

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

Contents

- [1 Previous Topic](#)
- [2 Working in Alert Central](#)
 - ◆ [2.1 Before You Begin](#)
 - ◆ [2.2 Procedure](#)
 - ◆ [2.3 Troubleshooting Tips](#)
 - ◆ [2.4 Related Topics](#)
- [3 Setting Alert Properties](#)
 - ◆ [3.1 Procedure](#)
 - ◆ [3.2 Troubleshooting Tips](#)
 - ◆ [3.3 Related Topics](#)
 - ◆ [3.4 What To Do Next](#)
- [4 How To Configure Alert Actions](#)
 - ◆ [4.1 Table: Alert Action Configuration](#)
 - ◆ [4.2 Configuring Alert Actions](#)
 - ◇ [4.2.1 Before You Begin](#)
 - ◇ [4.2.2 Procedure](#)
 - ◇ [4.2.3 What To Do Next](#)
 - ◇ [4.2.4 Related Topics](#)
 - ◆ [4.3 Configuring Emails for Alert Notification](#)
 - ◇ [4.3.1 Procedure](#)
 - ◇ [4.3.2 Related Topics](#)
- [5 Enabling Trace Downloads](#)
 - ◆ [5.1 Before You Begin](#)
 - ◆ [5.2 Procedure](#)
 - ◆ [5.3 Troubleshooting Tips](#)
 - ◆ [5.4 Related Topics](#)
- [6 Suspending Alerts on Cisco Unified Presence Nodes or Clusters](#)
 - ◆ [6.1 Procedure](#)
 - ◆ [6.2 Troubleshooting Tips](#)
 - ◆ [6.3 Related Topics](#)
- [7 Configuring Log Partition Monitoring](#)
 - ◆ [7.1 Before You Begin](#)
 - ◆ [7.2 Procedure](#)
 - ◆ [7.3 Related Topics](#)

Previous Topic

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

- [Working in Alert Central](#)
- [Setting Alert Properties](#)
- [How To Configure Alert Actions](#)

- [Enabling Trace Downloads](#)
- [Suspending Alerts on Cisco Unified Presence Nodes or Clusters](#)
- [Configuring Log Partition Monitoring](#)

Working in Alert Central

You can access Alert Central and perform the following tasks:

- sort alert information
- enable, disable, or remove an alert
- clear an alert
- view alert details

Before You Begin

Review the information about alerts.

Procedure

1. Perform one of the following actions:

- On the Quick Launch Channel:
 - ◆ Click **System**.
 - ◆ In the tree hierarchy, double-click **Tools**.
 - ◆ Click the Alert Central icon.
- Select **System > Tools > Alert > Alert Central**.

2. Perform one or more of the following actions:

If you want to:	Action
Set alert properties	See Setting Alert Properties .
Suspend alerts on Cisco Unified Presence nodes	See Suspending Alerts on Cisco Unified Presence Nodes or Clusters .
Configure emails for alert notification	See Configuring Emails for Alert Notification .
Configure alert actions	See Configuring Alert Actions .
Sort alert information in the Alert Status pane	1. Click the up/down arrow that displays in the column heading. For example, click the up/down arrow that displays in the Enabled or InSafeRange column
Sort alert history information	1. Click the up/down arrow in the columns in the Alert History pane. 2. Use the scroll bar on the right side of the Alert History pane to see alert history that is out of view in the pane.

Enable, disable, or remove an alert	<p>Perform one of the following actions:</p> <ol style="list-style-type: none"> 1. From the Alert Status window, right-click the alert and select Disable/Enable Alert (option toggles) or Remove Alert, depending on what you want to accomplish. 2. Highlight the alert in the Alert Status window and select System > Tools > Alert > Disable/Enable (or Remove Alert).
Clear either individual or collective alerts after they get resolved	<p>Perform one of the following actions:</p> <ol style="list-style-type: none"> 1. After the Alert Status window displays, right-click the alert and select Clear Alert (or Clear All Alerts). 2. Highlight the alert in the Alert Status window and select System > Tools > Alert > Clear Alert (or Clear All Alerts).
View alert details	<ol style="list-style-type: none"> 1. Perform one of the following actions <ul style="list-style-type: none"> ◇ After the Alert Status window displays, right-click the alert and select Alert Details. ◇ Highlight the alert in the Alert Status window and select System > Tools > Alert > Alert Details. 2. After you have finished viewing the alert details, click OK.

