Alerts

Alert Central Displays

Unified RTMT displays both preconfigured alerts and custom alerts in Alert Central. Unified RTMT organizes the alerts under the applicable tabs: System, Voice/Video, IM and Presence Service, Cisco Unity Connection, and Custom.

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

System Alerts

The following list comprises the preconfigured system alerts:

- AuthenticationFailed
- CiscoDRFFailure
- CoreDumpFileFound
- CpuPegging
- CriticalServiceDown
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutofSync
- HardwareFailure
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded

- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- LowAvailableVirtualMemory
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown (Applies to Unified Communications Manager clusters)
- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatched
- TotalProcessesAndThreadsExceededThreshold

Related Topics

System Alerts

Automatic Trace Download Activation

Some preconfigured alerts 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 the **Enable Trace Download** check box in Set Alert/Properties for the following alerts:

- CriticalServiceDown: CriticalServiceDown alert is generated when any service is down. CriticalServiceDown alert monitors only those services that are listed in RTMT Critical Services.

Note The Unified RTMT backend service checks status (by default) every 30 seconds. If service goes down and comes back up within that period, CriticalServiceDown alert may not be generated.

- CodeYellow: This alarm indicates that Cisco Unified Communications Manager initiated call throttling due to unacceptably high delay in handling calls.
- CoreDumpFileFound: CoreDumpFileFound alert is generated when the Unified RTMT backend service detects a new Core Dump file.

Note You can configure both CriticalServiceDown and CoreDumpFileFound alerts to download corresponding trace files for troubleshooting purposes. This setup helps preserve trace files at the time of crash.

Caution Trace Download may affect services on the node. A high number of downloads adversely impacts the quality of services on the node.

Voice and Video Alerts

The following list comprises the preconfigured Voice and Video alerts:

- BeginThrottlingCallListBLFSubscriptions
- CallAttemptBlockedByPolicy
- CallProcessingNodeCpuPegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- CARSchedulerJobFailed
- CDRAgentSendFileFailed
- CDRFileDeliveryFailed
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CiscoElmNotConnected
- CiscoGraceTimeLeft
- CiscoNoProvisionTimeout
- CiscoSystemInDemo
- CiscoSystemInOverage
- CiscoSystemSecurityMismatch
- CodeYellow
- DDRBlockPrevention
- DDRDown
- EMCCFailedInLocalCluster
- EMCCFailedInRemoteCluster
- ExcessiveVoiceQualityReports
- ILSHubClusterUnreachable
- ILSPwdAuthenticationFailed
- ILSTLSAuthenticationFailed
- IMEDistributedCacheInactive
- IMEOverQuota

- IMEQualityAlert
- IMEServiceStatus
- InsufficientFallbackIdentifiers
- InvalidCredentials
- LocationOutOfResource
- MaliciousCallTrace
- MediaListExhausted
- MgcpDChannelOutOfService
- NumberOfRegisteredDevicesExceeded
- NumberOfRegisteredGatewaysDecreased
- NumberOfRegisteredGatewaysIncreased
- NumberOfRegisteredMediaDevicesDecreased
- NumberOfRegisteredMediaDevicesIncreased
- NumberOfRegisteredPhonesDropped
- RecordingCallSetupFail
- RecordingGatewayRegistrationRejected
- RecordingGatewayRegistrationTimeout
- RecordingGatewaySessionFailed
- RecordingResourcesNotAvailable
- RecordingSessionTerminatedUnexpectedly
- RouteListExhausted
- RTMTSessionExceedsThreshold
- SDLLinkOutOfService
- TCPSetupToIMEFailed
- TLSConnectionToIMEFailed
- UserInputFailure

Related Topics

Voice and Video Alerts

IM and Presence Service Alerts

The following list comprises the preconfigured IM and Presence Service alerts:

- CTIGWModuleNotEnabled
- CTIGWProviderDown

- CTIGWUserNotLicenced
- CTIGWUserNotAuthorized
- CTIGWProviderFailedToOpen
- CTIGWQBEFailedRequest
- CTIGWSystemError
- EspConfigAgentMemAllocError
- EspConfigAgentFileWriteError
- EspConfigAgentNetworkOutage
- EspConfigAgentNetworkRestored
- EspConfigAgentHighMemoryUtilization
- EspConfigAgentHighCPUUtilization
- EspConfigAgentLocalDBAccessError
- EspConfigAgentProxyDomainNotConfigured
- EspConfigAgentRemoteDBAccessError
- EspConfigAgentSharedMemoryStaticRouteError
- ESPConfigError
- ESPConfigNotFound
- ESPCreateLockFailed
- ESPLoginError
- ESPMallocFailure
- ESPNAPTRInvalidRecord
- ESPPassedParamInvalid
- ESPRegistryError
- ESPRoutingError
- ESPSharedMemCreateFailed
- ESPSharedMemSetPermFailed
- ESPSharedMemAllocFailed
- ESPSocketError
- ESPStopped
- ESPStatsLogFileOpenFailed
- ESPVirtualProxyError
- ESPWrongIPAddress
- ESPWrongHostName

