts in Alert Central; however, you cannot delete preconfigured alerts.

The following list comprises the preconfigured alerts for the system:

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown

Note: The CriticalServiceDown alert only generates when the service status equals down (not for other states).

- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded

- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown

Note: The ServerDown alert generates when the currently "active" AMC (primary AMC or the backup AMC, when the primary is not available) cannot reach another node in a cluster. This alert identifies network connectivity issues in addition to a server down condition.

- SparePartitionLowWaterMarkExceeded
- SparePartitionHighWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadExceededThreshold

Related Topics

- [Getting More Information](#)

Alert Fields

You can configure both preconfigured and user-defined alerts in RTMT. You can also disable both preconfigured and user-defined alerts in RTMT. You can add and delete user-defined alerts in the performance-monitoring window; however, you cannot delete preconfigured alerts.

Table 1: Alert Customization provides a list of fields that you may use to configure each alert; users can configure preconfigured fields, unless otherwise noted.

Table 1: Alert Customization

Field	Description	Comment
Alert Name	High-level name of the monitoring item with which RTMT associates an alert	Descriptive name. For preconfigured alerts, you cannot change this field. For a list of preconfigured alerts, see Preconfigured Alerts .
Description	Description of the alert	You cannot edit this field for preconfigured alerts. For a list of preconfigured alerts, see Preconfigured Alerts .
Performance Counter(s)	Source of the performance counter	You cannot change this field.
Threshold	Condition to raise alert (value is...)	Specify up < - > down, less than #, %, rate greater than #, %, rate.

Cisco_Unified_Presence,_Release_7.x_--_About_Alerts

Value Calculated As	Method used to check the threshold condition	Specify value to be evaluated as absolute, delta (present - previous), or % delta.
Duration	Condition to raise alert (how long value threshold has to persist before raising alert)	Options include the system sending the alert immediately or after a specified time that the alert has persisted.
Node IDs	Cluster or list of nodes to monitor	Cisco Unified Presence nodes. Note: When you unassign a node, the system considers that node as removed from the currently monitored node list. When you reassign a node, that node is added back, and its settings get restored to default values.
Alert Action ID	ID of alert action to take (System always logs alerts no matter what the alert action.)	Alert action is defined first If this field is blank, that indicates that email is disabled.
Enable Alerts	Enable or disable alerts.	Options include enabled or disabled.
Clear Alert	Resets alert (change the color of an alert item from to black) to signal that the alert has been resolved	After an alert has been raised, its color will automatically change to and stay that way until you manually clear the alert. Use Clear All to clear all alerts.
Alert Generation Rate	How often to generate alert when alert condition persists	Specify every X minutes. (Raise alert once every X minutes if condition persists.) Specify every X minutes up to Y times. (Raise alert Y times every X minutes if condition persists.)
User Provide Text	Administrator to append text on top of predefined alert text	N/A
Severity	For viewing purposes (for example, show only Sev. 1 alerts)	Specify defaults that are provided for predefined (for example, Error, Warning, Information) alerts.

Related Topics

- [Getting More Information](#)

Alert Logs

The alert log stores the alert, which is also stored in memory. The memory is cleared at a constant interval, leaving the last 30 minutes of data in the memory. When the service starts/restarts, the last 30 minutes of the alert data load into the memory by the system reading from the alert logs that exist in all servers in the cluster. The alert data in the memory is sent to the RTMT clients on request.

Upon RTMT startup, RTMT shows all logs that occurred in the last 30 minutes in the Alert Central log history. The alert log periodically updates, and new logs are inserted into the log history window. After the number of logs reaches 100, RTMT removes the oldest 40 logs.

Cisco_Unified_Presence,_Release_7.x_--_About_Alerts

The following file name format for the alert log applies: AlertLog_MM_DD_YYYY_hh_mm.csv.

The alert log includes the following attributes:

- Time Stamp-Time when RTMT logs the data
- Alert Name-Descriptive name of the alert
- Node-Node name for where RTMT raised the alert
- Alert Message-Detailed description about the alert
- Description-Description of the monitored object
- Severity-Severity of the alert
- PollValue-Value of the monitored object where the alert condition occurred
- Action-Alert action taken
- Group ID-Identifies the source of the alert

The first line of each log file comprises the header. Details of each alert get written in a single line, separated by a comma.

Related Topics

- [Getting More Information](#)