Troubleshooting Tips

You can only remove user-defined alerts from RTMT. The Remove Alert option appears grayed out when you select a preconfigured alert.

Related Topics

- [About Alerts](#)
- [Getting More Information](#)

Setting Alert Properties

Using the alert notification feature, the application notifies you of system problems. The following configuration setup is required to activate alert notifications for a system performance counter:

From the RTMT Perfmon Monitoring pane, you can select the system perfmon counter and:

- Set up an email or a message popup window for alert notification.
- Determine the threshold for the alert.
- Determine the frequency of the alert notification (for example, the alert occurs once or every hour)
- Determine the schedule for when the alert activates (for example, on a daily basis or at certain times of the day).

Procedure

1. Perform one of the following actions:

If you want to:	Action
Set alert properties for a performance counter	<ol style="list-style-type: none"> 1. Display the performance counter. 2. From the counter chart or table, right-click the counter for which you want to configure the alert notification, and select Set Alert/Properties. 3. Check Enable Alert.
Set alert properties from Alert Central	<ol style="list-style-type: none"> 1. Access Alert Central. 2. Click the alert for which you want to set alert properties. 3. Perform one of the following actions: <ul style="list-style-type: none"> • Right-click the alert and select Set Alert/Properties. • Select System > Tools > Alert > Set Alert/Properties. • Check Enable Alert.

2. Select the severity level at which you want to be notified in the Severity list box.
3. Enter a description of the alert in the Description pane.
4. Click **Next**.
5. Configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes.

Setting	Description
Threshold Pane	
Trigger alert when following conditions met (Over, Under)	<p>Check and enter the value that applies.</p> <ul style="list-style-type: none"> ◇ Over-Check to configure a maximum threshold that must be met before an alert notification is activated. In the Over value field, enter a value. For example, enter a value that equals the number of calls in progress. ◇ Under-Check to configure a minimum threshold that must be met before an alert notification is activated. In the Under value field, enter a value. For example, enter a value that equals the number of calls in progress. <p>Tip: Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.</p>
Value Calculated As Pane	
Absolute, Delta, Delta Percentage	<p>Click the radio button that applies.</p> <ul style="list-style-type: none"> ◇ Absolute-Because some counter values are accumulative, select Absolute to display the data at its current status. ◇ Delta-Select Delta to display the difference between the current counter value and the previous counter value. ◇ Delta Percentage-Select Delta Percentage to display the counter performance changes in percentage.
Duration Pane	

Cisco_Unified_Presence,_Release_7.x_--_How_to_Configure_Alert_Messages

Trigger alert only when value constantly...; Trigger alert immediately	<ul style="list-style-type: none">◇ Trigger alert only when value constantly...-If you want the alert notification only when the value is constantly below or over threshold for a desired number of seconds, click this radio button and enter seconds after which you want the alert to be sent.◇ Trigger alert immediately-If you want the alert notification to be sent immediately, click this radio button.
Frequency Pane	
Trigger alert on every poll; trigger up to...	Select the radio button that applies. <ul style="list-style-type: none">◇ Trigger alert on every poll-If you want the alert notification to activate on every poll when the threshold is met, click this radio button.◇ Trigger up to...-If you want the alert notification to activate at certain intervals, click this radio button and enter the number of alerts that you want sent and the number of minutes within which you want them sent.
Schedule Pane	
24-hours daily; start/stop	Select the radio button that applies: <ul style="list-style-type: none">◇ 24-hours daily-If you want the alert to be triggered 24 hours a day, click this radio button.◇ Start/Stop-If you want the alert notification activated within a specific time frame, click the radio button and enter a start time and a stop time. If checked, enter the start and stop times of the daily task. For example, you can configure the counter to be checked every day from 9:00 am to 5:00 pm or from 9:00 pm to 9:00 am.

Troubleshooting Tips

For Cisco Unified Presence clusterwide alerts, the Enable/Disable this alert on following server(s) does not display in the Alert Properties window. Clusterwide alerts include number of registered phones, gateways, media devices, route list exhausted, media list exhausted, MGCP D-channel out of service, malicious call trace, and excessive quality reports.

Related Topics

- [About Alerts](#)
- [Working in Alert Central](#)
- [Getting More Information](#)

What To Do Next

[Configuring Alert Actions](#)

How To Configure Alert Actions

In RTMT, you can configure alert actions for every alert that is generated and have the alert action sent to email recipients that you specify in the alert action list.