- ICSACertificateCASignedTrustCertFound
- ICSACertificateFingerPrintMisMatch
- ICSACertificateValidationFailure
- InterclusterSyncAgentPeerDuplicate
- LegacyCUPCLogin
- NotInCucmServerListError
- PEAutoRecoveryFailed
- PEDatabaseError
- PEIDSQueryError
- PEIDSSubscribeError
- PEIDStoIMDBDatabaseSyncError
- PELoadHighWaterMark
- PEMemoryHighCondition
- PEPeerNodeFailure
- PESipSocketBindFailure
- PEStateDisabled
- PEStateLocked
- PEWebDAVInitializationFailure
- PWSSCBFindFailed
- PWSSCBInitFailed
- PWSAboveCPULimit
- PWSAboveSipSubscriptionLimit
- PWSRequestLimitReached
- SRMFailed
- SRMFailover
- SyncAgentAXLConnectionFailed
- UASCBFindFailed
- UASCBGetFailed
- XcpCmComponentConnectError
- XcpCmPauseSockets
- XcpCmStartupError
- XcpCmXmppdError
- XcpConfigMgrConfigurationFailure

- XcpConfigMgrHostNameResolutionFailed
- XcpConfigMgrJabberRestartRequired
- XcpConfigMgrR2RPasswordEncryptionFailed
- XcpConfigMgrR2RRequestTimedOut
- XcpDBConnectError
- XcpMdnsStartError
- XcpSIPFedCmComponentConnectError
- XcpSIPFedCmStartupError
- XcpSIPGWStackResourceError
- XcpThirdPartyComplianceConnectError
- XcpTxtConfComponentConfigError
- XcpTxtConfDBConnectError
- XcpTxtConfDBQueueSizeLimitError
- XcpTxtConfGearError
- XcpWebCmComponentConnectError
- XcpWebCmHttpdError
- XcpWebCmStartupError
- XcpXMPPFedCmComponentConnectError
- XcpXMPPFedCmStartupError

Related Topics

IM and Presence Service Alerts

Cisco Unity Connection Alerts

The following list comprises the preconfigured Cisco Unity Connection alerts.

- NoConnectionToPeer
- AutoFailoverSucceeded
- AutoFailoverFailed
- AutoFailbackSucceeded
- AutoFailbackFailed
- SbrFailed (Split Brain Resolution Failed)
- DiskConsumptionCloseToCapacityThreshold
- DiskConsumptionExceedsCapacityThreshold
- LicenseExpirationWarning

- LicenseExpired

Note The first six alerts apply only to Cisco Unity Connection cluster configurations.

Related Topics

Cisco Unity Connection Alerts

Alert Action Setup

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

The following table provides a list of fields that you will use to configure alert actions. Users can configure all fields, unless otherwise marked.

Table 1: Alert Action Configuration

Field	Description	Comment
Alert Action ID	ID of alert action to take.	Specify descriptive name.
Mail Recipients	List of e-mail addresses. You can selectively enable or disable an individual e-mail in the list.	—

Access Alert Central and Set Up Alerts

By using the following procedure, you can perform tasks, such as access Alert Central, sort alert information, enable, disable, or remove an alert, clear an alert, or view alert details.

Procedure

Step 1 Perform one of the following tasks:

a) On the Quick Launch Channel, do the following:

1. Click **System**.
2. In the tree hierarchy, double-click **Tools**.
3. Click the Alert Central icon.

b) Choose **System** > **Tools** > **Alert** > **Alert Central**.
The **Alert Central monitoring** window displays and shows the alert status and alert history of the alerts that the system has generated.

Step 2 Perform one of the following tasks:

a) Set alert properties.
b) Suspend alerts.
c) Configure e-mails for alert notification.
d) Configure alert actions.
e) Sort alert information in the Alert Status pane. Click the up/down arrow that displays in the column heading. For example, click the up/down arrow that displays in the Enabled or In Safe Range column.

   You can sort alert history information by clicking the up/down arrow in the columns in the Alert History pane. To see alert history that is out of view in the pane, use the scroll bar on the right side of the Alert History pane.

f) To enable, disable, or remove an alert, perform one of the following tasks:

   - From the Alert Status window, right-click the alert and choose **Disable/Enable Alert** (option toggles) or **Remove Alert**, depending on what you want to accomplish.
   - Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Disable/Enable (or Remove) Alert**.

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

g) To clear either individual or collective alerts after they get resolved, perform one of the following tasks:

   - After the **Alert Status** window displays, right-click the alert and choose **Clear Alert** (or **Clear All Alerts**).
   - Highlight the alert in the Alert Status window and choose **System** > **Tools** > **Alert** > **Clear Alert** (or **Clear All Alerts**).

   After you clear an alert, it changes from red to black.

h) To reset alerts to default configuration, perform one of the following tasks:

   - After the Alert Status window displays, right-click the alert and choose **Reset Alert to Default Config**, to reset that alert to the default configuration.
   - Choose **System** > **Tools** > **Alert** > **Reset all Alerts to Default Config**, to reset all the alerts to the default configuration.

i) To view alert details, perform one of the following tasks:

   - After the **Alert Status** window displays, right-click the alert and choose **Alert Details**.
   - Highlight the alert in the **Alert Status** window and choose **System** > **Tools** > **Alert** > **Alert Details**.

