APPENDIX F

CallManager Alert Descriptions and Default Configurations

The following list comprises the CallManager alerts, their definitions, and default settings.

- NumberOfRegisteredGatewaysIncreased, page F-19
- NumberOfRegisteredMediaDevicesDecreased, page F-19
- NumberOfRegisteredMediaDevicesIncreased, page F-20
- NumberOfRegisteredPhonesDropped, page F-20
- RouteListExhausted, page F-21
- SDLLinkOutOfService, page F-21
- TCPSetupToIMEFailed, page F-22
- TLSConnectionToIMEFailed, page F-23

BeginThrottlingCallListBLFSubscriptions

This alert occurs when the BeginThrottlingCallListBLFSubscriptions event gets generated. This indicates that the Cisco Unified Communications Manager initiated a throttling of the CallList BLF Subscriptions to prevent a system overload.

Default Configuration

Table F-1 Default Configuration for the BeginThrottlingCallListBLFSubscriptions RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: BeginThrottlingCallListBLFSubscriptions event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CallProcessingNodeCpuPegging

This alert occurs when the percentage of CPU load on a call processing server exceeds the configured percentage for the configured time.

Note If the administrator takes no action, high CPU pegging can lead to a crash, especially in CallManager service. CoreDumpFound and CriticalServiceDown alerts might also be issued.

The CallProcessingNodeCpuPegging alert gives you time work proactively to avoid a Cisco Unified Communications Manager crash.

Default Configuration

Table F-2 Default Configuration for the CallProcessingNodeCpuPegging RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Processor load over (90%)
Duration	Trigger alert only when value constantly below or over threshold for 60 seconds
Frequency	Trigger up to 3 alerts within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRAgentSendFileFailed

This alert gets raised when the CDR Agent cannot send CDR files from a Cisco Unified Communications Manager node to a CDR repository node within the Cisco Unified Communications Manager cluster.

Default Configuration

Table F-3 Default Configuration for the CDRAgentSendFileFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table F-3 Default Configuration for the CDRAgentSendFileFailed RTMT Alert (continued)

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRAgentSendFileFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRFileDeliveryFailed

This alert gets raised when FTP delivery of CDR files to the outside billing server fails.

Default Configuration

Table F-4 Default Configuration for the CDRFileDeliveryFailed RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRFileDeliveryFailed event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRHighWaterMarkExceeded

This alert gets raised when the high water mark for CDR files gets exceeded. It also indicates that some successfully delivered CDR files got deleted.

Default Configuration

Table F-5 Default Configuration for the CDRHighWaterMarkExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRHighWaterMarkExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

CDRMaximumDiskSpaceExceeded

This alarm gets raised when the CDR files disk usage exceeds the maximum disk allocation. It also indicates that some undelivered files got deleted.

Default Configuration

Table F-6 Default Configuration for the CDRMaximumDiskSpaceExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CDRMaximumDiskSpaceExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily

Table F-6 Default Configuration for the CDRMaximumDiskSpaceExceeded RTMT Alert

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

CodeYellow

The AverageExpectedDelay counter represents the current average expected delay to handle any incoming message. If the value exceeds the value that is specified in Code Yellow Entry Latency service parameter, the CodeYellow alarm gets generated. You can configure the CodeYellow alert to download trace files for troubleshooting purposes.

Default Configuration

Table F-7 Default Configuration for the CodeYellow RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco CallManager CodeYellowEntry event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Trace Download Parameters	Enable Trace Download not selected
Enable Email	Selected
Trigger Alert Action	Default

DBChangeNotifyFailure

This alert occurs when the Cisco Database Notification Service experiences problems and might stop. This condition indicates change notification requests that are queued in the database got stuck and changes made to the system will not take effect. Ensure that the Cisco Database Layer Monitor is running on the node where the alert exists. If it is, restart the service. If that does not return this alert to safe range, collect the output of **show tech notify** and **show tech dbstateinfo** and contact TAC for information about how to proceed.

Default Configuration

Table F-8 Default Configuration for the DBChangeNotifyFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: DBChangeNotify queue delay over 2 minutes
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 30 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DBReplicationFailure

This alarm indicates a failure in IDS replication and requires database administrator intervention.