Table: Alert Action Configuration provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table: Alert Action Configuration

Field	Description	Comment
Alert Action ID	ID of alert action to take	Specify descriptive name.
Mail Recipients	List of email addresses. You can selectively enable/disable an individual email in the list.	N/A

- [Configuring Alert Actions](#)
- [Configuring Emails for Alert Notification](#)

Configuring Alert Actions

Before You Begin

Set alert properties.

Procedure

1. Complete one or more of the following actions in the Alert Properties: Frequency and Schedule window:

If you want to:	Action
Trigger an alert action with this alert	Select the alert action that you want to send from the list box.
Add a new alert action	<ol style="list-style-type: none"> 1. Click Configure. 2. Click Add in the Alert Action window. 3. Enter a name for the alert action in the Name field. 4. Enter a description of the alert action in the Description field.
Edit an existing alert action	<ol style="list-style-type: none"> 1. Click Configure. 2. Highlight the alert action. 3. Click Edit. 4. Update the configuration. 5. Click OK.
Delete an alert action	<ol style="list-style-type: none"> 1. Click Configure.

	<ol style="list-style-type: none"> 2. Highlight the alert action. 3. Click Delete.
Add an email recipient to receive the alert action	<ol style="list-style-type: none"> 1. Click Configure. 2. Click Add in the Alert Action window. 3. Click Add again in the Recipients frame of the Action Configuration window. 4. Enter an email or epage address of the recipient in the Enter email/epage address field. 5. Click OK.
Enable email for a named email recipient	Check Enable Email .
Disable or delete an email recipient	Perform one of the following actions: <ul style="list-style-type: none"> ◇ Highlight the recipient and uncheck Enable. ◇ Highlight the recipient and click Delete.

2. Enter the text that you want to display in the email message in the User-defined email text box.
3. Click **Save** after you finish configuring the alert action.

What To Do Next

Enabling Trace Downloads

Related Topics

- [About Alerts](#)
- [Setting Alert Properties](#)
- [Configuring Emails for Alert Notification](#)
- [Getting More Information](#)

Configuring Emails for Alert Notification

Procedure

1. Select **System > Tools > Alert > Config Email Server**.
2. Enter the email recipient information in the Mail Server field.
3. Enter the port number of the mail server in the Port field. The default port is 25.
4. Click **Add** in the Recipients frame of the Mail Server Configuration window.
5. Enter an email or epage address of the recipient in the Enter email/epage address field.
6. Enter the text that you want to display in the email message in the Default Message text box.
7. Click **OK**.

Related Topics

- [About Alerts](#)
- [Setting Alert Properties](#)
- [Configuring Alert Actions](#)
- [Getting More Information](#)

Enabling Trace Downloads

Some preconfigured alerts will allow you to initiate a trace download based on the occurrence of an event. You can automatically capture traces when a particular event occurs by checking Enable Trace Download in Set Alert/Properties for the following alerts:

- CriticalServiceDown
- CoreDumpFileFound

Caution! Enabling Trace Download may affect services on the server. Configuring a high number of downloads will adversely impact the quality of services on the server.

Before You Begin

Configure alert actions.

Procedure

1. Click **Activate** in the Alert Properties: Email Notification window for alerts that do not allow trace download.
2. Perform the following actions for alerts, such as CriticalServiceDown, that allow trace download:
 1. Click **Next**.
 2. Check **Enable TCT Download** in the Alert Properties: TCT Download window.
 3. Enter the IP address, a user name, password, port and download directory path where the trace will be saved.
 4. Click **Test Connection** to ensure that you have connectivity with the SFTP server. **If the connection test fails, your settings will not be saved.**
 5. Click **OK**.
 6. Enter the number and frequency of downloads in the TCT Download Parameters window. Setting the number and frequency of download will help you to limit the number of trace files that will be downloaded. The setting for polling provides the basis for the default setting for the frequency.

Troubleshooting Tips

Enabling TCT Download may affect services on the server. Configuring a high number of downloads will adversely impact the quality of services on the server.

Related Topics

- [About Alerts](#)
- [Configuring Alert Actions](#)
- [Setting Alert Properties](#)
- [Getting More Information](#)

Suspending Alerts on Cisco Unified Presence Nodes or Clusters

You may want to temporarily suspend some or all alerts, either on a particular Cisco Unified Presence node or the entire cluster. For example, if you are upgrading the Cisco Unified Presence to a newer release, you would probably want to suspend all alerts until the upgrade completes, to ensure you do not receive emails or pages during the upgrade.