   Tip After you have finished viewing the alert details, click **OK**.

Set 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 select the system perfmon counter and perform the following actions:

- Set up an e-mail 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).

Tip To remove the alert for the counter, right-click the counter and choose Remove Alert. The option appears dim after you remove the alert.

Procedure

Step 1 Perform one of the following actions:

If you want to:	Action
Set alert properties for a performance counter	• Display the performance counter. • From the counter chart or table, right-select the counter for which you want to configure the alert notification, and select **Set Alert/Properties**. • Check the **Enable Alert** check box.
Set alert properties from Alert Central	• Access Alert Central. • Select the alert for which you want to set alert properties. Perform one of the following actions: ◦ Right-select the alert and select **Set Alert/Properties**. ◦ Select **System** > **Tools** > **Alert** > **Set Alert/Properties**. ◦ Check the **Enable Alert** check box.

Step 2 Select the severity level at which you want to be notified in the Severity list check box.

Step 3 Enter a description of the alert in the Description pane.

Step 4 Select **Next**.

Step 5 Configure the settings in the Threshold, Value Calculated As, Duration, Frequency, and Schedule panes.

Table 2: Counter Alert Configuration Parameters

Setting	Description
Threshold Pane	
Trigger alert when following conditions met (Over, Under)	Check and enter the value that applies: • 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. **Tip** Use these check boxes in conjunction with the Frequency and Schedule configuration parameters.
Value Calculated As Pane	
Absolute, Delta, Delta Percentage	Select the radio button that applies: • 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	
Trigger alert only when value constantly...; Trigger alert immediately	• 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, select 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, select this radio button.
Frequency Pane	

Setting	Description
Trigger alert on every poll; trigger up to...	Select the radio button that applies: • Trigger alert on every poll: If you want the alert notification to activate on every poll when the threshold is met, select this radio button. • Trigger up to...: If you want the alert notification to activate at certain intervals, select 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: • 24-hours daily: If you want the alert to be triggered 24 hours a day, select this radio button. • Start/Stop: If you want the alert notification activated within a specific time frame, select 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 a.m. to 5:00 p.m. or from 9:00 p.m. to 9:00 a.m.

Suspend Alerts

You may want to temporarily suspend some or all alerts; you can suspend alerts on a particular node or on an entire cluster. For example, if you are upgrading your system to a newer release, suspend alerts until the upgrade completes, so that you do not receive e-mails and e-pages during the upgrade.

Follow this procedure to suspend alerts in Alert Central.

Procedure

Step 1 Choose **System** > **Tools** > **Alert** > **Suspend cluster/node Alerts**.

Note Per node suspend states do not apply to clusterwide alerts.

Step 2 Perform one of the following actions:

- To suspend all alerts in the cluster, click the **Cluster Wide** radio button and check the **Suspend all alerts** check box.

- To suspend alerts per server, click the **Per Server** radio button and check the **Suspend** check box of each server on which you want alerts to be suspended.

Step 3 Click **OK**.

Note To resume alerts, choose **Alert** > **Suspend cluster/node Alerts** and uncheck the suspend check boxes.

Set up alerts for core dump and collect relevant logs

Core dumps can be difficult to reproduce so it is particularly important to collect the log files associated with them when they occur and before they are over written.

Set up an e-mail alert for core dumps, so that you are immediately notified when one occurs to assist in troubleshooting its cause.

Enable email alert

Procedure

Step 1 Select **System** > **Tools** > **Alert Central**.

Step 2 Right-click **CoreDumpFileFound** alert and select **Set Alert Properties**.

Step 3 Follow the wizard to set your preferred criteria, including checking the **Enable Email** check box.

Step 4 Select **System** > **Tools** > **Alert** > **Config Email Server**.

Step 5 Enter the e-mail server settings.

Collect logs

Follow this procedure to collect logs after you receive an e-mail alert.

Procedure

Step 1 Note which services initiated the alert, which are indicated by “Core” in the e-mail message.

Step 2 Select **Tools** > **Trace & Log Central** > **Collect Files** and select the relevant logs for all impacted services. For example, if the service is Cisco Presence Engine, collect the Cisco Presence Engine, Cisco XCP router and Cisco XCP Connection Manager logs. Or, if the service is Cisco XCP Router, collect the Cisco XCP Router, and Cisco XCP Connection Manager and Cisco Presence Engine logs.

Step 3 Generate the stack trace by running the following commands from the CLI:
utils core active list

utils core active analyze core *filename*

Step 4 Select **Tools** > **Trace & Log Central** > **Collect Files** and select the **RIS Data Collector PerfMon Log**.

Step 5 Select **Tools** > **SysLog Viewer** to collect the system logs.

a) Select a node.
b) Click **System Logs** > **messages** to view and save the messages.
c) Click **Application Logs** > **CiscoSyslog** to view and save the log file.

Step 6 Attach the collected files to your Cisco technical support case.