Note Be aware that DBReplicationFailure is based on the replication status perfmon counter (instead of DBReplicationFailure alarm as was previously the case). This alert gets triggered whenever the corresponding replication status perfmon counter specifies a value of **3** (Bad Replication) or **4** (Replication Setup Not Successful).

Default Configuration

Table F-9 Default Configuration for the DBReplicationFailure RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table F-9 Default Configuration for the DBReplicationFailure RTMT Alert (continued)

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: DBReplicationFailure occurred
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DDRBlockPrevention

This alert gets triggered when the IDSReplicationFailure alarm with alarm number 31 occurs, which invokes a proactive procedure to avoid denial of service. This procedure does not impact call processing; you can ignore replication alarms during this process.

The procedure takes up to 60 minutes to finish. Check that RTMT replication status equals 2 on each node to make sure that the procedure is complete. Do not perform a system reboot during this process.

Default Configuration

Table F-10 Default Configuration for the DDRBlockPrevention RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure alarm with alarm number 31 generated
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

DDRDown

This alert gets triggered when the IDSReplicationFailure alarm with alarm number 32 occurs. An auto recover procedure runs in the background and no action is needed.

The procedure takes about 15 minutes to finish. Check that RTMT replication status equals 2 on each node to make sure the procedure is complete.

Default Configuration

Table F-11 Default Configuration for the DDRDown RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: IDSReplicationFailure alarm with alarm number 32 generated
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert within 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

ExcessiveVoiceQualityReports

This alert gets generated when the number of QRT problems that are reported during the configured time interval exceed the configured value. The default threshold specifies 0 within 60 minutes.

Default Configuration

Table F-12 Default Configuration for the ExcessiveVoiceQualityReports RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of quality reports exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately

Table F-12 Default Configuration for the ExcessiveVoiceQualityReports RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEDistributedCacheInactive

This alarm gets generated when a Cisco Unified Communications Manager attempts to connect to the Cisco IME server, but the IME distributed cache is not currently active.

Ensure that the certificate for the Cisco IME server is provisioned and that the IME distributed cache has been activated via the CLI.

Default Configuration

Table F-13 Default Configuration for the IMEDistributedCacheInactive Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Inactive IME Distributed Cache
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEOverQuota

This alert indicates that the Cisco Unified Communications Manager servers that use this Cisco IME service have exceed the quota for published direct inward dialing numbers (DIDs) to the IME distributed cache. The alert includes the name of the Cisco IME server as well as the current and target quota values.

Ensure that you have correctly provisioned the DID prefixes on all of the Cisco Unified Communications Manager servers that use this Cisco IME service.

If you have provisioned the prefixes correctly, you have exceeded the capacity of your Cisco IME service, and you need to configure another service and divide the DID prefixes across the Cisco IME client instances (Cisco Unified Communications Managers) on different Cisco IME services.

Default Configuration

Table F-14 Default Configuration for the IMEOverQuota Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP over quota
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

IMEQualityAlert

This alert gets generated when Cisco Unified Communications Manager determines that a substantial number of Cisco IME calls fail back to PSTN or fail to be set up due to IP network quality problems. Two types of events trigger this alert:

- A large number of the currently active Cisco IME calls have all requested fallback or have fallen back to the PSTN.
- A large number of the recent call attempts have gone to the PSTN and not been made over IP.

When you receive this alert, check your IP connectivity. If no problems exist with the IP connectivity, you may need to review the CDRs, CMRs, and logs from the firewalls to determine why calls have fallen back to the PSTN or have not been made over IP.

Default Configuration

Table F-15 Default Configuration for the IMEQualityAlert Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cisco IME link quality problem
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll

Table F-15 Default Configuration for the IMEQualityAlert Alert (continued)

Value	Default Configuration
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InsufficientFallbackIdentifiers

This alert gets generated when too many Cisco IME calls that are currently in progress use the same fallback DID and no more DTMF digit sequences exist to allocate to a new Cisco IME call that Cisco Unified Communications Manager is processing. The new call continues, but the call cannot fallback to the PSTN if voice-quality deteriorates.