Procedure

1. Select **System > Tools > Alert > Suspend Cluster/Node Alerts**.
2. Perform one of the following actions:

If you want to:	Action
Suspend all alerts in the cluster	<ol style="list-style-type: none"> 1. Click Cluster Wide. 2. Check Suspend all alerts. 3. Click OK.
Suspend alerts per server	<ol style="list-style-type: none"> 1. Click Per Server. 2. Check Suspend for each server on which you want alerts to be suspended. 3. Click OK.
Resume alerts	<ol style="list-style-type: none"> 1. Select System > Tools > Alert > Suspend Cluster/Node Alerts. 2. Uncheck Suspend for each server on which you want alerts to resume. 3. Click OK.

Troubleshooting Tips

Per server suspend states do not apply to Cisco Unified Presence clusterwide alerts.

Related Topics

- [About Alerts](#)
- [Configuring Alert Actions](#)
- [Setting Alert Properties](#)
- [Getting More Information](#)

Configuring Log Partition Monitoring

Log Partition Monitoring, which is installed automatically with the system, uses configurable thresholds to monitor the disk usage of the log partition on a server. The Cisco Log Partitioning Monitoring Tool service starts automatically after installation of Cisco Unified Presence.

Every 5 minutes, Log Partition Monitoring uses the following configured thresholds to monitor the disk usage of the log partition on a server:

- `LogPartitionLowWaterMarkExceeded` (% disk space)-When the disk usage is above the percentage that you specify, LPM sends out an alarm message to syslog and an alert to RTMT Alert central. To save the log files and regain disk space, you can use trace and log central option in RTMT.
- `LogPartitionHighWaterMarkExceeded` (% disk space)-When the disk usage is above the percentage that you specify, LPM sends a n alarm message to syslog and an alert to RTMT Alert central.

In addition, Cisco Log Partitioning Monitoring Tool service checks the server every 5 seconds for newly created core dump files. If there are new core dump files, Cisco Log Partitioning Monitoring Tool service sends a `CoreDumpFileFound` alarm and an alert to Alert Central with information on each new core file.

When the log partition monitoring services starts at system startup, the service checks the current disk space utilization. If the percentage of disk usage is above the low water mark, but less than the high water mark, the service sends a alarm message to syslog and generates a corresponding alert in RTMT Alert central.

To configure Log Partitioning Monitoring, set the alert properties for the `LogPartitionLowWaterMarkExceeded` and `LogPartitionHighWaterMarkExceeded` alerts in Alert Central.

To offload the log files and regain disk space on the server, you should collect the traces that you are interested in saving by using the Real-Time Monitoring tool.

If the percentage of disk usage is above the high water mark that you configured, the system sends an alarm message to syslog, generates a corresponding alert in RTMT Alert Central, and automatically purges log files until the value reaches the low water mark.

Note: Log Partition Monitoring automatically identifies the common partition that contains an active directory and inactive directory. The active directory contains the log files for the current version of Cisco Unified Presence, and the inactive directory contains the log files for the previous installed version of Cisco Unified Presence. If necessary, the service deletes log files in the inactive directory first. The service then deletes log files in the active directory, starting with the oldest log file for every application until the disk space percentage drops below the configured low water mark. The service does not send an email when log partition monitoring purges the log files.

After the system determines the disk usage and performs the necessary tasks (sending alarms, generating alerts, or purging logs), log partition monitoring occurs at regular 5 minute intervals.

Before You Begin

To utilize the log partition monitor, verify that the Cisco Log Partitioning Monitoring Tool service, a network service, is running on each node in the cluster on Cisco Unified Serviceability. Stopping the service causes a loss of feature functionality.

Procedure

1. Select **Tools > Control Center > Network Services**.
2. Select the server where you want to monitor the disk usage from the Servers list box.
3. Click **Go**.
4. Verify the status of the Cisco Log Partition Monitoring Tool (LPM) under Performance and Monitoring Services.
5. Click the radio button next to Cisco LPM if the LPM is not running.
6. Click **Start**.

Related Topics

- [About Alerts](#)
- [Configuring Alert Actions](#)
- [Setting Alert Properties](#)
- [Getting More Information](#)