If this alert gets generated, note the fallback profile that associates with this call. Check that profile in Cisco Unified Communications Manager Administration, and examine the current setting for the "Fallback Number of Correlation DTMF Digits" field. Increase the value of that field by one, and check whether the new value eliminates these alerts. In general, this parameter should be large enough so that the number of simultaneous Cisco IME calls that are made to enrolled numbers that associate with that profile is always substantially less than 10 raised to the power of this number. For example, if you always have fewer than 10,000 simultaneous Cisco IME calls for the patterns that associate with this fallback profile, setting this value to 5 (10 to the power of 5 equals 100,000) should keep Cisco Unified Communications Manager from generating this alert.

However, increasing this value results in a small increase in the amount of time it takes to perform the fallback. As such, you should set the "Fallback Number of Correlation DTMF Digits" field to a value just large enough to prevent this alert from getting generated.

Instead of increasing the value of the DTMF digits field, you can add another fallback profile with a different fallback DID and associate that fallback profile with a smaller number of enrolled patterns. If you use this method, you can use a smaller number of digits.

Default Configuration

Table F-16 Default Configuration for the InsufficientFallbackIdentifiers Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Error
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Cannot allocate fallback identifier
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alerts within one minute
Schedule	24 hours daily

Table F-16 Default Configuration for the InsufficientFallbackIdentifiers Alert (continued)

Value	Default Configuration
Enable Email	Selected
Trigger Alert Action	Default

IMEServiceStatus

This alert indicates the overall health of the connection to the Cisco IME services for a particular Cisco IME client instance (Cisco Unified Communications Manager). The alert indicates the following states:

- 0—Unknown. Likely indicates that the Cisco IME service has not been activated.
- 1—Healthy. Indicates that the Cisco Unified Communications Manager has successfully established a connection to its primary and backup servers for the Cisco IME client instance, if configured.
- 2—Unhealthy. Indicates that the Cisco IME has been activated but has not successfully completed handshake procedures with the Cisco IME server. Note that this counter reflects the handshake status of both the primary and the secondary IME servers.

Default Configuration

Table F-17 Default Configuration for the IMEServiceStatus Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: VAP Connection Problem
Duration	Trigger alert immediately
Frequency	Trigger up to 1 alert every 60 minutes
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

InvalidCredentials

The alert indicates that the Cisco Unified Communications Manager cannot connect to the Cisco IME server because the username and/or password configured on Cisco Unified Communications Manager do not match those configured on the Cisco IME server.

The alert includes the username and password that were used to connect to the Cisco IME server as well as the IP address and name of the target Cisco IME server. To resolve this alert, log into the Cisco IME server and check that the configured username and password match the username and password that are configured in Cisco Unified Communications Manager.

Default Configuration

Table F-18 Default Configuration for the InvalidCredentials Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Credential Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowCallManagerHeartbeatRate

This alert occurs when the CallManager heartbeat rate equals less than the configured value.

Default Configuration

Table F-19 Default Configuration for the LowCallManagerHeartbeatRate RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: CallManager Server heartbeat rate below 24 beats per minute.

Table F-19 Default Configuration for the LowCallManagerHeartbeatRate RTMT Alert (continued)

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

LowTFTPServerHeartbeatRate

This alert occurs when TFTP server heartbeat rate equals less than the configured value.

Default Configuration

Table F-20 Default Configuration for the LowTFTPServerHeartbeatRate RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TFTP server heartbeat rate below 24 beats per minute
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MaliciousCallTrace

This indicates that a malicious call exists in Cisco Unified Communications Manager. The malicious call identification (MCID) feature gets invoked.

Default Configuration

Table F-21 Default Configuration for the MaliciousCallTrace RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Malicious call trace generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MediaListExhausted

This alert occurs when the number of MediaListExhausted events exceeds the configured threshold during the configured time interval. This indicates that all available media resources that are defined in the media list are busy. The default specifies 0 within 60 minutes.

Default Configuration

Table F-22 Default Configuration for the MediaListExhausted RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of MediaListExhausted events exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately

Table F-22 Default Configuration for the MediaListExhausted RTMT Alert (continued)

Value	Default Configuration
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

MgcpDChannelOutOfService

This alert gets triggered when the BRI D-Channel remains out of service.

Default Configuration

Table F-23 Default Configuration for the MgcpDChannelOutOfService RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: MGCP DChannel is out-of-service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredDevicesExceeded

This alert occurs when the NumberOfRegisteredDevicesExceeded event gets generated.

Default Configuration

Table F-24 Default Configuration for the NumberOfRegisteredDevicesExceeded RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical

Table F-24 Default Configuration for the NumberOfRegisteredDevicesExceeded RTMT Alert

Value	Default Configuration
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: NumberOfRegisteredDevicesExceeded event generated
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysDecreased

This alert occurs when the number of registered gateways in a cluster decreases between consecutive polls.

Default Configuration

Table F-25 Default Configuration for the NumberOfRegisteredGatewaysDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of registered gateway decreased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredGatewaysIncreased

This alert occurs when the number of registered gateways in the cluster increased between consecutive polls.

Default Configuration

Table F-26 Default Configuration for the NumberOfRegisteredGatewaysIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered gateways increased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesDecreased

This alert occurs when the number of registered media devices in a cluster decreases between consecutive polls.

Default Configuration

Table F-27 Default Configuration for the NumberOfRegisteredMediaDevicesDecreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered media devices decreased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredMediaDevicesIncreased

This alert occurs when the number of registered media devices in a cluster increases between consecutive polls.

Default Configuration

Table F-28 Default Configuration for the NumberOfRegisteredMediaDevicesIncreased RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered media devices increased
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

NumberOfRegisteredPhonesDropped

This alert occurs when the number of registered phones in a cluster drops more than the configured percentage between consecutive polls.

Default Configuration

Table F-29 Default Configuration for the NumberOfRegisteredPhonesDropped RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Threshold	Trigger alert when following condition met: Number of registered phones in the cluster drops (10%)
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

RouteListExhausted

This alert occurs when the number of RouteListExhausted events exceeds the configured threshold during the configured time interval. This indicates that all available channels that are defined in the route list are busy. The default specifies 0 within 60 minutes.

Default Configuration

Table F-30 Default Configuration for the RouteListExhausted RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Warning
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Number of RouteListExhausted exceeds 0 times within the last 60 minutes
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

SDLLinkOutOfService

This alert occurs when the SDLLinkOutOfService event gets generated. This event indicates that the local Cisco Unified Communications Manager cannot communicate with the remote Cisco Unified Communications Manager This event usually indicates network errors or a non-running remote Cisco Unified Communications Manager.

Default Configuration

Table F-31 Default Configuration for the SDLLinkOutOfService RTMT Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: SDLLinkOutOfService event generated

Table F-31 Default Configuration for the SDLLinkOutOfService RTMT Alert (continued)

Value	Default Configuration
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TCPSetupToIMEFailed

This alert occurs when Cisco Unified Communications Manager cannot establish a TCP connection to a Cisco IME server. This alert typically occurs when the IP address and port of the Cisco IME server are misconfigured in Cisco Unified Communications Manager Administration or when an Intranet connectivity problem exists and prevents the connection from being set up.

Ensure that the IP address and port of the Cisco IME server in the alert are valid. If the problem persists, test the connectivity between the Cisco Unified Communications Manager servers and the Cisco IME server.

Default Configuration

Table F-32 Default Configuration for the TCPSetupToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Critical
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: Connection Failure to Cisco IME server
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

TLSConnectionToIMEFailed

This alert occurs when a TLS connection to the Cisco IME service could not be established because the certificate presented by the Cisco IME service has expired or is not in the Cisco Unified Communications Manager CTL.

Ensure that the Cisco IME service certificate has been configured into the Cisco Unified Communications Manager.

Default Configuration

Table F-33 Default Configuration for the TLSConnectionToIMEFailed Alert

Value	Default Configuration
Enable Alert	Selected
Severity	Alert
Enable/Disable this alert on the following servers	Enabled on listed servers
Threshold	Trigger alert when following condition met: TLS Failure to Cisco IME service
Duration	Trigger alert immediately
Frequency	Trigger alert on every poll
Schedule	24 hours daily
Enable Email	Selected
Trigger Alert Action	Default

Additional Information

See the Related Topics, page 9-10.